Рекомендации для клиентов «Приорбанк» ОАО, пользующихся системой Интернет-Банк Prior Online.

Данная информация предназначена для того, чтобы помочь клиентам обеспечить должную безопасность при использовании Интернет-Банка.

Напоминаем, что в соответствии с Политикой безопасности, принятой в «Приорбанк» ОАО, секретные параметры (логин, пароль для входа, Авторизационный код, М-код) должны быть известны только Вам и никогда и ни при каких обстоятельствах не передаваться третьим лицам, в т.ч. сотрудникам банка.

Для повышения уровня безопасности рекомендуем Вам соблюдать следующие условия при использовании Интернет-банка Prior Online:

• На компьютере, который Вы используете для работы с системой Интернет-Банк, установлены и настроены антивирусное программное обеспечение и межсетевой экран (брандмауэр), и Вы регулярно обновляете ОС и базы данных антивируса.

• Убедитесь, что при открытии сайта www.prior.by Ваше соединение с банковским сервером происходит в защищенном режиме.

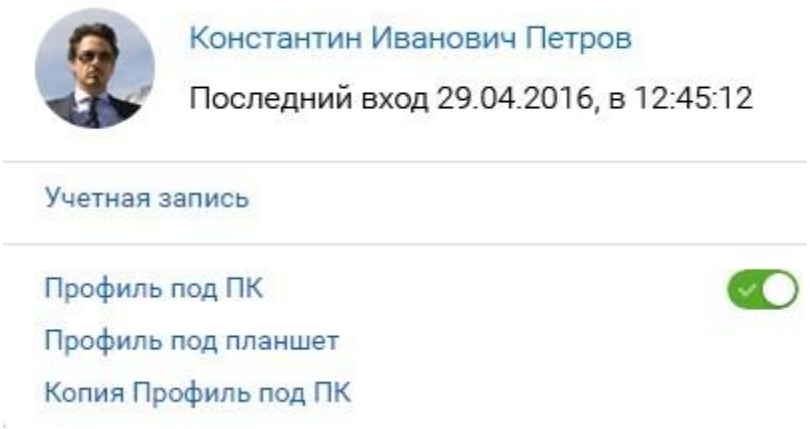
• В браузере отключено Автозаполнение/сохранение страниц, не допускается сохранение конфиденциальных страниц и паролей для последующего входа.

• Пароль для входа и Авторизационный код соответствуют рекомендациям, приведенным ниже (рекомендации по выбору надежного пароля и Авторизационного кода).

• Логин, пароль для входа и Авторизационный код не хранятся на общедоступных ресурсах, компьютере или цифровом носителе в открытом виде, и способ хранения исключает доступ к данной информации других лиц.

• Для Интернет-Банка не используются логин и пароль, которые уже используются Вами для авторизации на иных сайтах и социальных сетях (интернет-магазины, чаты и другие).

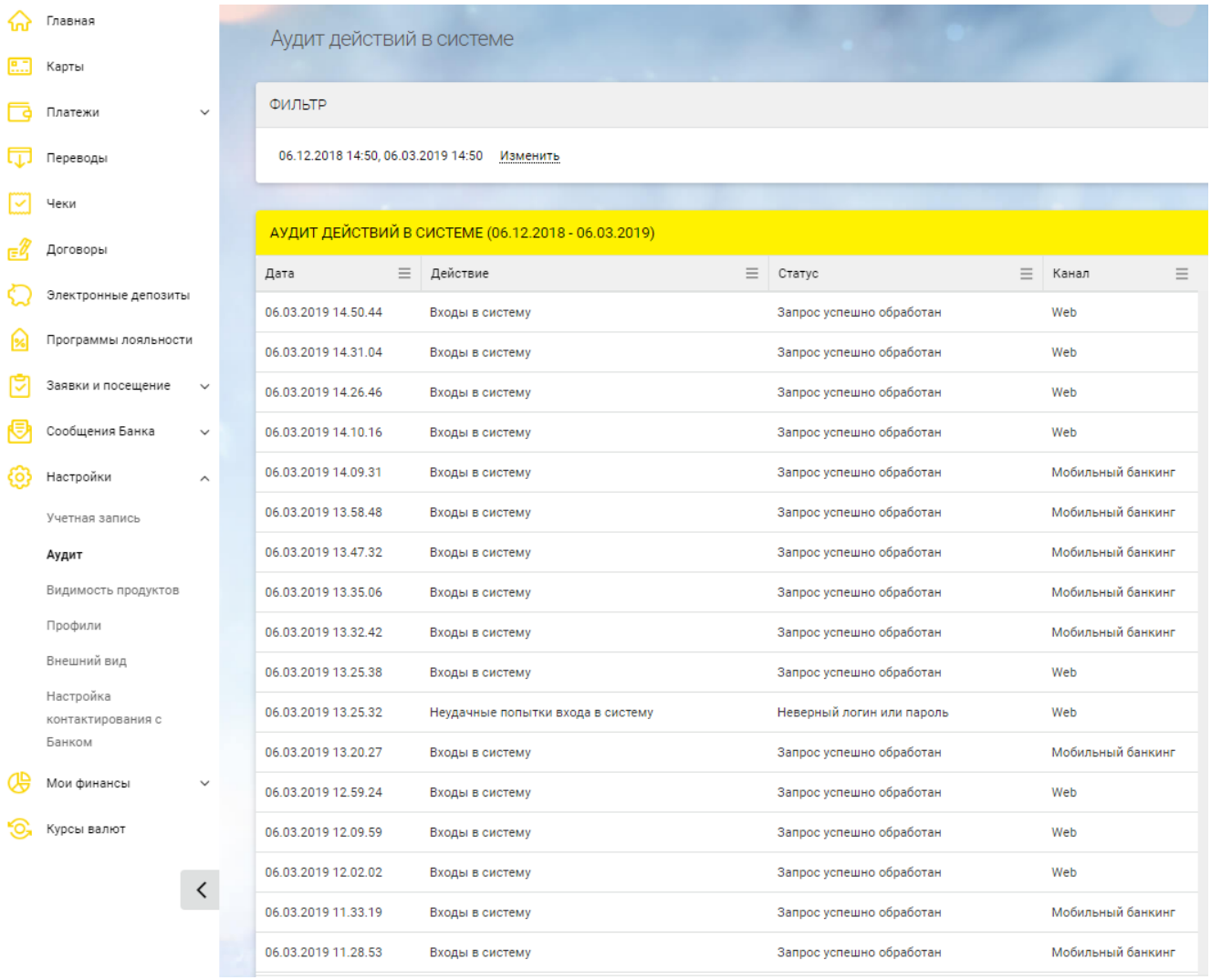
• При каждом входе в систему осуществляется контроль времени своего последнего посещения системы:



• Регулярно осуществляется контроль совершенных действий посредством аудита действий в системе. Действия, которые могут вызывать подозрение: «Неудачные попытки входа в систему», «Неудачные попытки ввода А-кода», «Входы в систему». В случае обнаружения вышеперечисленных действий, которые Вы не совершали, необходимо немедленно сообщить об этом сотрудникам банка:

• по телефонам: +375 17 289-90-90, 487 (Velcom, МТС или life:)), 187 по г. Минску,
+375 17 289-92-92 (круглосуточно),

• через форму обратной связи https://www.priorbank.by/feedback.



• Выход из системы осуществляется путем нажатия кнопки «Выйти», находящейся в верхнем правом углу экрана:

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. Пароль на вход в систему;
2. Авторизационный код, используемый при настройке и проведении платежей в системе;
3. Мобильный код (М-код), получаемый через SMS, при совершении платежа, либо при задании/изменении учетных данных Пользователя;
4. Имя пользователя в системе (логин);
5. Номера карточек (за исключением первых 6-и и последних 4-х цифр), PIN-коды и другая информация, размещенная на платежных карточках.

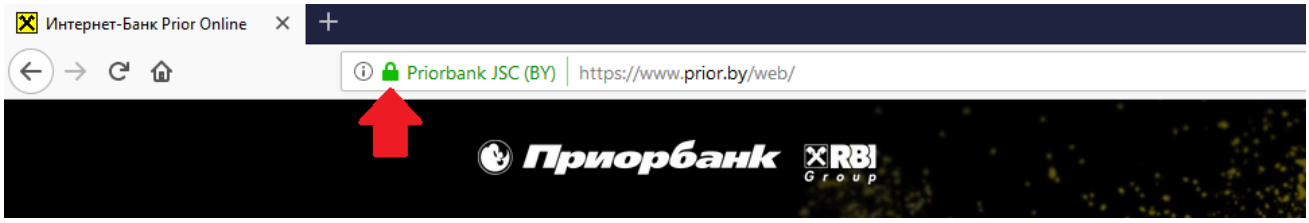
Разглашение указанной информации может создать предпосылки к осуществлению в отношении Вас мошеннических действий и привести к финансовым и моральным потерям, как для Вас, так и для Банка.

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

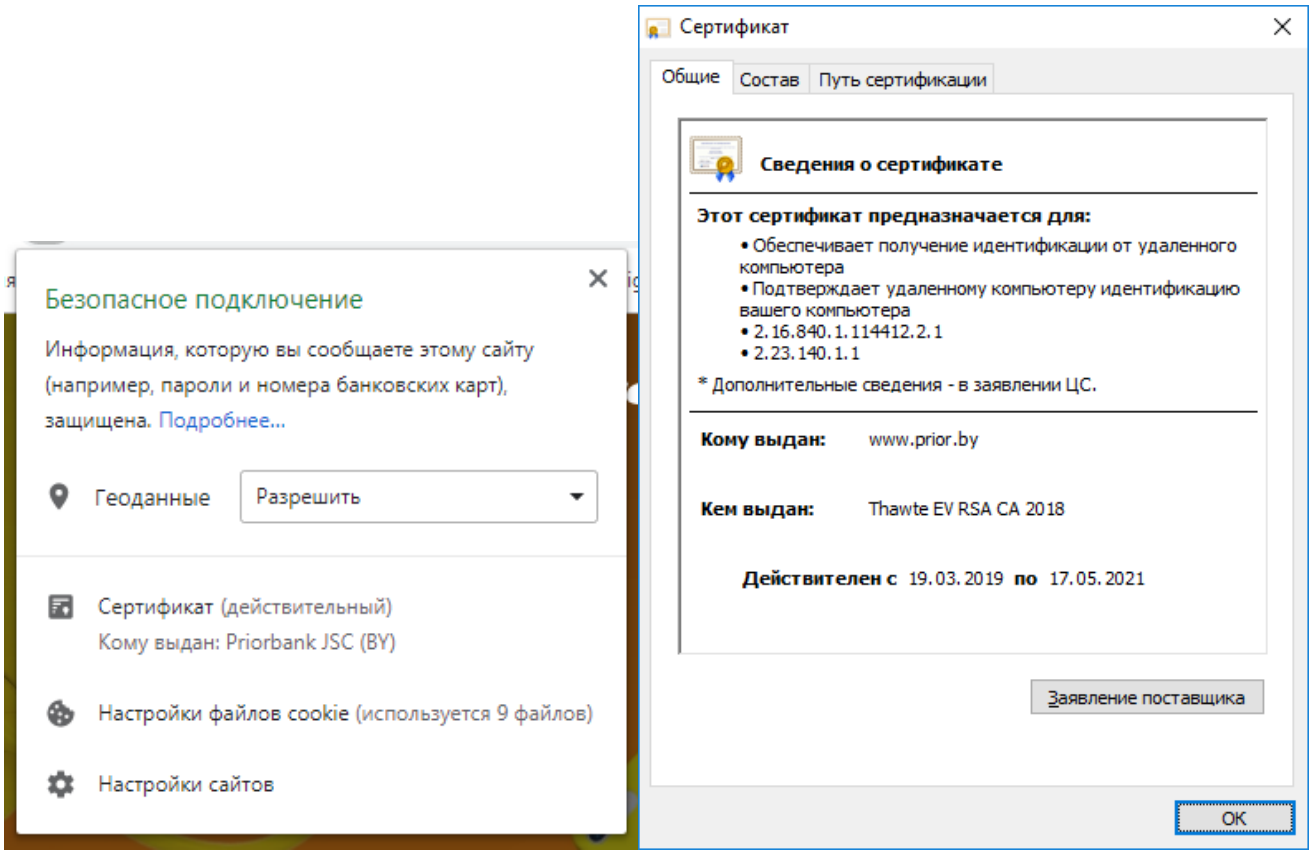
- по телефонам: +375 17 289-90-90, 487 (Velcom, МТС или life:)), 187 по г. Минску,
  +375 17 289-92-92 (круглосуточно),
- через форму обратной связи https://www.priorbank.by/feedback.

Как проверить, что соединение происходит в защищенном режиме.

Вы можете проверить подлинность сертификата сервера Интернет-Банка Prior Online, щелкнув на значке защищенного соединения:



«Замок» в адресной строке браузера подтверждает, что соединение защищено.



Рекомендации по выбору 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 8 знаков;

• Пароль должен представлять собой сочетание заглавных и строчных букв латинского алфавита, цифр и 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, qwerty, asdfghjkl, qwaszx 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 Tp#1ftssivhtc из начальных букв слов в предложении «This password # 1 for the security system is very hard to crack».

Автозаполнение/сохранение страниц

• При запросе окна браузера об использовании автозаполнения полей формы (логина и пароля) рекомендуем 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 настройках Вашего браузера.

• Чтобы Ваш обозреватель не допускал сохранения конфиденциальных страниц, рекомендуем отключить функцию форм в установках Вашего обозревателя. Для этого Вам необходимо установить соответствующие параметры в настройках Вашего браузера. Это поможет не сохранять данные (Пароль пользователя, имя пользователя и др.) на жёстком диске.