Основные рекомендации для безопасного использования Системы Банк-Клиент «ELBRUS Internet»

- Храните ключевые носители в надежном месте, где к ним будет исключен доступ третьих лиц. Подключайте ключевые носители к компьютеру только на время работы с системой.
- Используйте сложные пароли, состоящие из букв, цифр и специальных символов, которые вы сможете запомнить, не записывая.
- Ни при каких обстоятельствах не передавайте никому конфиденциальные данные для входа в систему (пароли, ключи, PIN-коды и т. д.), в том числе родственникам, коллегам или сотрудникам Банка.
- Райффайзенбанк не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные. Будьте бдительны: не отвечайте на подобные запросы.
- Если возможно, используйте для работы с системой выделенный компьютер (можно виртуальный), операционную систему или браузер.
- Установите на компьютере, который Вы используете для работы с системой, антивирусное программное обеспечение и межсетевой экран, настройте их в соответствии с рекомендациями поставщика. Регулярно устанавливайте обновления безопасности.
- Всегда корректно завершайте работу в системе в соответствии с указаниями соответствующего Руководства пользователя.
- Настройте и контролируйте уведомления о действиях, произведенных в системе (там, где эта услуга доступна).
- При возникновении подозрения, что Ваши конфиденциальные данные для входа в систему стали известны третьим лицам или обнаружении несанкционированных операций в системе незамедлительно обратитесь в службу поддержки системы по телефонам, указанным в Руководстве пользователя или в ближайшее отделение Райффайзенбанка.
- Не используйте одно и то же устройство для работы в «ELBRUS Internet»/ «ELBRUS Mobile» и приема/передачи сообщений с SMS-паролями.
- Обеспечьте сохранность мобильных устройств с установленным мобильным приложением, а также мобильных устройств, номера которых зарегистрированы в Банке для целей получения SMS-паролей. В случае утери мобильного устройства с установленным мобильным приложением, равно как и мобильного устройства, номер которого зарегистрирован в Банке для целей получения Пользователем SMS-паролей, незамедлительно отключите услугу SMS-OTP в Системе при помощи USB-token или проинформируйте Банк.
- Информируйте Подписантов о недопущении ситуаций переполнения памяти мобильных устройств, что может стать препятствием для приема SMS-сообщений с SMS-паролями.
- Информируйте Банк, в случае замены/утери зарегистрированной SIM-карты Подписанта, к которой подключена услуга SMS-OTP и/или SMS для Бизнеса.