Рекомендации по безопасности при работе с СДБО

1. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбой сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.) **ни при каких обстоятельствах не сообщать** данную информацию.
2. В случае **смены номера телефона** для SMS-оповещений **или утрате SIM-карты незамедлительно сообщить** об этом в Банк.
3. Применяемые в СДБО средства и способы защиты **следует держать в секрете**, не допуская ознакомления с ними посторонних лиц.
4. Рекомендуется для работы с СДБО **рекомендуется использовать отдельный компьютер**, который будет использоваться только для работы с системой (далее - Компьютер).
5. Физический доступ к Компьютеру иных лиц **должен быть ограничен**.
6. На Компьютере должно использоваться **только лицензионное программное обеспечение** с последними обновлениями**.**
7. На Компьютере **должно использоваться средство защиты от вредоносного кода** с актуальными вирусными базами, загружаемое с момента запуска компьютера.
8. На Компьютере **рекомендуется использование межсетевого экрана**, блокирующего неизвестный сетевой трафик.
9. Использование паролей:
   - **Сложность пароля** должна удовлетворять политикам безопасности: длина – не менее 8 символов, должны присутствовать буквы нижнего и верхнего регистра, цифры или специальные символы. Не допускается использования простых паролей (123456, qwerty и др.) – необходимо использовать различные сложные комбинации из букв (в т. ч. в разных регистрах) и цифр, не расположенных «подряд» на клавиатуре.
   - Хранение паролей на материальном носителе возможно только в сейфе
   - Необходимо осуществлять регулярную (минимум – 1 раз в 3 месяца) **смену паролей**
10. На Компьютере запрещено использование любых средств **удалённого (дистанционного) доступа.**
11. Не рекомендуется посещать ресурсы развлекательного характера, файлообменные ресурсы и социальные сети.
12. При работе с электронной почтой не рекомендуется открывать письма из **неизвестных источников**, вложения к ним и переходить по содержащимся в них ссылках**.**
13. Запрещена работа на Компьютере через **общедоступные сети** (бесплатный Wi-Fi и т.д.).
14. Клиент обязан руководствоваться эксплуатационной и технической документацией на отдельные программные и технические средства, используемые в составе СДБО, а также инструкциями по работе в СДБО передаваемыми Банком Клиенту в составе Рабочего комплекта.
15. При несоблюдении требований инструкций, технической и эксплуатационной документации на СКЗИ и прочие программные и программно-аппаратные средства, входящие в состав СДБО, запрещается использование СДБО в целом, а также ее отдельных компонентов, в том числе СКЗИ.

В случае возникновения наличия подозрений или подтверждённого факта **компрометации** средств защиты, необходимо **прекратить** работу в СДБО и **связаться** с Банком.