Приложение № 3
к Договору на обслуживание
Клиента АО «РУНА-БАНК»
с использованием системы Клиент-Банк

Правила безопасного использования системы Клиент–Банк

Использование системы Клиент–Банк потенциально несет в себе риски неблагоприятных последствий, связанных с хищением денежных средств, для его держателя, которые могут возникнуть в случае несанкционированного доступа к системе Клиент–Банк.

Технологии защиты операций в системе Клиент–Банк используют современные механизмы обеспечения безопасности и предоставляют удобство пользования услугой, обеспечивая при этом высокий уровень ее надежности и безопасности. Вместе с тем эффективность данных механизмов зависит также от выполнения Вами простых правил:

1. Подключайте носитель с ключами электронной подписи только на время работы в системе Клиент–Банк. Контролируйте доступ к Вашему ключу электронной подписи.
2. Запомните пароль для доступа к eToken. Никогда не записывайте его в местах, легко доступных посторонним лицам (на стикерах на мониторе, в файлах на рабочем месте и т.д.).
3. Никому не передавайте носитель с ключами и не сообщайте пароль от ключа.
4. Максимально ограничьте число сотрудников, допущенных к работе с ключами электронной подписи и местам хранения носителей ключей ЭП.
5. Помните, что сотрудники АО «РУНА-БАНК» никогда и ни в какой форме не будут запрашивать Ваш пароль. Игнорируйте любые сообщения по электронной почте, запрашивающие Ваши пароли либо данные счетов или содержащие ссылку на Web-страницу, где Вам предлагается эти данные ввести. Сообщайте в Банк обо всех подобных фактах.
6. Немедленно произведите внеплановую смену ключа ЭП при увольнении сотрудника, имевшего доступ к ключу Вашей электронной подписи.
7. Используйте современное антивирусное программное обеспечение. Регулярно обновляйте антивирусные базы и проводите полную антивирусную проверку Вашего компьютера и мобильного устройства для своевременного обнаружения вредоносных программ.
8. Установите и используйте персональный брандмауэр (firewall) на вашем компьютере. Это позволит предотвратить несанкционированный доступ к информации на компьютере.
9. Устанавливайте самые последние обновления Вашего браузера и операционной системы.
10. Скачивайте и устанавливайте мобильное приложение «РУНА-БАНК БИЗНЕС» только из официальных магазинов приложений Google Play, AppStore.
11. Не записывайте и не храните свой код доступа к мобильному приложению «РУНА-БАНК БИЗНЕС» на устройстве, с которого осуществляется работа в приложении.
12. Используйте безопасную авторизацию для входа в приложение по отпечатку пальца (при наличии на Вашем устройстве).
13. После завершения работы с документами и банковскими счетами каждый раз выполняйте выход из приложения (Меню → Выход).
14. При подозрении, что ваш код доступа к приложению стал известен посторонним лицам или при получении уведомлений об операциях по счету, которых вы не совершали, немедленно обратитесь в Банк и заблокируйте свою учетную запись.
15. Принимайте все возможные меры для предотвращения компрометации (несанкционированного использования) мобильного устройства и SIM-карты.
16. Храните в тайне аутентификационную информацию и обеспечивайте сохранность мобильного устройства и SIM-карты, с помощью которых осуществляется доступ к приложению.
17. Используйте технические средства повышения безопасности, предоставляемые Банком в соответствии с Приложением № 4 к настоящему Договору.
18. По требованию Банка прекратите использование указанного Банком ключа ЭП, сгенерируйте новый ключ ЭП и передайте новый сертификат ключа проверки ЭП в Банке.
19. Ежедневно проверяйте расходные и приходные операции в системе Клиент–Банк или в мобильном приложении.
20. Храните материальный носитель, содержащий ключ ЭП Клиента, в надежном месте, исключающем несанкционированный доступ к нему и его повреждение.
21. Не осуществляйте посредством системы Клиент–Банк незаконные финансовые операции, незаконную торговлю и любые другие операции в нарушение законодательства РФ.

Выполнение Вами данных мероприятий позволит значительно снизить риски совершения несанкционированных операций в системе Клиент–Банк.

При любых подозрениях на компрометацию ключа электронной подписи, а также при возникновении любых необычных ситуаций при работе с системой Клиент–Банк – немедленно обратитесь в АО «РУНА-БАНК».