1. Комплекс мер безопасности при работе с Системой «PSB On-Line».

ПАО «Промсвязьбанк» постоянно работает над повышением безопасности работы Клиентов, при этом максимально сохраняя удобство пользования услугами.

Для защиты клиентов используются:

- шифрование канала связи с использованием протокола TLS;
- Ключ ЭП для подтверждения операций;
- USB-ключи для генерации, надежного хранения и безопасной работы с Ключом ЭП;
- уведомление об IP адресе, с которого осуществлялся последний сеанс работы;
- лимиты (до 1 200 тыс. руб. в сутки) на рублевые операции при входе по логину и паролю.

При работе с Системой «PSB On-Line» необходимо следовать рекомендациям для повышения безопасности:

1. Использовать USB-ключи для хранения Ключа ЭП. Использование USB-ключа значительно повышает сохранность Ключа ЭП.

2. Ни при каких условиях не сообщать информацию о пароле к Ключу ЭП никому, включая сотрудников Банка, родственников, сотрудников Клиента (в том числе руководителей Уполномоченного лица) и иных третьих лиц.

3. Не хранить информацию о пароле от Ключа ЭП на любых носителях, включая компьютер. Если возникли подозрения, что кто-либо владеет информацией о пароле, необходимо обратиться в Банк, чтобы заблокировать соответствующий Сертификат
ключа проверки электронной подписи.

4. Производить замену Сертификата ключа проверки электронной подписи по истечении срока действия. Обращаем внимание, что в течение срока действия Сертификата замена Сертификата (с его активацией) может быть осуществлена в любое время по запросу Уполномоченного лица Клиента на формирование Сертификата при условии, что срок полномочий данного Уполномоченного лица Клиента не истек, и не поступила информация о прекращении его полномочий.

5. В случае изменения у Уполномоченных лиц Клиента имени, фамилии, отчества, полномочий или лишения их права работы в Системе немедленно направлять в Банк письменное заявление об аннулировании Сертификата по форме Приложения 10.6 к Договору дистанционного банковского обслуживания.

6. Блокировка ключей должна быть произведена немедленно в случае угрозы несанкционированного доступа к счетам, программно-аппаратным средствам Клиента, копирования или подозрения в копировании ключей третьими лицами, изменений состава лиц, имеющих доступ к Системе (обладающих правом использования секретного ключа). Не хранить файловые сертификаты на жестком диске компьютера. Хранить файловые сертификаты только на флеш-носителях, либо на CD-дисках в недоступном для посторонних лиц месте (сейфы, запираемые шкафы).

7. Не держать носители с Ключами ЭП постоянно вставленными в компьютер, использовать их только в случае необходимости заверения документов в «PSB On-Line». Не оставлять компьютер с активной Системой «PSB On-Line» без присмотра. Выходить из Системы «PSB On-Line», даже если необходимо отойти на непродолжительное время.

8. Ограничить доступ сотрудников и посторонних лиц к Ключам ЭП и компьютерам, с которых осуществляется работа с Системой «PSB On-Line».

9. Не используйте в качестве пароля для входа в Систему «PSB On-Line»:

- наименование организации;
- дату или год вашего рождения или близких вам людей;
- ваши имя и фамилию или имена и фамилии близких вам людей;
- последовательные цифры или буквы (например, 1234 или qwer).

10. Не сообщайте никому, включая работников Банка, логин, пароль для доступа в Систему «PSB On – Line» и одноразовые SMS-коды авторизации и подтверждения операций.

11. Не храните логин и пароль для доступа в Систему «PSB On – Line» на компьютере, мобильном устройстве (в т.ч. в виде текстовых файлов, SMS сообщениях), т.к. это может привести к их компрометации.

12. Осуществлять контроль над отправляемыми платежными документами при работе с Системой «PSB On-Line».

13. Не работать с Системой «PSB On-Line» с гостевых рабочих мест и иных, не проверенных, не принадлежащих Клиенту компьютеров (Интернет-кафе, киоски и т.д.).

14. Проверять информацию об IP-адресе, с которого осуществлялся предыдущий вход в Систему «PSB On-Line».

15. После окончания работы в Системе «PSB On-Line» обязательно закрывать окно системы с помощью кнопки "ВЫХОД". После выхода необходимо обязательно извлечь из компьютера носитель, на котором хранится Ключ ЭП.

16. Установить и активизировать антивирусное программное обеспечение. Регулярно обновлять антивирусные базы.

17. При каждом сеансе работы с Системой, проверять подлинность соединения. Убедиться, что используемый информационный ресурс не является ложным (фальсифицированным), для чего необходимо удостовериться, что соединение установлено именно с сервером ПАО «Промсвязьбанк», т.е. в адресной строке Интернет- страницы указан точный адрес: http://online.payment.ru/ или www.business.psbank.ru.

18. Установить и настроить персональный межсетевой экран (firewall) на компьютере, на котором осуществляется работа с Системой «PSB On-Line». Дополнительно можно настроить персональный межсетевой экран на доступ только к адресам Системы «PSB On-Line» в соответствии с техническими требованиями, которые представлены на сайте системы. При наличии возможности ограничить взаимодействие компьютера, на котором осуществляется работа с Системой «PSB On-Line», с сетью Интернет адресами Системы «PSB On-Line», на сетевом оборудовании (межсетевые экраны, маршрутизаторы).

19. Использовать лицензионное программное обеспечение из проверенных и надежных источников. Выполнять регулярные обновления операционной системы и прикладного программного обеспечения (браузер, программы для работы с документами и т.д.).

20. Клиенту могут поступать телефонные звонки от представителей Банка только в целях проверки легитимности произведенного платежа. Если позвонившее лицо, представившееся работником Банка, назвало реквизиты платежа, то ему можно подтвердить совершение платежа. В случае если названы реквизиты платежа, который Клиентом не совершался, необходимо сообщить о том, что данный платеж не совершался, войти в систему, найти платеж и отменить его, в дальнейшем действовать в соответствии с п. 21 настоящих Мер безопасности.

21. Если лицо, представившееся по телефону работником Банка, просит совершить какие-либо действия, то это, скорее всего, мошенник. Работники банка не могут просить ввести пароль или сообщить его, провести какую-то операцию и т.п. Если отображается правильный телефон, это еще не означает, что позвонили именно с него.

22. Если есть сомнения, то можно попросить позвонившего представиться (подразделение, фамилия, имя, отчество), завершить разговор и перезвонить по телефону банка - в этом случае, вы гарантированно попадете в Банк.

23. Если имеются основания считать, что звонивший не является работником банка, то необходимо действовать в соответствии с п. 21 настоящих Мер безопасности.

24. При обнаружении факта несанкционированного списания денежных средств со счета Клиента, попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, в том числе при обнаружении подозрительной активности на компьютере, с которого осуществляется работа с Системой «PSB On-Line» (самопроизвольные движения мышью, открытие/закрытие окон, набор текста), при изменении IP-адреса на неиспользуемый Клиентом, мошеннических действий в отношении Клиента и т.д., немедленно:

- сообщить в Банк о возможной попытке несанкционированного доступа к Системе «PSB On-Line» (или о списании денежных средств, если оно состоялось);

- сверить последние отправленные в Банк платежные документы, при обнаружении несанкционированных платежей написать заявление на приостановление/ограничение действия сертификатов;

- блокировать технические средства (в том числе, выключить компьютер используя «гибернацию» или «завершение работы»), используемые для работы в Системе «PSB On-Line»;

- предпринять меры по сохранению лог файла работы в сети Интернет (данные с прокси-сервера, брандмауэра клиента или запросить у оператора);

- представить в Банк подробное письменное описание обстоятельств компрометации ключей или несанкционированного доступа.

При возникновении дополнительных вопросов рекомендуем обращаться в Банк по номерам телефонов Службы технической поддержки, указанным на Интернет-странице системы (http://online.payment.ru/index0.html?contacts), или посредством электронной почты: Email: online@psbank.ru

2. Комплекс мер безопасности при работе с Мобильным приложением «Мой Бизнес».

При работе с Мобильным приложением «Мой Бизнес» необходимо следовать следующим рекомендациям и ваша работа будет полностью безопасной:

- Скачивайте приложение «Мой бизнес» на вашем мобильном устройстве только по ссылкам в авторизованных магазинах приложений (App Store или Google Play);

- Регулярно устанавливайте обновления безопасности для операционной системы вашего мобильного устройства;

- Установите пароль для входа на ваше мобильное устройство;

- Для входа в «Мой бизнес» необходимо ввести только логин и пароль.

- Обратите внимание: в «Мой бизнес» на операционной системе iOs вместо сочетания логин и пароль доступна авторизация по TouchID (по сканеру отпечатков пальцев), короткому коду и рафическому коду. Просим Вас учитывать, что выбор иного способа авторизации, кроме логина и пароля, не исключает возможность авторизации по логину и паролю вместо выбранного способа авторизации.

- Не используйте в качестве пароля и/или короткого кода дату или год вашего рождения, или близких вам людей.

- Не используйте в качестве пароля и/или короткого кода четыре последовательные цифры (например, 1234), одинаковые цифры (например, 1111).

- Не сообщайте никому, включая работников Банка, логин, пароль, короткий код, графический код для доступа в «Мой бизнес» и одноразовый SMS-код подтверждения операций.

- Не храните пароль и короткий код для доступа в «Мой бизнес» на своем мобильном устройстве (в т.ч. в виде текстовых файлов, в SMS сообщениях), т.к. это может привести к их компрометации (например, в случае утраты мобильного устройства).

- При авторизации **НЕ РАЗМЕЩАЙТЕ** экран мобильного устройства так, чтобы существовала возможность визуального считывания с него информации посторонними лицами (особенно, при авторизации по короткому коду или графическому паролю).

- Обратите внимание, что установлен лимит на проведение рублевых операций до 600 тыс. руб. в сутки.

- Не подвергайте мобильное устройство операциям повышения привилегий/взлома операционной системы мобильного устройства (например, jailbreak или root-доступ (доступ с правами администратора), установке "пиратских" прошивок, так как это ведет к отключению защитных механизмов, заложенных производителем мобильной платформы, что в свою очередь делает его уязвимым. В случае, если мобильное устройство будет подвергнуто операциям повышения привилегий/взлома операционной системы, Банк оставляет за собой право установить ограничения на использование Мобильного приложения, установленного на такое мобильное устройство, в том числе запрет на совершение операций по счетам Клиента.

- В случае утери или хищения Вашего мобильного устройства или, если у вас есть подозрение, что ваши логин и пароль, короткий код, графический код стали известны третьим лицам, как можно быстрее обратитесь в наш Колл-центр по телефону 8 800 333 25 50 и заблокируйте сертификат.

- Завершайте сеанс работы в приложении «Мой бизнес» сразу после проведения всех необходимых операций при помощи кнопки «Выход».

Никому не передавайте конфиденциальные данные для доступа в систему, не оставляйте без присмотра ваше мобильное устройство, не допускайте использование его третьими лицами.