МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ «PSB-RETAIL» ПАО «ПРОМСВЯЗЬБАНК» (ИНТЕРНЕТ-БАНКЕ)

1. **Для обеспечения безопасности работы в Системе "PSB-Retail" (далее - Система) Банком реализовано:**

1.1. Шифрование канала связи с использованием протокола SSL и сертификата, подписанного удостоверяющим центром Thawte, Inc.

1.2. Идентификация (номер Клиента или псевдоним) и аутентификация (пароль и разовый ключ из Таблицы разовых ключей либо Код подтверждения, предоставляемый в рамках сервиса «SMS-код» либо Сертификат ключа проверки электронной подписи (далее - Сертификат) для входа в Систему.

1.3. Средства подтверждения (разовый ключ из Таблицы разовых ключей либо Код подтверждения, предоставляемый в рамках сервиса «SMS-код») либо Ключ электронной подписи (далее – Ключ ЭП) для подтверждения подлинности, неизменности, целостности и авторства Поручений.

1.4. Направление SMS-сообщений (в рамках платного сервиса) о проведении транзакций по карточным счетам и/или уведомлений на адрес электронной почты Клиента (в рамках бесплатного сервиса) о действиях в Системе (вход в Систему, смена пароля, подключение услуг, проведение транзакций и т.д).

2. **В целях минимизации риска хищения средств при работе в Системе Клиент обязан обеспечить выполнение следующих требований:**

2.1. Не осуществлять вход в Систему и проведение операций в Системе с использованием чужого персонального устройства (компьютера, смартфона, планшета, коммуникатора, телефона), в том числе устройства, расположенного в общедоступных местах (интернет-кафе, киоски и т.д.).

2.2. Не осуществлять вход в Систему и проведение операций в Системе с использованием недоверенных (публичных) беспроводных сетей.

2.3. До входа в Систему удостоверяться в том, что устройство (компьютер, смартфон, планшет, коммуникатор, телефон), с использованием которого осуществляется работа в Системе, не заражено вирусами, на нем установлено (не отключено) и настроено антивирусное программное обеспечение, регулярно обновляются антивирусные базы.

2.4. Использовать только лицензионное программное обеспечение, регулярно обновлять операционную систему и прикладное программное обеспечение (браузер, программы для работы с документами и т.д.).

2.5. Использовать для доступа в Систему отдельную учетную запись пользователя компьютера. Доступ к этой учетной записи должен быть защищен паролем, неизвестным любым третьим лицам, включая сотрудников Банка и родственников.

2.6. Не оставлять устройство (компьютер, смартфон, планшет, коммуникатор, мобильный телефон) с активной Системой без присмотра.

2.7. При каждом сеансе работы с Системой, проверить подлинность соединения, для чего убедиться, что:

2.7.1. включен защищенный режим SSL, то есть в адресной строке браузера web-адрес начинается с символов «https://» на зеленом фоне и в окне web -браузера отражается символ «закрытый замок» (Изображение 2);

2.7.2. соединение установлено именно с сервером ПАО "Промсвязьбанк", то есть в адресной строке интернет-страницы указан точный адрес: https://retail.payment.ru/n/Default.aspx (не допускается никаких отличий в написании web-адреса, вплоть до любого знака) (Изображение 2)

2.7.3. в сертификате сайта в строке «Кому выдан» указано точное значение «retail.payment.ru» (Изображения 1, 2);

2.7.4. в сертификате сайта в строке «Кем выдан» указано точное значение «thawte Extended validation SSL CA» (Изображение 1, 2).

2.8. До начала проведения операций в Системе проверить историю входов в Систему на предмет соответствия действительным входам в Систему пользователем, отсутствия в ней сведений о входах с IP-адресов, неизвестных пользователю, а также на предмет отсутствия какой-либо истории, которая может свидетельствовать о нахождении на сайте злоумышленника, а не Банка.

2.9. Запрещено сообщать информацию о пароле на вход в Систему любым третьим лицам, включая сотрудников Банка и родственников.

2.10. Необходимо производить смену пароля на вход в Систему не реже одного раза в два месяца.

2.11. Запрещено осуществлять хранение информации о пароле на вход в Систему и Ключа ЭП на жестком диске компьютера, в памяти иного устройства, с использованием которого осуществляется выход в интернет, а также иным способом, делающим данную информацию доступной для третьих лиц.

2.12. В случае хранения Сертификата/Ключа ЭП на внешнем носителе подключать его к компьютеру только непосредственно перед подтверждением операции в Системе.

2.13. Необходимо подключить оповещение о входе в Систему, а также о иных действиях в Системе в разделе "Сервис оповещений" (в рамках бесплатного сервиса уведомлений на адрес электронной почты).

2.14. Не отключать опцию проверки разового ключа/кода подтверждения на входе в систему (таблица разовых ключей (ТРК)/сервис "SMS-код" предоставляется /подключается в любом офисе Банка бесплатно).

2.15. Использовать для подтверждения каждой операции в Системе (вход в систему, смена пароля, проведение транзакции и т.д.) только один разовый ключ из Таблицы разовых ключей. Разовые ключи запрашиваются Системой в порядке убывания; Запрещено вводить ключ с предыдущим номером из ТРК в случае отсутствия положительного результата ввода ключа (при каждой повторной попытке входа в Систему или подтверждения поручения Система должна запросить ключ из ТРК с тем же номером, что и при первой попытке). В этом случае необходимо незамедлительно обращаться в Банк по телефонам (495)-787-33-33, 8-800-333-03-03, либо по номеру телефона, указанному на платежной карте, эмитированной ПАО "Промсвязьбанк".

2.16. Необходимо обращать пристальное внимание на неанонсированные Банком изменения страниц входа в Систему и работы с ней (интерфейс Системы), особенно касающиеся безопасности. При возникновении подозрений в подмене злоумышленником страниц Интернет-банка запрещено звонить по номеру телефона, указанному на подозрительной странице, а необходимо незамедлительно связаться с Банком по телефонам (495)-787-33-33, 8-800-333-03-03, либо по номеру телефона, указанному на платежной карте, эмитированной ПАО "Промсвязьбанк".

2.17. Для получения актуальной информации обо всех изменениях и регламентных работах в Интернет-банке необходимо не реже одного раза в 14 (четырнадцать) дней осуществлять вход в Систему.

2.18. Запрещено сообщать любую персональную информацию, а также разовые ключи из Таблицы разовых ключей в ответ на SMS-сообщения и звонки от лиц, представляющихся сотрудниками ПАО "Промсвязьбанк" и сообщающими о блокировке/разблокировке доступа в Систему. О каждом случае таких обращений необходимо незамедлительно сообщать по телефонам (495)-787-33-33, 8-800-333-03-03, либо по номеру телефона, указанному на платежной карте, эмитированной ПАО "Промсвязьбанк".

2.19. Необходимо заблокировать (запретить) выполнение по доверенности действий с SIM-картой, номер которой представляется Банку для направления на него Кодов подтверждения в рамках сервиса «SMS-код» (при предоставлении оператором мобильной связи такой возможности). Данная мера применяется для предотвращения злоумышленного использования номера телефона (переоформление номера на третье лицо по фальсифицированной и/или отмененной доверенности).

2.20. Необходимо незамедлительно обращаться в Банк для блокировки сервиса "SMS-код" при неполадках SIM-карты, утере мобильного (сотового) телефона с SIM-картой, отдельно SIM-карты, на номер которой посредством SMS-сообщений направляются Коды подтверждения.

2.21. Перед вводом Кода подтверждения сверять реквизиты подтверждаемой операции с параметрами, указанными в соответствующем SMS-сообщении, направленном в рамках сервиса "SMS-код" (код подтверждения действует 300 секунд с момента отправки).

2.22. Стирать защитный слой со значения ключа на ТРК только непосредственно перед его использованием.

2.23. Обязательно осуществлять выход из Системы, при необходимости на любое, даже непродолжительное, время, оставить вне контроля (поля зрения) устройство, на котором осуществляется работа в Системе и/или устройство, на которое направляются SMS-сообщения с Кодами подтверждения.

2.24. После окончания работы в Системе необходимо в обязательном порядке закрыть окно Системы с помощью кнопки "Выход из интернет-банка", а также извлечь из компьютера носитель, на котором хранится Сертификат/Ключ ЭП, если операции осуществлялись с его использованием.

3. Требования к формированию пароля:

3.1. длина пароля должна быть не менее 8 символов.

3.2. пароль должен содержать латинские буквы, набранные в разных регистрах (a-Z, A-z) и цифры.

3.3. при смене пароля для входа в систему новое значение должно отличаться от предыдущего не менее чем на 3 символа.

3.4. новое значение пароля для входа в систему не должно совпадать с предыдущими паролями на протяжении четырех смен.

3.5. пароль не должен являться персональной информацией (имена и даты рождения членов семьи, адреса, телефоны и т.п.) или распространенным (словарным) словом (например, «password», «default», «admin», «guest»- это ненадежный пароль).

3.6. пароль не должен являться копией других паролей пользователя, используемых в личных целях (на развлекательных и почтовых сайтах в Интернете); пароль не должен содержать последовательность одинаковых символов и групп символов (например, не должны применяться пароли, состоящие из одинаковых цифр или из одинаковых букв).

4. При возникновении подозрений в осуществлении несанкционированных операций в Системе либо при компрометации пароля на вход в Систему или Средства подтверждения/Ключа ЭП необходимо последовательно выполнить следующие действия:

4.1. Выйти из Системы с помощью кнопки "Выход из интернет-банка".

4.2. Заблокировать устройства, используемые для работы в Системе (в том числе, выключить/перевести в режим гибернации (сна) компьютер).

4.3. Незамедлительно обратиться в Банк для смены пароля, приостановления дистанционного обслуживания в Системе, отмены Таблицы разовых ключей и/или приостановления/аннулирования действия Сертификата/Ключа ЭП и/или для блокировки сервиса "SMS-код". Это можно сделать в офисе Банка, а также по звонку в Контакт-центр (8-800-333-03-03) с последующим оформлением в Банке соответствующих письменных заявлений. Смена номера телефона, к которому подключен Сервис "SMS-код" возможна только по заявлению, оформленному в офисе Банка.

4.4. В письменном заявлении описать обстоятельства компрометации пароля, разовых ключей, кодов подтверждений, ключей усиленной электронной подписи или несанкционированного доступа, либо другую информацию по фактам, вызвавшим Ваши подозрения.

4.5. Возобновление доступа в систему и возобновление действия Сертификата/Ключа ЭП и работы сервиса "SMS-код" производится в офисе Банка при личном обращении клиента. Заблокированная Таблица разовых ключей разблокировке не подлежит. Для работы с Системой необходимо получить новую Таблицу разовых ключей лично в офисе Банка.

5. О проявлении злоумышленных действий в Системе, требующих незамедлительного обращения в Банк, могут свидетельствовать следующие факты:

5.1. В истории поручений в Системе указаны поручения, которые Вы не совершали.

5.2. Подозрительная активность на компьютере, с которого осуществляется работа с Системой (самопроизвольные движения курсором мыши, открытие/закрытие окон, набор текста и т.п.).

5.3. Осуществлен запрос следующего разового ключа из Таблицы разовых ключей для повторного подтверждения входа в Систему или Поручения;

5.4. Осуществлен запрос на ввод разового ключа из Таблицы разовых ключей для подтверждения выполнения действий, не связанных с входом в Систему или совершением

операций в Системе (подтверждение ознакомления с какими-либо правилами, инструкциями, или для подтверждения входа в какой-либо раздел системы, открытия страницы).

5.5. Входящий звонок от лиц, представляющихся работниками ПАО "Промсвязьбанк", уведомляющих Вас о регламентных/восстановительных работах в Системе или Банке.

5.6. Получение сообщения о блокировке/разблокировке доступа в Систему.

5.7. Изменение адреса в адресной строке браузера при работе с Системой.

5.8. Наличие в истории входов в Систему информации о входе в Систему с незнакомого IP-адреса.

5.9. Невозможность получения доступа к Системе по причине несовпадения пароля при введении заведомо верного пароля.

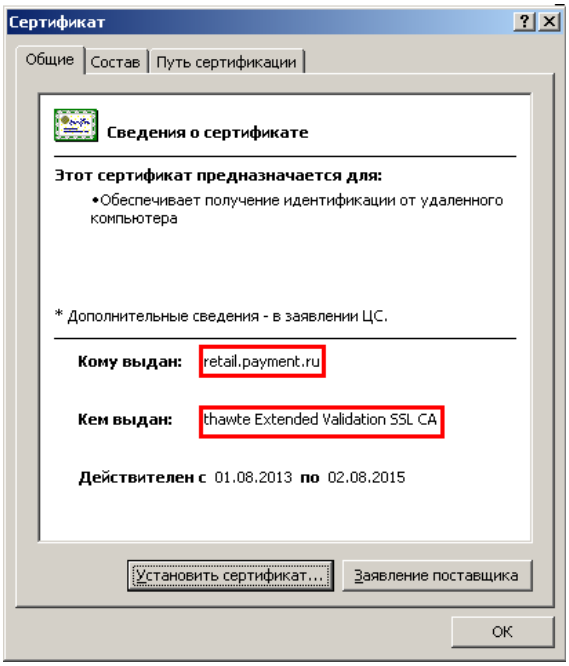
5.10. “Зависание” Системы при одновременной нормальной работе других интернет-ресурсов.

5.11. Изменение интерфейса или настроек безопасности Системы без предварительного уведомления на сайте Банка либо оповещения путем направления SMS-сообщения/сообщения на адрес электронной почты.

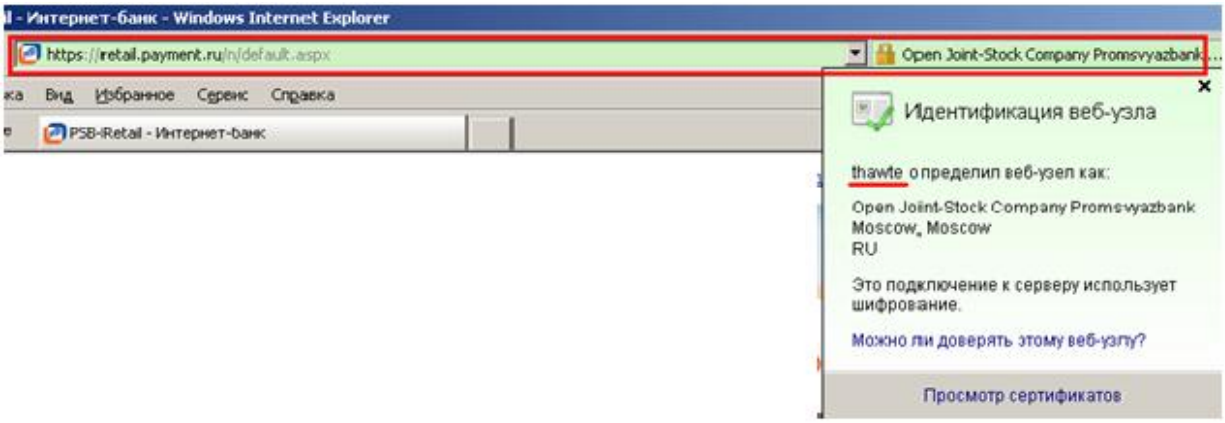
5.12. Внезапное приостановление работы SIM-карты, на номер которой посредством SMS-сообщений направляются Коды подтверждения (блокировка SIM-карты). Возможно незаконное изготовление третьими лицами дубликата SIM-карты (необходимо обратиться к оператору мобильной связи).

5.13. Подозрительная работа (зависание, самопроизвольные: рассылки SMS-сообщений, звонки, скачивание и загрузка сторонних приложений) мобильного устройства, с которого осуществляется работа с Системой.

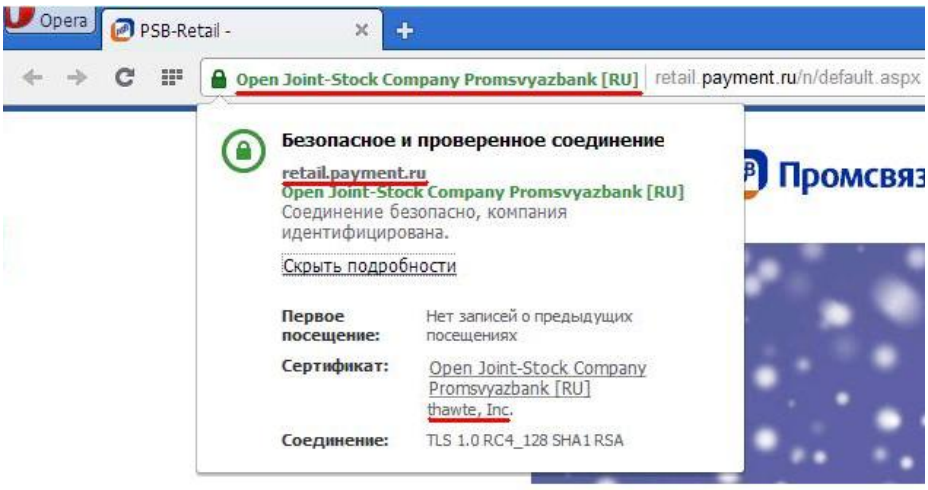
Изображение 1
Сведения о сертификате



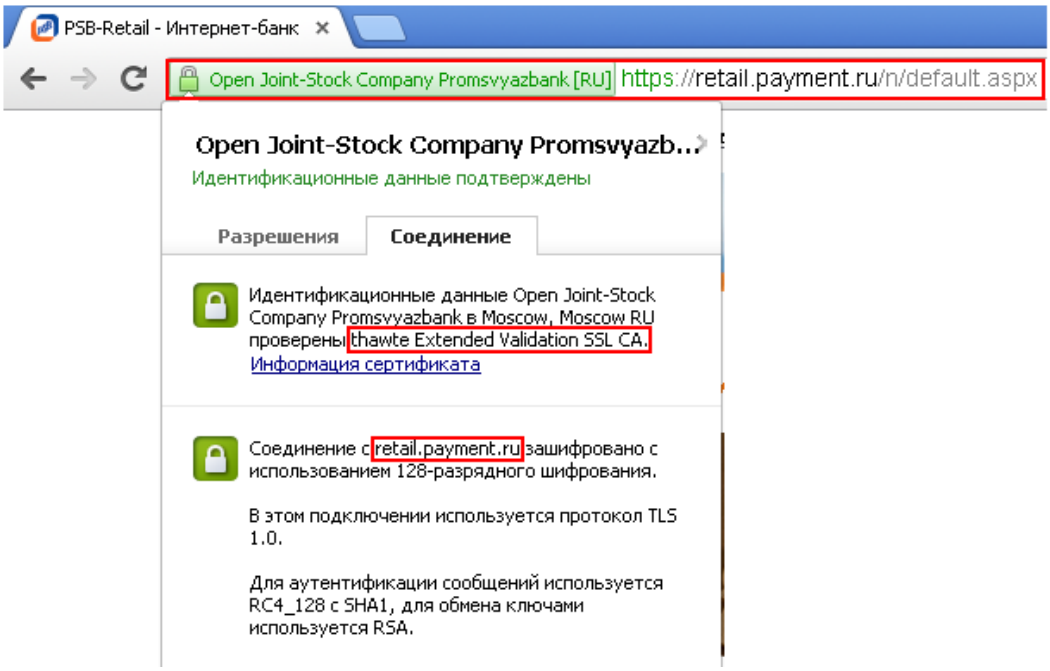
Изображение 2
2.1. Для Internet Explorer



2.2. Для Opera



2.3. Для Google Chrome



2.4. Для Mozilla Firefox