



АКЦИОНЕРНОЕ ОБЩЕСТВО
«МУРМАНСКИЙ СОЦИАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК»

Уважаемые Клиенты! В целях минимизации рисков, связанных с осуществлением несанкционированных переводов денежных средств с использованием системы «МСКБ Бизнес», заботясь о Вашей безопасности, БАНК «МСКБ» (АО) разработал следующие рекомендации по реализации защитных мер при использовании системы «МСКБ Бизнес»:

- Используйте лицензионную операционную систему на компьютере, применяемом для работы в системе «МСКБ Бизнес». В операционной системе обязательно должна быть включена функция автоматической загрузки и установки обновлений операционной системы и прикладного программного обеспечения.
 - На компьютере, используемом для работы в системе «МСКБ Бизнес», должно быть установлено и включено антивирусное программное обеспечение и персональный сетевой экран с постоянно обновляющимися в автоматическом режиме базами.
 - Все прикладное и системное программное обеспечение, установленное на компьютере с системой «МСКБ Бизнес», должно быть лицензионным и получено из доверенного источника. Избегайте установки на компьютер ненужного программного обеспечения.
 - Работу пользователя в операционной системе с системой «МСКБ Бизнес» рекомендуется организовать в режиме «обычного пользователя» (классификация в системе Microsoft Windows - Пользователи).
 - Установите сложные пароли на доступ в операционную систему, BIOS и систему «МСКБ Бизнес».
 - Рекомендуем отключить возможность автозапуска программ со всех подключаемых и встроенных устройств хранения данных, сетевых и сменных носителей информации.
 - Настоятельно рекомендуем отключить функцию подключения к удаленному рабочему столу операционной системы (Свойства системы - вкладка «Удаленный доступ» - «Не разрешать подключения к этому компьютеру»), а также исключить установку на компьютере с системой «МСКБ Бизнес» программ удаленного администрирования (Radmin, TeamViewer, Ammyu Admin и т.д.).
 - Подключайте носитель с электронной подписью только на время работы в системе «МСКБ Бизнес», а в иное время обеспечьте его размещение в надежном хранилище (сейфе). Не оставляйте ключевой носитель без контроля, никогда не передавайте его ни при каких обстоятельствах третьим лицам, не копируйте данные с ключевого носителя.
 - Используйте услугу sms-информирования о движении по счету.
 - Ежедневно контролируйте движение по счету, получая выписки по нему.
 - Установите лимит на сумму одного платежа.
 - В случае возможности установите ограничение на право работы с системой «МСКБ Бизнес» с определенных сетевых адресов.
 - Используйте для осуществления платежей выделенный компьютер. Ограничьте к указанному компьютеру физический доступ, путем размещения его в отдельном помещении с ограниченным доступом.
 - Постарайтесь не допускать третьих лиц к компьютеру с системой «МСКБ Бизнес», особенно оказывающих услуги аутсорсинга в области информационных технологий без заключения договора.
-



АКЦИОНЕРНОЕ ОБЩЕСТВО
«МУРМАНСКИЙ СОЦИАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК»

- При работе в сети Интернет будьте бдительны, устанавливайте дополнительные программы и приложения, только если вы доверяете их разработчику. Никогда не открывайте вложения в письмах, полученных по электронной почте, от неизвестных отправителей.
- С целью защиты от фишинг-атак (поддельные веб-страницы) при доступе в систему «МСКБ Бизнес» осуществляйте постоянный визуальный контроль за адресной строкой web-обозревателя (браузера) на соответствие веб-адресу банка - <https://dbo.bank-mscb.ru>, <https://ibank.bank-mscb.ru> или <https://дбо.банк-мскб.пф>, а также на отсутствие ошибок в сертификате безопасности веб-узла.

ВНИМАНИЕ!!!

- В случае выхода из строя компьютера с системой «МСКБ Бизнес» (например, компьютер неожиданно перезагрузился и больше не загружается).
- В случае выявления вредоносного программного обеспечения.
- В случае потери ключевого носителя или подозрения в его компрометации.
- В случае выявления электронных платежных документов в системе «МСКБ Бизнес», передача которых не осуществлялась.
- В случае поступления информации (sms-информирование, выписки по счетам) об операциях по счету, которые не осуществлялись.

Немедленно сообщите об этом
в службу технической поддержки Банка с 09.30 до 18.00 по телефону –
(8152) 230-914,
либо операционному работнику с 09.30 до 17.00 по телефону –
(8152) 230-373.
