**1. Рекомендации Банка по выполнению правил информационной безопасности при эксплуатации системы ДБО:**

1.1. Не передавать конфиденциальную информацию другим лицам, пользоваться своей электронной подписью самостоятельно.

1.2. Не записывать коды, логины и пароли на бумажных носителях, доступных другим лицам.

1.3. Не сообщать коды, логины и пароли IT-специалистам для проверки работы системы ДБО, в случае необходимости проведения таких проверок самостоятельно применять свой логин и пароль.

1.4. Обеспечить безопасное хранение защищенного носителя с ключом электронной подписи в недоступном месте: сейф, запираемый металлический шкаф и т.п. Подключать защищенный носитель к компьютеру только во время работы в системе дистанционного банковского обслуживания, не оставлять защищенный носитель постоянно подключенным к компьютеру.

1.5. Ограничить доступ к компьютеру, используемому для работы с системой дистанционного банковского обслуживания, обеспечить охрану помещения, в котором он установлен.

1.6. Контролировать действия IT-специалистов (особенно внештатных) в момент технического обслуживания, установки программного обеспечения на компьютере, используемом для работы с Системой ДБО.

1.7. Осуществлять постоянный контроль за отправляемыми платежными документами, а также состоянием банковских счетов посредством Системы ДБО.

1.8. Регулярно, не реже одного раза в три месяца, производить смену паролей доступа в компьютер, с которого осуществляется работа в Системе ДБО, а также паролей доступа в Систему ДБО. Пароль должен отвечать следующим требованиям:

– длина не менее девяти символов;

– должен состоять из строчных и (или) заглавных букв латинского алфавита, как минимум одного специального знака и одной цифры;

– не должен состоять из легко подбираемых комбинаций (qwerty, 12345678, admin, password) или их вариантов (!qwerty, 12345678, @dmin, passw0rd), совпадать с датой рождения, номером телефона, именем учетной записи и другими общедоступными данными;

– не должен совпадать с паролем на вход в компьютер и в личные сервисы сети Интернет.

1.9. В обязательном порядке производить смену ключа электронной подписи и паролей в следующих случаях:

– при смене ответственных лиц, имеющих права доступа в Систему ДБО;

– при обнаружении фактов доступа посторонних лиц к компьютеру или защищенному носителю с ключом электронной подписи, а также при подозрении о таком доступе (в том числе удаленном).

1.10. Обеспечить защиту компьютера, с которого выполняется работа с Системой ДБО:

– ограничить доступ в сеть Интернет. Рекомендуем использовать для работы в Системе ДБО выделенный компьютер с выходом в Интернет через межсетевой экран (брандмауэр, firewall), разрешить доступ к минимально необходимым для работы IP-адресам, каковыми являются: IP-адреса Системы ДБО, IP-адреса сервера, с которого осуществляется обновление операционной системы, IP-адреса сервера, с которого осуществляется обновление антивирусного программного обеспечения;

– не пользоваться сервисами обмена мгновенными сообщениями (ICQ, Skype, Mail.Ru-Агент и т.п.), программами удаленного администрирования, не использовать компьютер для получения почты и доступа к другим личным сервисам сети Интернет;

– установить лицензионное антивирусное программное обеспечение, не реже одного раза в день обновлять его.

– обеспечить своевременную установку обновлений операционной системы и прикладных программ;

– отключить встроенные учетные записи «Администратор» и «Гость»;

– отключить службы «Удаленный реестр» и «Удаленное управление Windows»;

– работать на компьютере с правами «Пользователь»;

– использовать только лицензионное программное обеспечение, полученное из доверенных источников;

– не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте.

– отключить автозапуск любых внешних носителей;

– не отвечать на подозрительные письма электронной почты, SMS-сообщения, иные сообщения, направленные по другим каналам связи, с просьбой выслать/сообщить/передать/предоставить ключ электронной подписи, пароль доступа и другие конфиденциальные данные.