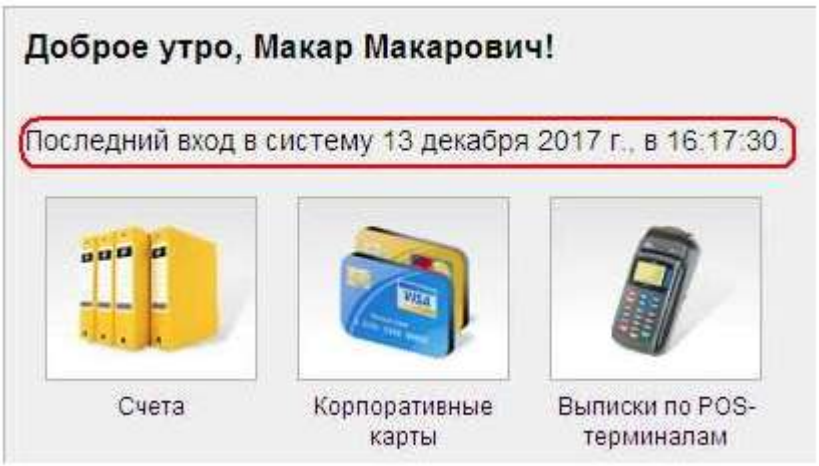
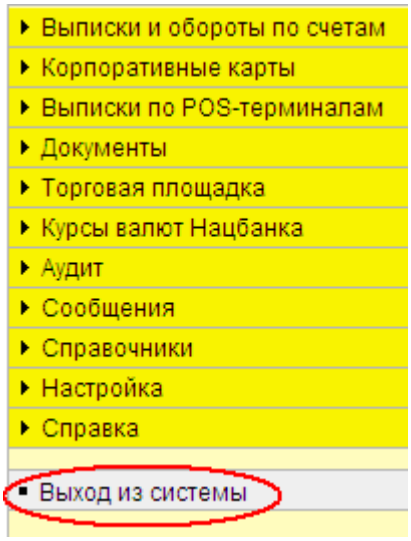
Рекомендации для клиентов «Приорбанк» ОАО, пользующихся системой Интернет-Банк для юридических лиц и индивидуальных предпринимателей

- Данная информация предназначена для того, чтобы помочь клиентам обеспечить должную безопасность передачи данных через Интернет при использовании Интернет-Банка.
- Установите на компьютере, который Вы используете для работы с системой Интернет-Банк, антивирусное программное обеспечение и межсетевой экран (firewall), настройте их в соответствии с рекомендациями поставщика. Регулярно устанавливайте обновления безопасности.
- При открытии сайта www.ib.priorbank.by убедитесь, что Ваше соединение с банковским сервером происходит в защищенном режиме (по Протоколу TLS).
- Отключите Автозаполнение/сохранение страниц, а также проверьте, чтобы Ваш браузер не допускал сохранения конфиденциальных страниц. Не соглашайтесь на предложение браузера сохранить пароль для последующего входа.
- Никогда и ни при каких обстоятельствах никому не передавайте свои секретные параметры (Имя пользователя, пароль для входа, Авторизационный код, ЭЦП). Ознакомьтесь с Политикой безопасности, принятой в «Приорбанк» ОАО.
- Придумайте себе надёжные Пароль и Авторизационный код.
- Не сохраняйте свои Имя пользователя, пароль для входа и Авторизационный код на компьютере/цифровом носителе, доступ к которому имеют другие лица.
- Не используйте для Интернет-Банка Имя пользователя и пароль, которые уже используются Вами для авторизации на сайтах социальной сети (интернет-магазины, чаты и другие).
- Контролируйте время своего последнего посещения системы:



– Всегда выходите из системы по кнопке «Выход из системы»:



Политика безопасности

Никто из работников банка, лиц и организаций, связанных с банком, или кто бы то ни было никогда и ни при каких обстоятельствах не может и не должен просить либо требовать предоставления конфиденциальной информации, касающейся электронных каналов обслуживания. К конфиденциальной информации относятся:

1. Имя пользователя,
2. Пароль на вход в систему,
3. Авторизационный код, используемый при настройке и проведении платежей в системе,
4. ЭЦП,
5. Номера карточек, PIN-коды и другая информация, размещенная на пластиковых карточках.

Разглашение указанной информации может создать предпосылки к осуществлению в отношении Вас мошеннических действий и привести к финансовым и моральным потерям, как для Вас, так и для Банка.

В случае обращения к Вам по телефону, посредством почтовых или электронных рассылок, личного либо любого другого запроса на предоставление указанной информации, пожалуйста, немедленно сообщите об этом сотрудникам банка:

- **по телефонам: +375 17 289-90-87**
- **487 (Velcom, МТС или life:))**
- **187 по г. Минску**
- **+375 17 289-92-92 (круглосуточно)**
- **на e-mail: prior@priorbank.by**
- **по факсу: +375 17 289-91-91 либо любым другим способом**

Протокол TLS

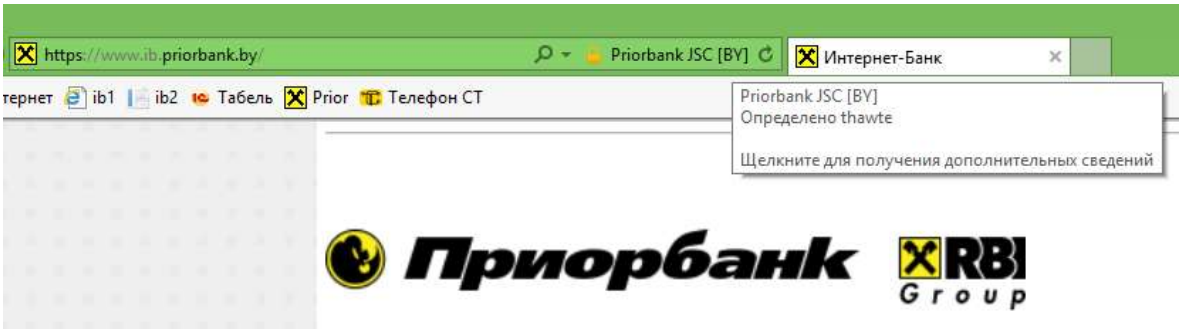
TLS (Transport Layer Sockets) — это протокол, который защищает данные, пересылаемые между веб-обозревателями (браузерами) и веб-серверами. При работе этого протокола создаётся защищенный канал, по которому информация может передаваться между браузером и сервером в закодированном виде, с тем, чтобы никто не смог исказить информацию или получить к ней доступ.

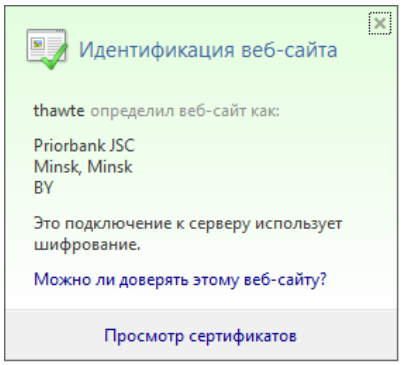
Любая страница, адрес которой начинается с **https**, передается в защищённом виде с помощью TLS. Буква «s», добавленная к знакомому HTTP (Hypertext Transfer Protocol), означает secure, то есть
«защищённый».

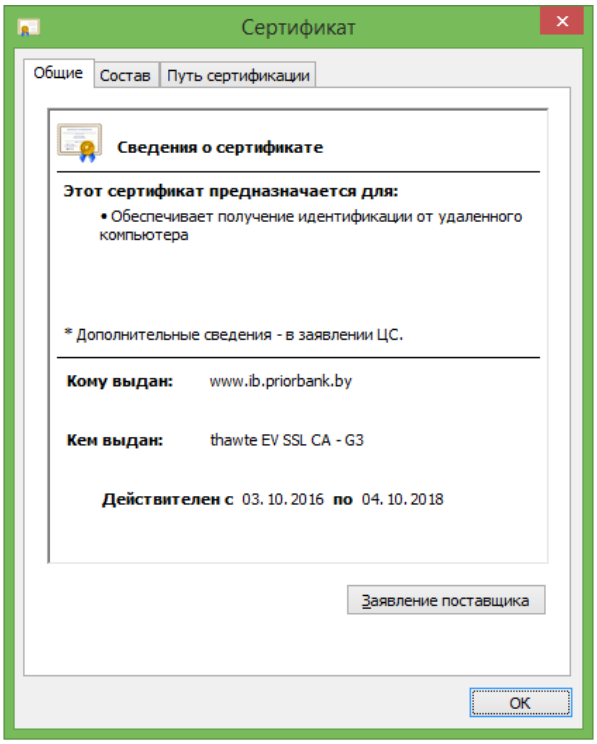
Пользователям не нужно предпринимать никаких специальных действий, чтобы переключиться на TLS-соединение — клиентский криптографический протокол TLS встроен в браузер.

Как проверить, что соединение происходит в защищенном режиме.

Вы можете проверить подлинность сертификата сервера Интернет-Банка Prior Online, щелкнув на значке защищенного соединения «Priorbank JSC [BY]».







Выбор надежного пароля

Надежный пароль — это такой пароль, который трудно угадать, но легко запомнить. Слишком сложные пароли, скорее всего, будут записаны и вследствие этого станут ненадёжными.

Чтобы пароль было трудно угадать, он должен обладать специфическими синтаксическими характеристиками.

При выборе пароля желательно следовать следующим правилам:

- Пароль должен состоять, по меньшей мере, из 6 знаков (чем длиннее пароль, тем лучше);
- Пароль должен представлять собой сочетание заглавных и строчных букв латинского алфавита, цифр и, если возможно, спецсимволов;
- Не следует выбирать в качестве пароля (чтобы исключить вероятность определения пароля путем перебора) слова, содержащихся в стандартных словарях: имена, сокращения, слова, взятые из словарей (включая иностранные словари) или логические последовательности;
- Пароль не должен содержать в себе повторяющихся последовательностей знаков (например, в слова «access» содержится больше двух идентичных знаков, следующих друг за другом), очевидных последовательностей или узоров, образуемых символами, нанесенными на клавиши клавиатуры (например, asdfghjkl или erdfcv).
- Перемежайте короткие слова цифрами или специальными символами, например, this;Is:One.good:PassWord или 3Doggiesareloud!
- Создавайте аббревиатуру из начальных букв слов, составляющих предложение, которое вы можете без труда запомнить. Например, вы можете составить аббревиатуру Tpftssivhtc из начальных букв слов в предложении «This password for the security system is very hard to crack».

Автозаполнение/сохранение страниц

При запросе окна обозревателя об использовании автозаполнения полей формы (логина и пароля) следует отказаться от данной функции. Если возможность автозаполнения личной информации в формах вашего обозревателя уже активизирована, Вы можете отключить эту функцию вручную в настройках обозревателя. Для этого Вам необходимо установить соответствующие параметры в меню *«Сервис»(Tools) → «Свойства обозревателя»(Internet Options) → «Содержание»(Content) → «Автозаполнение»(AutoComplete).*

Чтобы Ваш обозреватель не допускал сохранения конфиденциальных страниц (SSL-page), необходимо отключить функцию форм в установках Вашего обозревателя. Для этого Вам необходимо установить соответствующие параметры в меню *«Сервис»(Tools) → «Свойства обозревателя»(Internet Options) → «Содержание»(Content) → Формы (Forms)* Это поможет не сохранять данные (Пароль пользователя, имя пользователя и др.) на жёстком диске.