Приложение 9
К Правилам
Дистанционного банковского обслуживания
физических лиц с использованием системы
«Интернет-банк»

Требования Банка по информационной безопасности при Обслуживании Клиента с использованием системы «Интернет-банк»

Помните, что соблюдение требований Банка по информационной безопасности при использовании системы «Интернет-банк» (далее - Система) минимизирует риск осуществления несанкционированного доступа к счетам Клиентов. В этом случае Клиент принимает на себя все риски осуществления несанкционированного доступа к банковским счетам Клиента при использовании Системы, а Банк освобождается от какой-либо ответственности и не обязан возмещать Клиенту убытки, включая, но не ограничиваясь, возвратом суммы операции, совершенной без согласия Клиента.

Для обеспечения безопасности работы в Системе применяются:

- шифрование канала связи с использованием протокола SSL и сертификата, подписанного удостоверяющим центром THAWTE;
- идентификация и аутентификация Клиента;
- сеансовые ключи для подтверждения операций с использованием Системы;
- рассылка уведомлений о совершенных операциях в Системе на абонентский номер Клиента;
- изменение статуса ЭД в Системе по мере осуществления операций**;**
- предоставление выписки по счетам с использованием Системы по мере осуществления операций.

1. Требования при организации рабочего места для Обслуживания с использованием Системы

1.1. На компьютере или мобильном устройстве (мобильный телефон, планшетный компьютер и т.п.), используемом Клиентом для Обслуживания с использованием Системы должно быть установлено только лицензионное программное обеспечение, включая операционную систему и средства защиты. Клиент обязан использовать операционные системы и программное обеспечение, на которые разработчик регулярно выпускает обновления, в том числе связанные с повышением уровня безопасности.

1.2. Компьютер (мобильное устройство), используемый для Обслуживания в Системе, не должен быть заражен вирусами. Клиент обязан установить и активизировать антивирусное программное обеспечение. Антивирусные средства защиты должны соответствовать классу “Internet Security”. Клиент обязан регулярно (автоматически) обновлять антивирусные базы и проверять компьютер на вирусы. Обращаем внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о ваших Средствах доступа.

1.3. Клиент обязан установить автоматическое обновление операционной системы, средств защиты и интернет-браузера, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости обновляемых систем.

1.4. Клиент обязан установить на компьютер или мобильное устройство межсетевой экран (брандмауэр, файервóл) с «Белым списком», в котором будут указаны только необходимые адреса (сервер Системы, сервера обновлений операционной системы, средств защиты, интернет-браузера и других необходимых приложений). Это позволит предотвратить несанкционированный доступ к информации на компьютере (мобильном устройстве).

1.5. Клиент обязан устанавливать программное обеспечение только с доверенных источников (рекомендуемых производителем или поставщиком программного обеспечения) и использовать широко известные браузеры.

1.6. Работа на компьютере или мобильном устройстве должна производиться под ограниченными в правах учетными записями (без прав администратора).

1.7. Функция «Автоматическое выполнение» для подсоединяемых к компьютеру или мобильному устройству внешних носителей (копакт-дисков, флэш-карт и т.д.) должна быть отключена.

1.8. Чужие компьютеры или «недоверенные» компьютеры (интернет-кафе, киоски и т.д.) не должны использоваться для Обслуживания с использованием Системы. При использовании недоверенных компьютеров значительно возрастает риск кражи ваших Средств доступа (логина/пароля, сеансового ключа).

1.9. Компьютер или мобильное устройство для Обслуживания с использованием Системы не должно

использоваться для посещения сайтов, отличных от сайта Системы.

1.10. Доступ посторонних лиц к компьютеру и мобильному устройству, с которого Вы осуществляете Обслуживание с использованием Системы, должен быть ограничен.

2. Требования к действиям клиентов при работе с Системой

2.1. При самом первом входе в Систему вручную, с помощью клавиатуры компьютера, введите в адресной строке браузера адрес Системы в интернете. В дальнейшем допускается добавить данную web-страницу в раздел «Избранное» браузера и входить в Систему только по этой ссылке.

2.2. Клиент обязан не входить в Систему по чужим ссылкам (особенно баннерным или полученным через почту), поскольку существует множество способов фальсифицировать адрес.

2.3. При входе в Систему Клиент обязан удостовериться, что:

- в адресной строке браузера действительно указан адрес Системы в интернете;
- соединение действительно происходит в защищенном режиме SSL, при этом веб-браузер должен показывать значок закрытого замка, в адресной строке браузера присутствует наименование протокола соединения «https».
- сертификат сайта выдан удостоверяющим центром THAWTE и соответствует сайту Системы в интернете. Для этого, откройте информацию о сертификате и убедитесь, что издателем (кем выдан) является «Thawte SSL CA»;
- за Клиентом не ведется наблюдение, в том числе с использованием технических средств.

2.4. При самом первом входе в Систему Клиент обязан сменить пароль, полученный в Банке. Клиент обязан периодически производить замену пароля для входа в Систему.

При формировании пароля требуется соблюдать следующие правила:

- длина пароля должна быть не менее 8 символов;
- необходимо использовать латинские буквы, набранные в разных регистрах (a-z, A-Z, a-Z), цифры и специальные символы;
- при смене пароля для входа в Систему новое значение должно отличаться от предыдущего не менее чем на 3 символа;
- новое значение пароля для входа в Систему не должно совпадать с предыдущими паролями на протяжении четырех смен;
- пароль не должен основываться на информации, которую можно легко угадать или узнать (имена, номера телефонов, даты рождения, идентификаторы пользователей, наименования рабочих станций и т.п.);
- пароль не должен являться персональной информацией (имена и даты рождения членов семьи, адреса, телефоны и т.п.);
- пароль не должен являться словарным словом (например, «password» - это ненадежный пароль);
- 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).

2.5. Запрещается сообщать информацию о пароле любым лицам, включая сотрудников Банка, родственников и иных третьих лиц.

2.6. Запрещается сохранять пароль для входа в Систему в легкодоступных местах, на любых носителях, включая компьютер. Запрещается сохранять ключевую информацию на жестких/сетевых дисках компьютера, в реестре операционной системы.

2.7. Опция дополнительной проверки одноразового сеансового ключа при входе в Систему не должна быть отключена. Отключение данной опции существенно снижает безопасность Системы. При подключенной опции дополнительной проверки при входе в Систему необходимо вводить только один сеансовый ключ.

2.8. Запрещается стирать защитный слой со скретч-карты Набора сеансовых ключей заранее до проведения операции, когда ключ будет использован, во избежание получения информации о значении ключа третьими лицами.

2.9. Клиент обязан обращать внимание на изменения привычного вида страниц входа в Систему или подтверждения операции. При возникновении сомнений, действительно ли содержимое страницы отправлено с сервера Банка, Клиент обязан позвонить в Единую справочную службу Банка или попробовать открыть ту же страницу Системы на другом компьютере или мобильном устройстве.

2.10. Клиент обязан не реже одного раза в 14 (Четырнадцать) календарных дней осуществлять доступ в Систему, в том числе для ознакомления с информацией, публикуемой Банком в соответствии с п. 1.3.3. настоящих Правил. Клиент обязан внимательно контролировать все операции, совершенные с использованием Системы.

2.11. Клиент обязан блокировать компьютер или мобильное устройство при отсутствии за ним визуального контроля со стороны Клиента.

2.12. Запрещается оставлять компьютер или мобильное устройство с активным Соединением с Системой без присмотра. Клиент обязан завершить Соединение с Системой, даже при кратковременном перерыве в работе.

2.13. После окончания работы с Системой Клиент обязан закрыть окно Системы с помощью кнопки «Выход».

2.14. При любом неадекватном (отличающемся от обычного) поведении компьютера, используемом для доступа в Систему:

- *подозрительная активность на компьютере или подозрительная работа мобильного устройства, с которого осуществляется доступ в Систему (самопроизвольные движения мышью, открытие/закрытие окон, набор текста и т.п.);*
- *присутствие в Системе действий, которые Клиент не совершал;*
- *изменение адреса для соединения с Системой;*
- *невозможность получения доступа к Системе по причине несовпадения пароля на вход в Систему;*
- *изменение интерфейса Системы;*

а также, при возникновении опасений, что пароль/Набор сеансовых ключей Клиента стали известны посторонним лицам, или Клиент получил СМС-оповещение или выписку Банка об операциях, которые не совершал, *Клиент обязан* выполнить следующие действия:

- *выйти из Системы;*
- *заблокировать технические средства (в том числе, выключить компьютер), используемые для работы в Системе;*
- *немедленно обратиться в Единую справочную службу Банка для приостановления/ограничения дистанционного обслуживания в Системе и/или для отмены Набора сеансовых ключей по реквизитам, указанным на официальном сайте Банка или в Договоре Присоединения.*