КОМПЛЕКС МЕР БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ИНТЕРНЕТ-БАНКОМ

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

Настоящий Комплекс мер безопасности при работе с Системой «PSB On-Line» распространяется на Интернет-банк «PSB Мой бизнес».

Для защиты клиентов используются:

- шифрование канала связи с использованием протокола TLS и ГОСТ;
- Ключ ЭП для подтверждения операций;
- USB-ключи для генерации, надежного хранения и безопасной работы с Ключом ЭП;
- Сервис электронной подписи Удостоверяющего центра (Сервис электронной подписи);
- уведомление об IP адресе, с которого осуществлялся последний сеанс работы;
- лимиты на рублевые операции (до 3 000 000 руб. в сутки) при использовании SMS-кодов (Push-код) в качестве подтверждения волеизъявления на подписание Электронных документов Неквалифицированной ЭП с использованием его Ключа ЭП, созданного с использованием Сервиса электронной подписи (вход по логину и паролю, подтверждение SMS/ Push), данный лимит не применяется к платежам, проводимым с использованием Системы Быстрых Платежей НСПК Банка России.
- лимиты на валютные операции (до 4 000 000 руб. в сутки) при использовании SMS-кодов (Push-код) в качестве подтверждения волеизъявления на подписание Электронных документов Неквалифицированной ЭП с использованием его Ключа ЭП, созданного с использованием Сервиса электронной подписи (вход по логину и паролю, подтверждение SMS/ Push). Лимит на валютные перевод рассчитывается в рублях по курсу Банка России, установленному на момент направления в Банк валютного перевода.
- Сертифицированные ФСБ технологии «myDSS[1]» при использовании биометрических данных, заданных на мобильном устройстве клиента в качестве подтверждения его волеизъявления на подписание Электронных документов Неквалифицированной ЭП с использованием его Ключа ЭП, созданного с использованием Сервиса электронной подписи (вход по логину и паролю)

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

1. Использовать (по выбору Клиента): USB-ключи для хранения Ключа ЭП; Сервис электронной подписи, обеспечивающий удаленную реализацию функций

[1] Сертификат соответствия ФСБ России на исполнение Комплектации 3 (КриптоПро DSS 2.0) DSS+myDSS с аутентификацией и подтверждением операций формирования ЭП с использованием помощью мобильных приложений для iOS и Android.

централизованного создания и хранения Ключа ЭП, создания и проверки усиленной неквалифицированной электронной подписи электронных документов, аутентификации Владельца СКП ЭП при осуществлении доступа к Сервису электронной подписи и выполнении операций с использованием принадлежащих им Ключей ЭП. Использование USB-ключа и Сервиса электронной подписи значительно повышает сохранность Ключа ЭП.

2. При генерации ключей электронной подписи, ключей проверки электронной подписи и формировании запроса на выпуск сертификата ключа проверки электронной подписи для работы в системе «PSB ON – LINE» в офисе банка на специальном компьютере:

   2.1 Клиент принимает решение:
   - о самостоятельной генерации Ключей электронной подписи (ЭП), Ключей проверки ЭП и формировании Запроса на выпуск Сертификатов ключа проверки электронной подписи на аппаратно-программных средствах, находящихся в свободном доступе третьих лиц и не имеющих жесткого диска или иного несъемного материального носителя для хранения информации;
   - о сохранении Ключей ЭП и Ключей проверки ЭП на предоставленных Банком USB-ключах с соблюдением обязательных рекомендаций Банка по порядку эксплуатации USB-ключей (Приложение 10.5 к Правилам[2]);
   - о предоставлении таких Сертификатов ключа проверки электронной подписи Банку для регистрации в качестве Владельцев Сертификатов ключа проверки электронной подписи Уполномоченных лиц Клиента.

   2.2 Клиент принимает все необходимые меры для генерации ключей ЭП в условиях, обеспечивающих невозможность компрометации ключа ЭП, исключающих возможность раскрытия третьим лицам информации о Ключах ЭП, находящихся в его распоряжении или Уполномоченных им лиц несанкционированного использования Ключей ЭП третьими лицами, а также замену СКП ЭП (с их активацией) Уполномоченными лицами Клиента с перевыпуском Ключей ЭП и Ключей проверки ЭП на аппаратно-программных средствах Клиента в соответствии с Правилами до получения услуг, предоставляемых Банком Клиенту в рамках Системы. Подписание Уполномоченным лицом Клиента его действующей ЭП Запроса на формирование СКП ЭП, содержащего сгенерированный им новый Ключ проверки ЭП, и направление его в адрес Банка, как УЦ, признается в качестве подтверждения достоверности сведений о направленном им Ключе проверки ЭП.

   2.3 Клиент самостоятельно несет последствия, наступившие в результате нарушения Клиентом и/или его Уполномоченным лицом требований настоящего Комплекса мер безопасности.

   2.4 В случае возникновения подозрений в Компрометации ключей либо в случае выявления каких-либо несанкционированных действий, совершенных третьими лицами, Клиент обязуется немедленно блокировать технические средства, используемые для работы Системы; немедленно сообщать об этом в Банк в порядке, предусмотренном Правилами.

[2] Правила обмена электронными документами по Системе «PSB On-Line» в ПАО «Промсвязьбанк»

3. Ни при каких условиях не сообщать никому, включая сотрудников Банка, родственников, сотрудников Клиента (в том числе руководителей Уполномоченного лица) и иных третьих лиц:
- пароль к Ключу ЭП;
- логин, пароль для доступа в Систему «PSB On–Line»;
- одноразовые SMS-коды авторизации и подтверждения операций (при использовании Сервиса электронной подписи).

3.1 Вход в Систему «PSB On–Line» возможен с использованием логина и пароля, являющихся основными средствами идентификации и аутентификации Клиента при использовании Сервиса электронной подписи, с подтверждением входа одноразовым SMS-кодом авторизации.

3.2 Подтверждение входа одноразовыми SMS-кодами можно отключить, подписав заявление в Системе «PSB On-Line» или в Мобильном приложении «Мой Бизнес». При отключённом подтверждении входа одноразовыми SMS-кодами, будет приходить информационное сообщение о входе.

Отказ от подтверждения входа одноразовыми SMS-кодами повлечет **СНИЖЕНИЕ** уровня безопасности при работе с Системой «PSB On-Line» и Мобильным приложением «Мой Бизнес», что может привести к реализации мошеннических действий в отношении Клиента.

4. Не хранить информацию о пароле от Ключа ЭП, логин и пароль для доступа в Систему «PSB On-Line» на любых носителях, в т.ч. на компьютере, мобильном устройстве, в т.ч. в виде текстовых файлов, записей в книге контактов, программ текстовых заметок, SMS сообщениях, т.к. это может привести к их компрометации. Если возникли подозрения, что кто-либо владеет указанной информацией, необходимо НЕЗАМЕДЛИТЕЛЬНО обратиться в Банк, чтобы заблокировать соответствующий Сертификат ключа проверки электронной подписи.
5. Производить замену Сертификата ключа проверки электронной подписи до истечения 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.
6. 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 Правилам обмена электронными документами по Системе «PSB On-Line».
7. 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).
8. 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.

7.1. При пользовании Системой «PSB On-Line», в т.ч. при создании Сертификата ключа проверки электронной подписи ООО Крипто Про и регистрации Пользователя УЦ, НЕ ИСПОЛЬЗУЙТЕ SIM-карты (номера мобильных телефонов), полученные без оформления договора об оказании услуг связи, ИЛИ без включения в договор об оказании услуг связи сведений об абоненте, ИЛИ в случае включение в такой договор недостоверных сведений, либо, в случае, если договор об оказании услуг связи был заключен без соблюдения процедуры идентификации абонента, в т.ч. по документу, удостоверяющему личность. Например, НЕ ДОПУСКАЕТСЯ ИСПОЛЬЗОВАНИЕ SIM-карт (номеров мобильного телефона), полученных без оформления документов в местах массового скопления граждан.

7.2. В случае утери, хищения или получения иным способом неуполномоченным лицом доступа к SIM-карте с номером мобильного телефона, сообщенного Клиентом при получении Сертификата ключа проверки электронной подписи (а также номера мобильного телефона, на который направляются SMS-сообщения), как можно быстрее обратитесь в наш Колл-центр по телефону 8 800 333 25 50 и заблокируйте сертификат.

7.3. При утрате или прекращении использования номера мобильного телефона, сообщенного Клиентом при получении Сертификата ключа проверки электронной подписи, а также при утрате, прекращении использования, хищении или получении иным способом неуполномоченным лицом доступа к мобильному устройству, на которое направляются Push-сообщения, как можно быстрее обратитесь в наш Колл-центр по телефону 8 800 333 25 50 и заблокируйте сертификат. Помните, что операторы сотовой связи могут передать номер мобильного телефона другому абоненту, если он будет неактивным длительное время.

9. Ограничить доступ сотрудников и посторонних лиц к Ключам ЭП и компьютерам, с которых осуществляется работа с Системой «PSB On-Line».
10. 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).

11. Осуществлять контроль над отправляемыми платежными документами при работе с Системой «PSB On-Line».
12. 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.), а также терминальных серверов общего доступа.
13. Проверять информацию об IP-адресе, с которого осуществлялся предыдущий вход в Систему «PSB On-Line».
14. 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.

15. Установить и активизировать антивирусное программное обеспечение. Регулярно обновлять антивирусные базы.
16. 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 https://business.psbank.ru.
17. Результат отображения надежного и защищенного соединения в строке адреса ресурса зависит от используемого браузера.
18. Установить и настроить персональный межсетевой экран на компьютере (Брандмауэр или Firewall), 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, роутеры).
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.). Не устанавливать на компьютере, на котором осуществляется работа с Системой «PSB On-Line», программное обеспечение удаленного управления, в том числе TeamViewer, RAdmin, VNC и иное подобное программное обеспечение.
20. Клиенту могут поступать телефонные звонки от представителей Банка только в целях проверки легитимности операции по Счету и проверки использования Системы «PSB On-Line» с согласия Клиента.

    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. 20 настоящих Мер безопасности.

    Информация, полученная Банком по телефону или иному средству связи, указанному Клиентом Банку, в том числе не подтверждение по телефону (иному средству связи) операции по Счету и/или не подтверждение использования Системы «PSB On-Line» с согласия Клиента (представителя Клиента), не рассматривается Банком в качестве заявления Клиента на отзыв распоряжения на перевод денежных средств, но может являться основанием для возникновения у Банка подозрений о том, что операция по Счету направлена не на осуществление предпринимательской деятельности, а на противоправные цели (в т.ч. на хищение денежных средств Клиента) и/или о несанкционированном доступе к Системе «PSB On-Line» неуполномоченных лиц.

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.20 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:

- отключить технические средства, используемые для работы в Системе «PSB On-Line», в том числе выполнить отключение компьютера от сети Интернет, путем разрыва сетевого соединения (отключить сетевой шнур, выключить роутер или сразу же компьютер от электросети, не используя способы отключения «Гибернация» или «Завершение работы»);
- 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 НЕЗАМЕДЛИТЕЛЬНО написать заявление на приостановление/ограничение действия сертификатов;
- при обнаружении неисполненных несанкционированных платежных поручений НЕЗАМЕДЛИТЕЛЬНО сообщить в Банк о попытке несанкционированного доступа к Системе «PSB On-Line» (в т.ч. по телефону банка: **8 800 333 25 50**, e-mail: business@psbank.ru) и представить в Банк заявление на отзыв распоряжения;
- 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.