Уважаемые клиенты АКБ «ФОРА-БАНК» (АО),
напоминаем Вам о необходимости соблюдать правила безопасности
при использовании системы Дистанционного банковского обслуживания
для Юридических Лиц:

1. Для работы в системе Дистанционного банковского обслуживания для Юридических Лиц (далее Система ДБО ЮЛ) используйте отдельный компьютер. Ограничьте к нему доступ.
2. Используйте на компьютере только лицензионное Программное обеспечение.
3. Используйте лицензионное антивирусное программное обеспечение.
4. Поддерживайте его антивирусные базы в актуальном состоянии. Проводите периодическое полное антивирусное сканирование компьютера (рекомендовано раз в неделю).
5. Регулярно обновляйте операционную систему компьютера, на котором используется Система ДБО ЮЛ.
6. Работа с Системой ДБО ЮЛ должна проводиться с использованием учетных записей, не имеющих административные привилегии в операционной системе.
7. Никогда не записывайте логины и пароли на бумаге, мониторе или клавиатуре, не сохраняйте логины и пароли в файлах на компьютере. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы (например: #, &, [и т.д.). Регулярно (не реже 1 раза в 3 месяца) проводите смену паролей.
8. Перед вводом своего пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта **https://client.forabank.ru/** наличие сертификата безопасности. В случае обнаружения подозрительных web-сайтов, доменные имена (адреса) и стиль оформления которых сходны с именами и оформлением официальных сайтов АКБ «ФОРА-БАНК» (АО), незамедлительно сообщите об этом в Банк.
9. Не сообщайте посторонним лицам, а также кому бы то ни было, логины и пароли доступа к компьютеру, с которого осуществляется подключение к Системе ДБО ЮЛ, логины и пароли доступа к Системе ДБО ЮЛ, историю операций, контактные и учетные данные, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к Вашим счетам.

ФОРАБАНК

10. Межсетевым экраном запретите отправку в Интернет информации, инициированной программами, не имеющими соответствующих полномочий.
11. Подключайте USB-носитель с секретными ключами к компьютеру только после запроса от Системы ДБО ЮЛ (к примеру, при отправке сообщения, П\П и т.п.). После окончания работы с Системой ДБО ЮЛ носитель с секретным ключом должен быть извлечен из компьютера, доступ к компьютеру заблокирован.
12. По окончанию рабочего дня выключайте компьютер, имеющий доступ к Системе ДБО ЮЛ.
13. Носитель с ключевой информацией должен использоваться только владельцем ключа и храниться в месте, исключающем доступ третьих лиц (сейф, опечатываемый бокс, закрывающийся металлический ящик).
14. Не подключайте к компьютеру, который используется для взаимодействия с Системой ДБО ЮЛ, непроверенные на наличие вирусов внешние носители (USB флеш-накопители, внешние жесткие магнитные диски и т.п.).
15. Проверяйте суммы платежей и реквизиты перевода перед подтверждением их в Системе ДБО ЮЛ.

ПОМНИТЕ, *Банк никогда не просит провести тестовые переводы в системе ДБО.*

16. При получении по электронной почте вложений, пришедших из подозрительных источников, не открывайте вложения-исполняемые файлы и не включайте макросы в документах Microsoft Office, если не уверены в надежности отправителя.
17. Не посещайте сайты, не относящиеся к Вашей профессиональной деятельности.

В целях снижения риска несанкционированного доступа к **Мобильному Банку** и поддержания его в работоспособном состоянии:

18. Устанавливайте Мобильный Банк из официальных источников, рекомендуемых Банком (Google Play или App Store).
19. Не передавайте третьим лицам идентификатор ключа, необходимый для подключения к Мобильному Банку.

ФОРАБАНК

20. На мобильном устройстве используйте операционную систему, соответствующую минимальным требованиям, размещенную на сайте Банка.
21. Своевременно обновляйте операционную систему мобильного устройства.
22. Своевременно обновляйте Мобильный Банк.
23. При наличии технической или функциональной возможности мобильного устройства, используйте средства защиты от воздействия вредоносного программного кода (антивирус). Своевременно обновляйте антивирусное программное обеспечение и антивирусные базы. Проводите периодическое полное антивирусное сканирование мобильного устройства (рекомендовано раз в неделю).
24. При наличии технической или функциональной возможности мобильного устройства, установите дополнительный режим защиты доступа к мобильному устройству (вход по код-паролю, отпечатку пальца и т.п.).
25. При проведении операций проверяйте суммы платежей и реквизиты операции в СМС-сообщении, содержащем разовый пароль. Информация должна совпадать с Вашей операцией.

В случае выявления аномалий на Вашем **Устройстве** или в **Системе ДБО** (не можете войти в Систему ДБО, непроизвольное мерцание экрана, движение мыши, произвольное открытие и закрытие окон, программ и т.п.), обнаружили совершение или попытку кражи денежных средств, незамедлительно отключите **Устройство** и обратитесь в АКБ «ФОРА-БАНК» (АО) по телефонному номеру **8 (800) 100-98-89**.

При утрате (потере, хищении) Вашего **Устройства**, для предотвращения несанкционированного списания Ваших денежных средств, незамедлительно обратитесь в АКБ «ФОРА-БАНК» (АО) по телефонному номеру **8 (800) 100-98-89.**

Служба информационной безопасности
АКБ «ФОРА-БАНК» (АО).