ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ФИЗИЧЕСКИХ ЛИЦ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В соответствии с Общими условиями обслуживания физических лиц «СИБСОЦБАНК» ООО (далее – Общие условия) Банк обязуется предоставлять Клиенту услуги ДБО при условии присоединения Клиента в целом и полностью к Общим условиям, при наличии технической возможности, а также при условии успешной Идентификации и Аутентификации Клиента.

Предоставление Клиенту доступа к услугам ДБО в рамках Сервиса «FAKTURA.RU», осуществляется в Подразделении Банка при личном обращении Клиента в момент присоединения Клиента к Общим условиям:

- при заключении договора банковского счета, договора банковского вклада, договора на выпуск и обслуживание карты;
- путем подачи отдельного заявления.

Договоры ДБО, заключенные до вступления в силу Общих условий путем присоединения к Правилам системы Интернет-банк для физических лиц «КРАЕВОГО КОММЕРЧЕСКОГО СИБИРСКОГО СОЦИАЛЬНОГО БАНКА» ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ, действуют на условиях настоящих Правил дистанционного банковского обслуживания физических лиц. Заключение дополнительных договоров/соглашений не требуется.

При заключении ДОГОВОРА в пользу третьего лица доступ к услугам ДБО не предоставляется.

1.2. Правила дистанционного банковского обслуживания физических лиц (далее – Правила) определяют порядок предоставления Банком услуг ДБО в рамках Сервиса «FAKTURA.RU», а также порядок взаимодействия Банка и Клиента в рамках данной системы.

Правила сервиса «FAKTURA.RU», расположены в сети Интернет по адресу https://cft.group/contracts/

Руководство пользователя оператор сервиса «FAKTURA.RU» размещает на сайте www.faktura.ru

Моментом ознакомления Клиента с опубликованной информацией считается момент, с которого информация доступна для Клиентов.

1.3. Внесение изменений и дополнений в Правила, осуществляется Банком в одностороннем порядке. Изменения доводятся Банком до сведения Клиента посредством уведомления не позднее, чем за 10 (Десять) дней до даты вступления в силу таких изменений. Уведомление осуществляется путем опубликования на Официальном сайте Банка.

1.4. Банк определяет условия использования системы Интернет-банк, меры безопасности при работе в системе Интернет-банк (Приложение 3 к Общим условиям) и доводит эту информацию до Клиента любыми не запрещенными способами, в том числе путем опубликования на Официальной сайте Банка.

1.5. Подключение Клиента к системе Интернет-банк осуществляется при условии присоединения к Общим условиям, ознакомления и принятия Клиентом настоящих Правил. Подключаясь к системе Интернет-банк, Клиент соглашается использовать сервис «FAKTURA.RU» для обмена электронными документами и информацией с Банком в порядке и на условиях, определённых Правилами сервиса «FAKTURA.RU».

1.6. Оператор сервиса «FAKTURA.RU» предоставляет доступ Клиенту к сервису «FAKTURA.RU» и осуществляет информационное и технологическое обслуживание Клиента и Банка в рамках сервиса. Сервис «FAKTURA.RU» доступен по адресу www.faktura.ru.

Банк осуществляет регистрацию Клиента (предоставление возможности Клиенту использовать сервис «FAKTURA.RU» для обмена информацией) в сервисе «FAKTURA.RU». В процессе регистрации Банк:

- осуществляет проверку документов и полномочий Клиента в объеме, достаточном для открытия Счета и управления Счетом в Банке;
- обеспечивает получение Клиентом уникального логина и пароля для обмена электронными документами и информацией.
- получает от Клиента информацию об основном номере телефона, адресе электронной почты (при наличии);
- передает сведения о Клиенте, а также вышеуказанную информацию в сервис «FAKTURA.RU».

1.7. Банк оказывает Клиенту услуги ДБО с использованием сервиса «FAKTURA.RU». Банк самостоятельно определяет набор услуг, к которым Клиенту может быть предоставлен доступ, с учетом технических возможностей и заключенных с Клиентом договоров (Приложение 1 к Общим условиям).

1.8. Доступ Клиента к услугам ДБО через сеть Интернет осуществляется при условии его успешной Идентификации и Аутентификации на основании логина и пароля. Основным идентификатором Клиента в системе Интернет-банк является логин.

В случае утраты пароля Клиент лично обращается в Подразделение Банка с документом, удостоверяющим личность. Новый пароль является временным и подлежит замене Клиентом.

1.9. Распоряжения Клиента, переданные в электронных документах (распоряжения о списании денежных средств, заявления, заявки) направляются Банку только при условии успешного подтверждения операций, совершенных Клиентом в сервисе «FAKTURA.RU», разовыми секретными паролями, направленными Клиенту оператором сервиса «FAKTURA.RU» на основной номер телефона, зарегистрированный Банком.

В системе Интернет-банк используется только один основной номер телефона. Изменение основного номера телефона осуществляется только при личном визите Клиента в офис Банка и подачи Заявления по форме, установленной Банком.

1.10. Необходимость подтверждения операции разовым секретным паролем определяет оператор сервиса «FAKTURA.RU» и доводит данную информацию до Клиента путем ее отображения в сервисе «FAKTURA.RU» при совершении операции, а также в Руководстве пользователя.

1.11. Клиент соглашается с тем, что пароль и разовый секретный пароль являются аналогом собственноручной подписи. Электронные документы, подтвержденные паролями и/или разовым паролем, признаются Сторонами равнозначными документам на бумажном носителе и могут служить доказательством в суде.

1.12. Стороны признают, что способы и средства обеспечения информационной безопасности, используемые при подключении Клиента к услугам ДБО и при осуществлении обмена электронными документами в системе Интернет-банк, указанные в Руководстве пользователя, достаточны для защиты от несанкционированного доступа к персональным данным, Счетам и операциям Клиента в системе, а также подтверждения авторства и подлинности электронных документов.

1.13. Клиент самостоятельно и за свой счет обеспечивает подключение своих вычислительных средств к сети Интернет, а также обеспечивает их защиту от несанкционированного доступа и вредоносного программного обеспечения.

1.14. Банк самостоятельно определяет типы Счетов и виды операций и информации, доступные Клиенту.

На Счета, открытые на основании договора банковского вклада/счета, распространяются ограничения установленные условиями договора, являющегося основанием открытия Счета.

1.15. Банк самостоятельно определяет лимиты на совершение операций в системе Интернет-банк (Приложение 2 к Общим условиям). Банк доводит до Клиента информацию о лимитах любыми не запрещенными способами, в том числе путем опубликования на Официальной сайте Банка.

Банк вправе в одностороннем порядке изменять лимиты на совершение операций в системе Интернет-банк. Изменения доводятся Банком до сведения Клиента посредством уведомления не позднее, чем за 10 (Десять) дней до даты вступления в силу таких изменений. Уведомление осуществляется путем опубликования на Официальном сайте Банка.

1.16. Банк исполняет распоряжения Клиента не позднее рабочего дня, следующего за днем поступления в Банк соответствующего электронного документа, за исключением случаев выявления операций, соответствующих признакам осуществления перевода денежных средств без добровольного согласия Клиента. Электронные документы, поступившие в Банк после окончания операционного дня, официально установленного Банком, считаются поступившими на следующий рабочий день.

1.16.1. В соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» Банк и оператор сервиса «FAKTURA.RU» выявляют операции, соответствующие признакам осуществления перевода денежных средств без добровольного согласия Клиента.

Признаки осуществления перевода денежных средств без добровольного согласия Клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети Интернет по адресу: www.cbr.ru.

1.16.2. При выявлении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, Банк до осуществления списания денежных средств со Счета Клиента приостанавливает исполнение распоряжения о совершении такой операции, а также Банк в праве приостановить предоставление услуг Интернет-банк на срок не более 2 (Двух) календарных дней.

Банк после выполнения действий по приостановлению исполнения распоряжения:

1) уведомляет Клиента одним из следующих способов на усмотрение Банка: путем телефонного звонка, отправки письма на электронный адрес Клиента, SMS/Push-уведомлений, по системе «Интернет-банк» либо путем вручения письменного уведомления:

– о приостановлении исполнения распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, а также приостановлении предоставления услуг ДБО;
– о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия Клиента;

2) незамедлительно запрашивает у Клиента подтверждение возобновления исполнения распоряжения.

При получении от Клиента подтверждения возобновления исполнения распоряжения Банк незамедлительно возобновляет исполнение распоряжения, а также восстанавливает Клиенту доступ к услугам ДБО. При неполучении от Клиента подтверждения возобновления исполнения распоряжения Банк возобновляет исполнение распоряжения, а также восстанавливает Клиенту доступ к услугам ДБО по истечении двух календарных дней после дня совершения им действий по приостановлению исполнения распоряжения.

1.16.3. При выявлении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, оператор сервиса «FAKTURA.RU» приостанавливает исполнение распоряжения о совершении такой операции, а также блокирует возможность предоставления распоряжений о списании денежных средств.

Ответственный сотрудник оператора сервиса «FAKTURA.RU» связывается с Клиентом по основному номеру телефона, для подтверждения/опровержения Клиентом факта отправки распоряжения о списании денежных средств.

Идентификация Клиента осуществляется в соответствии с идентификационными данными, предоставленными Банком. Данными, необходимыми для Идентификации физического лица в качестве Клиента Банка являются: ФИО Клиента, паспортные данные Клиента, предоставленные Банком оператору сервиса «FAKTURA.RU», информация о ЭД, отправленных ранее Клиентом.

На основании беседы с Клиентом ответственный сотрудник оператора сервиса «FAKTURA.RU» принимает решение о возобновлении исполнения распоряжения о совершении такой операции, восстановления возможности предоставления распоряжений о списании денежных средств.

Если физическим лицом, с которым связался ответственный сотрудник оператора сервиса «FAKTURA.RU», не пройдена процедура Идентификации, оператор сервиса «FAKTURA.RU» уведомляет об этом Банк. В течение двух календарных дней Банк принимает решение возобновлении исполнения распоряжения Клиента или его отмене. С этой целью сотрудник Банка связывается с Клиентом по основному номеру телефона. В случае изменения ФИО, паспортных данных, исполнение распоряжения Клиента возобновляется только после обновления имеющихся у Банка сведений. Изменение указанных сведений проводится при личном обращении Клиента в Банк.

При невозможности связаться с Клиентом в целях подтверждения/опровержения факта отправки распоряжения Клиентом по истечении двух календарных дней ЭД передается в Банк. Банк возобновляет исполнение распоряжения. Если ранее Клиенту была заблокирована возможность предоставления распоряжений о списании денежных средств, то возможность отправки распоряжений о списании денежных средств восстанавливается.

1.16.4. В случае утраты (утери, кражи) устройства, используемого для работы в системе Интернет-банк, и/или выявления Клиентом использования системы Интернет-банк без его согласия, Клиент незамедлительно после обнаружения указанных фактов, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, обязан направить Банку уведомление любым из доступных способов:
– по телефону +7(3852) 370228 либо по телефону Подразделения Банка, в котором заключен договор банковского счета;
– по электронной почте af@sibsoc.ru;
– посредством системы Интернет-банк;
– при личном визите Клиента в Банк.

В случае обращения Клиента по телефону, работник Банка идентифицирует его в соответствии с идентификационными данными, предоставленными Клиентом Банку. Данными, необходимыми для Идентификации физического лица являются: ФИО Клиента, паспортные данные Клиента.

Банк, получив уведомление Клиента, приостанавливает предоставление Клиенту услуг ДБО (блокирует доступ Клиента к услугам ДБО). Возобновление доступа к услугам ДБО осуществляется при личном визите Клиента в Банк.

1.16.5. Банк направляет в Банк России информацию обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия Клиента в порядке, установленном Банком России (в том числе сведения об операциях, о Счетах и вкладах, в отношении которых были зафиксированы случаи и (или) попытки осуществления переводов денежных средств без согласия Клиента).

1.17. В сервисе «FAKTURA.RU» реализован форматно-логический контроль полноты заполнения реквизитов распоряжений, а также контроль лимитов на совершение операций. Распоряжения Клиента передаются Банку и принимаются Банком к исполнению после проверки полноты и корректности реквизитов распоряжений.

1.18. Банк взимает с Клиента комиссионное вознаграждение за совершение операций в системе Интернет-банк. Размер комиссионного вознаграждения за предоставление Банком услуг устанавливается Тарифами. Клиент поручает Банку списывать комиссионное вознаграждение за предоставленные услуги со Счета Клиента, к которому предоставлено распоряжение. Банк не предоставляет услугу, если на Счете Клиента недостаточно денежных средств для оплаты комиссионного вознаграждения. В случае отсутствия денежных средств на Счете Клиента, к которому предоставлено распоряжение, Банк вправе без дополнительного распоряжения Клиента списать комиссионное вознаграждение за предоставленные услуги с любых Счетов Клиента в Банке, если это не противоречит режиму соответствующего Счета, либо не исполнить распоряжение Клиента.

В случае недостаточности средств на Счетах Клиента для списания сумм комиссионного вознаграждения Банк вправе производить частичное списание данных сумм в пределах имеющихся средств.

1.19. Доступ Клиенту к услугам ДБО прекращается:

1.19.1. в случае подачи Клиентом заявления в письменном виде при личном визите в Подразделение Банка или передачи заявления Банку посредством системы Интернет-банк;

1.19.2. в случае прекращения / расторжения ДОГОВОРА;

1.19.3. в случае если из достоверных источников получена информация (представлены документы) о смерти Клиента в соответствии со статьей 418 Гражданского кодекса Российской Федерации.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Банк обязуется:

2.1.1. Обеспечить регистрацию Клиента в сервисе «FAKTURA.RU» и предоставить Клиенту логин, временный пароль для доступа в систему Интернет-банк и получения услуг ДБО.

2.1.2. Принимать к исполнению поступившие от Клиента электронные документы, оформленные в соответствии с законодательством Российской Федерации, требованиями нормативных документов Банка России, настоящих Правил и договоров между Клиентом и Банком, при условии прохождения Клиентом авторизации в системе Интернет-банк, т.е. однозначного совпадения логина и пароля, а также разового секретного пароля. Банк исполняет принятые электронные документы не позднее рабочего дня, следующего за днем их получения от Клиента.

2.1.3. Не разглашать и не передавать третьим лицам информацию о Клиенте и его операциях, за исключением случаев, предусмотренных законодательством Российской Федерации и настоящими Правилами.

2.1.4. Обеспечить сохранность информации об операциях Клиента в системе Интернет-банк в течение срока, установленного законодательством Российской Федерации.

2.1.5. В случае невозможности предоставления услуг ДБО по техническим или иным причинам разместить на Официальном сайте Банка или в системе Интернет-банк соответствующую информацию.

2.1.6. Информировать Клиента о мерах информационной безопасности при использовании системы Интернет-банк, рисках Клиента и возможных последствиях для Клиента в случае несоблюдения им мер информационной безопасности, рекомендованных Банком. Информирование осуществляется в системе Интернет-банк, в Подразделениях Банка.

2.2. Банк имеет право:

2.2.1. В одностороннем порядке прекратить предоставление услуг ДБО в случае нарушения Клиентом своих обязательств по настоящим Правилам.

2.2.2. Списывать со Счетов Клиента комиссионное вознаграждение за услуги ДБО в соответствии с Тарифами Банка.

2.2.3. Отказать Клиенту в проведении операции в случае отсутствия на Счетах Клиента средств для списания комиссионного вознаграждения за проведение операции, указания неправильных реквизитов получателя перевода или некорректном заполнении реквизитов.

2.2.4. Приостановить на 24 часа предоставление услуг ДБО при выявлении фактов и признаков нарушения информационной безопасности.

2.2.5. Устанавливать лимиты на совершение операций в системе Интернет-банк, а также реализовывать в системе Интернет-банк другие механизмы, снижающие риски Банка и Клиента.

2.2.6. В одностороннем порядке вносить изменения в настоящие Правила с предварительным уведомлением Клиента не менее чем за 10 календарных дней через Официальный сайт Банка.

2.2.7. При выявлении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, приостановить исполнение распоряжения

Клиента о совершении операции на срок не более 2 (Двух) календарных дней и направить информацию о случаях и (или) попытках осуществления переводов денежных средств без добровольного согласия Клиента в Банк России.

2.2.8. Приостановить предоставление услуг ДБО в случае действия (бездействия) Клиента, препятствующего работнику СПБ завершить обновление сведений, полученных в результате Идентификации Клиента (в том числе при отсутствии связи с Клиентом в системе Интернет-банк и/или по номеру мобильного телефона и/или адресу электронной почты, предоставленным Клиентом и зарегистрированным Банком) до получения указанных сведений.

2.3. Банк не несет ответственность:

2.3.1. В случае невозможности предоставления услуг ДБО по независящим от Банка обстоятельствам, в том числе по причине непредставления Банку сторонними организациями, сервисов необходимых для услуги ДБО.

2.3.2. За последствия компрометации логина, пароля и/или разовых секретных паролей Клиента, а также за убытки, понесенные Клиентом в связи с неправомерными действиями третьих лиц, если Клиент не уведомил Банк в порядке, установленном п. 1.16.4 настоящих Правил.

2.3.3. В случаях финансовых потерь, понесенных Клиентом, в связи с нарушением или ненадлежащим исполнением Клиентом рекомендаций по обеспечению безопасности при работе с системой Интернет-банк, а также требований по защите автоматизированного места от вредоносного кода.

2.3.4. В случаях необоснованного или ошибочного перечисления Клиентом денежных средств получателям через систему Интернет-банк. Клиент самостоятельно урегулирует вопрос возврата денежных средств с их получателями.

2.4. Клиент обязуется:

2.4.1. Уплачивать Банку комиссионное вознаграждение за услуги ДБО в соответствии с Тарифами.

2.4.2. Проходить авторизацию в системе Интернет-банк, с использованием логина и пароля, а также разового пароля, если это предусмотрено Руководством пользователя. После прохождения вышеуказанной процедуры авторизации направляемые Клиентом электронные документы, признаются однозначно подписанными Клиентом, при этом, средством подтверждения в данном случае являются одновременно используемые логин и пароль (разовый пароль - если это предусмотрено Руководством пользователя).

2.4.3. Хранить в тайне и не передавать другим лицам логин и пароль, а также разовые секретные пароли.

2.4.4. Обеспечить защиту автоматизированного рабочего места от вредоносного кода посредством использования антивирусного программного обеспечения

2.4.5. При компрометации или подозрении на компрометацию пароля незамедлительно произвести смену пароля в системе Интернет-банк. При невозможности незамедлительно выполнить смену пароля, а также в случае компрометации или подозрении на компрометацию логина незамедлительно обратиться в Банк.

2.4.6. В случае изменения именных и/или паспортных данных представить в Банк новые сведения и документы, их подтверждающие.

2.4.7. Предоставлять Банку актуальные сведения об основном номере телефона, адресе электронной почты. В случае их изменения сообщить Банку актуальные сведения в порядке, предусмотренном настоящими Правилами.

2.4.8. Ознакомиться с рекомендациями по обеспечению безопасности при работе с Интернет-банком, а также мерами информационной безопасности, размещенными в Руководстве пользователя, а также неукоснительно их соблюдать.

2.5. Клиент имеет право:

2.5.1. Получать услуги ДБО, к которым Банком предоставлен доступ, в соответствии с Руководством пользователя.

2.5.2. В случае возникновения у Клиента претензий, связанных с предоставлением услуг ДБО, оформить соответствующее заявление в Подразделении Банка.

2.5.3. В случае необходимости обратиться в Подразделение Банка для получения письменного подтверждения об операции, произведенной в системе Интернет-банк.

3. ПРОЧИЕ УСЛОВИЯ

3.1. За невыполнение или ненадлежащее выполнение обязательств, установленных настоящими Правилами, Банк и Клиент несут ответственность в соответствии с законодательством Российской Федерации.

3.2. В случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно

запрещающих или препятствующих осуществлению Банком своих функций по настоящим Правилам, и иных обстоятельств, не зависящих от Банка, Банк освобождается от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.

3.3. Обязательства Банка по настоящим Правилам считаются прекращенными с даты прекращения обязательств Банка по договорам и дополнительным соглашениям к ним Клиента, указанным в Заявлении.

Приложение 1
к Общим условиям обслуживания
физических лиц «СИБСОЦБАНК»
ООО

Перечень услуг системы Интернет-банк

1. Операции по текущим счетам, счетам по вкладам

Перевод денежных средств со счета Клиента на другой счет Клиента
Перевод денежных средств со счета Клиента на счет другого Клиента
Перевод денежных средств со счета Клиента на свой счет или счет другого физического лица, открытый в другой кредитной организации
Перевод денежных средств со счета Клиента, открытого в рублях, в бюджет и государственные внебюджетные фонды, в пользу юридических лиц и индивидуальных предпринимателей
Перевод денежных средств для погашения задолженности по кредиту со счета
Перевод денежных средств физическому лицу по номеру мобильного телефона в сервисе Система быстрых платежей
Оплата услуг в сервисе Федеральная Система «Город»
Перевод денежных средств в сервисе «Золотая корона»
Покупка-продажа безналичной иностранной валюты за безналичные рубли по курсам, установленным Банком

2. Информационные операции

Получение информации о текущем размере остатка средств на счете (вкладе)
Получение выписки по счету
Получение информации о курсах покупки-продажи безналичной иностранной валюты
Получение информации об условиях договоров банковского вклада
Создание шаблонов переводов со счетов
Получение информации о кредитных продуктах Клиента:

- об открытых кредитных продуктах Клиента (лимит кредита, дата очередного планового платежа, сумма минимального платежа, текущая задолженность, остаток средств на счете);
- о графике платежей по кредиту;
- о произведенных платежах

Передача сообщений, заявлений в Банк
Получение сообщений, предложений из Банка

Приложение 2
к Общим условиям обслуживания
физических лиц «СИБСОЦБАНК»
ООО

Лимиты на совершение операций в системе Интернет-банк

С целью снижения рисков Клиента и Банка устанавливаются следующие лимиты на операции, осуществляемые Клиентом с использованием системы Интернет-банк:

1. перевод денежных средств в другие кредитные организации:

суточный лимит на перевод денежных средств другим физическим лицам, а также юридическим лицам и индивидуальным предпринимателям в другие кредитные организации (на сумму платежей в течение одного дня (календарные сутки по московскому времени) – **150 000 рублей**;

месячный лимит на перевод денежных средств на собственный счет физического лица, открытый в другой кредитной организации (на сумму платежей в течение одного месяца (календарный месяц по московскому времени) или специальный счет оператора финансовой платформы, бенефициаром по которому выступает указанное физическое лицо. Без ограничения Банком размера или количества таких операций в пределах установленного настоящей частью совокупного ежемесячного размера операций– **30 000 000 рублей.**

на основании письменного заявления Клиента Банк может изменить суточный и/или месячный лимит на перевод денежных средств в другие кредитные организации.

2. перевод денежных средств на счета Клиентов Банка (юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой, физических лиц) – **без ограничений.**

3. перевод денежных средств между собственными счетами Клиента – **без ограничений**.

Приложение 3
к Общим условиям обслуживания
физических лиц «СИБСОЦБАНК»
ООО

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ ИНТЕРНЕТ-БАНК

Использование системы Интернет-банк потенциально несет в себе риски неблагоприятных последствий, связанных с хищением денежных, настоящее приложение описывает риски, возникающие на стороне Клиента при использовании системы Интернет-банк, и определяет перечень мер по снижению этих рисков.

1. Описание рисков

1.1. Основным риском при использовании системы Интернет-банк является риск получения злоумышленником несанкционированного доступа к управлению Счетом Клиента и к документам Клиента, передаваемым в Банк через систему Интернет-банк.

1.2. Последствиями несанкционированного доступа могут быть списание денежных средств со Счета Клиента или утечка конфиденциальной информации о совершаемых Клиентом операциях.

2. Способы несанкционированного доступа к системе Интернет-банк

2.1. Основными способами получения несанкционированного доступа к системе Интернет-банк являются:

- перехват злоумышленником управления компьютером, мобильным устройством Клиента;
- кража логина и пароля Клиента для входа в систему Интернет-банк;
- перехват данных, передаваемых Клиентом в Банк и получаемых Клиентом из Банка.

Получение несанкционированного доступа может быть осуществлено:

- злоумышленниками, получившими доступ к компьютеру, мобильному устройству Клиента через сеть Интернет или иные каналы связи.
- третьими лицами, имеющими физический доступ к компьютеру, мобильному устройству Клиента.

3. Признаки несанкционированного использования рабочего места Клиента, предназначенного для работы в системе Интернет-банк:

3.1. В истории поручений в системе Интернет-банк указаны поручения, которые Вы не совершали.

3.2. Подозрительная активность на компьютере, с которого осуществляется работа (самопроизвольные движения курсором мыши, открытие/закрытие окон, набор текста и т.п.).

3.3. Осуществлен запрос на ввод разового пароля для подтверждения выполнения действий, не связанных с входом в систему Интернет-банк или совершением операций (подтверждение ознакомления с какими-либо правилами, инструкциями, или для подтверждения входа в какой-либо раздел системы, открытия страницы).

3.4. Входящий звонок от лиц, представляющихся работниками «СИБСОЦБАНК» ООО, уведомляющих Вас о регламентных/восстановительных работах в системе Интернет-банк или Банке.

3.5. Получение сообщения о блокировке/разблокировке доступа в систему Интернет-банк.

3.6. Изменение адреса в адресной строке браузера при работе с системой Интернет-банк.

3.7. В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).

3.8. Невозможность получения доступа к системе Интернет-банк по причине несовпадения пароля при введении заведомо верного пароля.

3.9. “Зависание” системы Интернет-банк при одновременной нормальной работе других интернет-ресурсов.

3.10. Внезапное приостановление работы SIM-карты, на номер которой посредством SMS-сообщений направляются разовые пароли (блокировка SIM-карты). Возможно незаконное изготовление третьими лицами дубликата SIM-карты (необходимо обратиться к оператору мобильной связи).

3.11. Данный перечень признаков несанкционированного использования системы Интернет-банк не является исчерпывающим. В зависимости от новых видов атак список может дополняться или корректироваться. Извещения о новых признаках публикуются на Официальном сайте Банка.

4. Для обеспечения безопасности работы в системе Интернет-банк реализовано

4.1. Шифрование канала связи с использованием протокола SSL/TLS и сертификата, подписанного удостоверяющим центром.

4.2. Идентификация (логин) и Аутентификация (пароль и разовый пароль) для входа в систему Интернет-банк.

4.3. Средства подтверждения (разовый пароль) для подтверждения подлинности, неизменности, целостности и авторства распоряжений Клиента.

4.4. Направление SMS-сообщений о проведении транзакций по Счетам Клиента о действиях в системе Интернет-банк (вход в систему Интернет-банк, смена пароля, подключение услуг, проведение транзакций и т.д) (сервис подключается отдельно).

5. Рекомендации Клиенту при работе в системе Интернет-банк:

5.1. Меры, направленные на обеспечение безопасной работы в системе Интернет-банк.

Клиенту, в целях снижения возможного риска несанкционированного использования рабочего места в системе Интернет-банк и списания третьими лицами денежных средств со Счета Клиента, необходимо выполнять следующие организационные и технические меры:

5.1.1. Для входа в Интернет-банк вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего мобильного телефона для входа или дополнительной проверки персональной информации в системе Интернет-банк.

5.1.2. Никогда и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в Интернет-банк или для подтверждения платежей, даже работникам банка.

5.1.3. Обязательно сверяйте текст SMS-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS-сообщении указан пароль для платежа, который вы не совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему Счету платеж, ни в коем случае не вводите его в Интернет-банке и не называйте его, в том числе сотрудникам Банка.

5.1.4. В случае утери мобильного телефона, на который приходят SMS-сообщения с разовым паролем, немедленно заблокируйте (замените) SIM-карту.

5.1.5. Запишите контактный телефон вашего банка в адресную книгу или запомните его. В случае если в личном кабинете системы Интернет-банк вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в Банк по ранее записанному вами телефону.

5.1.6. Используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным ПО и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры.

5.1.7. При вводе личной информации, ПОМНИТЕ, что любой веб-адрес в адресной строке Интернет-банка должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя, так как они будут переданы в отрытом (незашифрованном) виде и могут быть перехвачены.

5.1.8. Используйте виртуальную клавиатуру для ввода пароля.

5.1.9. Будьте внимательны: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в Банк с целью оперативного блокирования доступа!

5.1.10. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

5.1.11. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора.

5.1.12. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагируйте на ошибки.

5.1.13. Запретите в межсетевом экране соединение с интернет по протоколам FTP, SMTP. Разрешите соединения SMTP только с конкретными почтовыми серверами, на которых зарегистрированы ваши электронные почтовые ящики.

5.1.14. Не давайте разрешения неизвестным программам выходить в Интернет.

5.1.15. При работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.

5.1.16. При использовании мобильного приложения Faktura.ru:

- устанавливайте мобильные приложения Faktura.ru только из авторизованных магазинов App Store и Google Play. Перед установкой приложения убедитесь, что их разработчиком является Center of Financial Technologies;
- используйте антивирусное программное обеспечение, в случае, если оно доступно для вашего телефона/смартфона;

- устанавливайте пароль для доступа на ваше мобильное устройство;
- устанавливайте и своевременно обновляйте лицензионные антивирусные программы на вашем мобильном устройстве;
- всегда совершайте выход из мобильного приложения Faktura.ru после окончания работы;
- не храните логин и пароль для доступа в приложение на своём мобильном устройстве или в общедоступном месте и не сообщайте его другим лицам;
- ни при каких обстоятельствах не передавайте и не сообщайте никому (в том числе работникам банка, родственникам и друзьям) данные для входа в мобильное приложение, пароли для подтверждения платежей, а также номера ваших карт и CVV2/CVC2 коды;
- никогда не отвечайте на электронные письма, входящие звонки, SMS-сообщения, письменные/устные обращения, в которых запрашивается персональная информация для входа в приложение;
- в случае утери мобильного телефона или в случае обнаружения подозрительных действий, совершенных от вашего имени в Сервисе, незамедлительно обратитесь в банк;
- по окончании работы в мобильном приложении обязательно необходимо завершить сеанс работы с системой выбором пункта меню «Выйти».

5.2. Требования к формированию пароля:

Составляйте пароль с учетом следующих рекомендаций:

5.2.1. Длина пароля должна быть не менее 8 символов.

5.2.2. Пароль должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы (@ , # , $, % , < , ^ , & , *).

5.2.3. Не рекомендуется использовать «слабые» пароли. К «слабым» паролям относятся следующие пароли:

- пароли, содержащие в том или ином виде имя входа (Логин)
- личная информация, которая относительно легко может стать известной злоумышленникам, например, даты рождения, номера телефонов, клички домашних животных, имена детей и др.
- слова, которые можно найти в словаре
- слова компьютерной терминологии, например, команды операционной системы, названия оборудования, программ и др.
- комбинации расположенных рядом символов клавиатуры, например, qaz, qwerty, 123456 и др.
- любое из указанного выше, набранное в транслитерации
- любое из указанного выше, дополненное цифрами
- любое из указанного выше, набранное в обратном порядке
- любое из указанного выше, набранное в верхнем регистре

5.2.4. Пароль не должен являться копией других паролей пользователя, используемых в личных целях (на развлекательных и почтовых сайтах в Интернете); пароль не должен содержать последовательность одинаковых символов и групп символов (например, не должны применяться пароли, состоящие из одинаковых цифр или из одинаковых букв).

5.2.5. Несколько способов составить надежный пароль.

Надежный пароль — это пароль не только легкий для запоминания, но и достаточно хорошо защищенный от угадывания или вычисления методом перебора по словарю/словарям.

Ниже приведены варианты генерации надежного пароля:

Пример 1. Придумайте в качестве пароля хорошо запоминающуюся осмысленную фразу, например Santa Claus. Измените чередование строчных и прописных знаков, используйте вместо пробела знак подчеркивания: sANTA_cLAUS. Набирайте ваш пароль на клавиатуре со сдвигом на одну клавишу, например, вправо: dSMYS+I:SID.

Пример 2. Можно использовать в качестве пароля какую-нибудь стихотворную фразу (например, «Мне нравится, что вы больны не мной») и из каждого слова включить в пароль первые две буквы, при этом поставив английскую раскладку клавиатуры (например, в данном случае получится пароль Vyyhxnds,jytvy).

Пример 3. Взять какое-нибудь сложное, но известное вам профессиональное слово (например, цистрансизомерия) и вставить в его середину какой-нибудь цифровой код (например, год открытия изомерии Ю. Либихом – 1823), при этом установив английскую раскладку клавиатуры. Из этих данных получится хороший пароль - wbc18nhfyc23bpjvthbz

В описанных случаях вам достаточно помнить лишь ключевую фразу и то, что с ней надо сделать. Это проще запоминания набора случайных символов, и в то же время данные преобразования дают достаточно надежный пароль.

Выполнение вами данных рекомендаций позволит значительно снизить риски совершения несанкционированных операций в системе Интернет-банк.

6. При возникновении подозрений в осуществлении несанкционированных операций в системе Интернет-банк, несанкционированного доступа к компьютеру, мобильному

устройству, либо при компрометации пароля, разового пароля на вход в систему Интернет-банк:

6.1. Выйти из системы Интернет-банк.

6.2. Заблокировать устройства, используемые для работы в системе Интернет-банк (в том числе, выключить/перевести в режим гибернации (сна) компьютер).

6.3. Незамедлительно обратиться в Банк для смены пароля, приостановления дистанционного обслуживания в системе Интернет-банк.

6.4. В письменном заявлении описать обстоятельства компрометации пароля, разовых паролей, несанкционированного доступа, либо другую информацию по фактам, вызвавшим подозрения.

6.5. Возобновление доступа в систему Интернет-банк производится в офисе Банка при личном обращении Клиента.