**Дополнительное соглашение**

**к Договору об обмене электронными документами по системе «Интернет Банк»**

**от \_\_\_\_\_\_\_\_\_\_\_\_ г.**

г. Москва «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 201\_\_\_г.

Акционерное общество «Инвестиционный Банк «ФИНАМ», именуемое в дальнейшем «Банк», в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, именуемое в дальнейшем «Клиент», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, заключили настоящее Дополнительное соглашение к Договору об обмене электронными документами по системе «Интернет-Банк» от \_\_\_\_\_\_\_\_\_\_\_\_ г. (далее – Соглашение), определяющее порядок использования Клиентом мобильного приложения «Mobile-Банкинг».

**1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

Система «Интернет-банк (Система), Электронный документ (ЭД), Электронная подпись (ЭП), Уполномоченные лица, Компрометация ключей и иные термины и определения соответствуют терминам и определениям, указанным в Договоре «Об обмене электронными документами по системе «Интернет-Банк», заключенном между Банком и Клиентом.

1.1. *Договор* – Договор «Об обмене электронными документами по системе «Интернет Банк» заключенный между Банком и Клиентом.

1.2. *Ключ серверной подписи* — это Ключ электронной подписи Уполномоченного лица Клиента, который:

* хранится в зашифрованном виде на Мобильном устройстве Уполномоченного лица Клиента.
* доступ к Ключу серверной подписи осуществляется с помощью пароля, который создаётся Уполномоченным лицом Клиента и известен только ему. В процессе работы вместо ввода пароля при использовании Ключа серверной подписи может использоваться механизм подтверждения действий с использованием отпечатка пальца, что равносильно вводу пароля.
* ввод Уполномоченным лицом пароля к Ключу серверной подписи или использование отпечатка пальца является использованием такого Ключа серверной подписи.
* Ключ серверной подписи используется только для подписания ЭД созданных с использованием Приложения.

1.3. *Ключ проверки* – открытый ключ Серверной подписи – ключ проверки Серверной подписи, представляющий собой уникальную последовательность символов, однозначно связанную с Ключом Серверной подписи, и предназначенную для проверки подлинности Серверной подписи.

1.4. *Мобильное приложение «Mobile-Банкинг» (Приложение)* – программа, позволяющая Уполномоченным лицам Клиента осуществить доступ к Системе через Мобильные устройства, удовлетворяющие требованиям, перечисленным в разделе Системные требования.

 1.4.1. Приложение предоставляет Уполномоченным лицам выполнять следующие действия в Системе в пределах функциональных и технических возможностей, описанных в Руководстве пользователя Приложения Mobile-Банкинг для корпоративных клиентов:

* осуществлять круглосуточный доступ к Счетам;
* работать как через Приложение, так и через Систему.
* иметь доступ к Электронным документам, созданным и отправленным в Банк через Систему.

 1.4.2. Предусмотрены следующие варианты использования Приложения:

**Информационный режим** – режим Приложения, в котором доступен только просмотр информации по Счетам Клиента (текущие остатки, обороты, последние поступления, выписки), а также просмотр Распоряжений, созданных в Системе. При работе в данном режиме ответственность за предоставление прав доступа для использования Приложения Уполномоченными лицами Клиента несет Управляющий Сервисом;

**Полнофункциональный режим** — режим Приложения, в котором, помимо функций доступных в Информационном режиме, возможно создание Электронных документов и их подписание Серверной подписью, а также обмен информационными сообщениями с Банком.

1.5. *Мобильное устройство* – мобильный телефон, планшетный компьютер, "умные" часы или аналогичное мобильное устройство Уполномоченного лица Клиента, используемое для работы в Приложении.

1.6. *Одноразовый код* – информация в электронной форме, создаваемая путем формирования псевдослучайной цифровой или буквенно-цифровой последовательности символов, автоматически направляемая в виде SMS–сообщения на телефонный номер Уполномоченного лица Клиента, указанный в Заявлении по Договору об использовании Системы «Интернет Банк» (Приложение № 1 к Договору) и используемая Уполномоченным лицом Клиента для подтверждения перевода денежных средств на основании ЭД подписанного ЭП в Приложении.

1.7. *Код доступа* – секретная последовательность символов, используемая Уполномоченным лицом Клиента в целях доступа к Приложению и проведения Банком аутентификации. Код доступа не должен состоять из последовательных цифр в прямом или обратном порядке или одинаковых цифр.

1.8. *Период доступа* **–** промежуток времени с момента запуска Уполномоченным лицом Приложения на своем Мобильном устройстве до момента, когда Банк принудительно прерывает доступ в Систему. Период доступа составляет 10 (десять) минут и может быть изменен Банком в одностороннем порядке в целях безопасности и защиты информации.

1.9. *Руководство пользователя Приложения Mobile-Банкинг для корпоративных клиентов (Руководство пользователя)* – документ, в котором изложен порядок работы в Приложении, в т.ч. порядок подключения и настройки Приложения, порядок создания в Приложении и использования Серверной подписи. Руководство пользователя размещается на веб-сайте Банка в сети Интернет: <http://finambank.ru/>.

1.10. *Серверная подпись* — Электронная подпись, созданная посредством Ключа серверной подписи.

1.11. *Сертификат* – сертификат Ключа проверки серверной подписи, представляющий собой электронный документ, подтверждающий принадлежность Ключа проверки серверной подписи владельцу сертификата. Сертификат выпускается Банком в электронном виде после создания Уполномоченным лицом Клиента Ключа серверной подписи и подписания им ЭП в Системе ЭД «Заявление на выпуск сертификата ключа проверки ЭП»,.

 Сертификат может быть выпущен только для Уполномоченного лица Клиента, имеющего право подписи платежных документов согласно Договору.

 Срок действия Сертификата не превышает одного календарного года с даты его выдачи. Срок действия Сертификата не может превышать срок полномочий, предоставленных Уполномоченному лицу Клиента. По окончании срока действия Сертификат автоматически отзывается.

1.12. *Сторона* – Банк и Клиент при их совместном упоминании.

1.13*. Управляющий Сервисом* – единоличный исполнительный орган Клиента юридического лица / Индивидуальный предприниматель / лицо, занимающееся частной практикой, который имеет право на подключение и предоставление Уполномоченным лицам Информационного или Полнофункционального режима в соответствии с Приложением № 1 к настоящему Соглашению. В Руководстве пользователя к Приложению Управляющий Сервисом может именоваться: «руководителем», «ответственным сотрудником» или иным подходящим по смыслу термином.

**2. СИСТЕМНЫЕ ТРЕБОВАНИЯ К МОБИЛЬНЫМ УСТРОЙСТВАМ**

Приложение работает на Мобильных устройствах со следующими операционными системами:

* iOS (версия 8.0 и выше);
* Android (версия 4.1 и выше).

Скачивание и установку Приложения необходимо осуществить только из официальных магазинов приложений Google Play или AppStore. Разработчиком Приложения должна быть указана компания «БИФИТ».

Для работы Приложения необходим доступ к Интернету.

Для работы Приложения на "умных" часах необходимо:

* устройство с операционной системой Android (версия 6.1 и выше);
* установленная на устройстве версия Google Play Services 9.4.0 и выше;
* установленная на устройстве программа для синхронизации с "умными" часами (Android

 Wear).

Приложение запрещено к установке в случае если системная программная часть подверглась модификации, несанкционированной производителем (устройство подвергнуто процедурам «Jailbreak», получению «Root»-прав, разблокировке загрузчика, установке версий операционных систем от неофициальных разработчиков).

**3. ПРЕДМЕТ СОГЛАШЕНИЯ**

3.1. Предметом настоящего Cоглашения является использование Клиентом Приложения для обмена с Банком Электронными документами путем получения доступа к Системе через любые Мобильные устройства, удовлетворяющие требованиям, перечисленным в разделе 2 «Системные требования к Мобильным устройства» настоящего Соглашения.

3.2. Стороны признают, что применяемые в Системе и при работе Приложения средства криптографической защиты информации, обеспечивающие создание и проверку Серверной подписи, достаточны для подтверждения подлинности и авторства Электронного документа.

3.3. Стороны признают, что программные и технические средства, используемые Банком и Клиентом, являются достаточными для обеспечения информационной безопасности при обмене Электронными документами.

3.4. Стороны признают, что применяемая технология генерации, создания и хранения Ключа серверной подписи полностью исключает возможность получения прямого доступа к Ключу серверной подписи с целью его копирования, переноса на внешний носитель или использования для формирования ЭП вне Мобильного устройства без знания пароля к Ключу серверной подписи, который известен только Уполномоченному лицу Клиента (п. 1.2. Соглашения).

3.5. Стороны признают, что создание подлинной Серверной подписи в ЭД от имени Уполномоченного лица Клиента, невозможна без использования Ключа серверной подписи Уполномоченного лица Клиента, доступ к которому имеет только Уполномоченное лицо Клиента.

3.6. Стороны признают, что Электронный документ, созданный с использованием Приложения и подписанный Серверной подписью, является документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью Уполномоченных лиц Клиента.

3.7. Стороны признают, что Электронные документы, подписанные Серверной подписью с использованием Приложения, признаются надлежащим доказательством для урегулирования разногласий в соответствии с условиями Договора. Информация в электронной форме, не имеющая Серверной подписи, Электронным документом не признается и при возникновении спорных вопросов доказательственного значения не имеет.

3.8. Стороны признают в качестве единой шкалы времени при работе с Приложением Московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

3.9. Стороны признают надлежащим уведомление Клиента о совершенных операциях с использованием Приложения в порядке и сроки, установленными в разделе 4 Соглашения.

3.10. Банк взимает вознаграждение за обслуживание Клиента в Системе с использованием Приложения в размере, порядке и сроки, предусмотренные действующими Тарифами Банка.

 **4. ОБЩИЕ ПОЛОЖЕНИЯ**

4.1. Использование Клиентом Приложения возможно путем установки его на Мобильном устройстве.

4.2. Доступ к Системе с использованием Приложения доступен Клиенту 24 часа в сутки 7 дней в неделю в течение срока действия настоящего Соглашения, за исключением случаев, связанных с проведением профилактических, регламентных и аварийных работ.

4.3. Полный перечень функциональных и технических возможностей Приложения приведен в Руководстве пользователя.

4.4. . Порядок подключения и управления Клиентом Сервисом и порядок использования ЭП в Мобильном приложении «Mobile-Банкинг» приведены в Приложении № 1 к Соглашению.

4.5. Действие настоящего Соглашения распространяется на все Счета Клиента, подключенные к Системе.

4.6. Инициатором сеансов связи с использованием Приложения является Клиент.

4.7. Уполномоченные лица Клиента обязаны выполнять выход из Приложения каждый раз после завершения работы в Приложении.

4.8. Обработка Банком Распоряжений, подписанных Серверной подписью в Приложении, осуществляется в порядке и сроки, предусмотренные для Распоряжений, получаемых посредством Системы с учетом ограничения по сумме, определенные Договором банковского счета. Максимальная сумма Распоряжения, подписанного Серверной подписью в Приложении, составляет 200 000,00 (Двести тысяч) рублей.

4.9. О получении Банком ЭД, исполнении Банком ЭД, об отрицательном результате процедур приема ЭД к исполнению, об отказе в исполнении, а также об иных событиях, информирование Клиента о которых является обязательным в соответствии с Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» и Положением Банка России от 19 июня 2012 г. № 383-П «О правилах осуществления перевода денежных средств» Банк информирует Клиента не позднее дня, следующего за днем совершения операции, путем размещения информации о совершении операции в Системе в виде выписки по Счету и/или путем присвоения ЭД Клиента соответствующего статуса в соответствии с Договором. Дополнительно к указанному выше способу информирования, по отдельному заявлению Клиента, Банк вправе (при наличии технической возможности) информировать Клиента о совершении операций по Счету посредством направления СМС-сообщений или сообщений на адрес электронной почты.

4.10. В случае компрометации Ключа серверной подписи, утраты, хищения, выбытия Мобильного устройства из владения Уполномоченного лица Клиента или обнаружения факта совершения несанкционированных операций с использованием Ключа серверной подписи Клиент обязан незамедлительно, но не позднее дня, следующего за днем получения информации о совершенной операции или установления соответствующего факта уведомить Банк об этом путем предоставления на бумажном носителе письменного заявления в свободной форме подписанного Уполномоченным лицом Клиента.

4.11. Консультации по вопросам технической поддержки работы Приложения Банк осуществляет по рабочим дням (пятидневная рабочая неделя) с 10 часов 00 минут до 18 часов 30 минут по московскому времени.

**5. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

5.1. Помимо прав и обязанностей, предусмотренных разделом 4 Договора, Банк:

5.1.1. обязан обеспечить предоставление доступа Уполномоченных лиц Клиента к Системе с использованием Приложения 24 часа в сутки 7 дней в неделю;

5.1.2. приостановить доступ к Системе с использованием Приложения, путем временной блокировки доступа Клиента к Системе в случае выявления Банком признаков, свидетельствующих о противоправном использовании Приложения;

5.1.3. расторгнуть Соглашение путем выбора одного из нижеуказанных действий:

* направления Клиенту письма на бумажном носителе в произвольной форме за подписью уполномоченного лица;
* направления Клиенту уведомления в Системе за подписью уполномоченного лица.

5.1.4. вправе вносить изменения и дополнения в Руководство пользователя в одностороннем порядке.

5.2. Помимо прав и обязанностей, предусмотренных разделом 4 Договора, Клиент обязан:

5.2.1. до начала использования Приложения обеспечить ознакомление Уполномоченных лиц с рекомендациями по безопасности использования Приложения, определенными в Приложении № 2 к настоящему Соглашению;

5.2.2. хранить в тайне аутентификационную информацию (код доступа к Приложению и пароль к Ключу серверной подписи) и обеспечить сохранность Мобильного устройства и SIM-карты, с помощью которых осуществляется доступ к Приложению. Клиент обязуется принимать все возможные меры для предотвращения компрометации (несанкционированного использования) Мобильного устройства и SIM-карты;

5.2.3. уведомлять Банк о смене лиц, уполномоченных работать с Системой;

5.2.4. в случае обоснованных подозрений о компрометации Приложения или использования Приложения неустановленными третьими лицами незамедлительно принять меры для блокировки доступа к Системе через Приложение и уведомить Банк в порядке и сроки, определенные разделом 4 настоящего Соглашения. В случае самостоятельной блокировки через Приложение, Клиент также обязан уведомить об этом Банк;

5.2.5. для возобновления работы в Полнофункциональном режиме Уполномоченным лицам Клиента необходимо создать новые Ключи серверной подписи и получить Сертификаты ключа проверки серверной подписи в соответствии с порядком предусмотренным Приложением № 1 к настоящему Соглашению.

5.2.6. ежедневно проверять выписки по Счетам в Системе и статусы, присвоенные ЭД Клиента или сообщения, направленные Банком.

5.3. Клиент вправе:

5.3.1.досрочно прекращать действие Ключей серверной подписи путем направления в Банк Уведомления о прекращении действия Ключа серверной подписи и соответствующего ему Сертификата ключа проверки серверной подписи.

5.3.2. расторгнуть Соглашение путем выбора одного из нижеуказанных действий:

* направления посредством Системы в Банк ЭД «Заявление на отключение услуги» (создается автоматически при выборе услуги «Mobile-Банкинг» раздела «Управление услугами» и нажатии на кнопку «Отключить»;
* представления в Банк заявления о расторжении Соглашения.

5.4. Соглашение считается расторгнутым по истечении трех рабочих дней с момента совершения действий, указанных в п. 5.1.3. или 5.3.2.настоящего Соглашения.

5.5. Стороны несут иные обязанности, предусмотренные соответствующими приложениями и (или) соглашениями.

**6. ДЕЙСТВИЕ СОГЛАШЕНИЯ**

6.1. Соглашение вступает в силу с момента подписания его Сторонами

6.2. Расторжение Соглашения допускается по инициативе Клиента или Банка. Соглашение будет считаться расторгнутым с даты, указанной в п. 5.4. настоящего Соглашения.

6.3. Прекращение действия Соглашения не освобождает Стороны от ответственности за нарушения условий Соглашения, возникшие в течение срока его действия, а также от исполнения невыполненных обязательств.

**7. ОТВЕТСТВЕННОСТЬ СТОРОН И ЕЕ ОГРАНИЧЕНИЕ**

7.1. Ответственность за достоверность информации и подлинность Серверной подписи в ЭД несет Сторона, отправившая ЭД.

7.2. В случае утери Уполномоченным лицом Клиента контроля над Мобильным устройством или SIM-картой, с помощью которых осуществляется доступ к Приложению, равно как и нарушения конфиденциальности Кода доступа к Приложению и/или пароля к Ключу серверной подписи, у Клиента возникает существенный риск ознакомления третьих лиц с информацией о Счетах Клиента или несанкционированного списания денежных средств со Счетов.

7.3. Банк не несёт ответственности за ущерб, причиненный Клиенту в результате использования третьими лицами Ключа серверной подписи Уполномоченного лица Клиента.

7.4. Банк не несет ответственности за ущерб, причиненный Клиенту при компрометации (несанкционированном использовании) Мобильного устройства и/или SIM-карты, с помощью которых осуществляется доступ к Приложению, равно как и при компрометации Кода доступа к Приложению или пароля к Ключу серверной подписи.

7.5. Банк не несет ответственности за неисполнение или несвоевременное исполнение Распоряжения Клиента в форме Электронного документа, если таковые произошли из-за отсутствия инициативы Клиента в установлении сеанса связи с Банком.

7.6. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Приложения, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной Стороны.

7.7. Банк не несет ответственности за перебои и некачественную работу сети Интернет, каналов связи и сети электропитания.

7.8. Банк не несет ответственности за ошибки в операционной системе, в среде исполнения Java-программ и другом системном и прикладном программном обеспечении, а также за результаты работы любых других программ, которые могут повлиять на безопасность и функционирование Приложения.

7.9. Банк не несет ответственности за полные или частичные сбои и ошибки в функционировании Приложения, связанные с ошибками Уполномоченных лиц Клиента и любых других третьих лиц, допущенными Клиентом в процессе использования Приложения.

7.10. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств по Соглашению в случае возникновения обстоятельств непреодолимой силы. Обстоятельства непреодолимой силы понимаются в соответствии со статьей 401 Гражданского кодекса Российской Федерации.

7.11. Банк не несет ответственности за утечку информации по каналам связи сотового оператора.

7.12. Банк не несет ответственности в случае невозможности получения Клиентом информации через Приложение, обусловленной техническими проблемами, возникшими не по вине Банка, в том числе возникшими по вине Интернет-провайдера или оператора сотовой связи.

7.13. В случае если действия Клиента и (или) третьих лиц, использующих Электронную подпись Клиента, привели к сбоям в работе Системы, либо иным образом причинили убытки Банку, либо другим пользователям Системы, Клиент возмещает Банку и (или) другим пользователям Системы, понесенные ими убытки.

7.14. Клиент несет ответственность за наступление неблагоприятных последствий, связанных с несоблюдением обязанности по ежедневному ознакомлению с информацией о совершенных операциях.

**8. РАЗРЕШЕНИЕ СПОРОВ**

8.1. Все споры, вытекающие из Соглашения, подлежат досудебному урегулированию в соответствии с условиями Договора.

8.2. В случае возникновении конфликтных ситуаций между Клиентом и Банком при использовании Приложения, Стороны обязуются участвовать в рассмотрении споров в соответствии с разделом 5 «Урегулирование разногласий» Договора.

**9. ПРОЧИЕ УСЛОВИЯ**

9.1. Если условия Договора и условия настоящего Соглашения распространяются на одни и те же правоотношения Сторон, то при использовании Приложения приоритетными считаются условия настоящего Соглашения.

9.2. Настоящее Соглашение является неотъемлемой частью Договора и составлено в 2 (Двух) экземплярах, из них по одному экземпляру - для каждой из сторон.

**10. АДРЕСА И РЕКВИЗИТЫ СТОРОН**

|  |  |
| --- | --- |
|  **Банк** |  **Клиент** |
| Адрес: Россия, 127006 г. Москва, пер. Настасьинский, д.7, стр.2.к/с 30101810745250000604 в ГУ Банка России по ЦФО ,ОГРН 1037739001046, ИНН 7709315684, БИК 044525604. |  Адрес:  ОГРН:  ИНН: КПП:р/с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  БИК: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |

**М.П. М.П.**

*Приложение № 1 к Дополнительному соглашению к Договору об обмене электронными документами*

*по системе «Интернет Банк»*

*от\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_*

**1. Порядок подключения и управления мобильным приложением**

**«Mobile-Банкинг» АО «Банк «ФИНАМ»**

1. **Общие условия**

1.1. Банк имеет право отказать Клиенту в подключении Приложения в любом из перечисленных случаев:

* в случаях, предусмотренных действующим законодательством РФ.
* при некорректном совершении Клиентом действий при дистанционном подключении.
* при некорректном заполнении Клиентом Заявления (в случае личного визита в Банк).

1.2. Предоставление роли Управляющего Сервисом осуществляется Банком единоличному исполнительному органу Клиента - юридического лица / Индивидуальному предпринимателю / лицу, занимающемуся частной практикой, при наличии у него действующего Ключа ЭП для работы в Системе.

1.3. Для безопасного использования Приложения Клиент должен обеспечить выполнение рекомендаций, изложенных в «Памятке по безопасному использованию мобильного приложения «Mobile-Банкинг» (Приложение) АО «Банк «ФИНАМ» (Приложение № 2 к Соглашению).

**2. Подключение, настройка и отключение Приложения для использования Клиентом Приложения в «Информационном режиме»**

**2.1. Дистанционное подключение и настройка Приложения Клиентом**

2.1.1. Для доступа к Системе через Приложение Управляющему Сервисом необходимо:

* подключить Приложение и осуществить настройки Приложения в Системе в разделе «Управление услугами», выбрав услугу «Mobile-Банкинг» и нажав кнопку «Подключить»;
* выбрать Уполномоченных лиц, которым будет предоставлен доступ к Системе при помощи Приложения, указать номера мобильных телефонов Уполномоченных лиц, которым будет предоставлен доступ к Системе при помощи Приложения и нажать кнопку «Сохранить»;
* после настройки Приложения уведомить Уполномоченных лиц, которым предоставлен доступ к Системе при помощи Приложения, о необходимости установки Приложения на их Мобильные устройства.

2.1.2. Уполномоченное лицо, которому предоставлен доступ к Системе, для подключения Приложения, совершает следующие действия:

* скачивает через магазины приложений Google Play или AppStore Приложение и устанавливает его на Мобильное устройство;
* при первом входе в Приложение указывает номер телефона, на который Банком будет отправлено SMS-сообщение с кодом подтверждения и после его получения вводит полученный код подтверждения в соответствующее поле (количество неудачных попыток ввода кода подтверждения и срок его действия ограничены).
* создает Код доступа к Приложению, который будет использоваться для аутентификации в Приложении.

2.1.3. После подключения Уполномоченное лицо Клиента может работать в Приложении в Информационном режиме.

2.1.3.1. Каждый раз при входе в Приложение необходимо вводить Код доступа. При этом количество неудачных попыток ввода Кода доступа ограничено и после исчерпания попыток ввода Уполномоченному лицу необходимо повторно выполнить процедуру регистрации Приложения на Мобильном устройстве и создать новый Код доступа. Код доступа не подлежит восстановлению, поэтому при нажатии на Мобильном устройстве «Сбросить код доступа» необходимо заново осуществить регистрацию Приложения на Мобильном устройстве.

2.1.4. Изменение перечня Уполномоченных лиц, которым предоставлен доступ к услуге, их

номеров мобильных телефонов осуществляется Управляющим Сервисом дистанционнов Системе через услугу «Mobile-Банкинг» раздела «Управление услугами»:

* для изменения перечня лиц, которым предоставлен доступ к Системе при помощи Приложения, Управляющий Сервисом удаляет учетную запись и, при необходимости, создает новую учетную запись;
* для изменения номера мобильного телефона лица, которому предоставлен доступ к Системе при помощи Приложения, Управляющий Сервисом удаляет учетную запись и создает новую учетную запись с новым номером телефона;
* для отключения доступа к Приложению Управляющий Сервисом нажимает кнопку «Отключить».

2.1.5. Отключение Приложения осуществляется:

* Управляющим Сервисом Клиента дистанционно в Системе через услугу «Mobile-Банкинг» раздела «Управление услугами» путем нажатия на кнопку «Отключить».

**2.2. Подключение, настройка и отключение Приложения Клиентом при личном визите в Банк**

Клиент может подключить, настроить и отключить Приложение, обратившись в Банк и предоставив соответствующие Заявления по форме, установленной Банком.

**3. Настройка Приложения для его использования Клиентом в «Полнофункциональном режиме»**

3.1. Для работы в Полнофункциональном режиме Уполномоченное лицо Клиента, имеющее право подписи Распоряжений в Системе, посредством Приложения может дистанционно создать Ключ серверной подписи.

3.1.1. Создание Ключа серверной подписи возможно путем совершения последовательных действий, указанных в Руководстве пользователя в разделе «Создание ключа серверной подписи», после введения Кода доступа и успешного входа в Приложение.

3.1.2 Для хранения Ключа серверной подписи Уполномоченному лицу Клиента необходимо выбрать в Приложении его хранение на Мобильном устройстве и создать Пароль к Ключу серверной подписи.

Просмотр информации о таком ключе и его использование возможно только с Мобильного устройства, на котором он сохранен.

3.1.3. После создания Ключа серверной подписи Уполномоченное лицо Клиента в Системе подписывает ЭД «Заявление на выпуск сертификата ключа проверки ЭП», которое направляется в Банк на рассмотрение.

3.2. Уполномоченное лицо Клиента, на чье имя выпускается Сертификат, обязан явиться в Банк для оформления Заявления на выпуск сертификата ключа проверки ЭП в бумажном виде в случае, если у данного лица Клиента изменился документ, удостоверяющий личность.

В печатной форме Заявления на выпуск Сертификата должны быть заполнены реквизиты документа, удостоверяющего личность. Заявление на выпуск сертификата ключа проверки ЭП в бумажном виде подается в Банк в двух экземплярах и заверяется Клиентом (либо его уполномоченным лицом) и оттиском печати Клиента (при наличии печати).

3.3. Банк при получении от Клиента ЭД «Заявление на выпуск сертификата ключа проверки ЭП» осуществляет проверку соблюдения условий для выпуска Сертификата, указанных в п.3.3.1. Приложения № 1 к Соглашению, и совершает одно из нижеуказанных действий:

* выпускает Уполномоченному лицу Сертификат и активирует Ключ серверной подписи. В этом случае Уполномоченное лицо Клиента может использовать Приложение в Полнофункциональном режиме.
* отказывает Клиенту в выпуске для Уполномоченного лица Клиента Сертификата и в этом случае Уполномоченное лицо Клиента может использовать Приложение только в Информационном режиме.

3.3.1.Выпуск Сертификата осуществляется Банком при соблюдении следующих условий:

* Уполномоченное лицо Клиента, для которого выпускается соответствующий Сертификат, имеет право подписи Распоряжений согласно Договору;
* в случаях, указанных в пункте 3.2. Приложения № 1 к Соглашению, Уполномоченное лицо Клиента явилось в Банк для подтверждения личности и оформления «Заявления на выпуск сертификата ключа проверки ЭП» на бумажном носителе.

*Приложение № 2 к Дополнительному соглашению*

*к Договору об обмене электронными документами*

*по системе «Интернет Банк»*

 *от\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_*

**ПАМЯТКА**

**по безопасному использованию мобильного приложения «Mobile-Банкинг» (Приложение)**

**АО «Банк «ФИНАМ»**

 В целях повышения уровня безопасности использования Приложения, АО «Банк «ФИНАМ» рекомендует:

1. Устанавливать Приложение исключительно по ссылкам в авторизованных магазинах приложений (App Store или Google Play). Разработчиком Приложения должна быть указана компания – АО «БИФИТ».
2. Регулярно устанавливать обновления безопасности для операционной системы Вашего мобильного устройства.
3. Использовать лицензионные, постоянно обновляемые средства антивирусной защиты.
4. Использовать средства блокировки входа на Ваше мобильное устройство (Код доступа, Пин-код, TouchID, FaceID и иные).
5. Никому не сообщать Код доступа в Приложение, Пароль к Ключу серверной подписи и одноразовый SMS-код подтверждения операций. Сотрудники АО «Банк ФИНАМ» никогда не просят сообщить или ввести куда-либо конфиденциальную информацию.
6. Не хранить Код доступа в Приложение на своем мобильном устройстве в открытом виде.
7. Если у Вас есть подозрение, что Ваши реквизиты доступа в Приложение стали известны третьим лицам, в Приложении необходимо осуществить процедуру сброса Кода доступа и незамедлительно обратиться в Банк.
8. В случае потери или хищения Вашего Мобильного устройства незамедлительно сообщить об этом Банку и с помощью системы «Интернет Банк» осуществить отключение Приложения.
9. Завершать сеанс работы в Приложении сразу после проведения всех необходимых операций при помощи кнопки «Выход».
10. Не посещать с использованием Мобильного устройства, на котором установлено Приложение, сайты сомнительного содержания, а также не переходить по ссылкам и не открывать вложения из писем от подозрительных и неизвестных отправителей.
11. При получении любых сообщений или писем, связанных с работой Приложения, обращать внимание на отправителя. Подобные сообщения должны поступать только с официального номера или адреса электронной почты АО «Банк ФИНАМ».
12. Не устанавливать на Мобильное устройство, на котором используется Приложение, программное обеспечение неизвестных разработчиков, распространяемое из сторонних источников (малоизвестных сервисов распространения приложений).
13. Не использовать Приложение на Мобильных устройствах, системная программная часть которых подверглась модификации, несанкционированной производителем (устройство подвергнуто процедурам «Jailbreak», получению «Root»-прав, разблокировке загрузчика, установке версий операционных систем от неофициальных разработчиков).
14. При отсутствии необходимости, не использовать Приложение для совершения операций по Счету или совершения иных юридически значимых действий при подключении мобильного телефона к публичным сетям WiFi.