УТВЕРЖДЕНО
Протокол Правления
ОАО «Белагропромбанк»
от 17.02.2017 №13

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ РАБОТЫ КЛИЕНТА В ПОДСИСТЕМЕ «ИНТЕРНЕТ-КЛИЕНТ» СДБО

1. ПОДСИСТЕМА «ИНТЕРНЕТ-КЛИЕНТ»

1.1. Клиент на момент заключения Договора должен иметь рабочее место, оборудованное собственными программно-техническими средствами (за исключением мультипользовательского рабочего места).

Рекомендуемая конфигурация рабочего места - персональный компьютер со следующими характеристиками:

операционная система - Windows 7SP1 и выше;

браузер - Google Chrome 91 и выше, Mozilla Firefox 88 и выше, MS Edge;

устройство для чтения/записи носителя личных ключей ЭЦП и шифрования (USB-порт).

1.2. Подключение Клиента к подсистеме «Интернет-Клиент» (в том числе в режиме мультипользовательское рабочего места) осуществляется с предоставлением банком Клиенту съемных носителей для записи и хранения личных ключей ЭЦП или с использованием съемных носителей, предоставленных Клиентом нижеперечисленных типов:

Avest AvToken;

Avest AvPass (не для удаленного использования);

Avest AvBign;

1.3. В случае использования Клиентом ключей ЭЦП, сертификаты которых зарегистрированы в удостоверяющем центре сертификатов банка, стороны устанавливают следующий порядок генерации (перегенерации) и регистрации (отзыв) сертификатов открытых ключей подсистемы «Интернет-Клиент»:

первоначальный выпуск ключа ЭЦП и формирование запроса на сертификат открытого ключа осуществляется лично владельцем ключа ЭЦП, в качестве которого может выступать руководитель Клиента либо его уполномоченное лицо в соответствии с представленными в банк документами, подтверждающими полномочия уполномоченного лица (далее - Клиент);

выпуск ключей ЭЦП производится Клиентом самостоятельно на своем рабочем месте либо в согласованное с банком время на специально оборудованном рабочем месте подразделения банка;

Клиент производит генерацию личного ключа ЭЦП с установкой пароля на доступ к нему, который хранит в тайне. Уполномоченный работник банка при этом контролирует правильность внесения Клиентом данных в поля Мастера создания запроса на сертификат Персонального менеджера

сертификатов и при необходимости оказывает помощь Клиенту;

Клиент распечатывает и удостоверяет своей подписью и печатью (при ее наличии) данные, внесенные в бланк карточки открытого ключа проверки ЭЦП, на бумажном носителе в двух экземплярах и передает один экземпляр уполномоченному работнику банка;

уполномоченный работник банка заверяет своей подписью на бланке карточки открытого ключа проверки ЭЦП подлинность подписи Клиента.

В случае предоставления банком съемного носителя для записи личных ключей ЭЦП оформляется Акт приема-передачи съемных носителей криптографической защиты информации (по установленной ЛПА банка форме).

Ключи ЭЦП вводятся в действие и имеют юридическую значимость (силу) для СДБО с момента регистрации сертификата открытого ключа Клиента в СДБО и ограничиваются датой действия сертификата либо датой его отзыва.

1.4. При необходимости в случаях, не противоречащих законодательству, Клиент вправе дополнительно предоставить полномочия для совершения банковских операций с использованием СДБО уполномоченному представителю на основании доверенности или внутреннего распорядительного документа (приказ, распоряжение), в котором в обязательном порядке должен присутствовать образец его собственноручной подписи, указан подробный перечень закрепленных за уполномоченным представителем операций и срок действия полномочий.

Копия доверенности или распорядительного документа должна быть представлена Клиентом в банк для последующей проверки (контроля) полномочий и образца подписи уполномоченного представителя.

В случаях предоставления Клиентом – индивидуальным предпринимателем доверенности без образца подписи уполномоченного представителя вышеуказанный индивидуальный предприниматель дополнительно представляет в банк копию трудового (или) гражданско-правового договора, заключенного с данным уполномоченным представителем (в котором присутствует образец собственноручной подписи уполномоченного представителя).

Для предоставления функций просмотра и создания документа (без подписания ЭЦП) Клиент вправе самостоятельно предоставить доступ (логин и пароль) лицам в соответствии со своими внутренними распорядительными документами.

1.5. Смена (отзыв) сертификатов открытых ключей производится при утрате, повреждении (отказе в работе) ключей ЭЦП:

стороны производят те же действия, что и при первичной генерации и регистрации сертификатов открытых ключей, но при этом новый (другой) съемный носитель используется при повреждении или утере старого;

открытый ключ проверки ЭЦП Клиента, идентификационная информация которого указана в заявлении для отзыва сертификата (произвольной формы), удаляется из каталога открытых ключей банка с

момента времени, определенного заявлением. Идентификационная информация – комбинация не менее двух параметров, указанных в карточке открытого ключа:

фамилия, имя и отчество,

личный (идентификационный) номер гражданина Республики Беларусь,

серийный номер сертификата,

идентификатор ключа субъекта (Subject Key Identifier).

1.6. При выходе из строя в период эксплуатации Клиентом съемного носителя, предоставленного банком, ремонт или замена осуществляется за счет Клиента.

При расторжении Договора без перехода на использование других подсистем СДБО Клиент не позднее даты его расторжения прекращает использование съемных носителей ключей криптографической защиты информации. Уполномоченный работник банка отзывает в удостоверяющем центре сертификатов банка все сертификаты открытых ключей, которые закреплены за расторгаемым Договором.

1.7. При необходимости смены (отзыва) сертификата открытого ключа Клиента или при изменении реквизитов Клиента производится генерация нового ключа ЭЦП на Клиентском съемном носителе для записи личных ключей ЭЦП. В случае предоставления банком съемного носителя для записи личных ключей ЭЦП оформляется Акт приема-передачи съемных носителей криптографической защиты информации (по установленной ЛПА банка форме); оформляется новая карточка открытого ключа проверки ЭЦП, и только после ее удостоверения изменения вступают в силу. Действие старого сертификата открытого ключа прекращается с момента регистрации в СДБО нового сертификата открытого ключа.

1.8. Установка необходимого программного обеспечения криптографической защиты на компьютер Клиента (за исключением мультипользовательского рабочего места) осуществляется Клиентом или его исполнителем в соответствии с требованиями Инструкции по установке. Пакет необходимого программного обеспечения и инструкций по установке и настройке размещен в ZIP-архиве в каталоге «Программы и документация» на сайте https://i25-client.belapb.by.

Для работы в мультипользовательском рабочем месте Клиент или его исполнитель должен иметь при себе съемный носитель с записанным личным ключом ЭЦП.

1.9. Владельцу ключа ЭЦП или его исполнителю категорически запрещается:

передавать съемный носитель другим лицам, делать с него копии и пытаться воздействовать на него программными средствами, не предоставленными банком;

записывать на съемный носитель ключей криптографической защиты постороннюю информацию;

оставлять в считывателе съемный носитель ключей криптографической защиты без личного надзора;

нарушать целостность программных модулей и файлов данных, входящих в систему криптографической защиты.

1.10. Исполнитель Клиента должен хранить в тайне пароль к личному ключу, а также съемный носитель в месте, обеспечивающем его недоступность другим лицам.

1.11. Исполнитель Клиента обязан незамедлительно обратиться в обслуживающее подразделение банка в следующих случаях:

невыполнения функции ЭЦП и шифрования из-за сбоев в работе Средств криптографической защиты информации;

утери (кражи) съемного носителя ключей криптографической защиты;

подозрения, что подсистемой «Интернет-Клиент» и (или) ключевым носителем воспользовалось другое лицо.

В случае утери (кражи) съемного носителя ключей криптографической защиты и (или) возникновения подозрения, что подсистемой «Интернет-Клиент» и (или) съемным носителем воспользовалось другое лицо, Исполнитель Клиента оперативно по телефону сообщает Уполномоченному работнику банка или в Контакт-центр с использованием контрольного слова (фразы) или путем сообщения ФИО, личного номера из паспорта о намерении временно заблокировать действия сертификата открытого ключа, после чего либо таким же образом разблокировать действие сертификата открытого ключа, либо представить в банк заявление на отзыв сертификата открытого ключа, содержащее информацию о наступлении вышеуказанных случаев (произвольной формы).

1.12. Смена ключей криптографической защиты Клиенту производится незамедлительно при утере съемного носителя или возникновении подозрения, что подсистемой «Интернет-Клиент» и (или) съемным носителем воспользовалось другое лицо, а также по желанию исполнителя Клиента при условии выполнения процедуры, описанной в пункте 1.5.

1.13. Отзыв сертификатов открытых ключей производится в установленном банком порядке.

1.14. Рекомендуемые меры по защите съемных носителей и компьютеров, используемых для работы в СДБО:

съемные носители следует хранить в защищенных местах (сейфах, запирающихся ящиках);

съемные носители должны использоваться только уполномоченными лицами;

запрещено передавать съемный носитель одного уполномоченного лица другому уполномоченному лицу;

запрещено устанавливать съемные носители в компьютеры, не используемые для работы в СДБО;

запрещено оставлять съемные носители установленными в компьютерах после завершения сеанса работы в СДБО;

запрещено изготавливать копии ключей ЭЦП, используемых для работы в СДБО;

следует регулярно обновлять все программное обеспечение,

установленное на компьютерах;

на компьютерах должно быть установлено антивирусное программное обеспечение;

обновление антивирусного программного обеспечения следует производить не реже раза в сутки;

не реже раза в неделю следует производить полное антивирусное сканирование жестких дисков компьютеров;

сетевое оборудование, обеспечивающее доступ Клиента в сеть Интернет, или межсетевой экран компьютера, применяемого для работы в СДБО, должны блокировать любые сетевые пакеты, передаваемые с данного компьютера на серверы, не относящиеся к СДБО, веб-сайту банка, службам обновления установленного программного обеспечения и антивирусных баз.

2. ПОДСИСТЕМА «МОБИЛЬНЫЙ БАНК»

2.1. Подсистема «Мобильный банк» функционирует при условии подключении Клиента к подсистеме «Интернет-Клиент» (в том числе в режиме мультипользовательского рабочего места).

2.2. Для подключения к подсистеме «Мобильный банк» Клиент должен иметь мобильное устройство (планшет, мобильный телефон (смартфон)) на следующих платформах:

iOS 8 и выше (операционная система для смартфонов и планшетов Apple);

Android 4.0 и выше (операционная система для иных смартфонов и планшетов).

2.3. Загрузка приложения на мобильное устройство осуществляется Клиентом самостоятельно из AppStore или GooglePlay.

2.4. Для подключения услуги отправки платежей с использованием подсистемы «Мобильный банк» Клиент должен в заявлении на подключение[1] указать номер мобильного телефона, на который будет установлено приложение Belapb Business, и подтвердить свое согласие на использование для подписания расчетных документов в «Мобильном банке» кода подтверждения, который будет поступать на указанный номер телефона (вместо ЭЦП).

Логин и пароль Клиента для входа в подсистему «Мобильный банк» совпадает с логином и паролем Клиента для входа в подсистему «Интернет-Клиент».

---

[1]В Заявлении на подключение к подсистеме «Интернет-Клиент» (приложение 1 к Условиям обслуживания юридических лиц и индивидуальных предпринимателей с использованием подсистемы «Интернет-Клиент»), заявлении на комплексное обслуживание юридического лица (индивидуального предпринимателя), заявлении на комплексное обслуживание вновь зарегистрированного юридического лица (индивидуального предпринимателя)) в соответствии с ЛПА, регламентирующим порядок открытия, переоформления и закрытия банковских и иных счетов юридическим лицам и индивидуальным предпринимателям, или Заявлении на подключение к услуге отправки платежей «Мобильный Банк» (по форме, установленной Банком) в случае если подключение не было выполнено при первоначальной регистрации Клиента в СДБО «Интернет-Клиент».

3. ПАРОЛЬНАЯ ПОЛИТКА КЛИЕНТА

С целью осуществления безопасности работы подсистемы «Интернет-Клиент» Клиент обязуется:

3.1. использовать для ввода логина от 6 (шести) до 20 (двадцати) символов;

3.2. производить изменение временного пароля при первом входе в систему;

3.3. использовать для ввода пароля от 6 (шести) до 32 (тридцати двух) символов;

3.4. использовать для ввода пароля буквы, цифры, символы «_», «-» и «.»;

3.5. вводить пароль с содержанием буквы разного регистра и минимум 1 (одной) цифры, число повторяющихся символов должно быть меньше 3 (трех);

3.6. использовать индикатор сложности пароля, который определяет и помогает Клиенту выбрать безопасный пароль для работы в подсистеме «Интернет-Клиент»;

3.7. производить смену пароля не реже одного раза в месяц (новые и старые пароли должны отличаться набором символов);

3.8. производить изменение пароля при возможной его компрометации;

3.9. для смены пароля необходимо ввести текущий пароль и дважды ввести новый пароль;

3.10. хранить пароль в секрете.

4. МЕРЫ БЕЗОПАСНОСТИ КЛИЕНТА

С целью осуществления безопасности работы подсистемы «Интернет-Клиент» Клиент обязуется:

4.1. Не сообщать персональные либо иные конфиденциальные данные (логин и пароль от СДБО, пароль ключа ЭЦП, личный номер паспорта, историю операций, контактные и учетные данные) посторонним лицам, даже если они представляются сотрудниками банка, процессингового центра, службы, проводящей социологические опросы и т.п.

4.2. Четко регламентировать и соблюдать порядок использования компьютера, с которого осуществляется взаимодействие с СДБО, в том числе список лиц и порядок доступа к компьютеру. Рекомендуется иметь утвержденный список сотрудников организации, включая ответственных сотрудников и технический персонал, которым разрешен доступ к компьютеру, с которого осуществляется работа в СДБО.

4.3. Не использовать указанный компьютер для доступа к другим сайтам в Интернете. Если это невозможно, на компьютере, с которого осуществляется работа в СДБО, соблюдать строгие правила безопасной работы. Установить и использовать только лицензионное программное обеспечение (операционная система, офисные пакеты, антивирус) и осуществлять ежедневные обновления антивирусных баз. Проводить регулярную установку обновлений

безопасности системного и прикладного программного обеспечения в соответствии с рекомендациями его производителей. Не подключать к компьютеру непроверенные на наличие вирусов переносные носители (флешки), не открывать подозрительных электронных писем, максимально ограничить использование мессенджеров (Skype, Viber, Telegram). На компьютере, с которого осуществляется работа в СДБО, работать под учетной записью с правами «Пользователь». Не запускать программы, полученные из недоверенных источников (файлообменные сайты, торрент-трекеры, взломанные программы и взломщики, недоверенные расширения браузеров, переключатели клавиатуры и т.п.). Использовать межсетевой экран, внимательно следить за информацией, которую он сообщает. Межсетевой экран должен блокировать любые сетевые пакеты, передаваемые с данного компьютера на серверы, не относящиеся к СДБО, веб-сайту банка, службам обновления установленного программного обеспечения и антивирусных баз.

4.4. Никогда не записывать логины и пароли на мониторе или клавиатуре, не хранить их в открытом виде на жестком диске компьютера. Если записали пароли на бумажном носителе, что также не рекомендуется делать, хранить их в недоступном для посторонних лиц месте (сейф, запираемый ящик, металлический шкаф). Не использовать одинаковые логин и пароль для доступа к СДБО, ключу ЭЦП и другим сайтам или системам. При составлении пароля использовать прописные и строчные буквы, цифры, а также различные символы. Не использовать в качестве пароля свои имя, фамилию, дату рождения и номера телефона, придумать длинную парольную фразу, которую легко запомнить именно вам и использовать ее в качестве пароля.

4.5. Для входа на Интернет-ресурсы банка всегда набирать адреса сайтов вручную или пользоваться закладками браузера, которые сделали сами. При переходе на сайт банка с других Интернет-ресурсов проверять достоверность ссылки. Обращать внимание на то, что адрес СДБО должен начинается с «https://», а не с «http://» (https://i25-client.belapb.by).

4.6. Никогда не отвечать на электронные письма, в которых запрашиваются конфиденциальные данные, не переходить по указанным в них ссылкам, не открывать вложенные файлы, не звонить по указанным телефонам. Все письма, запрашивающие конфиденциальные данные, являются мошенническими! Банк никогда не просит передать конфиденциальные данные по электронной почте.

4.7. Не пользоваться СДБО в Интернет-кафе и прочих местах общественного доступа к сети Интернет, в том числе публичными незащищенными Wi-Fi сетями.

4.8. Присоединять носитель с ключом ЭЦП к компьютеру непосредственно перед началом работы с СДБО, а по окончании работы извлекать его из компьютера. Хранить данный носитель в недоступном для посторонних лиц месте (сейф, запираемый ящик, металлический шкаф).

4.9. В случае если доступ к СДБО осуществлялся с использованием постороннего компьютера, не сохранять на нем идентификационные данные и

другую информацию, а после завершения всех операций убедиться, что идентификационные данные и другая информация не сохранились. После возвращения к штатному персональному компьютеру обязательно сменить пароли доступа к СДБО.

4.10. Регулярно не реже одного раза в месяц производить смену пароля доступа к ключам ЭЦП, не позволять третьим лицам производить за Клиента смену паролей ключей ЭЦП. При увольнении ответственного сотрудника, имевшего доступ к ключу ЭЦП, обязательно сообщать в банк и заблокировать ключ ЭЦП.

4.11. При возникновении любых подозрений на компрометацию ключа ЭЦП, кражу носителя ключа ЭЦП обязательно сообщить в банк и заблокировать ключи ЭЦП.

4.12. В случае обнаружения вредоносного программного обеспечения на компьютере, с которого осуществляется взаимодействие с СДБО, после его удаления незамедлительно сменить пароль в СДБО.

4.13. При обнаружении подозрительных действий, признаков подозрительных действий, совершенных от имени Клиента в СДБО, незамедлительно сменить пароль, сообщать об инциденте в банк и производить смену ключей ЭЦП.

4.14. Проверять реквизиты входящих SMS-сообщений. SMS-сообщения от банка могут приходить только с номеров «Belagroprom», «Belapb», «BELAPB.BY», «1207», «1208».

4.15. При получении Viber-рассылки от банка убедиться, что она совершена с официального аккаунта (отправитель – БЕЛАГРОПРОМБАНК, присутствует официальный логотип, есть отметка в виде зеленой «галочки» и информация о том, что отправитель прошел проверку Viber, при получении сообщения – не всплывает окно о том, что пришло сообщение не из Вашей адресной книги).

4.16. Использовать только официальные приложения банка из магазинов App Store, Google Play. Все официальные приложения банка описаны на корпоративном сайте банка www.belapb.by.