Приложение № 15
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

РЕКОМЕНДАЦИИ
по безопасной работе Клиента в Мобильном приложении Системы ДБО ЮЛ

1. ПОДКЛЮЧЕНИЕ МОБИЛЬНОГО ПРИЛОЖЕНИЯ:

1.1. Подключение Мобильного приложения выполняется Клиентом на своем средстве доступа (смартфоне на операционной системе Android), самостоятельно и за свой счет.

1.2. Для этого средство доступа должно быть подключено к информационно-телекоммуникационной сети «Интернет».

1.3. Клиенту рекомендуется обеспечивать безопасность и целостность программных средств на своем средстве доступа посредством:

— использования средств защиты от вирусов с актуальными антивирусными базами;

— исключения использования на своем средстве доступа программ-закладок и прочего опасного и потенциально опасного программного обеспечения;

— обеспечить установку программ из достоверных источников;

— не допускать несанкционированного доступа третьих лиц к программным средствам и средствам защиты информации, с помощью которых осуществляется обмен электронными документами с Банком.

1.4. В качестве достоверного источника понимается использование Официального сайта Банка в Сети интернет, при этом скачивая установочные файлы с Официального сайта Банка, Клиент обязуется сверить контрольную сумму скачиваемого файла с аналогичной информацией, размещенной на Официальном сайте Банка, а также самостоятельно выполнить необходимые настройки на своем средстве доступа по установке такого типа файлов, если того требует операционная система средства доступа.

2. МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В МОБИЛЬНОМ ПРИЛОЖЕНИИ:

2.1. Для полнофункционального режима работы с возможностью наложения электронной подписи на электронные документы в Мобильном приложении используется только защищённый носитель ключевой информации USB-токен с USB-адаптером. Без применения USB-токена, работа в Мобильном приложении возможна только в режиме просмотра информации (с закрытым доступом на осуществление расходных операций по Счетам).

2.2. Хранение ключей ЭП допускается только на защищённом носителе ключевой информации.

2.3. Категорически запрещается использовать носитель ключевой информации в других целях и на других устройствах, не предназначенных для работы в Мобильном приложении или Web-версии («Интернет-Банк»)

2.4. При утрате или компрометации ключа ЭП уполномоченное лицо Клиента обязано незамедлительно приостановить любую работу в Мобильном приложении, в том числе остановить операции с электронными документами, при нетипичной (подозрительной) работе средства доступа, извлечь из него ключевой носитель, сообщить в Банк о случившемся инциденте в порядке, указанном в Договоре об использовании системы дистанционного банковского обслуживания «Клиент-Банк».

2.5. При утрате или подозрении на компрометацию средства доступа (смартфон) с подключённым Мобильным приложением, Клиент обязан обратиться в Банк для временного приостановления (блокировки) доступа к Системе ДБО ЮЛ.

2.6. Банк оставляет за собой право заблокировать ключ ЭП Уполномоченного лица Клиента с последующим уведомлением, при выявлении или подозрении факта компрометации ключа ЭП, выявлении факта несоответствия Уполномоченного лица Клиента с лицами, указанными в карточке образцов подписей, выявлении несоответствия реквизитов организации Клиента с данными в Мобильном приложении, подозрении или выявлении несанкционированного списания денежных средств.

2.7. Разблокирование (возобновление действия) ключа ЭП Уполномоченных лиц Клиента осуществляется Банком не позднее дня, следующего за днём устранения выявленных нарушений и представления Клиентом в Банк необходимых актуальных данных и документов.

3. ХРАНЕНИЕ ИНФОРМАЦИИ ПО СФОРМИРОВАННЫМ И ПРОВЕДЕННЫМ ДОКУМЕНТАМ ЧЕРЕЗ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ:

3.1. Информацию о платежах и переводах через Мобильное приложение можно получить в меню «Платежи»: «В работе», «В Банке», «Исполнено».

3.2. Для формирования выписки по счету необходимо зайти в меню «Счета».

3.3. Информация о работе Мобильного приложения хранится в соответствующих регистрах Системы ДБО ЮЛ в течение пяти лет.