УТВЕРЖДЕНО

Распоряжение заместителя председателя правления банка

28.12.2017 № 598

(в редакции распоряжения заместителя председателя правления банка

02.03.2023 № 63)

РЕГЛАМЕНТ
обслуживания бизнес-клиентов в системе дистанционного банковского обслуживания ОАО «Белгазпромбанк»

Общие положения и термины

Администратор Клиента (далее – Администратор) – пользователь с правами администратора, уполномоченный Клиентом на создание учетных записей других пользователей, управление настройками пользователей, назначение им прав, создание для них временных паролей и являющийся контактным лицом Клиента в системе дистанционного банковского обслуживания (далее – СДБО).

ГосСУОК – Государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

Интернет-банк «Бизнес» – сервис СДБО, предназначенный для оперативного взаимодействия Клиента с Банком через сеть Интернет на сайте Банка по адресу: corporate.bgpb.by посредством интернет-браузера, и обеспечивающий получение информации, формирование, передачу, регистрацию и исполнение распоряжений Клиентов.

Менеджер Клиента – работник Точки продаж, в должностные обязанности которого входит прием и обработка заявлений Клиентов на подключение к СДБО, изменение Администратора, восстановления параметров Администратора, выдачу дубликата ключа и т.д., прием и обработка карточек открытого ключа, оформленных Клиентами, расчетно-кассовое обслуживание Клиентов.

Мобильное приложение – сервис СДБО, предназначенный для оперативного взаимодействия Клиента и Банка с использованием программного обеспечения, предоставляемого Банком и устанавливаемого Пользователем Клиента на его мобильном устройстве, а также обеспечивающего получение информации, формирование, передачу, регистрацию и исполнение распоряжений Клиента в рамках реализованных в нем функций. К мобильному приложению относится Мобильное приложение «BGPB Business».

Партнерский сервис – сервис СДБО, предназначенный для оперативного взаимодействия Клиента и Банка с использованием программного обеспечения, предоставляемого Партнером, заключившим соглашение с Банком, и

обеспечивающий получение информации, формирование, передачу, регистрацию и исполнение распоряжений Клиентов в рамках реализованных в нем функций, согласно условиям заключенного соглашения.

Пользователь – физическое лицо - сотрудник Клиента, имеющий права, определенные Администратором Клиента, на работу в СДБО.

Сервис СДБО – определенный Банком способ предоставления Клиенту услуг дистанционного банковского обслуживания (далее – ДБО). К сервисам СДБО относятся: Интернет-банк «Бизнес», Мобильное приложение «BGPB Business» и Партнерские сервисы.

Точка продаж – структурное подразделение Банка, осуществляющее открытие счетов и расчетно-кассовое обслуживание Клиентов. К Точкам продаж, на которые распространяется действие настоящего Регламента, относятся центры банковских услуг, операционное управление департамента корпоративного бизнеса, отделы по работе с бизнес-клиентами дирекций, отделы управления продаж розничных продуктов департамента розничного бизнеса.

Иные термины и определения настоящего Регламента толкуются в соответствии с Правилами обслуживания бизнес-клиентов в ОАО «Белгазпромбанк».

1. Регистрация и подключение к Интернет-банк «Бизнес»

1.1. Доступ к услуге ДБО посредством Интернет-банк «Бизнес» (далее – Система) осуществляется Клиентом путем использования сайтов, расположенных в доменной зоне *. bgpb.by.

Клиент должен ознакомиться с Условиями дистанционного банковского обслуживания бизнес-клиентов, являющимися разделом Правил обслуживания бизнес-клиентов в ОАО «Белгазпромбанк», на сайте Банка или сайте системы https://corporate.bgpb.by (далее – Сайт системы).

1.2. Для осуществления операций, требующих подписания электронных документов, Клиентом используются ключи электронно-цифровой подписи (далее – ЭЦП).

1.3. Для осуществления операций, требующих подписания документов в электронном виде посредством Мобильного приложения «BGPB Business», Клиентом используются компоненты безопасности Мобильного приложения «BGPB Business» по генерации электронной подписи и иные компоненты безопасности, предоставляемые Банком, в т.ч. в рамках Партнерских сервисов.

1.4. Доступ к Системе предоставляется только Клиентам, имеющим счет в Банке, либо на основании отдельных договоров с Банком.

1.5. Для подключения к Системе Клиент должен назначить Администратора.

Роль Администратора может выполнять руководитель, главный бухгалтер Клиента либо другое уполномоченное Клиентом лицо.

1.6. В функции Администратора входит подключение Клиента к Системе, генерация и отправка ссылки, пароля активации для привязки к Клиенту учетных

записей других Пользователей Клиента, а также настройка прав Пользователей Клиента.

Для входа в Систему Пользователями используются логин и пароль.

1.7. Для регистрации в Системе Администратор заполняет «Заявление на подключение к системе дистанционного банковского обслуживания» (далее – Заявление), распечатывает его в двух экземплярах, подписывает у уполномоченного лица Клиента, обладающего правом первой или единственной подписи, и заверяет, при наличии, оттиском печати.

1.8. Подписанное Заявление с указанием необходимого количества электронных ключей передается в Банк Менеджеру Клиента, который осуществляет его прием и обработку.

1.9. После проверки Заявления Менеджер Клиента передает представителю Клиента указанное в Заявлении количество электронных ключей, о чем делается отметка в нижней части Заявления. В случае использования Клиентом сертификатов открытых ключей проверки ЭЦП, изданных республиканским удостоверяющим центром ГосСУОК, электронные ключи Клиенту не выдаются.

Второй экземпляр Заявления с отметкой Банка о принятии Заявления к рассмотрению передается Клиенту.

1.10. Не позднее двух рабочих дней с даты принятия Заявления от Клиента осуществляется обработка Заявления на стороне Банка.

1.11. В случае успешной обработки Заявления Банк осуществляет подключение Клиента к Системе и взимает вознаграждение с Клиента за регистрацию и подключение к Системе и за сопровождение Системы в порядке и в соответствии с действующим Перечнем вознаграждений за операции юридических лиц и индивидуальных предпринимателей, проводимые ОАО «Белгазпромбанк».

1.12. В случае неуспешной обработки Заявления Банк осуществляет информирование Клиента об отказе в предоставлении услуги ДБО. Дальнейшая работа в СДБО Клиенту не доступна.

1.13. Менеджер Клиента также осуществляет прием и обработку:

заявлений Клиентов на изменение Администратора, восстановление параметров Администратора, выдачу дубликата ключа и т.д. в соответствии с локальными правовыми актами (далее – ЛПА) Банка;

карточек открытого ключа, оформленных Клиентами, в соответствии с ЛПА Банка.

2. Администрирование Пользователей Клиента и настройка прав доступа

2.1. Администратор управляет правами всех Пользователей Клиента.

2.2. Для предоставления доступа к Системе другим Пользователям Администратор в Системе в разделе «Настройка» - «Пользователи» генерирует и отправляет ссылки и пароли активации для привязки к Клиенту учетных

записей других Пользователей в соответствии с инструкцией, расположенной на Сайте системы в разделе «Справка» - «Установка криптозащиты».

2.3. Администратор должен отправить ссылку соответствующему Пользователю и передать ему пароль активации.

2.4. Соответствующий Пользователь должен использовать полученные от Администратора ссылку и пароль в течение одного часа.

2.5. Администратор обязан своевременно настраивать и контролировать права для каждого Пользователя по усмотрению Клиента, используя в Системе раздел «Настройка» - «Пользователи».

2.6. В случае использования первой и второй подписи в соответствии с карточкой с образцами подписей Клиента в Системе должны быть обязательно зарегистрированы в качестве Администратора или Пользователя уполномоченное лицо, обладающее правом первой подписи, а также уполномоченное лицо, обладающее правом второй подписи.

В случае использования единственной подписи уполномоченное лицо, обладающее этим правом в соответствии с карточкой с образцами подписей Клиента, должно быть обязательно зарегистрировано в Системе в качестве Администратора или Пользователя. При необходимости в Системе могут быть зарегистрированы иные Пользователи.

Под правом единственной подписи понимается тип права подписи Пользователя в Системе, позволяющий подписывать электронные документы и документы в электронном виде без подтверждения иных лиц, указанных в карточке с образцами подписей Клиента. Право единственной подписи предоставляется:

уполномоченным лицам Клиента, имеющим право первой подписи, при отсутствии в карточке с образцами подписей уполномоченных лиц с правом второй подписи;

уполномоченному лицу Клиента, имеющему право второй подписи, на основании доверенности лица с правом первой подписи (только при использовании ЭЦП, удостоверенной ГосСУОК);

иному уполномоченному лицу Клиента на основании доверенности лица с правом первой подписи.

В соответствии с абзацами третьим и четвертым части третьей настоящего пункта Банк определяет полномочия лиц для предоставления права единственной подписи на основании доверенности на дату предъявления доверенности в Банк.

Клиент обязан незамедлительно уведомить Банк и в месячный срок со дня изменений указанных сведений предоставить информацию:

об изменении сведений, подлежащих включению в карточку с образцами подписей;

об окончании/изменении сроков полномочий, в т.ч. указанных в доверенности(-ях).

При необходимости Клиент обязан оформить новую карточку с образцами подписей в порядке, установленном законодательством.

В случае если требующая замены карточка с образцами подписей в указанный срок не оформлена, Банк отказывает в исполнении документов Клиента по проведению расчетов до оформления новой карточки с образцами подписей.

3. Установка криптозащиты

3.1. Для уполномоченных Пользователей Администратор должен настроить права подписей, используя в Системе раздел «Настройка» - «Пользователи», на основании карточки с образцами подписей Клиента и/или доверенности. У Пользователя может быть право первой, второй или единственной подписи, в соответствии с карточкой с образцами подписей Клиента и/или доверенностью.

3.2. После завершения процедуры регистрации Пользователь, обладающий правом подписи, самостоятельно загружает и устанавливает специальное программное обеспечение в соответствии с Инструкцией по установке криптозащиты для Системы (Инструкция по установке криптозащиты находится на Сайте системы в разделе «Справка» - «Установка криптозащиты»).

3.3. Пользователь, обладающий правом подписи, самостоятельно формирует запрос на сертификат в Системе в разделе «Настройка» - «Запрос на сертификат» для дальнейшего его предоставления в Банк.

3.4. Пользователь распечатывает и подписывает карточку открытого ключа ЭЦП в двух экземплярах.

Если карточка открытого ключа ЭЦП принадлежит уполномоченному лицу с правом единственной или первой подписи, то ее дополнительно удостоверять не требуется.

Если карточка открытого ключа ЭЦП принадлежит лицу с правом второй подписи, то ее необходимо дополнительно удостоверить у уполномоченного лица Клиента (руководителя или иного уполномоченного органа субъекта хозяйствования).

3.5. Подписанная и удостоверенная карточка открытого ключа ЭЦП в двух экземплярах передается Клиентом в Банк Менеджеру Клиента.

3.6. Не позднее следующего рабочего дня Банком производится выпуск сертификата.

Второй экземпляр карточки открытого ключа ЭЦП с отметками Банка передается Клиенту.

3.7. После выпуска сертификата Банком Пользователь в Системе самостоятельно производит установку сертификата на свой компьютер. После выполнения данной процедуры Пользователь может использовать ключ ЭЦП для подписания документов.

3.8. При использовании Клиентом ключа ЭЦП ГосСУОК Пользователь, обладающий правом подписи, самостоятельно загружает и устанавливает специальное программное обеспечение и выполняет все необходимые действия для регистрации сертификата ГосСУОК в Банке в соответствии с инструкцией

по установке криптозащиты для Системы с сертификатом ГосСУОК (Инструкция по установке криптозащиты находится на Сайте системы в разделе «Справка» - «Установка криптозащиты»).

4. Работа в Системе

4.1. Для работы в Системе необходимо использовать один из браузеров последних версий: Internet Explorer, Opera, Google Chrome, Яндекс браузер либо Firefox.

4.2. Электронные документы перед отправкой в Банк должны быть подписаны ЭЦП Пользователя(ей) Клиента в соответствии с карточкой с образцами подписей Клиента и/или доверенностью.

4.3. Клиент обязан контролировать состояние электронных документов и документов в электронном виде:

состояние «Отправлен» у документа появляется после его отправки в Банк;

состояние «Прошел предварительный контроль» у документа появляется после проверки в Банке основных параметров документа и ЭЦП или мобильной (электронной) подписи;

состояние «Проведен» у документа появляется после его обработки Банком, у расчетного документа – при его отправке в банк получателя или отражении по счетам Банка;

состояние «Отклонен» у документа устанавливается при его отклонении Банком.

4.4. Если документ отклонен, то причина отклонения отражается на экране при просмотре соответствующей операции. При необходимости уточнения причины отклонения Пользователь связывается с Менеджером Клиента.

4.5. В течение времени обработки Банком электронных документов и документов в электронном виде Клиент контролирует текущее состояние своих счетов с помощью просмотра остатков и запроса выписки по счетам в онлайн-режиме.

4.6. По завершении времени приема Банком электронных документов и документов в электронном виде Пользователь, для обеспечения контроля, запрашивает в Системе выписку по счету. Если в полученной выписке какой-либо из переданных электронных документов или документов в электронном виде, влияющих на движение средств по счету, отсутствует, Клиент должен связаться с Менеджером Клиента для выяснения ситуации.

Окончательное состояние счетов Клиента определяется выпиской с изображением штампа Банка.

5. Работа в Мобильном приложении «BGPB Business»

5.1. Для подключения Мобильного приложения «BGPB Business» необходимо с использованием мобильного устройства с доступом в сеть Интернет загрузить из официального магазина приложений Google Play, App

Store, соответствующего операционной системе мобильного устройства (Android, iOS соответственно), Мобильное приложение «BGPB Business».

5.2. Подключение Мобильного приложения «BGPB Business» доступно только зарегистрированным в Системе Клиентам.

5.3. Для работы с Мобильным приложением «BGPB Business» необходимо использовать мобильное устройство на платформе Android версии 5 и выше, iOS версии 9.3.5 и выше, а также иметь настроенное стабильное соединение с сетью Интернет.

5.4. Реквизитами активации Мобильного приложения «BGPB Business» являются имя Пользователя (логин) и пароль доступа, используемые Клиентом для доступа в Систему. Для активации в Мобильном приложении «BGPB Business» необходимо ввести указанные реквизиты с учетом регистра клавиатуры: заглавные, строчные буквы. Для продолжения активации, Пользователь проставляет отметку, подтверждая, что он ознакомлен и согласен с Правилами обслуживания бизнес-клиентов в ОАО «Белгазпромбанк».

5.5. Для завершения активации Пользователь должен ввести код активации, который направляется Банком посредством смс-сообщения на ранее предоставленный Пользователем и зарегистрированный Банком для данного Пользователя мобильный номер. В случае ввода правильного кода активации на мобильном устройстве формируется ключ мобильной подписи (далее – ключ МП) Пользователя и сохраняется в безопасном хранилище на устройстве Пользователя.

5.6. По результатам успешной активации Пользователь задает цифровой авторизационный код. Дальнейшая работа с Мобильным приложением «BGPB Business» Пользователем обеспечивается посредством использования авторизационного кода, который применяется для входа и подтверждения операций в Мобильном приложении «BGPB Business».

6. Подписание документов в электронном виде в Мобильном приложении «BGPB Business»

6.1. Доступ к подписанию документов в электронном виде в Мобильном приложении «BGPB Business» (далее – мобильная подпись) может быть предоставлен Пользователям, подключенным к Мобильному приложению «BGPB Business» и обладающим правом единственной подписи в соответствии с карточкой с образцами подписей Клиента.

6.2. Для подключения мобильной подписи Администратор в Системе в разделе «Настройка» - «Пользователи» - «Изменить настройки пользователя» наделяет Пользователя с правом единственной подписи правом на использование мобильной подписи. Для совершения дальнейших регистрационных действий Пользователь заполняет и подписывает заявление на использование мобильной подписи в Системе своей действующей ЭЦП.

6.3. После успешной обработки заявления на использование мобильной подписи Пользователю предоставляется право совершать банковские операции,

сделки и услуги, которые реализованы в Мобильном приложении «BGPB Business», посредством подписания документов в электронном виде.

6.4. Каждый документ в электронном виде, направляемый в Банк для исполнения, снабжается мобильной подписью. Мобильная подпись формируется только в Мобильном приложении «BGPB Business» Пользователя с использованием ключа МП и авторизационного кода. Мобильная подпись обеспечивает неизменность данных документа в электронном виде и позволяет установить автора документа.

6.5. Для отключения мобильной подписи Администратор в Системе может ограничить доступ Пользователя к мобильной подписи, исключив у Пользователя право на мобильную подпись в разделе «Настройка» - «Пользователи» - «Изменить настройки пользователя».

6.6. Банк может ограничить Пользователям использование мобильной подписи на основании обращения Клиента к Менеджеру Клиента или в случаях, предусмотренных Правилами обслуживания бизнес-клиентов в ОАО «Белгазпромбанк» или законодательством.

6.7. Порядок подписания документов в электронном виде, проверки мобильной подписи на таких документах, порядок их исполнения и хранения, а также порядок формирования ключа МП устанавливаются Банком в ЛПА.

7. Партнерские сервисы

7.1. Для предоставления доступа к Партнерским сервисам Администратор устанавливает Пользователям в Системе в разделе «Настройка» - «Пользователи» - «Изменить доступ Пользователя к внешним системам» права на необходимый Партнерский сервис.

7.2. Консультацию по подключению и работе с Партнерским сервисом обеспечивает Партнер, предоставляющий сервис.

7.3. Регистрация и подключение Клиента к Партнерскому сервису осуществляется посредством:

совершения Клиентом на сайте в сети Интернет, принадлежащем Партнеру, соответствующих действий, предусмотренных Правилами обслуживания бизнес-клиентов в ОАО «Белгазпромбанк»;

установки (инсталляции) на устройство Клиента программного обеспечения, принадлежащего Партнеру, и акцепта Клиентом договора и (или) соглашения с Партнером об использовании соответствующего программного обеспечения, что влечет за собой акцепт настоящего Регламента;

установки (инсталляции) на мобильное устройство Клиента мобильного приложения, принадлежащего Партнеру, и акцепта Клиентом договора и (или) соглашения с Партнером об использовании соответствующего мобильного приложения, что влечет за собой акцепт настоящего Регламента.

8. Режим работы СДБО

8.1. Банк осуществляет круглосуточный режим приема и предварительный контроль электронных документов и документов в электронном виде Клиента.

8.2. Исполнение электронных документов и документов в электронном виде Клиента осуществляется в соответствии с режимом обслуживания Клиентов при проведении расчетно-кассовых операций, определяемым Банком в соответствии с Регламентом обслуживания Клиентов в течение банковского дня и Правилами обслуживания бизнес-клиентов в ОАО «Белгазпромбанк».

8.3. В случае необходимости Банк направляет Клиенту посредством СДБО сообщения организационного, технического и рекламного характера, а также другие электронные сообщения. Клиент обязуется эти сообщения читать, соблюдать требования, в них установленные, и учитывать при организации своей деятельности.

8.4. По вопросам технического сопровождения СДБО Пользователи по телефонам могут обращаться в службу технической поддержки Банка в соответствии с режимом работы, указанным на Сайте системы.

8.5. В случаях технического сбоя в работе СДБО Банк принимает все необходимые меры по восстановлению ее работоспособности в ближайшее время.

9. Электронные почтовые и чат сервисы ДБО

9.1. В рамках СДБО допускается использование различных сервисов электронной коммуникации (почтовые сервисы, чаты) между специалистами Банка и Пользователями, ссылки на которые размещаются на сайте Банка или в Мобильном приложении.

9.2. При использовании электронных почтовых и чат сервисов в рамках СДБО со стороны Клиентов не допускается:

9.2.1. использование ненормативной лексики, бранных, вульгарных, нецензурных, оскорбительных, ругательных или иных аналогичных слов, речевых оборотов и выражений, а равно слов, речевых оборотов и выражений, сходных с указанными выше до степени смешения;

9.2.2. распространение любого рода рекламной или иной незапрашиваемой Банком либо не связанной с совершением банковских операций, сделок и услуг, которые реализованы в СДБО, информации;

9.2.3. направление бессмысленных, крайне эмоциональных, малозначительных сообщений, повторное направление одинаковых по сути сообщений (вопросов).

9.3. Как правило, ответы на электронные сообщения направляются Банком Пользователям посредством тех же каналов и на те же адреса, с которых они поступили в Банк. В случаях указания Пользователями в электронных сообщениях дополнительных контактных данных для ответа Банк вправе их не использовать.

9.4. При использовании почтовых и чат сервисов в рамках СДБО работники Банка не вправе требовать, а Пользователи обязаны не сообщать

полные идентификаторы счетов, остатки по счетам, полные номера банковских платежных карточек, пароли и другие сведения, составляющие коммерческую и банковскую тайну. Для уточнения источника проблемы допускается использование только маскированных, неполных идентификаторов, однако с учетом сохранения возможности специалистам Банка однозначно определить контрагента и операцию, касательно которой обращается Пользователь.

9.5. Электронные почтовые и чат сервисы в рамках СДБО не являются адресом электронной почты Банка.

10. Обеспечение безопасности

10.1. Клиент при работе в Системе обязан выполнять следующие правила:

10.1.1. для обеспечения конфиденциальности данных аутентификации (логин/пароль, авторизационный код, код активации), вводимых в компьютер или устройство, которое используется для работы с СДБО, по возможности использовать устройства с работающими системами защиты, такими как:

ограничение доступа к устройству;

активное антивирусное программное обеспечение с обновленными базами данных;

система автоматического обновления операционной системы;

10.1.2. при открытии сайта СДБО убедиться, что соединение с банковским сервером происходит в защищенном режиме;

10.1.3. убедиться, что идентификационные данные соответствующего сайта СДБО удостоверены, а сертификат сайта действителен;

10.1.4. не использовать функции браузера «Автозаполнение/Сохранение страниц», а также проверить, чтобы браузер не допускал сохранения конфиденциальных страниц (SSL-page);

10.1.5. не соглашаться на предложение браузера сохранить пароль для последующего входа;

10.1.6. обеспечивать сохранность и конфиденциальность реквизитов доступа и иной информации, необходимой для доступа и совершения операций с использованием СДБО, не разглашать такую информацию другим лицам (в т.ч. друзьям, знакомым, родственникам, работникам Банка и др.);

10.1.7. не сохранять свои логин и пароль к СДБО, авторизационный код, пароль к ключу ЭЦП на компьютере/цифровом носителе и/или бумажном носителе, к которому могут иметь доступ другие лица;

10.1.8. не использовать для СДБО логин и пароль, которые уже используются для авторизации Пользователя на других сайтах;

10.1.9. использовать надежные пароли (длиной не менее 6-и символов, из не менее 2-х алфавитов);

10.1.10. изменять пароль доступа к СДБО на регулярной основе, не реже чем раз в 90 дней, либо сразу, при наступлении событий, которые могли прямо или косвенно повлиять на его конфиденциальность;

10.1.11. не оставлять компьютер или другое устройство, посредством которого осуществляется работа в СДБО, без присмотра на время открытого сеанса;

10.1.12. не передавать третьим лицам свой и не использовать чужой ключ ЭЦП или пароль ключа ЭЦП;

10.1.13. осуществлять подключение электронного ключа (носителя электронного ключа) только для подписи электронных документов и не допускать постоянного нахождения ключа ЭЦП, подключенного к компьютеру/ ноутбуку;

10.1.14. всегда выбирать пункт «Выход из системы» по окончании сеанса работы с Системой, в том числе и перед закрытием окна браузера;

10.1.15. незамедлительно уведомлять Банк об известных фактах несанкционированных Клиентом операций с настройками Пользователей, операций по счетам, доступным посредством СДБО, или фактах незаконного использования третьими лицами реквизитов доступа и иной информации Клиента, необходимой для доступа и совершения операций с использованием СДБО;

10.1.16. внимательно изучать информацию, выводимую на экране монитора, выбирать действия из предлагаемых вариантов в соответствии со своими намерениями и внимательно проверять правильность вводимой информации.

10.2. Пользователь обязан обеспечивать сохранность личного ключа ЭЦП, а также незамедлительно сообщать Менеджеру Клиента в Банк о его утере или компрометации для принятия соответствующих мер по блокировке.

10.3. При использовании Мобильного приложения Клиент обязан выполнять следующие правила:

10.3.1. для обеспечения конфиденциальности реквизитов доступа, вводимых в мобильное устройство, которое используется для работы с Мобильным приложением, по возможности использовать устройства с работающими системами защиты, такими как:

ограничение доступа к устройству;

активное антивирусное программное обеспечение с обновленными базами данных;

10.3.2. не устанавливать Мобильное приложение на устройствах с нарушенной безопасностью операционной системы (на устройствах, где получены пользователем права суперпользователя – root, jailbreak);

10.3.3. обеспечивать конфиденциальность реквизитов доступа и иной информации (в том числе авторизационного кода, кода активации), необходимой для работы с Мобильным приложением, не разглашать такую информацию третьим лицам (в том числе родственникам, знакомым, любым работникам Банка, коллегам и др.);

10.3.4. не сохранять свои логин, пароль, авторизационный код на цифровом и/или бумажном носителе, к которому могут иметь доступ третьи лица;

10.3.5. на регулярной основе изменять реквизиты доступа к мобильному устройству, посредством которого осуществляется работа с Мобильным приложением;

10.3.6. не оставлять мобильное устройство, посредством которого осуществляется работа с Мобильным приложением, без присмотра на время открытого сеанса;

10.3.7. окончание сеанса работы с Мобильным приложением «BGPB Business» всегда завершать выбором функции «Выход»;

10.3.8. незамедлительно уведомлять Банк о фактах выполнения операций, несанкционированных Пользователями Мобильного приложения, или фактах незаконного использования третьими лицами реквизитов доступа и иной информации Клиента, необходимой для доступа и совершения операций с использованием Мобильного приложения.

10.4. При пользовании Партнерскими сервисами следовать так же правилам обеспечения безопасности такого сервиса, доводимым Партнером Клиенту при подключении к каждому Партнерскому сервису.

10.5. Пользователь обязуется внимательно изучать информацию, выводимую на экран устройства, выбирать действия из предлагаемых вариантов в соответствии со своими намерениями и внимательно проверять правильность вводимой информации.

11. Приостановление и возобновление услуг СДБО

11.1. Администратор имеет полномочия приостанавливать и возобновлять права на доступ и совершение операций в отношении других Пользователей. При этом Администратором используется раздел «Настройка» - «Пользователи» Системы.

11.2. Пользователь при необходимости может самостоятельно обратиться в службу технической поддержки Банка для приостановления оказания услуг Пользователю, в том числе используя электронные почтовые и чат сервисы.

Пользователь вправе инициировать приостановление пользования Мобильным приложением, используя функцию «Удалить активацию» в Мобильном приложении «BGPB Business, либо в одностороннем порядке отказаться от использования Мобильного приложения путем его удаления со своего мобильного устройства.

11.3. В случае неактивности со стороны Пользователя в течение более 60 дней производится автоматическая деактивация Мобильного приложения «BGPB Business». Для восстановления возможности работы с Мобильным приложением «BGPB Business» Пользователю необходимо заново пройти процедуру активации Мобильного приложения «BGPB Business» в соответствии с пунктами 5.4 – 5.6 настоящего Регламента.

11.4. Если при входе в Систему или при активации (регистрации) в Мобильном приложении «BGPB Business» Пользователь 6 (шесть) раз подряд неправильно ввел пароль доступа к Системе, учетная запись Пользователя

автоматически блокируется. Для восстановления доступа Пользователю необходимо связаться со службой технической поддержки Банка.

Если при авторизации в Мобильном приложении «BGPB Business» Пользователь 3 (три) раза подряд неправильно ввел авторизационный код, то Мобильное приложение «BGPB Business» автоматически деактивируется. Для восстановления работоспособности Мобильного приложения «BGPB Business» Пользователю необходимо выполнить повторную активацию Мобильного приложения «BGPB Business» в соответствии с пунктами 5.4 – 5.6 настоящего Регламента.