

ПУБЛИЧНАЯ ОФЕРТА НА ПОДКЛЮЧЕНИЕ ДИСТАНЦИОННОГО БАНКИНГА ДЛЯ ФИЗИЧЕСКИХ ЛИЦ/ЮРИДИЧЕСКИХ ЛИЦ

Настоящая oferta, опубликованная на сайте ЗАО «Банк Компаньон» (далее – Банк) <https://www.kompanion.kg>, является предложением Банка заключить Договор на подключение и использование Дистанционного банкинга.

Настоящая Oferta адресована физическим и юридическим лицам и является официальным публичным предложением Банка заключить Договор на подключение Дистанционного банкинга (далее «Договор», условия Договора размещены в настоящей Offerте) в соответствии с нормами гражданского законодательства Кыргызской Республики.

Договор о Предоставлении услуги Дистанционного банкинга считается заключенным и приобретает силу с момента подписания физическим или юридическим лицом заявления установленной формы, и означающего безоговорочное принятие физическим или юридическим лицом всех условий Offerты без каких-либо изъятий или ограничений на условиях присоединения.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ, ПРИМЕНЯЕМЫЕ В ДОГОВОРЕ

Интернет-банкинг - дистанционное управление Клиентом своим банковским счётом/счётами, открытым/открытыми в Банке по Генеральному договору банковского счёта. Использование системы «Интернет-банкинг» осуществляется посредством общедоступных каналов сети Интернет с использованием персонального компьютера или ноутбука и иных устройств клиента. Доступ к системе «Интернет-банкинг» осуществляется по адресу <http://www.kompanion.kg/> <https://online.kompanion.kg/login>.

Мобильный банкинг – дистанционное управление Клиентом своим банковским счётом/счётами открытым/открытыми в Банке по Генеральному договору банковского счёта. Использование системы «Мобильный банкинг» осуществляется посредством сообщений и команд, отправляемых Клиентом Банку с мобильного телефона и/или планшета и иных устройств с использованием мобильного приложения.

ОТР-ТОКЕН (далее по тексту – otp-token) – это специальное устройство, которое генерирует одноразовые пароли доступа (one-time password-ОТР) в систему «Интернет-банкинг» при каждом следующем посещении, а также обеспечивает идентификацию и аутентификацию Клиента.

Электронный платежный документ (далее по тексту - ЭПД) - дистанционное распоряжение и/или соответствующее заявление Клиента о совершении банковской операции по банковскому счёту, открытому в Банке, и/или осуществление другой операции по услугам Банка, передаваемое в Банк электронным способом, созданное и подтвержденное соответствующими идентификационными данными с использованием электронной подписи Клиента.

Электронная подпись - информация в электронной форме, которая присоединена к ЭПД и (или) логически связана с ним и которая используется для определения лица, от имени которого подписан ЭПД. ЭПД, подписанный электронной подписью Клиента, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью Клиента.

2. ПРЕДМЕТ ДОГОВОРА

2.1. Банк предоставляет Клиенту, имеющему доступ в сеть Интернет и/или соответствующее необходимое техническое оборудование, услуги по осуществлению банковских операций по счёту/счетам Клиента через системы «Интернет-Банкинг», «Мобильный Банкинг» (далее – системы дистанционного банкинга), на условиях, предусмотренных Генеральным договором счёта, на основании которого открыт счёт/счета и/или для размещения вкладов (депозитов) и/или кредитования Клиента в порядке и на условиях, предусмотренных законодательством Кыргызской Республики и/или предоставления иных услуг банка, предусмотренных условиями соответствующих договоров, заключенных с использованием электронной подписи Клиента.

2.2. Клиент оплачивает предоставляемые услуги в соответствии с тарифами Банка, действующими на момент совершения операции на условиях, предусмотренных настоящим Договором.

3. ПОРЯДОК И УСЛОВИЯ ОБСЛУЖИВАНИЯ КЛИЕНТА

3.1. В рамках настоящего Договора Клиенту могут быть предоставлены услуги в соответствии с тарифами Банка, указанными на сайте <http://www.kompanion.kg> и/или в соответствующем мобильном приложении Банка.

Указанный перечень услуг не является исчерпывающим и может быть изменен и/или дополнен Банком в одностороннем порядке путем размещения на Сайте <http://www.kompanion.kg> соответствующей информации.

3.2. Подключение Клиента к системе «Интернет-Банкинг» производится на основании письменного заявления на подключение к системе «Интернет-Банкинг» по форме Банка, в котором указывается счет/счета Клиента, подключаемые к обслуживанию через систему «Интернет-Банкинг», список ответственных сотрудников Клиента с распределением по ролям (исполнитель, верификатор, контролер и авторизатор) документы, подтверждающие полномочия указанных лиц, а также документы, удостоверяющие их личности и иные сведения по усмотрению Банка.

3.3. Обслуживание в системах дистанционного банкинга предоставляется Клиенту удаленно через сеть Интернет с помощью персонального компьютера, планшета, мобильного телефона и других устройств Клиента.

3.4. Клиент получает право на обслуживание в системах дистанционного банкинга после

заключения настоящего Договора, получения в Банке идентификационных данных для доступа в системы дистанционного банкинга и ознакомлении с Правилами пользования дистанционным банкингом (Интернет-банкинг, Мобильный банкинг), которые находятся в Приложении №1 и являются неотъемлемой частью настоящего Договора.

3.5. Стороны признают, что идентификационные данные для доступа в системы дистанционного банкинга являются аналогом электронной подписи Клиента, которая регламентируется законодательством Кыргызской Республики (далее – КР). Стороны настоящего Договора также признают, что идентификационные данные для доступа в системы дистанционного банкинга признаются равнозначными собственноручной подписи Клиента/уполномоченных лиц, указанных в карточке образцов подписей и оттиска печати Клиента.

3.6. Дополнительным средством защиты является получение одноразовых паролей на номера телефона, предоставленные клиентом или использование отпечатков пальца/face id через SMS рассылку/push уведомления и иные способы аутентификации. Вход в системы дистанционного банкинга без одноразового пароля невозможен, за исключением случаев пользования соответствующим мобильным оборудованием, с использованием номера телефона Клиента, предоставленного Банку или биометрических данных клиента. Номер телефона Клиента указывается в заявлении на подключение услуг систем дистанционного банкинга.

3.7. В случае подачи заявления на подключение к системе «Интернет-Банкинг» с возможностью осуществления денежных переводов и/или конверсионных операций для юридических лиц/индивидуальных предпринимателей необходимо приобрести otp-token.

3.8. Ответственный сотрудник Клиента с ролью «Авторизатор» должен получить otp-token, для подтверждения всех совершаемых операций, по акту приема-передачи.

3.9. С момента передачи otp-token ответственному сотруднику Клиента, любой ЭПД, подтвержденный соответствующим ОТР и полученный по системе «Интернет-Банкинг/Мобильный банкинг», считается направленным Клиентом надлежащим образом и подлежит исполнению Банком в соответствии с условиями настоящего Договора.

3.10. Стороны признают, что ЭПД Клиента о произведении операции через системы дистанционного банкинга приравниваются к распоряжениям, полученным от Клиента на бумажном носителе, оформленном в соответствии с законодательством КР.

3.11. Распоряжения или заявление Клиента о произведении операций в системах дистанционного банкинга передаются электронным способом в виде ЭПД, подтвержденного Клиентом в системе.

3.12. ЭПД исполняются Банком в рабочие дни в соответствии с Перечнем услуг и графиком обслуживания в системах дистанционного банкинга, размещенных на сайте Банка. Исполнение ЭПД, поступивших после установленного времени, будет проведено следующим операционным днем.

3.13. Расчет в безналичной форме становится безотзывным для Клиента в момент получения подтверждения о принятии платежного документа к исполнению Банком и окончательным - в момент списания средств со счета/счетов Клиента.

3.14. Банк приостанавливает/прекращает доступ в системы дистанционного банкинга в случаях:

3.14.1. закрытия счёта/счетов, подключённых к обслуживанию через системы дистанционного банкинга»;

3.14.2. выполнения 3 (трёх) подряд неудачных попыток ввода идентификационных данных (имя пользователя, пароль);

3.14.3. не оплаты услуг Банка;

3.14.4. возникновения технических неисправностей при работе с системами дистанционного банкинга;

3.14.5. смены программного обеспечения и проведения профилактических работ;

3.14.6. возникновения спорной ситуации, связанной с использованием настоящего Договора;

3.14.7. в других случаях, предусмотренных законодательством КР.

3.15. В период устранения технических проблем Клиент должен осуществлять банковские операции с предоставлением в Банк платежного документа, оформленного на бумажном носителе подписанным Клиентом. Порядок предоставления/приёма жалоб и претензий Клиента, условия их рассмотрения и решения определяются в соответствии с законодательством КР.

3.16. Номер телефона для обслуживания Клиентов: 0312 33 88 00, 8800.

3.17. Все платежи, осуществляемые посредством удаленного/дистанционного обслуживания, считаются подтвержденными и окончательными (безусловными и безотзывными) с момента завершения взаиморасчетов в соответствующей системе поставщика услуг и проведения окончательных расчетов.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Банк обязуется:

4.1.1. после оплаты Клиентом надлежащих комиссий, в соответствии с тарифами Банка, зарегистрировать Клиента в системах дистанционного банкинга, согласно заявлению Клиента по форме Банка;

4.1.2. обслуживать Клиента в системах дистанционного банкинга в порядке, предусмотренном настоящим Договором;

4.1.3. сохранять банковскую тайну об операциях, производимых по счетам Клиента, и предоставлять сведения по ним только в случаях, предусмотренных законодательством КР;

4.1.4. немедленно блокировать учётную запись Клиента по письменному заявлению Клиента или по телефонному обращению после надлежащей верификации клиента (кодовое слово и/или паспортные данные и др.);

4.1.5. принять меры для устранения возможных технических проблем в разумные сроки.

4.2. Банк имеет право:

4.2.1. производить безакцептное (без согласия Клиента) списание с любых, открытых в Банке, счетов Клиента сумм комиссий/вознаграждения Банка за предоставленные услуги в момент совершения операции в системах дистанционного банкинга, а также списание ошибочно зачисленных сумм, в случаях установления факта ошибочного зачисления денежных средств на счет/счета Клиента, сумм любой задолженности Клиента перед Банком, а также в других случаях предусмотренных законодательством КР;

4.2.2. отказать Клиенту в совершении операции в системах дистанционного банкинга в случае неполного/неверного указания Клиентом реквизитов совершаемой операции, нарушения сроков ее совершения, несоответствия совершаемой операции законодательству КР, в том числе требований законодательства КР по противодействию или легализацию (отмыванию) преступных доходов и финансированию террористической или экстремистской деятельности, в случаях недостаточности денежных средств на счете/счетах Клиента для совершения операции и/или для оплаты вознаграждения Банка за совершаемую операцию, а также в случаях, предусмотренных законодательством КР;

4.2.3. в необходимых случаях затребовать от Клиента оформления документа на бумажном носителе с подписью Клиента для осуществления операции. При этом Банк не будет производить исполнение электронного документа до момента получения документа на бумажном носителе;

4.2.4. в целях безопасности осуществления электронных платежей заблокировать доступ в системы дистанционного банкинга Клиенту, если с момента последнего обращения Клиента в Банк с использованием систем дистанционного банкинга прошло более 3(трех) месяцев. Возобновление доступа Клиента к системам дистанционного банкинга, производится по письменному заявлению Клиента;

4.2.5. устанавливать/изменять общие лимиты по операциям в системах дистанционного банкинга;

4.2.6. требовать у Клиента предоставления документов, подтверждающих законность и экономическую целесообразность операции в случаях, предусмотренных действующим законодательством КР;

4.2.7. отказать в одностороннем порядке в проведении операций по счету в случаях, предусмотренных законодательством КР;

4.2.8. в одностороннем порядке изменять условия настоящего Договора, при этом способы оповещения Клиента могут быть следующие: сообщение в системах дистанционного банкинга или путем направления письменного уведомления. В случае изменения Банком условий оферты, изменения вступают в силу с момента размещения измененных условий оферты на сайте <https://www.companion.kg>, если иной срок не указан Банком при таком размещении;

4.2.9. в одностороннем порядке расторгнуть настоящий Договор в случаях,

предусмотренных законодательством КР.

4.3. Клиент обязан:

4.3.1. обеспечить наличие у себя программно-технических средств, обеспечивающих возможность выхода в Интернет;

4.3.2. соблюдать и руководствоваться Правилами пользования дистанционным банкингом (Интернет-банкинг, Мобильный банкинг) для Клиента при работе в системах дистанционного банкинга, установленными в Приложении №1;

4.3.3. проверять после отправки ЭПД факт получения и исполнения Банком переданных ЭПД. При не подтверждении факта получения и/или исполнения - обращаться с запросом в Банк для выяснения причины, по которой данный ЭПД не получен и/или не исполнен Банком;

4.3.4. при проведении обмена ЭПД применять системы обработки, хранения и защиты информации только на исправном и проверенном на отсутствие компьютерных вирусов персональном компьютере;

4.3.5. обеспечить конфиденциальность при использовании идентификационных данных (имя пользователя, пароль);

4.3.6. немедленно сообщать Банку об обнаружении несанкционированного доступа либо попытки несанкционированного доступа, а также о случаях утери, хищений идентификационных данных Клиента, изменения/утери номера;

4.3.7. не использовать предоставляемые Банком услуги в противозаконных целях, в том числе не осуществлять действия/операции, направленные на осуществление деятельности по легализации (отмыванию) преступных доходов и финансированию террористической или экстремистской деятельности;

4.3.8. по требованию Банка предоставить в течение 3 (трех) рабочих дней документы, подтверждающие законность и экономическую целесообразность операции/операций в соответствии с требованиями законодательства КР.

4.4. Клиент вправе:

4.4.1. пользоваться услугами в порядке и на условиях, предусмотренных настоящим Договором;

4.4.2. обращаться в Банк с требованием о блокировании идентификационных данных Клиента (имени пользователя, пароля) в случаях обнаружения несанкционированного доступа либо попытки несанкционированного доступа в системы дистанционного банкинга;

4.4.3. при необходимости получать в Банке подтверждение на бумажном носителе (заверенные копии) исполнения платежных поручений по банковским операциям, произведенным по системам дистанционного банкинга и выписок по счёту/счётам за необходимый период;

4.4.4. за консультирование по правилам работы систем дистанционного банкинга по

запросу Клиента с выездом специалиста Банка к Клиенту взимается плата в размере, установленном тарифами Банка. Вызов осуществляется заявкой Клиента, оформленной в письменном виде и переданной по электронной почте, почте, факсу или лично;

4.4.5. на основании заявления установить суточные лимиты и лимиты на одну операцию в пределах общих лимитов, установленных Банком;

4.4.6. изменять идентификационные данные (имя пользователя, пароль).

5. ПОРЯДОК ОПЛАТЫ УСЛУГ

5.1. Клиент обязуется оплачивать услуги Банка, согласно действующим тарифам Банка, если иное не предусмотрено дополнительным соглашением к настоящему Договору. Тарифы размещаются на информационных стендах в операционных залах и на сайте Банка.

5.2. Банк может изменить тарифы в одностороннем порядке. Измененные тарифы доводятся до Клиента не менее чем за 30 (тридцать) календарных дней до вступления их в силу путем размещения их на информационных стендах в операционных залах и на сайте Банка или информационным уведомлением в системах дистанционного банкинга.

5.3. Оплата услуг Банка по настоящему Договору производится путем безакцептного списания денежных средств с любого/любых счета/счетов Клиента. Банк имеет право использовать денежные средства на любом из счетов Клиента с конвертацией их по курсу покупки Банка соответствующей валюты для оплаты услуг за проведение операций Клиента.

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Клиент несет ответственность за сохранность и обеспечение конфиденциальности средств доступа в системы дистанционного банкинга (имя пользователя, пароль, OTP-token), за убытки, возникшие в результате несанкционированного использования средств доступа, а также за неисполнение/ненадлежащее исполнение условий настоящего Договора.

6.2. Клиент несет ответственность за соблюдение правил по использованию платежных инструментов и порядка оформления платежных документов в соответствии с законодательством КР.

6.3. Клиент несет риск и ответственность за невыполнение или ненадлежащее выполнение установленных мер безопасности и конфиденциальности, а также Правил пользования дистанционным банкингом (Интернет-банкинг, Мобильный банкинг) (Приложение №1).

6.3.1. Клиент несет ответственность за все операции, проведенные в период с момента утери номера телефона и/или идентификационных данных (имя пользователя, пароль), до момента обращения Клиента в Банк с целью блокировки доступа в системы дистанционного банкинга.

6.4. Стороны освобождаются от ответственности на период действия обстоятельств непреодолимой силы (форс-мажор). Сторона, ссылающаяся на форс-мажорные обстоятельства, обязана уведомить другую Сторону в письменном виде не позднее 10 (десяти) рабочих дней со дня наступления таких обстоятельств, с предоставлением подтверждающего документа, выпущенного компетентным государственным органом.

6.5. Банк не несет ответственность:

6.5.1. за неисправность и/или безопасность: оборудования, программного обеспечения Клиента, коммуникаций в каналах связи, за средства и услуги, обеспечиваемые третьей стороной (провайдер доступа к Интернету и пр.);

6.5.2. за невыполнение или ненадлежащее выполнение Клиентом установленных мер безопасности и конфиденциальности, а также Правил пользования дистанционным банкингом (Интернет-Банкинг, Мобильный банкинг) (Приложение №1);

6.5.3. за невыполнение указаний Клиента с использованием систем дистанционного банкинга, если на счет Клиента был наложен арест или операции по нему были приостановлены Клиентом в порядке, предусмотренном настоящим Договором, Генеральным договором счета и/или в соответствии с законодательством КР;

6.5.4. за получение неуполномоченным лицом информации, если данная информация была отправлена Банком на электронный адрес, указанный Клиентом в заявлении, а также за изменение Клиентом электронного адреса для получения информации, без уведомления Банка;

6.6. Во всем ином, что не предусмотрено настоящим Договором, Стороны несут ответственность в соответствии с Генеральным договором счета и законодательством КР.

7. СРОК ДЕЙСТВИЯ ДОГОВОРА

7.1. Настоящий Договор действует до его расторжения путем письменного обращения Клиента в Банк, или до даты расторжения Генерального договора банковского счета.

7.2. Стороны вправе расторгнуть настоящий Договор в одностороннем порядке, уведомив об этом другую Сторону в письменной форме не менее чем за 10 (десять) рабочих дней до даты его расторжения, с обязательным выполнением всех обязательств и взаиморасчетов по настоящему Договору.

8. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

8.1. Любые споры, возникающие по настоящему Договору разрешаются путем переговоров.

8.2. В случае невозможности разрешения споров путем переговоров, споры разрешаются в соответствии с законодательством КР.

9. ПРОЧИЕ УСЛОВИЯ

9.1. Стороны признают, что любые уведомления, корреспонденция и т.д. считаются доставленными, если направлены по адресам, указанным в настоящем Договоре. В случае изменения - по адресу, указанному в письменном уведомлении.

9.2. Стороны признают, что используемые ими по настоящему Договору системы дистанционного банкинга являются достаточными для обеспечения надежной и эффективной работы при обработке, хранении, приеме и передаче информации.

9.3. Стороны признают используемую технологию достаточной для защиты от несанкционированного доступа, а также для подтверждения подлинности ЭПД.

9.4. Стороны признают, что при утере, хищении, передаче третьим лицам или использовании третьими лицами идентификационных данных или устройств доступа, вся ответственность за несанкционированный доступ к системе ложиться на Клиента.

Во всем ином, не предусмотренном настоящим Договором, Стороны руководствуются Генеральным договором счета и/или законодательством КР.

10. РЕКВИЗИТЫ БАНКА

ЗАО «Банк Компаньон»

Адрес: 720044, Кыргызская Республика

г.Бишкек, ул.Шота Руставели, 62

БИК: 113001

ОКПО: 23672096

ИНН: 01210200410119

Приложение №1

**к Договору на подключение дистанционного банкинга
(Интернет-Банкинг) для физических лиц/юридических лиц - публичная оферта**

**ПРАВИЛА ПОЛЬЗОВАНИЯ ДИСТАНЦИОННЫМ БАНКИНГОМ
(ИНТЕРНЕТ-БАНКИНГ, МОБИЛЬНЫЙ БАНКИНГ)
для физических лиц/юридических лиц**

1. Требования при работе:

- 1.1. обеспечить режим конфиденциальности в отношении нахождения рабочего места Клиента для работы в системах дистанционного банкинга, средств OTP или сертификатов безопасности Клиента, логинов и паролей к операционной системе рабочего места Клиента;
- 1.2. после окончания работы в системах дистанционного банкинга корректно завершать работу с использованием программной кнопки «Выход»;
- 1.3. отключить в операционной системе рабочего места Клиента для работы в системах дистанционного банкинга функцию автозапуска съемных носителей информации;
- 1.4. подключать рабочее место Клиента для работы в системах дистанционного банкинга к сети Интернет только во время работ с системами дистанционного банкинга;
- 1.5. перед входом в личный кабинет убедиться, что защищенное соединение по протоколу [https](https://kompanion.kg) установлено именно с официальным сайтом Банка (<https://kompanion.kg>);
- 1.6. обеспечить у пользователей системы на рабочем месте наличие учетной записи в операционной системе, защищенной паролем;
- 1.7. не сохранять пароль в текстовых файлах на компьютере, либо на других носителях информации;
- 1.8. никогда ни при каких обстоятельствах не сообщать никому пароль – он не требуется сотрудникам Банка и службе технической поддержки для вашего подключения, обслуживания и поддержки сервиса в работоспособном состоянии;
- 1.9. не использовать рабочее место Клиента для подключения к социальным сетям в сети Интернет, к форумам, конференциям, чатам, телефонным сервисам и иным сайтам, содержащим потенциально вредоносные программы, а также для чтения почты и открытие почтовых документов от адресатов, не заслуживающих доверия;
- 1.10. не раскрывать логины и пароли третьим лицам, включая сотрудников Банка (в том числе при обращении неустановленных лиц от имени Банка по телефону, электронной почте, через SMS);
- 1.11. не сохранять логины и пароли в текстовых файлах на жестком диске рабочего места Клиента, либо на других электронных носителях информации.

2. Рекомендации при работе:

- 2.1. использовать для работы с системами дистанционного банкинга выделенное рабочее место Клиента, не используемое Клиентом в других целях;

- 2.2. обеспечить функционирование на рабочем месте Клиента лицензионной (не контрафактной) операционной системы Microsoft Windows XP/2003/Vista/7, Apple Macintosh Mac OS X или старше, Linux, Android, iOS и ее своевременное обновление согласно рекомендациям компании-разработчика в целях устранения, выявленных в ней уязвимостей, позволяющих получить доступ к конфиденциальной информации;
- 2.3. обеспечить функционирование на рабочем месте Клиента лицензионного (не контрафактного) антивирусного программного обеспечения и его своевременное обновление согласно рекомендациям компании-разработчика в целях недопущения заражения рабочего места Клиента вредоносным программным обеспечением, способным предоставить доступ к системам дистанционного банкинга Клиента неуполномоченным третьим лицам;
- 2.4. обеспечить функционирование на рабочем месте Клиента лицензионного (не контрафактного) программного обеспечения «брандмауэр (firewall)» в режиме блокирования несанкционированного удаленного доступа к рабочему месту из сети Интернет и локальной сети Клиента;
- 2.5. ограничить доступ к рабочему месту Клиента/где будет использоваться OTP на рабочем месте клиента и обеспечить наличие минимальных прав для изменения конфигурации операционной системы рабочего места Клиента (наличие прав администратора нежелательно);
- 2.6. не работать в системах дистанционного банкинга в сети Интернет, используя источник подключения из мест, не заслуживающих доверия (интернет-кафе), или используя общественные каналы связи (бесплатный Wi-Fi и т.п.);
- 2.7. обращать внимание на любые изменения и ошибки программного обеспечения во время установления соединения в системах дистанционного банкинга Банка или в работе систем дистанционного банкинга, при возникновении любых сомнений в правильности работы дистанционного банкинга незамедлительно прекратить работу и обратиться в Банк в целях установления отсутствия/наличия несанкционированных операций,
- 2.8. переходить на <https://www.online.kompanion.kg> / только по ссылке с официального сайта Банка (www.kompanion.kg);
- 2.9. осуществлять скачивание мобильного приложения только с PlayMarket или AppStore;
- 2.10. в случае появления предупреждений браузера о перенаправлении на другой сайт при подключении к системам дистанционного банкинга, отложить совершение операций и обратиться в службу технической поддержки Банка в целях установления причине перенаправления.
- 2.11. сообщать уполномоченным сотрудникам Банка о любых попытках узнать пароль в системы дистанционного банкинга;
- 2.12. регулярно проверять историю операций и выписки для отслеживания ошибок или неавторизированных операций по счету;

- 2.13. покидать сайт, где осуществляются электронные операции, даже если персональный компьютер и/или иное любое оборудование оставлено без присмотра на короткий срок;
- 2.14. выходить из системы после осуществления электронных операций; перед осуществлением любых онлайн операций или предоставление личной информации должен убедиться, что используется правильная веб-страница или приложение систем дистанционного банкинга. Необходимо остерегаться фальшивых веб-страниц, мобильных приложений созданных в целях мошенничества;
- 2.15. перед входом в систему, убедиться в безопасности веб-страницы, проверив наличие Унифицированных Указателей Ресурсов (URL), которые должны начинаться с «https», а на статусе интернет-браузера должен появиться знак защищенного соединения;
- 2.16. Не исполнение вышеперечисленных требования и рекомендаций Клиентом, будет являться основанием для возложения ответственности за оспариваемые операции посредством систем дистанционного банкинга на Клиента.