

ЦЕЛЬ НАСТОЯЩЕЙ ПАМЯТКИ – В ПРЕДОСТЕРЕЖЕНИИ КЛИЕНТОВ ОТ ВОЗМОЖНЫХ СЛУЧАЕВ МОШЕННИЧЕСТВА, НАД КОТОРЫМИ БАНК НЕ ИМЕЕТ ПРЯМОГО КОНТРОЛЯ, И ПРИ КОТОРЫХ КРАЙНЕ ВАЖНА ОСВЕДОМЛЕННОСТЬ КЛИЕНТОВ И СОХРАНЕНИЕ ИХ БДИТЕЛЬНОСТИ.

Вместе с тем обращаем Ваше внимание, что Система дистанционного банковского обслуживания «Интернет-Клиент» для юридических лиц, индивидуальных предпринимателей, крестьянских (фермерских) хозяйств, частных нотариусов, адвокатов, частных судебных исполнителей, профессиональных медиаторов (далее - Система) зарекомендовала себя как наиболее надежный и безопасный способ работы с Банком, и позволяет контролировать состояние своих счетов, подготавливать и направлять в Банк на исполнение платежные и иные документы, а также получать широкий спектр актуальной финансовой информации без непосредственного обращения в Банк.



В СЛУЧАЕ КОМПРОМЕТАЦИИ ДАННЫХ ИЛИ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ТРАНЗАКЦИЙ ВАМ НЕОБХОДИМО ОБРАТИТЬСЯ В CONTACT CENTRE БАНКА ПО СЛЕДУЮЩИМ ТЕЛЕФОНАМ:



**8 8000 801 888 - БЕСПЛАТНЫЙ НОМЕР ДЛЯ ЗВОНКА С ГОРОДСКИХ ТЕЛЕФОНОВ ПО РЕСПУБЛИКЕ КАЗАХСТАН;
7888 - БЕСПЛАТНЫЙ НОМЕР ДЛЯ ЗВОНКА С ГОРОДСКИХ ТЕЛЕФОНОВ ПО РЕСПУБЛИКЕ КАЗАХСТАН.**



- ❑ Избегайте подключений к веб-сайту Системы по баннерным ссылкам или по ссылкам, содержащимся в электронных письмах. Проверьте, что установлено защищенное SSL-соединение с официальным сайтом Системы, по адресу <https://ib.bankrbk.kz> и её новой версии по адресу <https://online.bankrbk.kz>. Рекомендуем ввести адрес веб-сайта самостоятельно и добавить его в закладки браузера. Если Вы заметили, что адрес веб-сайта в адресной строке браузера изменился, **НЕ ВВОДИТЕ** Ваш Логин и Пароль, немедленно закройте данный сайт и обратитесь в Банк.
- ❑ Ни при каких обстоятельствах **НЕ РАЗГЛАШАЙТЕ** Пароли доступа к Системе. Пароли являются конфиденциальной информацией и должны быть известны только лицу, для которого Банком создан Логин для доступа в Систему. Пароль для доступа в Систему должен быть не менее 8 символов, содержать буквы, цифры и специальные символы.
- ❑ **НЕ СОХРАНЯЙТЕ** Ваш **ПАРОЛЬ В ИНТЕРНЕТ-БРАУЗЕРЕ И ТЕКСТОВЫХ ФАЙЛАХ** на компьютере либо на других электронных носителях информации, так как это может привести к его краже и компрометации.
- ❑ **НЕ СОХРАНЯЙТЕ** на компьютере и не устанавливайте файлы и (или) программы, полученные не из доверенных источников, по электронной почте или скачанные из Интернета.
- ❑ Ни при каких обстоятельствах **НЕ ПЕРЕДАВАЙТЕ** Ключевой носитель с ЭЦП и устройство OTP-Token другому лицу, предпринимайте все меры для предотвращения его несанкционированного копирования.

ПАРОЛЬ, КЛЮЧЕВОЙ НОСИТЕЛЬ С ЭЦП, УСТРОЙСТВО OTP-ТОКЕН ДЛЯ ВХОДА И РАБОТЫ С СИСТЕМОЙ - ЭТО ВАША ЛИЧНАЯ КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ.

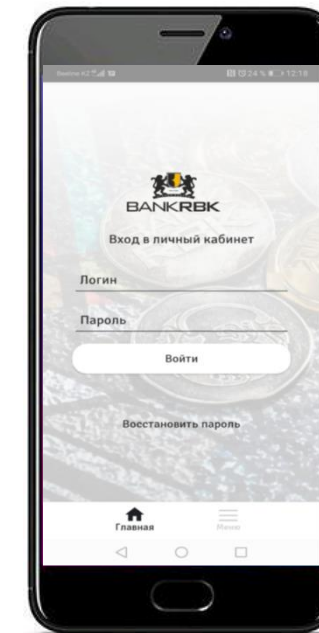
Официальный сайт Системы
<https://ib.bankrbk.kz>
<https://online.bankrbk.kz/>



- ❑ Для предотвращения копирования Регистрационного свидетельства (ЭЦП) и личных конфиденциальных данных **НЕОБХОДИМО**:
 - **ИСПОЛЬЗОВАТЬ** Ключевой носитель с ЭЦП, устройство OTP-Token **ТОЛЬКО** в момент подписания платежных документов в Системе;
 - **ИЗБЕГАТЬ** публичных мест с публичными точками доступа в интернет (например интернет-кафе), осуществлять банковские операции со специально выделенного на эти цели персонального компьютера;
 - **НЕ ПЕРЕДАВАТЬ** Ключевой носитель с ЭЦП, устройство OTP-Token посторонним лицам.
- ❑ В случае рассекречивания Вашего Пароля к Системе, утери/кражи устройства OTP-Token, Ключевого носителя с ЭЦП или несанкционированного копирования Регистрационного свидетельства (ЭЦП), подозрений на несанкционированное использование Системы и (или) Регистрационного свидетельства (ЭЦП), а также в иных случаях, которые могут привести к несанкционированному доступу к счетам Вашей Компании, необходимо **НЕЗАМЕДЛИТЕЛЬНО** уведомить об этом Банк по телефонам: **8 8000 801 888, 7888**.

ОТВЕТСТВЕННОСТЬ ЗА ХРАНЕНИЕ ЛИЧНЫХ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ, УСТРОЙСТВ OTP-ТОКЕН, КЛЮЧЕВОГО НОСИТЕЛЯ С ЭЦП И ПАРОЛЕЙ ВОЗЛАГАЕТСЯ НА ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ. ХРАНИТЕ КЛЮЧЕВЫЕ НОСИТЕЛИ С ЭЦП, УСТРОЙСТВА OTP-ТОКЕН, ЛОГИН И ПАРОЛЬ В МЕСТАХ, К КОТОРЫМ ОГРАНИЧЕН ДОСТУП ТРЕТЬИХ ЛИЦ.

- ❑ Во время доступа в Систему **ИСПОЛЬЗУЙТЕ ПОЛИТИКИ БЕЗОПАСНОСТИ** операционной системы для ограничения прав доступа Пользователю. Это поможет снизить риск реализации различных атак на рабочую станцию и причинения ущерба Компании от возможных действий деструктивного характера злоумышленников.



- ❑ **МАКСИМАЛЬНО ОГРАНИЧЬТЕ** доступ к компьютеру, на котором установлена Система.
- ❑ Ежедневно анализируйте информацию о принятых и непринятых Банком Электронных документах, а также немедленно информируйте Банк о случаях несанкционированного зачисления (перечисления) денег.
- ❑ При утере мобильного телефона, на который Банк отправляет SMS-уведомления, или неожиданном прекращением работы SIM-карты Вам следует как можно быстрее обратиться к своему оператору мобильной связи и заблокировать SIM-карту, а также проинформировать об этом Банк.
- ❑ Всегда выходите из Системы через ссылку «Выход», в этом случае Ваш сеанс будет прекращен немедленно и корректно.
- ❑ По завершении работы в Системе **ОТКЛЮЧИТЕ И ИЗВЛЕКИТЕ** Ключевой носитель с ЭЦП из USB-порта компьютера. Не оставляйте Ключевой носитель с ЭЦП постоянно подключенным к компьютеру. Подключайте его только при необходимости работы в Системе.
- ❑ **БЛОКИРУЙТЕ КОМПЬЮТЕР** и обязательно извлекайте из USB-порта персонального компьютера Ключевой носитель с ЭЦП, если требуется покинуть рабочее место.
- ❑ Своевременно **УСТАНАВЛИВАЙТЕ ОБНОВЛЕНИЯ ОПЕРАЦИОННОЙ СИСТЕМЫ** своего компьютера, рекомендуемые компанией-производителем.
- ❑ Используйте **ЛИЦЕНЗИОННОЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ** и **РЕГУЛЯРНО ВЫПОЛНЯЙТЕ АНТИВИРУСНУЮ ПРОВЕРКУ** для своевременного обнаружения вредоносных программ.



БАНК ВЛАДЕЕТ ВСЕЙ НЕОБХОДИМОЙ ИНФОРМАЦИЕЙ И НИКОГДА, НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ ОСУЩЕСТВЛЯЕТ ЗВОНКИ ПО ТЕЛЕФОНУ, РАССЫЛКУ ЭЛЕКТРОННЫХ ПИСЕМ, SMS-СООБЩЕНИЙ С ПРОСЬБОЙ ПРЕДОСТАВИТЬ ВАШ ПАРОЛЬ К СИСТЕМЕ, А ТАКЖЕ НЕ РАСПРОСТРАНЯЕТ ПО ЭЛЕКТРОННОЙ ПОЧТЕ ПРОГРАММЫ И ИХ ОБНОВЛЕНИЯ. ДЛЯ РЕШЕНИЯ ТЕХНИЧЕСКИХ ИЛИ ИНЫХ ПРОБЛЕМ В СИСТЕМЕ СОТРУДНИКУ БАНКА НЕ НУЖНО ЗНАТЬ ВАШ ЛИЧНЫЙ ПАРОЛЬ.