


### Меры безопасности при работе в ПТК «Интернет-банк» для юридических лиц

Для обеспечения безопасности работы в системе ПТК «Интернет-банк» для юридических лиц применяются:

- Шифрование канала связи с использованием протокола TLS;
- Ключ усиленной электронной подписи (неквалифицированная электронная подпись) для авторизации и подтверждения операций;
- Рассылка уведомлений об операциях и событиях безопасности;
- Автоматическое отключение сессии при неактивности более 30 минут;
- Дополнительная аутентификация по SMS (по умолчанию отключена);
- Настройка фильтров IP-адресов (по умолчанию отключена);
- Дополнительное подтверждение подозрительных платежей (фрод-мониторинг).

Для повышения безопасности работы в ПТК «Интернет-банк» рекомендуется соблюдать следующие правила:

- Не используйте для работы в ПТК «Интернет-банке» недоверенные, чужие компьютеры (интернет-кафе, киоски и т.п.);
- Не оставляйте компьютер или мобильное устройство без присмотра с авторизованным ПТК «Интернет-банк»;
- Исключите доступ посторонних лиц к компьютеру, используемому для работы с ПТК «Интернет-банк»;
- Используйте только лицензионное программное обеспечение и регулярно обновляйте его;
- Используйте только лицензионное антивирусное программное обеспечение, регулярно обновляйте его базы и периодически производите полную проверку компьютера на вирусы;
- Используйте виртуальную клавиатуру при вводе пароля для защиты от вредоносных программ считывающих нажатия клавиш;
- Всегда проверяйте, правильный ли адрес отображается в строке браузера, действительно ли соединение происходит в защищенном режиме – в окне браузера должен быть изображен зеленый значок закрытого замка

 BANK PERVOMAISKY PJSC [RU] <https://internet.1mbank.ru/user/login>

- Не назначайте пароль на ключ электронной подписи, используемый в ПТК «Интернет-банк», в любых других системах и сервисах;
- Не сообщайте пароль на ключ электронной подписи, используемый в ПТК «Интернет-банк» третьим лицам. **Банк «Первомайский» (ПАО) НИКОГДА не запрашивает пароли своих клиентов;**

- Не храните ключ усиленной электронной подписи на жестком диске компьютера. Рекомендуется использовать флеш-носитель, лучше всего – eToken ГОСТ (можно приобрести в офисе Банка);
- Не оставляйте eToken ГОСТ или другие носители с ключом, подключенным к компьютеру после завершения работы в ПТК «Интернет-банк». Рекомендуется подключать носитель с ключом только для авторизации в ПТК «Интернет-банк» и подтверждения операций;
- Храните носитель с ключом в недоступном для посторонних лиц месте.

**Если у Вас есть подозрения, что с Вашего счета произведен мошеннический платеж, позвоните по телефону горячей линии.**

**Если у Вас есть подозрения, что Ваш ключ электронной подписи и/или пароль на ключ, используемый для входа в ПТК «Интернет-банк» и подписания электронных документов, попали в чужие руки, обязательно позвоните по телефону горячей линии для блокировки Вашей учетной записи в системе.**

**Телефон горячей линии**

**8-800-100-5-100**

**(звонок бесплатный)**