Приложение № 4
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**
**Клиенту по обеспечению информационной безопасности при эксплуатации Системы ДБО ЮЛ ключевой информации и СКЗИ**

1. **Рекомендации по организационному обеспечению безопасности АРМ Клиента с Системой ДБО ЮЛ.**

1.1. В организации Клиента назначаются (определяются) должностные лица, ответственные за обеспечение информационной безопасности и эксплуатацию Системы ДБО ЮЛ.

1.2. В организации Клиента разрабатываются нормативные документы, регламентирующие вопросы информационной безопасности и эксплуатации Системы ДБО ЮЛ.

1.3. К работе с Системой допускаются работники, имеющие навыки работы на персональном компьютере, ознакомленные с Условиями.

1.4. Работа в информационно-телекоммуникационной сети «Интернет» на ПК пользователя Системы не должна допускать посещения сайтов сомнительного содержания, развлекательных ресурсов, сайтов социальных сетей, игровых интернет-ресурсов. Рекомендуется на таких АРМ предоставлять доступ к информационно-телекоммуникационной сети «Интернет» только для соединения с Официальным сайтом Банка для работы в Системе.

1.5. Не допускается запуск на АРМ пользователя Системы программ несанкционированного снятия защиты с программного обеспечения.

1.6. Не допускается установка программного обеспечения, позволяющая осуществлять перехват, преобразование данных Системы.

1.7. Обеспечить своевременную установку обновлений безопасности операционной системы и прикладных программ на АРМ.

1.8. В настройках операционной системы АРМ Клиента необходимо отключить автозапуск программ с внешних носителей.

2. **Рекомендации по размещению АРМ Клиента с Системой ДБО ЮЛ и режиму охраны.**

2.1. Помещения, в которых размещаются АРМ Клиента и используются средства криптографической защиты информации, должны иметь ограниченный доступ и обеспечивать конфиденциальность проводимых работ.

2.2. Размещение помещений с ограниченным доступом и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц, и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

2.3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

2.4. Входные двери помещений с ограниченным доступом должны быть оборудованы механическим и кодовым замками, или хотя бы одним из них, обеспечивающими надежное закрытие помещений, а также местом для опечатывания двери в нерабочее время.

2.5. Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

2.6. Размещение технических средств в помещении с ограниченным доступом должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается через окна.

2.7. В помещения с ограниченным доступом допускаются руководитель организации Клиента, технические сотрудники, сопровождающие работу Системы и ответственные за работу с ключевой информацией (Уполномоченные лица) на АРМ Клиента для работы в Системе. При этом, право самостоятельной работы на АРМ в Системе разрешено только Уполномоченным лицам Клиента, техническим сотрудникам только в присутствии Уполномоченных лиц.

2.8. Системные блоки АРМ Клиента с Системой ДБО ЮЛ, оборудуются средствами контроля вскрытия (пломба, голографическая наклейка на местах вскрытия крышек корпуса).

2.9. При передаче в ремонт АРМ Клиента, должно быть удалено программное обеспечение, предназначенное для работы в Системе. В случае невозможности удаления, из системного блока должен быть изъят жёсткий диск.

2.10. По возврату АРМ Клиента из ремонта, перед началом эксплуатации, ПК должен быть проверен лицензионными средствами антивирусной защиты с актуальными базами данных сигнатур вирусов, а также обследован на наличие стороннего/неизвестного программного обеспечения, не предназначенного для работы в Системе ДБО ЮЛ.

**3. Рекомендации по обеспечению безопасности при работе с ключевой информацией.**

3.1. Порядок хранения и использования ключевых документов должен исключать возможность несанкционированного доступа к ним.

3.2. Все носители ключевой информации должны быть зарегистрированы в журнале поэкземплярного учёта с указанием даты постановки на учёт, даты генерации секретного ключа, номера ключа, фамилии ответственного исполнителя и его подписи.

3.3. Учёт и обеспечение хранения ключевой информации, носителей, поручается руководством Клиента сотруднику, ответственному за информационную безопасность в организации либо ответственным за работу с ключевой информацией в Системе ДБО ЮЛ, каждый из которых несёт персональную ответственность за её сохранность. Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключён.

3.4. В случае сменного режима работы, отпуска, болезни и т.п., ответственных, передача носителей ключевой информации осуществляется по акту или журналу приёма-передачи, с указанием даты и времени передачи, номера ключевого носителя, идентификатора Ключа ЭП, ФИО сотрудников и подписей.

3.5. Для хранения ключевых носителей, предназначенных для работы в Системе, выделяются сейфы или металлические хранилища для каждого ответственного, которые оборудованы внутренними замками и имеют место для опечатывания в конце рабочего дня. Сейф должен быть надёжно закреплён к полу или стене. Вторые экземпляры ключей от сейфа или металлического хранилища должны храниться в службе безопасности или у руководителя организации, не имеющих права его опечатывания. Дубликаты должны быть помещены в боксы или конверты, опечатаны, с проставлением печати или подписи на месте склеивания конверта. Хранение ответственным носителей ключевой информации в сейфе или металлическом хранилище, закреплённом за другим, не допущенным к ключевой информации лицом, разрешается только в отдельно опечатанном пользователем боксе, пакете, которое имеет место для опечатывания.

3.6. Подключать съемные носители с ключевой информацией необходимо только в момент начала работы с Системой и обязательно извлекать его из ПК сразу после окончания работы в Системе. В остальных случаях, по завершении работы в Системе, ключевые носители должны находиться в сейфе.

3.7. При транспортировке ключевых носителей с ключевой информацией создавать условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на ключевую информацию.

3.8. Запрещается снимать несанкционированные копии ключевой информации с носителей, знакомить с содержанием ключевых носителей, передавать лицам, не допущенным к работе с ними, хранить ключевую информацию на жёстких дисках ПК, устанавливать носитель в порты ПК, не предназначенных для работы в Системе ДБО ЮЛ записывать на носители постороннюю информацию.

3.9. Уничтожение выведенных из действия закрытых ключей ЭП производить путём двойного форматирования по истечении одного рабочего дня с момента генерации и ввода в действие нового ключа ЭП, при условии, что новый ключ ЭП записан на другой носитель ключевой информации, с отметкой в журнале учёта и хранения ключевой информации.

3.10. Своевременно проводить смену ключевой информации при окончании срока действия, смене Уполномоченных лиц, имеющих право подписи, а также при обнаружении факта компрометации ключей ЭП.

**4. Рекомендации по обеспечению безопасности при использовании услуги SMS-подтверждения и SMS-оповещения**

4.1. Необходимо ограничить доступ к телефону, на номер которого приходят SMS с кодами подтверждения платежей.

4.2. При смене номера телефона SMS-подтверждения или его утере, незамедлительно обращайтесь в Банк для его замены в Системе ДБО ЮЛ. Добавление/Изменение номера телефона SMS-оповещения выполняется Клиентом самостоятельно (без обращения в Банк) в меню «Мониторинг» Системы ДБО ЮЛ, при условии полученного в установленном порядке доступа.

4.3. Перед вводом кода для подтверждения платежа, полученного по SMS, убедитесь, что информация, полученная в SMS, соответствует фактическим реквизитам платежа (проверяйте счёт, сумму, БИК и т.д.)

4.4. Для SMS-услуг не рекомендуется использовать модели телефонов с операционными системами iOS и Android, которые подвержены компрометации и взлому, в следствие чего, злоумышленник может получить возможность перехвата SMS сообщений.

5. При этом обязательным условием предоставления Банком SMS-подтверждения и SMS-оповещения является наличие технической возможности у оператора сотовой связи, осуществляющего обслуживание телефонного номера, принимать и отправлять SMS-сообщения между SMS-Центром Банка и Клиентом с использованием данного номера.