Приложение № 4
к Правилам комплексного банковского
обслуживания физических лиц
в «Банк Кремлевский» ООО

ОБЩИЕ УСЛОВИЯ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ФИЗИЧЕСКИХ ЛИЦ В «БАНК КРЕМЛЕВСКИЙ» ООО

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Авторизация − процедура идентификации Клиента с целью получения Банком подтверждения возможности предоставления Клиенту информации по Счету в Системе, совершения других действий в рамках Договора в порядке, предусмотренном настоящими Условиями.

Аналог собственноручной подписи (АСП) − персональный идентификатор Клиента, являющийся контрольным параметром правильности составления всех обязательных реквизитов платежного документа, Заявления и неизменности их содержания.

Договор о предоставлении дистанционного банковского обслуживания (Договор) − договор между Банком и Клиентом о предоставлении дистанционного банковского обслуживания, заключенный путем присоединения Клиента к Общим условиям дистанционного банковского обслуживания физических лиц в «Банк Кремлевский» ООО, далее - Условия дистанционного банковского обслуживания физических лиц, включающий в себя в качестве составных и неотъемлемых частей Общие условия дистанционного банковского обслуживания физических лиц в «Банк Кремлевский» ООО с использованием системы дистанционного банковского обслуживания физических лиц («Интернет-банк/Мобильный банк»), Заявление на присоединение к Условиям дистанционного банковского обслуживания физических лиц и Тарифы, являющийся в соответствии со статьей 428 Гражданского кодекса Российской Федерации Договором присоединения. Договор присоединения считается заключенным со дня регистрации Клиента в Системе.

Документ, подписанный АСП (ДПАСП) − документ, созданный в системе дистанционного банковского обслуживания физических лиц («Интернет-банк/Мобильный банк»), подписанный аналогом собственноручной подписи, переданный Клиентом Банку по Каналам доступа с прохождением определенной Банком процедуры приема- передачи. Клиент признает, что ДПАСП, сформированный и переданный в соответствии с настоящими Условиями, имеет равную юридическую силу и влечет такие же правовые последствия, что и документ, оформленный на бумажном носителе и подписанный собственноручной подписью Клиента.

Журнал аудита − список всех событий, произошедших и зафиксированных Системой в электронном виде с указанием даты и времени происхождения события, типа события и других атрибутов в зависимости от типа события.

Заявление − Заявление физического лица (Клиента) по форме Банка на присоединение к Условиям дистанционного банковского обслуживания физических лиц. Оформляется при обращении клиента в Банк с целью предоставления доступа к Системе. Стороны признают юридическую значимость Заявления, поступившего по электронным каналам связи, в т.ч. по сети Интернет через Систему в электронной форме, подтвержденные Клиентом АСП.

Интернет-банк − канал доступа, позволяющий Клиентам получать банковские и сопутствующие им услуги, доступные в Системе дистанционного банковского обслуживания физических лиц («Интернет-банк/Мобильный банк»), посредством сети Интернет.

Канал доступа − совокупность программных и/или технических средств, обеспечивающих обмен информацией между Клиентом и Банком, к каналам доступа относятся Интернет-банк и Мобильный Банк.

Кодовое слово – определенная Клиентом комбинация букв русского алфавита и цифр (цифры указываются по желанию Клиента), сообщение которого по телефону или иному средству связи сотруднику Банка признается надлежащим подтверждением того, что соответствующее физическое лицо является Клиентом и имеет право на получение информации, составляющей банковскую тайну такого Клиента, а также используемое Клиентом:

- для блокирования своей работы в Системе ДБО;
- для предоставления Банком Клиенту (по запросам Клиента информации обо всех счетах Клиента, открытых в Банке;
- для предоставления Банком Клиенту возможности в случаях и порядке, предусмотренных Правилами комплексного банковского обслуживания, приложениями к ним, использовать Кодовое слово как средство аутентификации Клиента в рамках идентификации Клиента по телефону, в том числе при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.

Клиент несет полную ответственность за разглашение Кодового слова, а также за последствия такого разглашения.

Контактные данные − полученный от Клиента и зарегистрированный в Системе номер мобильного телефона (и соответствующий ему уникальный номер SIM-карты), электронный почтовый ящик (e-mail), иные данные Клиента, позволяющие Банку проинформировать Клиента о совершенных в Системе операциях.

Мобильный банк − канал доступа, позволяющий Клиентам получать банковские и сопутствующие им услуги, доступные в Системе, посредством использования мобильного устройства (смартфона, планшетного компьютера и т.п.), сети Интернет и соответствующего Приложения.

Несанкционированная операция − Операция, совершенная без согласия Клиента на её совершение.

Номер банковской карты − уникальный цифровой номер на лицевой стороне банковской карты.

Пароль − средство авторизации в виде секретной (известной только Клиенту) комбинации символов, соответствующей присвоенному Клиенту Логину. Первоначальный пароль присваивается Клиенту в момент регистрации Клиента в Системе и в дальнейшем должен быть Клиентом изменен.

Платежная инструкция (ПИ) − предварительно определенная процедура, которая устанавливает порядок формирования и обработки распоряжения Клиента на совершение операции по его платежным картам. ПИ предназначены для автоматизации формирования ДПАСП.

Приложение − программное обеспечение для Устройства доступа, позволяющее Клиенту получать банковские и сопутствующие им услуги в канале Мобильный банк. Приложение самостоятельно устанавливается Клиентом на Устройство доступа с сайтов сети Интернет www.itunes.apple.com, www.play.google.com.

Одноразовый ключ (ОК) − одноразовый ключ представляет собой уникальную последовательность цифр, созданную генератором одноразовых ключей или Системой с целью формирования Клиентом аналога собственноручной подписи или дополнительного средства Авторизации Клиента в Системе. Одноразовые ключи, созданные Системой, предоставляются Клиенту sms-сообщением на номер мобильного телефона Клиента, зарегистрированного в Системе, или push-уведомлением на мобильное устройство Клиента, зарегистрированное в Системе.

Система / Система ДБО (система дистанционного банковского обслуживания физических лиц «Интернет-банк/Мобильный банк») − комплекс программно-аппаратных средств, предназначенный для дистанционного управления Счетом. Система является электронным средством платежа для формирования, обработки, хранения, передачи и защиты ДПАСП.

Средство авторизации в Системе − Уникальное имя Клиента, пароль, одноразовый ключ.

Стороны − Банк и Клиент.

Условия − настоящие Общие Условия дистанционного банковского обслуживания физических лиц в «Банк Кремлевский» ООО.

Правила безопасности − Правила безопасности при работе в системе дистанционного банковского обслуживания физических лиц («Интернет банк»/«Мобильный банк»).

Уникальное имя клиента (Логин) − уникальное имя Клиента в Системе, которое присваивается Клиенту в момент первоначальной регистрации в Системе и в дальнейшем может быть Клиентом изменено.

Устройство доступа − устройство, с помощью которого Клиент осуществляет обмен данными с Системой при передаче ДПАСП по Каналу доступа.

Push-уведомление - это уведомление, направляемое Банком на мобильное устройство Клиента, которое может содержать текстовую и/или графическую информацию для автоматической обработки приложением или отображения Клиенту (в том числе одноразовый код, новости и предложения Банка и иную информацию).

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Общие условия являются типовыми для всех физических лиц, определяют положения Договора предоставления Клиенту дистанционного банковского обслуживания с использованием Системы ДБО (далее - Договор).

2.2. Заключение Договора осуществляется путем присоединения Клиента к Общим условиям в целом в соответствии с п.п. 1 ст. 428 Гражданского кодекса Российской Федерации. Присоединение Клиента к Условиям осуществляется одним из указанных ниже способов:

- предоставление в Банк подписанного Клиентом Заявление (Приложение № 1 к Правилам комплексного банковского обслуживания физических лиц в «Банк Кремлевский» ООО);
- предоставление в Банк посредством сети Интернет Заявление в виде электронного документа, подписанного специальным кодом, созданным с использованием Системы и переданный Банком на номер мобильного телефона Клиента. Подписанное Клиентом Заявление является офертой Клиента Банку заключить Договор. Действия Банка по регистрации Клиента в Системе являются акцептом оферты Клиента по заключению Договора. Договор считается заключенным с момента регистрации Клиента в Системе.

2.3. В соответствии с п. 3 ст. 847 Гражданского Кодекса Российской Федерации Стороны в рамках настоящего Договора признают в качестве АСП пароль, сформированный Клиентом или Системой.

2.4. При заключении Договора Клиент предоставляет Банку заверения о следующих обстоятельствах:

- все проводимые операции в соответствии с Договором, носят добросовестный характер, осуществляются не в целях придания правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления, не осуществляются в целях иной противоправной деятельности, не направлены на финансирование организаций или лиц, деятельность которых запрещена законодательством Российской Федерации либо

иностранным законодательством, не связаны с получением ненадлежащей налоговой выгоды или иными противоправными действиями или злоупотреблениями правами;

- вся информация, предоставленная Клиентом Банку в связи с заключением и исполнением Договора, соответствует действительности, является полной и точной во всех отношениях, и Клиент не скрывает никаких фактов, которые, если бы они были известны Банку, могли бы оказать неблагоприятное влияние на решение Банка о заключении и исполнении соответствующей сделки;

- информация и документы, предоставленные Клиентом Банку в связи с заключением Договора, а также информация и документы, которые будут предоставлены Клиентом Банку в процессе исполнения указанной сделки, получены Клиентом на законных основаниях и для их предоставления Банку Клиентом получены все предусмотренные применимым законодательством согласия и разрешения третьих лиц, в том числе согласия физических лиц, персональные данные которых содержатся в указанной информации и документах, на передачу Клиентом этих персональных данных Банку и их обработку Банком и третьими лицами.

3. ПРЕДОСТАВЛЕНИЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

3.1. Банк предоставляет Клиенту доступ к Системе при наличии технической возможности. Услуги Системы включают в себя предоставление информации Клиенту о состоянии его Счетов и перечне услуг Банка, а также направление в Банк ДПАСП, в том числе:

- получение сообщений от Банка, в том числе в формате временных паролей для подтверждения операций по ДПАСП;
- получение услуг Банка, а также иной информации о Банке и его партнерах, которая может быть интересна Клиенту;
- внутрибанковские переводы, в том числе между счетами Клиента;
- оплата услуг в пользу третьих лиц;
- операции по Счету (просмотр операций по Счету, / блокировка банковской карты / формирование и печать выписки по Счету / осуществление безналичных переводов со Счета). Совершение операций по Счету посредством Системы определяется также действующими условиями Договора текущего банковского счета/Договора текущего банковского счета с использованием банковской карты и наличием технической возможности;
- получение информации об ДПАСП, которая включает в себя любую информацию об исполнении Банком ДПАСП, необходимую для его исполнения, информацию об отмене ПАСП, информацию об отказе Банка в исполнении ДПАСП;
- прием и исполнение ДПАСП.

3.2. Клиент может самостоятельно зарегистрироваться в Системе, получить Логин и Пароль на официальном интернет-сайте Системы https://elf.faktura.ru/elf/app/?site=kremlevsky (при наличии технической возможности).

3.3. Предоставление Клиенту доступа к Системе сопровождается передачей Клиенту Пароля SMS сообщением на указанный в Заявлении номер мобильного телефона.

3.4. Авторизация Клиента в Системе, отправка ДПАСП в Банк, а также иные действия осуществляются по следующим Каналам доступа, поддерживаемым Системой:

- Интернет-банк;
- Мобильный банк.

3.5. Действия Клиента в Системе – отправка ДПАСП, Авторизация, результаты проверки ДПАСП, а также иные действия фиксируются в Журнале аудита. Журнал аудита ведется Системой в одном экземпляре в электронном виде на оборудовании Банка.

3.6. Стороны признают, что Журнал аудита является достаточным доказательством и может использоваться Банком в качестве подтверждения действий Клиента в Системе, в том числе извлечения из него могут предъявляться суду в качестве доказательства факта передачи Клиентом ДПАСП, а также фактов совершения Клиентом других операций посредством Системы, зафиксированных в Журнале аудита.

3.7. Стороны признают, что ДПАСП, соответствующий требованиям, изложенным в п. 8.2 настоящих Условий, равнозначен по своей юридической силе подписанным Клиентом документам на бумажном носителе, оформленным в соответствии с требованиями настоящих Условий и действующего законодательства Российской Федерации, нормативных актов Банка России, действующими в отношении таких документов.

3.8. Стороны признают, что посредством Системы также возможно заключение между Сторонами соглашений путем направления Клиентом ДПАСП, являющегося акцептом (согласием) Клиента на оферту (предложение) Банка. В этом случае Стороны могут распространить действие Условий на заключенное таким образом соглашение, прямо указав на это в тексте оферты или акцепта.

3.9. Стороны соглашаются с тем, что информирование Клиента о совершенных в Системе операциях (изменение статуса ДПАСП) осуществляется следующими способами:

- уведомлением Клиента с помощью SMS-уведомления и/или Push-уведомления;
- изменением Банком статуса ДПАСП, просмотр статуса ДПАСП доступен Клиенту после прохождения процедуры Авторизации:
- на официальном интернет-сайте Системы https://elf.faktura.ru/elf/app/?site=kremlevsky, в разделе «История операций»;
- в Приложении, в разделе «История»;
- предоставлением в Банке информации об операциях.

3.10. Банк осуществляет переводы денежных средств по поручению Клиента в рабочий день получения ДПАСП, если документ получен до 16.00 часов, в пятницу и предпраздничные дни – до 14.00 часов московского времени, либо не позднее следующего рабочего дня, если ДПАСП получен после указанного времени.

Прием ДПАСП от Клиента осуществляется Банком круглосуточно, за исключением перерывов связанных с проведением технических работ, информирование о которых осуществляется дополнительно на официальном сайте Банка http://kremlinbank.ru.

3.11. Банк информирует Клиентов о мерах безопасности при работе в ДБО, рисках Клиента и возможных последствиях для Клиента в случае несоблюдения им мер информационной безопасности, рекомендованных Банком. Информирование осуществляется на сайте Банка и/или в подразделениях Банка, и/или путем отправки SMS-сообщений на номер мобильного телефона Клиента, зарегистрированный для доступа к Мобильному банку, и/или Push-уведомлений на Мобильное устройство Клиента с установленным Приложением, в Системе, и/или иными способами, установленным в ДБО.

4. СРЕДСТВА АВТОРИЗАЦИИ

4.1. С целью повышения уровня безопасности Банк вправе по своему усмотрению запрашивать для Авторизации любую комбинацию Средств авторизации. При несогласии Клиента на изменение установленной ранее комбинации Средств авторизации Банк имеет право прекратить или частично приостановить доступ Клиента к Системе по одному или нескольким Каналам доступа, предварительно уведомив об этом Клиента по доступным каналам связи.

4.2. Клиент вправе в любое время самостоятельно изменить значение Средства авторизации в соответствии с предоставленными Системой возможностями. Запрос на изменение значения Средства авторизации должен быть подтвержден при помощи АСП и может быть передан в Банк Клиентом с использованием одного из Каналов доступа.

4.3. Средство авторизации по требованию Клиента может быть заблокировано по телефону 8(499)241- 88-14, в Системе, в Банке, при условии, что Банк может установить, что требование о блокировке Средств авторизации исходит от Клиента (проверка кодового слова или по иным ранее установленным Банком каналам связи с Клиентом).

4.4. Уникальное имя клиента может быть предоставлено Клиенту в Системе при условии, что Банк может установить, что требование о предоставлении Уникального имени исходит от Клиента (проверка кодового слова или по иным ранее установленным Банком каналам связи с Клиентом).

4.5. Первоначальный пароль может быть предоставлен Клиенту в Системе при условии, что Банк может установить, что требование о предоставлении первоначального Пароля исходит от Клиента (проверка кодового слова или по иным ранее установленным Банком каналам связи с Клиентом).

4.6. Банк вправе в одностороннем порядке устанавливать и/ или изменять срок действия Пароля.

5. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

5.1. В случае утраты Средства авторизации и (или) его использования без согласия Клиента, Клиент обязан заблокировать Средство авторизации незамедлительно после обнаружения факта утраты Средства авторизации и (или) его использования без согласия Клиента, но не позднее даты, следующей за датой получения от Банка уведомления в соответствии с п. 3.9 настоящих Условий, об исполнении или отказе в исполнении ДПАСП, подтвержденного скомпрометированными Средствами авторизации.

5.2. Клиент обязан сообщить в Банк незамедлительно после обнаружения, но не позднее даты, следующей за датой информирования Клиента об исполнении или отказе в исполнении ДПАСП в соответствии с п. 3.9 настоящих Условий, о фактах ошибочно списанных или зачисленных сумм, либо ином ненадлежащем исполнении (неисполнении) Банком ДПАСП. При отсутствии возражений от Клиента надлежащее исполнение ДПАСП считается подтвержденным Клиентом.

5.3. Клиент обязан ежедневно самостоятельно контролировать исполнение Банком ДПАСП. При несогласии с исполненным ДПАСП Клиент должен обратиться в Банк с письменным заявлением, составленным по форме, установленной Банком, и подписанным Клиентом. По истечении 30 (тридцати) календарных дней с даты исполнения ДПАСП Банк имеет право не принимать претензию Клиента.

5.4. Клиент проинформирован и соглашается с тем, что использование дистанционного банковского обслуживания через сеть Интернет связано с рисками:

- получение несанкционированного доступа к конфиденциальной информации третьими лицами;
- компрометации Средств авторизации Клиента;
- иные риски мошеннических действий третьих лиц.

5.5. Для минимизации рисков, указанных Банком в п. 5.4 настоящих Условий, Клиент обязан выполнять требования Банка, изложенные в Правилах безопасности при работе в системе дистанционного банковского обслуживания физических лиц «Интернет-банк/Мобильный банк» (далее - Правила безопасности) (Приложение № 1 к настоящим Условиям), и соблюдать «Меры безопасности», опубликованные на сайте Банка (https://www.kremlinbank.ru/private/plastic-card/security-card/).

5.6. До заключения Договора Клиент обязан ознакомиться с Правилами безопасности.

5.7. Клиент обязуется предпринимать все необходимые меры для исполнения Правил безопасности. При этом Клиент обязуется самостоятельно отслеживать изменения данных Правил безопасности, размещенных на сайте Банка в разделе «Меры безопасности» (https://www.kremlinbank.ru/private/plastic-card/security-card/).

5.8. Настоящим Клиент соглашается, что невыполнение Правил безопасности является нарушением порядка использования Системы и может повлечь за собой совершение операции без согласия Клиента. Банк не несет ответственности за убытки, возникшие вследствие неисполнения Клиентом Правил безопасности, а также за убытки, возникшие вследствие несанкционированных действий третьих лиц, если такие действия стали возможными не по вине Банка.

5.9. В случае несогласия Клиента с действиями Банка в рамках Договора, в том числе опротестования Клиентом операции, проведенной Банком по ДПАСП, Банк имеет право запросить у Клиента подтверждения выполнения Клиентом Правил безопасности, и Клиент обязуется своевременно предоставить данные подтверждения.

5.10. Клиент вправе в одностороннем порядке, без объяснения причин отказаться от использования Системы, предоставив в письменной форме в Банк Заявление на отключение от всех Систем ДБО, используемых по Договору ДБО. Договор считается расторгнутым с момента принятия Банком Заявление на отключение от всех Систем ДБО, используемых по Договору ДБО.

5.11. Клиент обязан письменно информировать Банк об изменении всех сведений, предоставленных Клиентом Банку при заключении Договора, в том числе указанных в соответствующих Заявлениях, включая фамилию, имя, отчество, данные документа, удостоверяющего личность, адрес места жительства (регистрации) или места пребывания, сведения в отношении Клиента (Выгодоприобретателя и Бенефициарного владельца при наличии) в течение 5 (Пяти) календарных дней со дня их изменения или возникновения следующих обстоятельств:

- изменение контактной информации (информации для связи с Клиентом) и наступление других обстоятельств, способных повлиять на исполнение обязательств по Договору;
- вынесено определение суда о признании обоснованным заявления о признании гражданина банкротом и введении реструктуризации долгов;
- об отмене доверенности, выданной представителю Клиента. Поскольку Договор заключается с целью предоставления услуг в Системе конкретному Клиенту, а также учитывая особый характер отношений между Банком и Клиентом, связанных с распоряжением его денежными средствами, Клиент обязуется направлять в Банк уведомления, предусмотренные настоящим пунктом Условий, только в письменной форме на бумажном носителе за собственноручной подписью, с приложением документов (заверенных в установленном порядке копий), подтверждающих произошедшие изменения и достоверно отражающих содержание таких изменений, если иной порядок направления уведомлений не предусмотрен соглашением Сторон.

5.12. Клиент обязан в случае изменения номера мобильного телефона, утери, кражи, пропажи и иных случаях его передачи третьим лицам по любым основаниям, немедленно обратиться в офис Банка или по телефону 8 (499) 241-88-14 для изменения информации о зарегистрированном номере телефона, либо заблокировать доступ к Системе.

5.13. Клиент вправе на основании заявления устанавливать в отношении операций, осуществлялемых с использованием Системы дистанционного банковского обслуживания («Internet-Banking») по переводу денежных средств и выдаче кредита следующие ограничения:

- на осуществление операций по переводу денежных средств;
- максимальной суммы одной операции по переводу денежных средств на счета третьих лиц или максимальной суммы операций по переводу денежных средств на счета третьих лиц за определенный период времени (сутки, неделя, месяц);
- возможность изменения Клиентом максимальной суммы одной операции по переводу денежных средств на счета третьих лиц или максимальной суммы операций по переводу денежных средств на счета третьих лиц за определенный период времени (сутки, неделя, месяц);

- на осуществление операций по выдаче кредита;

- максимальной суммы выдачи кредита на имя Клиента или максимальной суммы выдачи кредита на имя Клиента за определенный период времени (определяется Клиентом самостоятельно);

- возможность изменения Клиентом максимальной суммы выдачи кредита на имя Клиента или максимальной суммы выдачи кредита на имя Клиента за определенный период времени (определяется Клиентом самостоятельно).

5.14. Осуществлять оплату услуг Банка в соответствии с действующими Тарифами.

5.15. Клиент признает, что:

- аудио запись телефонных переговоров, осуществленная и представленная Банком;

- информация о попытках (в том числе, о неуспешных попытках) соединения с Клиентом, предоставленная Банком на основании отчета программного комплекса Банка, с помощью которого осуществляется управление автоматической телефонной станцией Банка, по телефону Клиента, номер которого указан, соответственно, в предоставленных Банку Заявлениях, иных заявлениях, связанных с подключением системы «ДБО», а также в имеющейся в Банке анкете Клиента, являются надлежащими допустимыми доказательствами в случае возникновения спора, связанного с настоящими Правилами, в том числе, в суде.

6. ПРАВА И ОБЯЗАННОСТИ БАНКА

6.1. Банк обязуется информировать Клиента об исполнении или отказе в исполнении ДПАСП незамедлительно с момента исполнения или отказа в исполнении ДПАСП, порядок информирования определен в п. 3.9 настоящих Условий.

6.2. Банк обязуется хранить ДПАСП и направленные Клиенту уведомления об исполнении или отказе в исполнении ДПАСП в соответствии с действующим законодательством Российской Федерации.

6.3. Банк обязуется принять все необходимые меры организационного и технического характера для обеспечения режима конфиденциальности в отношении известных Банку значений Средств авторизации Клиента в т.ч. указанные в п. 3.11 настоящих Условий.

6.4. Банк вправе отказаться от выполнения или приостановить на неопределенный срок исполнение ранее переданного Клиентом и зарегистрированного Банком ДПАСП, уведомив Клиента об этом посредством SMS-уведомления или Push-уведомления или по телефону, если:

- имеется информация, свидетельствующая о нарушении Клиентом требований настоящих Условий;

- проводимая Клиентом операция противоречит действующему законодательству Российской Федерации;

- имеются обоснованные предположения нарушения Клиентом требований по использованию Средств авторизации;

- имеется информация о попытке использования логина Клиента с незарегистрированным в Системе номером дубликата SIM карты (номера мобильного телефона, зарегистрированного в Системе для Клиента).

- проводимая Клиентом операция имеет признаки, указывающие на необычный характер сделки, установленные законодательством Российской Федерации и нормативными актами Банка России, а также в случаях возникновения обоснованных подозрений в нарушении Клиентом заверений, указанных в п. 2.4 настоящих Условий;

- Клиентом не представлены документы, установленные пунктами 5.13 и 6.5 настоящих Условий.

6.5. Банк вправе запросить документы и сведения, необходимые Банку для осуществления функций, предусмотренных действующим законодательством Российской Федерации, в том числе:

- документы и сведения, раскрывающие экономический смысл проводимой операции;
- документы и сведения, необходимые Банку для целей установления и идентификации выгодоприобретателя по проводимой операции;
- Контактные данные Клиента, необходимые Банку для информирования Клиента об исполнении или отказе в исполнении ДПАСП;
- иные документы и сведения по усмотрению Банка.

6.6. В случае отказа Банка от выполнения или приостановки выполнения переданного Клиентом и полученного Банком ДПАСП Банк обязуется в течение одного рабочего дня принять меры к оповещению Клиента о факте отказа одним из указанных в п. 3.9 настоящих Условий способом с указанием причины отказа или приостановки.

6.7. Банк вправе в одностороннем порядке вводить постоянные или временные ограничения на исполнение ДПАСП Клиента, в т.ч. ограничение минимальной и максимальной суммы, количество и объем операций. В случае введения ограничений для неограниченного круга Клиентов Банк доводит данную информацию путем ее публикации в Системе. В случае введения индивидуальных ограничений – Банк оповещает Клиента при его Авторизации в Системе.

6.8. Если Клиент не проходил процедуру Авторизации в Системе:

- более 180 (Сто восемьдесят) календарных дней, Банк вправе заблокировать в Системе использование SIM карты клиента;
- более 360 (Триста шестьдесят) календарных дней, Банк вправе отключить Клиента от обслуживания в Системе.

6.9. Банк вправе отключить от Системы Счет Клиента в момент его закрытия.

6.10. Банк вправе вводить следующие ограничения для Клиентов:

- Блокировать доступ к Системе через определенные Банком Каналы доступа и Устройства доступа, в том числе ограничить перечень видов ДПАСП, отправка которых возможна Клиентом в Банк по определенному Банком Каналу доступа или с помощью определенного Банком Устройства доступа;
- Блокировать самостоятельную регистрацию Клиента в Системе, на официальном интернет сайте Системы https://elf.faktura.ru/elf/app/?site=kremlevsky;
- Блокировать в Системе возможность осуществления определенных типов операций со Счетами.

6.11. Допускается расторжение Договора в порядке, предусмотренном действующим законодательством Российской Федерации.

6.12. Банк вправе сократить срок исполнения ДПАСП, указанный в п. 3.10 настоящих Условий, предварительно уведомив Клиента.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Банк не несет ответственности за ущерб, возникший вследствие:

- несанкционированного использования третьими лицами Средств авторизации Клиента;
- отсутствия технической возможности отправки Клиенту одноразового ключа на указанный Клиентом номер мобильного телефона.

7.2. Банк не несет ответственность за невыполнение, несвоевременное или неправильное выполнение ДПАСП Клиента, если это было вызвано предоставлением Клиентом недостоверной информации или платежных реквизитов.

7.3. Банк не несет ответственность за полное, частичное неисполнение или несвоевременное исполнение своих обязательств, если неисполнение является следствием

форс-мажорных обстоятельств, включая пожар, отключение электроэнергии и линий связи, наводнение, землетрясение, военные операции, изменение действующего законодательства Российской Федерации, действия или решения органов государственной власти Российской Федерации, Банка России, забастовки и иные действия персонала телефонных компаний, провайдеров интернет-услуг, органов энергоснабжения, иные ограничения, объективно препятствующие исполнению Банком его обязательств.

7.4. Банк не несет ответственности по рискам Клиента, связанным с получением Клиентом услуг мобильной связи/по организации доступа к сети Интернет и ее использованию, в соответствии с договором между Клиентом и поставщиком услуг мобильной связи/Интернет (провайдером), в том числе Банк не отвечает за убытки Клиента, возникшие в результате обращения Клиента к Системе с использованием сети Интернет.

8. ДОКУМЕНТ, ПОДПИСАННЫЙ АНАЛОГОМ СОБСТВЕННОРУЧНОЙ ПОДПИСИ

8.1. Передача ДПАСП в Банк и регистрация полученного Банком ДПАСП производится Системой автоматически.

8.2. ДПАСП считается переданным Клиентом и полученным Банком, а соответствующая операция выполненной Банком от имени и по поручению Клиента, если соблюдены следующие требования:

- результат проверки АСП документа положительный;
- Системой подтверждено получение ДПАСП;
- ДПАСП присвоен специальный регистрационный номер.

8.3. Стороны договорились считать, что Клиент отказался от передачи документа до его отправки в Банк, если он не подтвердил его вводом АСП.

9. ПЛАТЕЖНЫЕ ИНСТРУКЦИИ

9.1. Универсальная платежная инструкция (далее по тексту - УПИ) - ПИ с одинаковым для всех Клиентов набором параметров. Одинаковыми могут быть все параметры или их часть.

9.2. Индивидуальная платежная инструкция (далее по тексту - ИПИ) - ПИ, в которой все параметры специфичны для Клиента и задаются Клиентом.

9.3. Индивидуальная постоянная платежная инструкция (далее по тексту - ИППИ) - ИПИ, предусматривающая автоматическое проведение Банком операций по Карте Клиента согласно установленному Клиентом графику.

9.4. Оформление ИПИ и ИППИ производится Клиентом самостоятельно в Системе. В этом случае Клиент указывает необходимые индивидуальные параметры каждой ПИ в ДПАСП.

9.5. Банк вправе отказать в оформлении ИПИ (ИППИ) или запретить использование ранее оформленной ИПИ (ИППИ), если предусмотренные ИПИ (ИППИ) операции противоречат действующему законодательству Российской Федерации, нормативным актам Банка России, настоящим Условиям или внутренним документам Банка.

9.6. Оформляя ИПИ, Клиент поручает Банку в дальнейшем на основании ДПАСП совершать банковские операции в соответствии с платежными и иными реквизитами, указанными при оформлении ИПИ.

9.7. Оформляя ИППИ, Клиент поручает Банку в дальнейшем автоматически совершать банковские операции в соответствии с графиком их проведения, платежными реквизитами, и иными параметрами, указанными при оформлении ИППИ.

10. ИЗМЕНЕНИЕ УСЛОВИЙ

10.1. В соответствии с ч. 1 ст. 450 Гражданского кодекса РФ Стороны пришли к соглашению, что изменения в Договор вносятся Банком в одностороннем порядке. Введение в действие новых условий Договора, в том числе, о начале оказания Банком новых услуг в Системе осуществляется путем доведения до сведения Клиента через систему сообщений об изменениях и нововведениях и обеспечения их технической доступности для Клиента и/или путем размещения информации на сайте Банка.

10.2. Изменения вступают в силу через 15 (Пятнадцать) календарных дней с момента их размещения на сайте Банка, если более поздний срок вступления их в силу не установлен в соответствующем сообщении Банка, за исключением изменений в перечне услуг Системы, которые вступают в силу с момента изменения Банком перечня и содержания бланков ДПАСП в Системе.

10.3. Клиент обязан не реже одного раза в 15 (Пятнадцать) календарных дней знакомиться с информацией, публикуемой Банком на сайте Банка. При необходимости получения дополнительных разъяснений по изменениям в условиях Договора Клиент вправе обратиться за ними по телефону 8 (499) 241-88-14 или в Банк. В случае несогласия с изменениями в условиях Договора Клиент вправе обратиться в Банк для его расторжения представив Заявление на отключение от всех Систем ДБО, используемых по Договору ДБО. Если в течение 15 (пятнадцати) календарных дней с момента изменений, если более поздний срок вступления изменений в силу не установлен в сообщении Банка, Клиент не обратился в Банк для расторжения Договора, Стороны соглашаются, что новые условия Договора приняты Клиентом полностью. Совершение Клиентом конклюдентных действий в рамках Договора является подтверждением ознакомления и согласия Клиента с действующими на данный момент редакцией Условий.

10.4. Банк не несет ответственности, если информация об изменении условий Договора, размещенная в установленном порядке и сроки, не была своевременно получена и/или изучена и/или правильно понята Клиентом.

10.5. Любые изменения условий Договора с момента их вступления в силу равно распространяются на всех Клиентов, в том числе заключивших Договор ранее даты вступления изменений в силу.

11. СРОК ДЕЙСТВИЯ И РАСТОРЖЕНИЕ ДОГОВОРА

11.1. Договор вступает в силу с момента регистрации Клиента в Системе на основании Заявления о присоединении к Условиям дистанционного банковского обслуживания.

11.2. Договор действует без ограничения срока.

11.3. Действие Договора может прекращаться в следующих случаях:

- обращение Клиента с Заявлением на отключение от всех Систем ДБО, используемых по Договору ДБО Клиентом, при этом остальные Договоры о предоставлении банковской услуги могут не расторгаться;
- расторжения Договора КБО, расторжения всех Договоров о предоставлении банковской услуги, закрытии всех счетов, открытых с использованием Систем ДБО;
- неиспользования Клиентом Системы ДБО в течение 6 месяцев подряд;
- заключения соглашения о расторжении Договора ДБО.

11.4. Если Договор расторгается по инициативе Банка, то Банк направляет по адресу Клиента уведомление о расторжении Договора с указанием даты расторжения Договора. Договор будет считаться расторгнутым с даты, указанной в уведомлении. Клиент считается получившим указанное в настоящем пункте уведомление по истечении 15 (Пятнадцати) календарных дней с даты направления Банком соответствующего уведомления вне зависимости от фактического его получения Клиентом.

11.5. Прекращение обязательств по Договору не влечет прекращения обязательств по иным договорам (соглашениям), заключенным между Клиентом и Банком.

12. УРЕГУЛИРОВАНИЕ РАЗНОГЛАСИЙ

12.1. В случае несогласия Клиента с действиями Банка по Договору, в том числе опротестования Клиентом операции, проведенной Банком по ДПАСП (далее - Спорная операция), Клиент до обращения в судебные органы подает в Банк письменное или электронное по каналу обратной связи на официальном интернет-сайте Банка (http://www.kremlinbank.ru) заявление с изложением сути претензии и детальным описанием Несанкционированной операции (далее – Претензия), а также, при необходимости, документы и материалы (например, бумажная распечатка спорного ДПАСП), подтверждающие обоснованность требований Клиента.

12.2. После анализа представленных Клиентом документов и материалов Банк в течение 30 (тридцати) календарных дней с даты получения Претензии Клиента или 60 (шестидесяти) календарных дней в случае, если Претензия Клиента связана с трансграничным переводом, составляет письменное Заключение. Сроки могут быть увеличены в соответствии с Правилами платежной системы при проведении претензионного цикла работ.

12.3. Один экземпляр Заключения направляется Клиенту почтой (заказным письмом с уведомлением или электронной почтой), но в любом случае не позднее срока рассмотрения Претензии, указанного в п. 12.2 настоящих Условий.

12.4. В случае признания Претензии Клиента правомерной и обоснованной Банк в течение одного рабочего дня с даты составления Заключения принимает решение о целесообразности и сроках удовлетворения Претензии Клиента.

12.5. В случае несогласия с Заключением Клиент может обратиться в судебные органы для разрешения возникших споров в соответствии с действующим законодательством Российской Федерации в судебном порядке.

13. ПРОЧИЕ УСЛОВИЯ

13.1. Клиент соглашается с тем, что все требования, уведомления и иные сообщения по настоящим Условиям могут направляться Сторонами друг другу в следующем порядке, если иной способ направления/доставки не предусмотрен настоящими Условиями:

- Уведомления Банка, касающиеся вопросов обслуживания Клиента – путем направления Клиенту письма средствами организации почтовой связи по последнему известному Банку адресу Клиента, путем непосредственной передачи при личной явке Клиента в Банк, путем направления по известному Банку адресу электронной почты, путем направления СМС-сообщения/push-уведомлением по последнему заявленному Клиентом Банку номеру мобильного телефона;
- Уведомления Клиентом Банку – в соответствии с официальными адресами и реквизитами, размещенными на сайте Банка.

14. ПРИЛОЖЕНИЯ К УСЛОВИЯМ

14.1. Правила безопасности при работе в системе дистанционного банковского обслуживания физических лиц «Интернет-банк»/ «Мобильный банк»

Приложение № 1
к Условиям дистанционного банковского
обслуживания физических лиц в «Банк Кремлевский» ООО

ПРАВИЛА БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ФИЗИЧЕСКИХ ЛИЦ «ИНТЕРНЕТ-БАНК/МОБИЛЬНЫЙ БАНК»

1. ОБЕСПЕЧЬТЕ БЕЗОПАСНОСТЬ УСТРОЙСТВА ДОСТУПА, С ИСПОЛЬЗОВАНИЕМ КОТОРОГО ОСУЩЕСТВЛЯЕТСЯ РАБОТА В СИСТЕМЕ «ИНТЕРНЕТ-БАНК/МОБИЛЬНЫЙ БАНК».

1.1. Перед входом в Систему необходимо удостовериться в том, что на Устройстве доступа, с использованием которого осуществляется работа в Системе, установлено, активировано и работает современное лицензионное антивирусное программное обеспечение, регулярно обновляются его антивирусные базы. Регулярное обновление антивирусных баз и проведение антивирусных проверок позволит Вам существенно снизить вероятность заражения Вашего Устройства вредоносными программами (особенно важно контролировать обновление, если нет постоянного подключения к сети Интернет). Если существуют подозрения или основания считать, что данное Устройство доступа может быть заражено вирусами – не осуществляйте с него работу в Системе.

1.2. На Устройстве доступа рекомендуется использовать только лицензионное программное обеспечение, регулярно устанавливать рекомендуемые производителями обновления, как операционной системы, так и прикладного программного обеспечения (в том числе браузера, PDF-ридера, Flash-плеера), это позволит своевременно устранить выявленные уязвимости. Обновления следует устанавливать только из доверенных источников (с официального сайта производителя).

1.3. Рекомендуется использовать на вашем Устройстве доступа персональный межсетевой экран для входа в Интернет. Это позволит значительно снизить риск удаленного управления злоумышленниками из сети Интернет и локальной сети вашим Устройством доступа и кражи конфиденциальной информации. Дополнительно в настройках персонального межсетевого экрана рекомендуется разрешить подключение вашего Устройства доступа только к северу Системы (https://elf.faktura.ru/elf/app/?site=kremlevsky) и серверам обновлений разработчиков программного обеспечения, любые иные подключения рекомендуется запретить.

1.4. Рекомендуется осуществлять работу с Системой с использованием отдельной учетной записи в операционной системе Устройства доступа, защищенной сложным паролем, известным только Вам (см рекомендации в п.3.3 настоящих Правил). Права пользователя в операционной системе Устройства должны быть минимально необходимыми, должна быть запрещена установка прикладного программного обеспечения за исключением необходимого для работы в Системе.

1.5. Рекомендуется избегать работы в Системе с использованием «недоверенных» Устройств доступа, таких как компьютеры в интернет-кафе или другие общедоступные устройства, «чужие» устройства, временно используемые вами и т.п. Крайне нежелательна работа с Системой из публичных беспроводных сетей (например, бесплатный Wi-Fi и т.п.), вместо этого лучше воспользуйтесь «мобильным интернетом» (GPRS / EDGE / HSPA / 3G / LTE соединение). В вышеописанных случаях существенно повышается риск кражи Ваших конфиденциальных данных и денежных средств. Если же данные рекомендации не могут быть Вами выполнены, то при первой же возможности измените пароль, войдя в Систему с «доверенного» Устройства доступа.

1.6. Не оставляйте без присмотра Ваше Устройство доступа с активной сессией работы в Системе, блокируйте доступ к Устройству при помощи пароля на время Вашего отсутствия.

1.7. По возможности исключите посещение с Устройства доступа потенциально опасных Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы, файлообменные сервисы и т.д.), а также работу с почтовыми сообщениями, полученными из недостоверных источников.

2. ВЫПОЛНЯЙТЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ «ИНТЕРНЕТ-БАНК».

2.1. Перед введением логина и пароля при входе в Систему убедитесь, что соединение установлено именно со стартовой страницы Системы и в адресной строке web-браузера отображается «https://elf.faktura.ru/elf/app/?site=kremlevsky». Злоумышленники могут создать мошеннический ресурс со сходным адресом и визуально похожим на сайт Системы интерфейсом. Если Вы заметили, что адрес сайта отличается или есть иные признаки, вызывающие подозрения подлинности сайта (например, сообщение web-браузера о перенаправлении на другой сайт), не вводите никакой конфиденциальной информации и незамедлительно сообщите о данном факте по телефону Банка 8(499) 241-88-14. Рекомендуется вводить адрес Системы только вручную в новом окне web-браузера в адресной строке и НЕ переходить на данную страницу по ссылкам из Интернет-ресурсов (за исключением www.kremlinbank.ru) или из e-mail / SMS-сообщений, даже если они отправлены от имени Банка.

2.2. При работе с Системой для обеспечения конфиденциальности между Банком и Вашим Устройством

доступа все данные передаются в зашифрованном виде. Перед началом работы в Системе необходимо удостовериться, что соединение установлено в защищенном режиме SSL. В префиксе в адресной строке web-браузера должен появиться символ S - httpS://.....ru, а также отобразится иконка «закрытый замок» (может отличаться для разных web-браузеров). Расположение иконки зависит от версии web-браузера, но как правило «закрытый замок» располагается в конце правой части адресной строки, либо в правом нижнем углу экрана. При клике на данное изображение должны отображаться сведения о SSL-сертификате (в строке «кем выдан» должно быть указано Thawte SSL CA).

2.3. После окончания работы в Системе обязательно завершайте сеанс работы с Системой с помощью кнопки «Выход» (в правом верхнем углу экрана).

2.4. При вводе логина и пароля в Системе рекомендуется использовать виртуальную клавиатуру. Использование виртуальной клавиатуры обезопасит Вас от кражи конфиденциальных данных в случае заражения Вашего Устройства доступа вредоносным программным обеспечением.

2.5. Контролируйте состояние Ваших счетов. Регулярно проверяйте в Системе (особенно перед проведением операции) разделы «История операций» (история операций и платежей, совершенных в Системе), раздел «Шаблоны» (перечень сохраненных шаблонов операций). В случае, если Вы обнаружили операции, которые Вы не выполняли; шаблоны, которые Вы не создавали, незамедлительно заблокируйте Вашу учетную запись в Системе. Вы можете сделать это, связавшись с Банком по телефону 8(499)241-88-14, или самостоятельно в Системе.

3. СОБЛЮДАЙТЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ, ОДНОРАЗОВЫХ SMS-ПАРОЛЕЙ, ОДНОРАЗОВЫХ КОДОВ.

3.1. Правила безопасности при использовании одноразовых SMS-паролей:

3.1.1. Для повышения уровня безопасности рекомендуется исключить работу с Системой через мобильные устройства (смартфоны), на телефонные номера которых настроено SMS-информирование с одноразовыми паролями. Эта мера значительно усложнит кражу денежных средств при заражении вирусом Вашего мобильного устройства.

3.1.2. Не используйте для получения одноразовых SMS-паролей не принадлежащие Вам мобильные устройства и телефонные номера.

3.1.3. Никогда не оставляйте без присмотра и не передавайте третьим лицам мобильные устройства, используемые Вами для получения одноразовых SMS-паролей.

3.1.4. Запрещается хранение на мобильном устройстве (в напоминаниях, SMS и т.п.) логина и пароля для входа в Систему. В случае хищения мобильного устройства или его заражения вирусом злоумышленники могут получить доступ к этой информации.

3.1.5. В случае потери (кражи) мобильного устройства или смены телефонного номера, на который приходят SMS-пароли, необходимо незамедлительно обратиться в Банк по телефону 8(499) 241-88-14 для блокировки учетной записи. В случае потери/кражи устройства также необходимо обратиться к оператору сотовой связи для блокировки SIM-карты.

3.1.6. Не используйте возможности переадресации или хранения архива СМС-сообщений в личном кабинете оператора связи.

3.1.7. Устанавливайте сложные пароли в личном кабинете оператора связи. Данная мера позволит уменьшить риски несанкционированного подключения услуги переадресации SMS-сообщений на телефонные номера злоумышленников и последующего перехвата одноразового пароля.

3.1.8. Рекомендуем обратиться к оператору связи и заблокировать выполнение каких-либо действий с Вашей SIM-картой по доверенности. Это не позволит злоумышленником переоформить на третье лицо Ваш телефонный номер по поддельной или недействительной доверенности.

3.1.9. В случае если у Вас без видимых на то причин перестала работать SIM-карта («сеть не найдена») необходимо незамедлительно обратиться за разъяснениями к оператору связи. В данном случае возможно мошенничество с использованием копии Вашей SIM-карты.

3.2. Правила безопасности при использовании push-уведомлений:

3.2.1. Одноразовые пароли посредством push-уведомлений доставляются только на одно доверенное устройство. Устройство становится доверенным только при подтверждении в мобильном банке, установленном на этом устройстве.

3.2.2. Если используется функция быстрого входа с помощью PIN-кода, периодически меняйте его на новый. Не рекомендуется использовать код, который совпадает с каким-либо используемым в другом сервисе, устройстве или приложении.

3.2.3. Если используется функция быстрого входа с помощью отпечатков пальцев, периодически проверяйте настройки своего устройства на предмет регистрации чужих отпечатков.

3.2.4. Помните, что одноразовые push-уведомления не сохраняются в истории сообщений и автоматически подставляется в поле для ввод одноразового пароля.

3.3. Дополнительные рекомендации для владельцев смартфонов:

3.3.1. Установите пароль на доступ к Вашему мобильному устройству. Используйте сложный пароль или пин-код. Средства блокировки по простому графическому ключу или фотографии не обеспечивают должного уровня защиты.

3.3.2. Не используйте мобильные устройства с расширенными правами (Jailbreak, Root или иные операции, не поддерживаемые официально производителями).

3.3.3. Установите на Вашем мобильном устройстве и регулярно обновляйте мобильный антивирус (рекомендуется использовать антивирус российского производителя, так как он учитывает региональную специфику вредоносного ПО).

3.3.4. Своевременно устанавливайте обновления для Вашего мобильного устройства и установленных на нем приложений. Установку производите только из доверенных источников (Google Play Market и Apple AppStore, маркеты производителей устройств и т.п.). Иные способы установки приложений и обновлений небезопасны. Недопустима установка или обновление приложений по ссылке в e-mail / SMS-сообщении от имени

Банка. Обратите внимание: Банк никогда не высылает писем и SMS-сообщений с прямыми ссылками на установку или обновление приложений.

3.3.5. При установке на Ваше мобильное устройство дополнительного программного обеспечения обращайте внимание на полномочия, которые необходимы программе. Не допускайте установки программ, которым требуются излишние полномочия, особенно в части чтения и отправки SMS-сообщений, доступа к сети Интернет, клавиатуре и т.п. Установку производите только из проверенных и надежных источников (Google Play Market и Apple appStore и т.п.). При наличии технической возможности рекомендуется включить на мобильном устройстве режим установки только подписанных приложений с проверкой сертификата. Не устанавливайте приложения по ссылкам, полученным от неизвестных Вам источников.

3.3.6. Если Вы заметили, что на Ваше мобильное устройство перестали приходить SMS, в том числе перестали приходить SMS-пароли от Банка, необходимо прекратить использование мобильного устройства. В данном случае возможно мошенничество с заражением Вашего мобильного устройства вирусом, перехватывающим SMS-сообщения. Для проверки рекомендуем установить SIM-карту в другое мобильное устройство, провести операцию в Системе и дождаться прихода SMS-пароля. Так же о заражении вирусом может свидетельствовать подозрительная работа устройства (самопроизвольные звонки и рассылки SMS, несанкционированная загрузка и установка программного обеспечения). В случае выявления данных фактов рекомендуем обратиться за помощью в службу технической поддержки производителя Вашего мобильного устройства.

3.4. Правила выбора и хранения пароля для входа в Систему:

3.4.1. Для работы с Системой необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:

3.4.1.1. Пароль должен иметь длину от 8 до 20 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков!#$%&()*+-./:;<=>?[\, используйте буквы верхнего и нижнего регистра;

3.4.1.2. Обратите внимание, что регистр и язык букв пароля имеет значение;

3.4.1.3. Пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.);

3.4.1.4. Пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера банковской карты и т.п.);

3.4.1.5. Пароль не должен содержать словарных слов (password, football, русские слова, набранные в английской кодировке, например, gfhjkm – пароль);

3.4.1.6. Пароль не должен совпадать с шестью предыдущими паролями и не должен совпадать с именем входа;

3.4.1.7. Пароль не должен быть копией или комбинаций паролей, используемых Вами в других системах или Интернет-ресурсах (операционная система Устройства, электронная почта, социальные сети, развлекательный ресурсы в сети Интернет и т.п.).

3.4.2. Никогда не сообщайте свой пароль третьим лицам, в том числе родственникам и сотрудникам Банка, вводите пароль только при работе в Системе. Помните, что сотрудник Банка не имеет права запрашивать у Вас пароль, даже если Вы самостоятельно обратились в Банк. Вводите пароль только в Системе, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль.

3.4.3. Не записывайте и не храните пароль в местах доступа третьих лиц. Запрещается хранить пароль на Устройстве доступа, мобильном устройстве, используемом для получения одноразовых SMS паролей, а также на иных электронных носителях, доступ к которым могут получить третьи лица.

3.4.4. Рекомендуется осуществлять смену пароля доступа к Системе не реже одного раза в 12 месяцев.

3.4.5. При возникновении подозрений, что Ваш пароль стал известен третьим лицам, необходимо незамедлительно сменить пароль или заблокировать доступ в Систему, обратившись в Банк по телефону 8(499)241-88-14, либо самостоятельно заблокировать доступ в Системе.

4. ОСТЕРЕГАЙТЕСЬ МОШЕННИЧЕСТВА.

4.1. Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по SMS или e-mail с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, кодовое слово, Ф.И.О., паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли, параметры банковских карт и другие конфиденциальные данные). Не отвечайте на такие сообщения.

4.2. Банк никогда не связывается с просьбой установить или обновить программное обеспечение, в своих электронных письмах никогда не рассылает программы. Не открывайте подозрительные файлы, присланные Вам по электронной почте.

4.3. При получении подозрительного сообщения от имени Банка не отвечайте на него, не переходите по

ссылкам, указанным в подозрительном сообщении. Мошенники могу создать ресурсы в сети Интернет с адресами, похожими на адреса сайта Банка https://i.название.ru. В сообщениях Банка никогда не будет просьбы зайти в Систему по указанной в сообщении ссылке.

4.4. При работе с Системой обращайте внимание на страницу входа и интерфейс Системы. Если у Вас возникли подозрения в подлинности сайта, необходимо незамедлительно прекратить работу и связаться с Банком по телефону 8 (499)241-88-14 (никогда не связывайтесь по телефону, указанному на подозрительной странице).

4.5. Для входа в Систему необходимо ввести логин и пароль (а в случае усиленного режима защиты дополнительно одноразовый пароль). Если Вам предлагается также заполнить иные поля (телефон, номер карты и т.п.) немедленно прекратите работу в Системе и сообщите об этом в Банк.

4.6. Банк никогда не запрашивает одноразовый пароль или пароль на вход в Систему для отмены операций. При вводе пароля Вы даете Банку право на проведение операции, отменить ее с помощью пароля нельзя.

4.7. Если Вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в Систему и одноразовый пароль.

4.8. Банк никогда не направляет сообщений о блокировке/разблокировке Вашей учетной записи в Системе. Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности Системы вследствие проведения каких-либо регламентных работ. Если Вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону 8 (499) 241-88-14 (никогда не связывайтесь с Банком по телефону, указанному в подозрительном сообщении).

4.9. Обращайте внимание на появление подозрительной активности на Вашем Устройстве доступа, например, самопроизвольные движение курсора на экране, набор текста и т.п.

4.10. Обращайте внимание на невозможность доступа к сайту Системы и нестабильную работу Системы («зависания») при нормальной работе других Интернет-ресурсов, а также на невозможность доступа к Системе по причине несовпадения логина и пароля (в случае корректного набора). Данные факты могут свидетельствовать о заражении Вашего Устройства доступа вредоносным программным обеспечением. Если зараженное устройство уже использовалось для доступа к Системе, то незамедлительно заблокируйте Вашу учетную запись в Системе. Вы можете сделать это по телефону

8(499) 241-88-14, или самостоятельно в разделе Системы «Параметры безопасности» (при этом вход в Систему должен быть осуществлен с «доверенного» устройства).

4.11. В случае несанкционированного списания денежных средств, для опротестования спорной операции, проведенной Банком по документу, подписанному аналогом собственноручной подписи ДПАСП (далее - Спорная операция), необходимо до обращения в судебные органы подать в Банк письменное или электронное заявление по каналу обратной связи на сайте Банка (www.kremlinbank.ru) с изложением сути претензии и детальным описанием Спорной операции (далее – Претензия), при необходимости приложить документы и материалы, подтверждающие обоснованность Ваших требований (например, бумажная распечатка спорного ДПАСП и/или файл с ДПАСП).

4.12. В случае если опротестованная операция не совершалась ни Клиентом, ни его Представителем, а также имеются иные признаки незаконного завладения денежными средствами (кражи) с использованием Системы, то Вам рекомендуется оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ). После чего предоставить в Банк копию заявления о возбуждении уголовного дела, либо копию талона-уведомления, подтверждающего непосредственное обращение в правоохранительные органы и содержащего порядковый номер из книги учета сообщений о преступлениях, содержащую отметку правоохранительного органа о его приеме.

В случае утраты, а также при возникновении подозрений, что Ваши логин и пароль, либо еще не введенные в Систему одноразовый код или SMS-пароль стали известны третьим лицам, (в том числе представившимся сотрудниками Банка) незамедлительно заблокируйте Вашу карты.

Помните, что Ваше оперативное обращение в Банк может предотвратить несанкционированное списание, либо приостановить списание денежных средств, снизив Ваши финансовые потери.