Приложении №2
к Условиям дистанционного банковского обслуживания с использованием системы «Приобанк Онлайн»
Прио-Внешторгбанка (ПАО)

Рекомендации
по информационной безопасности при работе
с системой дистанционного банковского обслуживания «Приобанк Онлайн» / Мобильный банк

1. Общие положения

Соблюдение всех правил, содержащихся в настоящих Рекомендациях, которые являются неотъемлемой частью Условий дистанционного банковского обслуживания с использованием системы «Приобанк Онлайн» (далее – Условия ДБО), позволит обеспечить максимальную сохранность денежных средств, а также снизит возможные риски при совершении операций в системе «Приобанк Онлайн» / Мобильный банк (далее – Система ДБО), в частности, при осуществлении платежей в пользу поставщиков услуг, переводах денежных средств по номеру телефона/ номеру карты/ реквизитам счетов как внутри Банка, так и в другие кредитные организации.

Клиент (Пользователь) уведомлен, что при невыполнении указанных Рекомендаций использование Системы ДБО не является безопасным. В случае невыполнения Клиентом указанных рекомендаций Клиент несет единоличную ответственность за все последствия своих действий. Клиент уведомлен, что при невозможности выполнения с его стороны всех указанных рекомендаций для обеспечения сохранности своих денежных средств Клиенту следует осуществлять банковские операции в отделениях Банка.

2. Меры по защите компьютера

Перед использованием системы «Приобанк Онлайн» проверьте настройки безопасности Вашего компьютера:

2.1. Установите и регулярно обновляйте лицензионное антивирусное программное обеспечение на Вашем компьютере. Произведите проверку Вашего компьютера на наличие вирусов. Действие вирусов может быть направлено на перехват Вашей персональной информации и передаче её злоумышленникам.

2.2. Установите и настройте персональный брандмауэр (firewall) на Вашем компьютере. Это позволит Вам запретить несанкционированный удаленный доступ к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа. Для обеспечения дополнительной безопасности Вы можете настроить брандмауэр на доступ только по адресам Системы ДБО «Приобанк Онлайн».

2.3. Своевременно устанавливайте обновления безопасности операционной системы Вашего компьютера, рекомендуемые компанией-производителем, в целях устранения выявленных в нем уязвимостей. Регулярно выполняйте обновления операционной системы и браузера Вашего компьютера, это значительно повысит его уровень безопасности.

2.4. Установите на Вашем компьютере пароли для учетных записей с правами администратора.

Рекомендуется использовать следующие правила составления пароля:

длина не менее 8 символов,

используйте строчные и прописные буквы,

используйте специальные символы (№, %, ?, &, * и т.п.),

используйте цифры,

пароль не должен содержать легко вычисляемые сочетания символов (имена, фамилии, наименования и т.п.), а также общепринятые сокращения.

2.5. Осуществляйте работу в системе «Приобанк Онлайн» на Вашем компьютере под учетной записью Пользователя, не имеющего прав администратора.

2.6. Избегайте посещения сайтов сомнительного содержания во избежание заражения Вашего компьютера вирусами.

3. Общие рекомендации при подключении Системы

3.1. Подключение к системе Банк осуществляет в случае успешной верификации номера мобильного телефона.

Если подключение к системе осуществляется в офисе Банка, то для проведения верификации, Клиенту необходимо сообщить код подтверждения, направленный Банком в СМС-сообщении на номер мобильного телефона Клиента, работнику Банка.

3.2. При подключении к системе дистанционно на основании распоряжения, сформированного на сайте Банка в сети Интернет (priovtb.com), Клиенту необходимо самостоятельно осуществить ввод временного пароля, направленного Банком в СМС-сообщении на номер мобильного телефона, зарегистрированный в Банке.

3.3. При осуществлении первого входа в систему изменить временный пароль на постоянный пароль. Необходимо применять в качестве паролей сложные комбинации заглавных и строчных букв и цифр, соблюдая следующие правила:

длина не менее 8 символов,

используйте строчные и прописные буквы,

используйте специальные символы (№, %, ?, &, * и т.п.),

используйте цифры,

пароль не должен содержать легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.п.)

Не использовать в качестве паролей:

- простые последовательности букв и цифр (например: Abc123, Qwerty789);
- номера телефонов и паспортов; - даты рождения и имена своих ближайших родственников;
- названия компьютеров, мониторов, окружающей вас оргтехники и любимых компаний (например: Apple123, Subaru222).

3.4. При подключении к системе хранить в секрете информацию, полученную от Банка для осуществления аутентификации в Системе: логин, временный пароль, постоянный пароль.

3.5. Для использования системы «Мобильный банк» осуществлять скачивание и установку приложения только при переходе по ссылкам с официального сайта Банка (priovtb.com) или через официальные магазины приложений (Google Play, Apple AppStore, Rustore, AppGallery для HUAWEI).
3.6. Устанавливать систему «Мобильный банк», в том числе с активированной функцией входа по отпечатку пальца/сканированию лица, исключительно на мобильные устройства, находящиеся в индивидуальном пользовании, защищать паролем доступ к такому мобильному устройству, не передавать мобильное устройство третьим лицам для временного использования.

4. Общие рекомендации при входе/использовании Системы

Для безопасного использования системы «Приобанк Онлайн» / Мобильный банк Клиент обязан выполнять следующие правила.
4.1. Не осуществлять Вход в систему в местах, где услуги Интернета являются общедоступными, и/или с использованием публичных беспроводных сетей, например, Интернет-кафе или общественный транспорт, а также в присутствии посторонних лиц.
4.2. До входа в систему убедиться в том, что устройство (компьютер, смартфон, планшет, телефон), с которого осуществляется работа с системой не заражено вирусами/вредоносным ПО, осуществляющих перехват и передачу данных с устройства, а также отсутствует несанкционированный доступ к устройству из сети интернет или локальной сети; установлено и работоспособно лицензионное антивирусное программное обеспечение, регулярно и своевременно обновляются антивирусные базы.
4.3. Для осуществления входа в систему «Приобанк Онлайн» рекомендуется использовать виртуальную клавиатуру.
4.4. Не оставлять без присмотра систему в активном состоянии, не осуществив выход из системы специальной кнопкой «Выход». В случае бездействия Пользователя в течение 15 минут, в целях безопасности Банк автоматически завершит сеанс использования системы. Пользователю необходимо заново произвести аутентификацию в системе.
4.5. Заходить в систему «Приобанк Онлайн» только с официального сайта Банка (priovtb.com).
4.6. При осуществлении входа в систему «Приобанк Онлайн» убедиться в безопасности соединения, включая наличие символа замка в адресной строке браузера.
4.7. При каждом входе в Систему ДБО проверять на соответствие дату и время последнего входа.
4.8. Выход из Системы ДБО осуществлять в соответствии с установленными процедурами. Не допускается закрывать браузер, предварительно не осуществив выход из ДБО.
4.9. Не отвечать на подозрительные звонки, электронные письма (в т.ч. переходить по ссылкам в электронных письмах) и сообщения из социальных сетей, в которых запрашивают конфиденциальную информацию (логин, пароль, Сеансовый ключ, Ключ мобильной подписи и т.п. информацию), в том числе от работников Банка и их родственников. Банк никогда не обращается к клиентам с подобными просьбами. Подробно о мерах безопасности и защиты от мошенничества - в разделе 6 настоящих Рекомендаций.
4.10. В целях безопасности, в системе «Приобанк Онлайн» рекомендуется изменять логин на любой другой, удобный для запоминания, с регулярностью изменения не реже одного раза в квартал, с соблюдением правил, указанных в п.3.3 настоящих Рекомендаций. Также, после возобновления доступа к ДБО по причине ранее произведенной блокировки, при первом входе в систему «Приобанк Онлайн» рекомендуется произвести изменение логина.
4.11. Обращать внимание на отправителя СМС-сообщений. Банк отправляет сообщения только от абонентов – PRIOVTB (priovtb). Не хранить в мобильном устройстве информацию, полученную от Банка в виде СМС-сообщений при получении временных паролей до момента его изменения.
4.12. При проведении операций сверяйте реквизиты перевода, в том числе сумму перевода/платежа на экране монитора с информацией в СМС-сообщении/Push-уведомлении, в котором направлен Сеансовый ключ для подтверждения операции.
4.13. В случае внезапного приостановления работы SIM-карты для номера телефона, который является зарегистрированным номером для направления Банком СМС-сообщений, незамедлительно обратиться к оператору мобильной связи для выяснения причин блокировки (возможно незаконное изготовление третьими лицами дубликата SIM-карты). В случае необходимости, осуществить блокировку ДБО, обратившись в Контакт-центр Банка.
4.14. Не передавать третьим лицам мобильное устройство, привязанное к учетной записи Пользователя, позволяющее получать Сеансовые ключи.
4.15. Использовать Систему ДБО, руководствуясь инструкциями Банка, в том числе Руководством пользователя «Приобанк Онлайн», размещенными на официальном сайте Банка в сети Интернет (priovtb.com).

5. Действия Пользователя при компрометации

5.1. При подозрении на компрометацию (возникновение подозрений на утечку информации) или утрате:
- логина;
- пароля (в т.ч. временного пароля);
- Сеансового ключа;
- Ключа мобильной подписи;
- устройства, привязанного к учетной записи Пользователя;
- сканирования лица;
- отпечатка пальца;

а также после обнаружения факта совершения в системе операции без согласия Пользователя,
Вы должны незамедлительно сообщить об этом в Банк обратившись в офис Банка лично или по телефонам Службы поддержки, указанным в п.8 настоящих Рекомендаций.
5.2. При получении информации от Пользователя о наступлении любого события, указанного в пункте 5.1 настоящих Рекомендаций, Банк незамедлительно производит блокировку ДБО и информирует Пользователя о данном событии.
Банк осуществляет блокировку доступа Клиента к Рабочему месту в Системе незамедлительно с момента поступления от Клиента заявления о блокировке.
5.3. Для разблокировки доступа к ДБО, в случае, если блокировка ДБО была произведена по инициативе Пользователя, Пользователю необходимо обратиться в любое подразделение Банка с документом, удостоверяющим личность, для подачи заявления на подключение. При разблокировке ДБО Банком предоставляются прежний логин и новый временный пароль.

6. Меры безопасности и защиты от мошенничества

Для безопасного использования системы «Приобанк Онлайн» / Мобильный банк Клиент обязан выполнять рекомендации ниже.

6.1. При получении какой-либо информации в формате СМС-сообщения, электронного письма или звонка убедитесь, что информация поступила именно от Банка. При этом, если:

- информация поступила не от Банка, или
- запрашиваемые действия требуют срочного ответа Клиента, или
- требуется предоставить, обновить или подтвердить персональную информацию Клиента, включая девичью фамилию матери или кодовое слово, ПИН-код, номер телефона, реквизиты банковской карты, имя Пользователя, пароль и т. д., или
- сообщение содержит форму для ввода персональной информации Клиента, или
- сообщается, что на счет Клиента неожиданно для него поступили денежные средства, или
- в сообщении содержится просьба войти в систему «Приобанк Онлайн» по указанной ссылке, или
- информация поступила не с официального телефонного номера Банка/адреса электронной почты, которые указаны на официальном сайте Банка в сети интернет, или
- в сообщении содержится просьба перейти на какой-либо сайт в сети интернет по указанной ссылке, или
- сообщение содержит явные опечатки или орфографические ошибки, или
- требуется установить/открыть приложение и произвести демонстрацию экрана,

Вы **не** должны совершать действий, которые могут привести к разглашению персональных данных, подтверждающих кодов и реквизитов Карты.

Вы должны незамедлительно сообщить в Банк о поступлении такого сообщения/письма/звонка по телефонам Службы поддержки, указанным в п.8 настоящих Рекомендаций.

6.2. При подозрении на любые возможные мошеннические действия, в том числе:

- несанкционированное использование Системы, в т.ч. если Клиент получил сообщение (ему стало известно) о совершенной без согласия Клиента операции,
- ПИН-код и реквизиты карты стали или могли стать известны посторонним лицам,
- при поступлении сообщения о несанкционированном входе в систему «Приобанк Онлайн»,

Вы должны незамедлительно сообщить об этом в Банк по телефонам Службы поддержки, указанным в п.8 настоящих Рекомендаций.

6.3. Для связи с Банком Вы обязаны использовать только номера телефонов Службы поддержки, указанные в п.8 настоящих Рекомендаций, или указанные на официальном сайте Банка в сети интернет, предварительно убедившись в правильности интернет-адреса Банка, в т.ч. домена.

6.4. Клиент единолично несет ответственность за соблюдение всего указанного выше в настоящем разделе порядка использования электронного средства платежа.

В случае нарушения порядка использования электронного средства платежа, повлекшего за собой совершение несанкционированной операции по счету Клиента, ответственность за последствия совершения такой несанкционированной операции несет Клиент.

Во всех случаях совершения несанкционированных операций по счетам Клиента в Банке Клиент обязан обращаться в правоохранительные органы с соответствующим заявлением.

Рассмотрение Банком претензии Клиента о совершении несанкционированной операции, подлежащей рассмотрению, не исключает необходимости обращения Клиента в правоохранительные органы по факту несанкционированной операции.

7. Блокирование рабочего места в ДБО

Блокирование рабочего места должно осуществляться Вами в целях безопасности в случаях, перечисленных в п.5, а также в других случаях по Вашему усмотрению. **Помните!** Блокирование рабочего места приведет к невозможности использования ДБО до момента ее разблокирования.

7.1. Блокирование рабочего места Вы можете осуществить одним из следующих способов:

- обратившись в любое подразделение Банка - с обязательным предъявлением документа, удостоверяющего личность.
- связавшись со Службой поддержки клиентов физических лиц — **8 (4912) 500-250** - с использованием **кодового слова**;

7.2. Разблокировать рабочее место Вы можете одним из способов:

- обратившись в любое подразделение Банка, с обязательным предъявлением документа, удостоверяющего личность;
- связавшись со Службой поддержки клиентов физических лиц — **8 (4912) 500-250** - с использованием **кодового слова.**

8. Службы поддержки

Контакт-центр банка — 8 (4912) 200-003;

Служба технической поддержки Банка — 8 (4912) 50-44-50;

Служба поддержки клиентов физических лиц — 8 (4912) 500-250 — с использованием кодового слова, которое Вы указали в Заявлении на присоединение к Условиям дистанционного банковского обслуживания «Приобанк Онлайн» и/или в Заявление на выпуск карты.