

ПАМЯТКА ПО БЕЗОПАСНОСТИ ОБСЛУЖИВАНИЯ СИСТЕМЫ ДБО ДЛЯ ФИЗИЧЕСКИХ ЛИЦ

АО «ПЕРВОУРАЛЬСКБАНК» придает большое значение обеспечению безопасности доступа к средствам Клиентов. Пожалуйста, внимательно прочитайте нижеизложенную информацию и следуйте нашим рекомендациям по работе с системой ДБО (далее - Система):

- Вход в Систему осуществляется **ТОЛЬКО** через корпоративный сайт АО «ПЕРВОУРАЛЬСКБАНК» (далее – Банк) <https://www.pervbank.ru/> <https://dbo.pervbank.ru/ibank2/> https://dbo.pervbank.ru/web_banking/ и официальные мобильные приложения Банка [PB.bank](#) и [PB.money](#).
- Если вам пришли письма, в том числе от имени Банка, содержащие требования (а так же просьбы или предложения) зайти на сайт, адрес которого начинается не с адреса банка <https://www.pervbank.ru/> <https://dbo.pervbank.ru>, прислать секретный ключ и/или пароль доступа к Системе, **НИ В КОЕМ СЛУЧАЕ** не отвечайте. Вам нужно немедленно сообщить об этом в Банк в рабочее время по телефону [+7 804 333-94-97](tel:+78043339497) Банк **НИКОГДА** не рассылает Клиентам подобные электронные письма, а также не рассылает по электронной почте программы для установки на компьютеры.
- **НИКОГДА** не отлучайтесь от компьютера или мобильного устройства, пока работаете в Системе.
- После завершения работы в Системе **СРАЗУ** нажимайте кнопку «Выход».
- Пользоваться средствами генерации (получения) одноразовых паролей может **ТОЛЬКО** Клиент.
- **НИ В КОЕМ СЛУЧАЕ** не передавайте средства генерации (получения) одноразовых паролей другим пользователям (в том числе ИТ-специалистам) даже для проверки работы Системы или настроек взаимодействия с Банком, и т. п. При необходимости такой проверки **ТОЛЬКО** Клиент должен использовать средства генерации (получения) одноразовых паролей, при этом убедившись, что пароли вводятся именно в интерфейс клиентской части Системы.
- **ОБЯЗАТЕЛЬНО** храните средства генерации (получения) одноразовых паролей, в надежном месте, исключая их повреждение и несанкционированный доступ к ним посторонних лиц. Вся ответственность за сохранность средств генерации (получения) одноразовых паролей полностью лежит на вас, как единственном их владельце.
- Вы должны обеспечить строго конфиденциальное использования паролей доступа и средств генерации (получения) одноразовых паролей. Работникам Банка для вашего обслуживания и поддержки Системы в работоспособном состоянии пароли **НЕ ТРЕБУЮТСЯ**.
- **ОБЯЗАТЕЛЬНО** применяйте средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные межсетевые экраны, антишпионское программное обеспечение и т.п.
- Как можно **БЫСТРЕЕ** производите смену паролей доступа или средств генерации (получения) одноразовых паролей, как в случае их рассекречивания, так и по требованию Банка.

- В случае выявления явных или косвенных признаков рассекречивания паролей доступа или наличия вредоносных программ в компьютере или на мобильном устройстве, используемом для работы в Системе, вам нужно **НЕЗАМЕДЛИТЕЛЬНО** уведомить об этом Банк по телефону: [+7 804 333-94-97](tel:+78043339497), либо лично явиться в Банк, чтобы заблокировать пароли доступа, с последующей их заменой. О нарушении секретности могут свидетельствовать следующие события:
 - утеря средств генерации (получения) одноразовых паролей, даже если они потом обнаружатся;
 - выход из строя средств генерации (получения) одноразовых паролей, когда невозможно достоверно определить причину их поломки (и допустима возможность того, что это произошло в результате действий злоумышленника);
 - обнаружение факта или угрозы использования (копирования) паролей доступа, средств генерации (получения) одноразовых паролей;
 - получение доступа к Системе неуполномоченных лиц (несанкционированная отправка электронных документов);
 - обнаружение ошибок в работе Системы, в том числе возникающих в связи с попытками нарушения информационной безопасности.
- Устанавливайте приложение для мобильного Банка и его обновления только из официального магазина приложений App Store и Google Play.
- Установите пароль доступа к вашему мобильному устройству.
- Не храните на мобильном устройстве конфиденциальную информацию (PIN коды платежных карт, пароли доступа, кодовое слово).
- Удаляйте конфиденциальную информацию в случае передачи мобильного устройства другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек устройства.
- В случае утери мобильного устройства с установленным Мобильным банком или обнаружения блокировки SIM-карты без Вашего ведома, незамедлительно заблокируйте доступ, позвонив в Банк.
- Соблюдайте общие правила безопасного использования мобильного устройства:
 - используйте только лицензионное программное обеспечение;
 - установите антивирус и регулярно обновляйте его;
 - избегайте настроек типа root и jailbreak;
 - не переходите по сомнительным ссылкам.

Помимо указанных выше правил Банк рекомендует также:

- **ИСКЛЮЧИТЬ** доступ посторонних лиц к компьютерам и мобильным устройствам, используемых для работы в Системе;
- На компьютерах и мобильных устройствах, используемых для работы в Системе, **ЗАПРЕТИТЬ** посещение всех интернет-сайтов, кроме необходимых для входа в Систему, а также установку развлекательных и игровых программ;
- Использовать **ТОЛЬКО** лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного ПО;
- При обслуживании компьютера и мобильных устройств ИТ-специалистами контролировать ВСЕ выполняемые ими действия;

- В качестве дополнительных мер по обеспечению безопасности **ВОСПОЛЬЗОВАТЬСЯ** предоставляемой Банком возможностью установки ежедневных лимитов.