Памятка по правилам безопасной работы

1. Пользователю систем дистанционного банковского обслуживания (далее – СДБО) необходимо иметь собственное рабочее место, соответствующее нижеследующим рекомендациям.

1.1. Персональный компьютер (стационарный или ноутбук) должен иметь характеристики, обеспечивающие работу под управлением операционной системы Microsoft Windows 11 и свободный USB-порт для работы с носителем ключевой информации (далее – НКИ).

На персональном компьютере должна быть установлена актуальная версия операционной системы Microsoft Windows 11, для которой выпускаются и доступны обновления[1] и актуальные версии браузеров, получающих регулярные обновления безопасности: Mozilla Firefox, Opera, Google Chrome, Microsoft Edge[2].

1.2. Для работы в подсистеме «Мобильный банк» (далее – приложение) пользователю рекомендовано иметь мобильное устройство (смартфон, планшет), работающее под управлением актуальных версий операционных систем:

iOS (операционная система для смартфонов и планшетов Apple);

Android (операционная система корпорации Google для смартфонов и планшетов);

HarmonyOS (операционная система для смартфонов и планшетов компании HUAWEI).

Загрузка приложения на мобильное устройство осуществляется пользователем самостоятельно из официальных магазинов приложений AppStore, Google Play, AppGallery. *Использование неофициальных источников (сторонних сайтов, файлообменников) категорически не рекомендуется в целях обеспечения безопасности данных.*

Запрещается использовать устройства с Root-правами (Android, HarmonyOS) или Jailbreak (iOS), так как это отключает встроенные механизмы защиты операционной системы. Использование таких устройств повышает риск компрометации данных и несанкционированного доступа к счетам пользователя.

2. Не рекомендуется использовать публичные и незащищенные беспроводные сети (Public Wi-Fi) для работы в СДБО. Для обеспечения конфиденциальности передаваемых данных необходимо использовать мобильный интернет (3G/4G/5G) или защищенные каналы связи, предоставленные доверенными интернет-провайдерами.

При использовании веб-версии СДБО необходимо убедиться, что адресная строка браузера начинается с защищенного протокола https:// (https://i25-client.belapb.by). Наличие символа «замок» в адресной строке

---

[1] Информация об актуальных версиях Microsoft Windows 11 доступна по ссылке https://learn.microsoft.com/ru-ru/windows/release-health/windows11-release-information.

[2] Информация об актуальных версиях браузеров доступна на соответствующих страницах сайтов производителей.

подтверждает использование зашифрованного соединения и наличие действующего сертификата безопасности.

3. В целях обеспечения безопасности при работе в СДБО пользователю необходимо ограничить физический доступ к рабочим местам (компьютерам), с которых осуществляются банковские операции. Доступ к таким компьютерам должен предоставляться исключительно уполномоченным работникам организации.

Для доступа к операционной системе компьютера в обязательном порядке должен быть установлен сложный пароль (сочетающий буквы, цифры и спецсимволы). Также необходимо активировать функцию автоматической блокировки экрана при неактивности пользователя (не более чем через 10 минут) для предотвращения несанкционированного доступа в отсутствие работника.

На компьютерах должно быть установлено лицензионное антивирусное программное обеспечение с функцией автоматического обновления антивирусных баз не реже одного раза в сутки.

4. В целях обеспечения безопасности пользователь обязан производить смену пароля в СДБО не реже одного раза в 180 календарных дней. Новый пароль должен существенно отличаться от предыдущих, не совпадать с логином и отвечать требованиям сложности (сочетать строчные и заглавные буквы, цифры и специальные символы). Пользователь обязан обеспечивать строгую конфиденциальность пароля; его передача третьим лицам или хранение в открытом виде (в том числе в текстовых файлах или на бумажных носителях) категорически запрещена.

Рекомендуется отключить функцию автозаполнения паролей в браузерах для страницы СДБО.

5. При работе с электронной почтой пользователю рекомендуется:

не открывать исполняемые файлы (.exe, .scr, .bat, .vbs, .js и др.);

проявлять предельную осторожность с архивами (.zip, .rar), особенно защищенными паролем, так как их содержимое недоступно для автоматической проверки антивирусом;

с осторожностью относиться к файлам .docm, .xlsm (документы с макросами), так как они могут содержать скрипты для загрузки вирусов;

не переходить по ссылкам из писем: для входа в СДБО использовать только ручной ввод адреса или сохраненные закладки;

всегда проверять реальный адрес отправителя (не только имя, но и домен после символа @) и не открывать вложения от неизвестных лиц.

Категорически запрещается отвечать на электронные письма, содержащие запросы конфиденциальных данных (пароли, коды подтверждения и иное). Помните: любое подобное сообщение является мошенническим.

Работники банка никогда не запрашивают персональную информацию или реквизиты доступа через электронную почту или мессенджеры.

6. В целях предотвращения кибермошенничества пользователю строго запрещено сообщать персональные и конфиденциальные данные (логин и

пароль от СДБО, пароль к ключу ЭЦП, коды из СМС/Push-уведомлений, паспортные данные, историю операций) любым третьим лицам.

Помните: настоящие работники банков, правоохранительных органов или служб поддержки никогда не запрашивают подобную информацию. Любые обращения с требованием сообщить эти данные следует расценивать как попытку хищения.

7. В случае возникновения подозрений на компрометацию данных (несанкционированный доступ третьих лиц к компьютеру, мобильному устройству или НКИ), а также при обнаружении операций, которые пользователь не совершал, необходимо незамедлительно сообщить об этом в обслуживающее подразделение банка для оперативной приостановки (при необходимости – блокировки) доступа к СДБО и действия сертификата ключа ЭЦП.