Приложение № 9
К Условиям предоставления и обслуживания
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 настройке и эксплуатации АРМ Клиента, на которых устанавливаются или используются клиентские части Системы ДБО ЮЛ

С целью минимизации рисков, связанных с подключением и использованием клиентской части Системы ДБО ЮЛ, Банк рекомендует:

1. Относительно организации доступа к операционной системе АРМ Клиента.

1.1. Учётная запись, под которой осуществляется работа в Системе ДБО ЮЛ, не должна иметь права доступа «Администратор» к операционной системе ("Администратор" в Windows). Учётная запись пользователя Системы ДБО ЮЛ должна быть уровня «пользователь» "User".

1.2. Учетная запись «Гость» должна быть отключена.

1.3. Не допускается автоматический вход пользователя в Систему ДБО ЮЛ (без ввода логина и пароля).

1.4. Пароли учетных записей и доступа в Систему ДБО ЮЛ должны соответствовать следующим требованиям:

- Содержать не менее восьми символов
- Включать буквы разных регистров (A, a,)
- Включать цифры (0-9)
- Включать специальные символы (@#$%&)

1.5. Запрещается оставлять пароли учетных записей пользователей в доступном месте, разглашать и передавать их другим лицам.

1.6. Пароли должны быть изменены в случае подозрения относительно их компрометации.

2. Относительно организации антивирусной защиты АРМ Клиента.

2.1. На АРМ Клиента должно быть установлено и настроено лицензионное антивирусное программное обеспечение актуальной версии, которая включает следующие компоненты:

- Файловый антивирус;
- Почтовый антивирус;
- Веб-антивирус;
- Защита от сетевых атак (Антихакер);
- Компонент защиты от рекламы (adware) и шпионского программного обеспечения (spyware);
- Программный межсетевой экран (firewall).

В случае отсутствия компонента "Программный межсетевой экран" необходимо установить отдельное программное дополнение с аналогичным функционалом.

2.2. Антивирусное ПО должно проводить активный мониторинг всех внешних носителей, которые подключаются к системе.

2.3. Антивирусное ПО должно проводить полную проверку жесткого диска компьютера на наличие вредоносного ПО не реже, чем один раз в неделю.

2.4. Почтовый антивирус должен проверять все входящие и исходящие сообщения.

2.5. Межсетевой экран должен быть настроен по принципу "минимизации" ресурсов.

2.6. Антивирусное ПО должно быть настроено таким образом, чтобы обеспечивать надежную защиту без участия пользователя.

2.7. Антивирус обязательно должен быть обновлен до актуальной версии, и обеспечивать ежедневное обновление базы данных сигнатур вирусов.

2.8. Если возникло подозрение, что АРМ заражён (нетипичная реакция на выполняемые команды пользователя, появляющиеся непонятные окна, получение незапрашиваемых SMS с ключом для входа или для проведения операции и т.п.) - немедленно прекратите работу в Системе, извлеките USB-токен и обратитесь к своему ИТ-специалисту для выяснения причин происходящего. До выяснения причин пользоваться Системой ДБО ЮЛ крайне не рекомендуется.

3. Относительно организации эксплуатации системного ПО

3.1. Все программное обеспечение (ПО) на АРМ Клиента (включая операционную систему), должно быть лицензионное, и получено из достоверных источников.

3.2. При распределении доступа к локальным ресурсам на АРМ Клиента должен быть применён принцип "минимизации" ресурсов:

– устанавливать только ПО для взаимодействия с Системой ДБО ЮЛ, и ПО системы защиты информации;

– установка иного ПО должно быть четко контролируемо и регламентировано только в случае крайней необходимости;

– пользователь системы должен осуществлять личный контроль за нетипичной робой компьютера и ПО (появление всплывающих окон, которых не было, изменение шрифтов Интернет-страницы Клиент-банка, появление ПО, которого он не устанавливал, и т. п.)

3.3. Все ресурсы общего пользования на АРМ Клиента должны быть отключены.

3.4. Не допускается установка на рабочие станции, которые задействованы при работе в Системе ДБО ЮЛ, программного обеспечения типа "удаленного администрирования" (TeamViewer, RemoteDesktop, Radmin, DameWare, VNC, Hamachi, RemoteOfficeManager и другие).

3.5. Все программное обеспечение должно постоянно обновляться.

3.6. Не устанавливайте и не сохраняйте подозрительные файлы, полученные из ненадёжных источников, неизвестных web-сайтов, присланные по электронной почте и т.д. Такие файлы необходимо немедленно удалять. В случае необходимости загрузки файла, обязательно проверьте его антивирусным ПО перед использованием.

4. Относительно организации безопасной работы в Системе ДБО ЮЛ посредством Web-интерфейса

4.1. Не проводить работу в Системе ДБО ЮЛ с рабочих станций, которые находятся в "не доверенной" зоне (Интернет-кафе, в местах, где установлено видео наблюдение, на домашнем ПК).

4.2. При необходимости доступа сотрудников к другим ресурсам сети Internet, отправки/получения электронной почты, пользования социальными сетями и прочее, необходимо использовать отдельный ПК.

4.3. Держать в тайне пароль. При подозрении, относительно компрометации пароля следует немедленно его изменить. При вводе пароля убедитесь, что за Вами никто не наблюдает.

4.4. Не допускается хранение носителей ключевой информации в доступном месте без визуального присмотра.

4.5. Не допускается передача носителей ключевых данных посторонним лицам.

4.6. Запрещается оставлять без присмотра АРМ Клиента с авторизованной (запущенной к исполнению) Системой ДБО ЮЛ. При необходимости покинуть рабочее место АРМ, произвести блокирование учётной записи, путём одновременного нажатия комбинации клавиш Win+L, или Ctrl+Alt+Del, после чего выбрать «Блокировка».

4.7. При завершении работы выполнить выход из Системы ДБО ЮЛ, отсоединить носитель ключевой информации USB-токен.

4.8. Не используйте функцию хранения паролей, которое предлагается браузером или другим ПО.

4.9. Не допускается осуществлять доступ к Системе ДБО ЮЛ с использованием общедоступных беспроводных сетей. Если Ваша организация использует корпоративную беспроводную сеть, доступ к ней должен быть организован по "белым спискам" MAC адресов и строго ограничен. Должен быть установлен уровень шифрования сессии WPA2 с шифрованием по стандарту AES.

4.10. Для хранения секретных ключей следует использовать защищенные носители ключевой информации, которые рекомендуются Банком.

4.11. О любых замеченных значительных и/или нетипичных изменениях в работе Системы ДБО ЮЛ, таких например как изменение интерфейса сайта https://cb.chbrr.crimea.com или его частей, появление необходимости

выполнения новых, ранее не используемых действий при работе с Системой, следует воздержаться от введения данных для авторизации в Системе ДБО ЮЛ и сообщить об этом в Банк по известным Вам телефонам.

4.12. При увольнении или смене должностных обязанностей Уполномоченных лиц, которые имели доступ к ключевым данным и Системе ДБО ЮЛ, выполните изменение паролей и перегенерацию ключей ЭП.

4.13. Необходимо обеспечить безопасную работу с Системой ДБО ЮЛ. Внимательно контролируйте состояние Ваших счетов (рекомендуется 1–2 раза в день), даже если Вы не проводите платёжные операции в Системе.

Кроме этого, стоит обратить внимание:

Банк ни в коем случае не станет осуществлять запрос с использованием электронной почты, SMS сообщений или телефонной связи Ваших паролей, номеров счетов и т.д. Банк не высылает своим Клиентам ссылки для осуществления обновлений, или загрузки и установки ПО (в том числе мобильного). При получении сообщений такого содержания ни в коем случае не раскрывайте конфиденциальные данные и известите об этом Банк.

В случае возникновения подозрения, относительно факта или попытки несанкционированного доступа к АРМ Клиента, Системе ДБО ЮЛ, немедленно прекратите работу с скомпрометированным компьютером, отсоедините его от сети и сообщите об этом в Банк по телефонам:

Служба поддержки Клиентов: +7(3652) 605-805; +7(978)835-2112; +7(978)835-2211; +7(978)0990380.

Уполномоченный работник Банка: +7(978)835-3113.

Придерживайтесь дальнейших рекомендаций Банка.