Приложение N1
к Правилам пользования
Интернет-Банкингом для физических лиц

ТРЕБОВАНИЯ

к техническому и программному обеспечению Клиента, а также к обеспечению информационной безопасности при работе в Интернет-Банкинге

1. Требования к программно-техническому обеспечению для работы в ИСББ и ИСББ-лайт

1.1. IBM PC совместимый персональный компьютер:
- 1.1.1. процессор Intel Pentium 200 (либо аналогичный) и выше;
- 1.1.2. жесткий диск с объемом свободного пространства не менее 150 Mb;
- 1.1.3. накопитель на гибких магнитных дисках 3,5 “ либо USB-порт для подключения флэш-памяти;
- 1.1.4. клавиатура со 101 клавишей;
- 1.1.5. манипулятор мышь либо аналогичное по функциям устройство;
- 1.1.6. VGA совместимый дисплей, поддерживающий разрешение не менее 800x600;
- 1.1.7. русифицированные операционные системы Microsoft Windows 2000-2003, XP и выше

1.2. Соединение TCP/IP с Интернет.

2. Требования по обеспечению информационной безопасности компьютера, с которого осуществляется работа в ИСББ и ИСББ-лайт

2.1. Компьютеры должны располагаться в помещениях, обеспечивающих невозможность несанкционированного доступа к ним.

2.2. Запрещается оставлять без контроля компьютер при включенном питании и загруженном Программном обеспечении. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана должно производиться с использованием пароля доступа.

2.3. Рекомендуется подключать компьютер к сети электропитания через устройства бесперебойного питания.

2.4. На компьютере должно быть установлено антивирусное программное обеспечение с выполнением регулярного обновления, а также установлен и настроен межсетевой экран (firewall).

2.5. На компьютере должны быть установлены обновления для операционной системы и офисных приложений, а также другого программного обеспечения (в соответствии с рекомендациями компании-разработчика).

2.6. Следует использовать программное обеспечение только из проверенных источников. Файлы, полученные из сети интернет, а также доставленные на сменных носителях, не следует исполнять и открывать без проведения предварительной антивирусной проверки.

2.7. На компьютере должна быть установлена парольная защита на вход в BIOS и в операционную систему. При выборе пароля необходимо следовать следующим рекомендациям:
- 2.7.1. пароль должен содержать не менее 6 символов;
- 2.7.2. не рекомендуется использовать в качестве пароля: имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об администраторе или пользователе; один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов; комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, “1234567” или “1йфячыц2” и т. п.);

2.8. Настройку компьютера должен выполнять специалист, обладающий необходимыми навыками по администрированию компьютерных систем.

3. Требования по обеспечению информационной безопасности мобильных устройств, с которых осуществляется работа в Мобильном Банке или в ИСББ-лайт

3.1. Услуга Мобильный банк должна быть зарегистрирована на номер телефона принадлежащий именно Вам.
3.2. На мобильное устройство должно быть установлено антивирусное программное обеспечение, полученное из официальных магазинов приложений мобильных платформ, которое необходимо своевременно обновлять.
3.3. Своевременно должны быть установлены официальные обновления операционной системы мобильного устройства, особенно если они относятся к Безопасности с официальных источников фирм разработчиков.
3.4. Ни при каких обстоятельствах не сообщайте конфиденциальные данные посторонним лицам (номер своей карты, счета, паспортные данные, логин, пароль и пр.). Банк владеет всей необходимой информацией и никогда, ни при каких обстоятельствах НЕ ОСУЩЕСТВЛЯЕТ РАССЫЛКУ ЭЛЕКТРОННЫХ ПИСЕМ, SMS-сообщений, звонков по телефону, с просьбой передать реквизиты платежной карты, ПИН-код к платежной карте, а также не распространяет по электронной почте программы и их обновления.
3.5. На мобильном устройстве должен быть установлен пароль доступа. Используйте сложные пароли, избегая легко угадываемых вариантов.
3.6. Хранение средства доступа к Мобильному банку на своем телефоне/планшете (в заметках, напоминаниях, SMS, и пр.) должно быть исключено.
3.7. При установке на мобильное устройство нового приложения, всегда обращайте внимание на разрешения, которые оно требует для своей работы, особенно на возможность доступа к SMS-сообщениям. Если разрешения вызывают подозрения или явно не соответствуют функционалу программы, лучше отказаться от ее использования.
3.8. При утере/краже мобильного устройства, на которое Банк отправляет SMS-сообщения с кодом подтверждения операции, или неожиданным прекращением работы SIM-карты, Вам следует как можно быстрее обратиться к своему оператору мобильной связи и заблокировать SIM-карту, а также проинформировать об этом Банк, обратившись в Службу поддержки клиентов Банка.
3.9. При потере/смене SIM-карты, передаче SIM-карты третьему лицу, обязательно сообщите об этом в Службу поддержки клиентов Банка.

4. Требования по обеспечению информационной безопасности при хранении и использовании Криптографических ключей (ИСББ)

4.1. Использование Криптографических ключей допускается только в рамках электронного документооборота.
4.2. Ключевые носители необходимо хранить в надежном месте, исключающем доступ к ним неуполномоченных лиц. Рекомендуется для хранения использовать надежные металлические хранилища.
4.3. **Не допускается:**
  4.3.1. снимать несанкционированные копии с Ключевых носителей;
  4.3.2. знакомить с содержанием Ключевых носителей или передавать Ключевые носители третьим лицам;
  4.3.3. выводить Ключи ЭП на дисплей компьютера или принтер;
  4.3.4. устанавливать Ключевой носитель в считывающее устройство компьютера, программные средства которого функционируют в непредусмотренных (нештатных) режимах;
  4.3.5. записывать на Ключевые носители постороннюю информацию.
4.4. В случае обнаружения факта компрометации Криптографических ключей необходимо немедленно произвести их замену или блокировку.