

Утвержден
Правлением АО КИБ «ЕВРОАЛЪЯНС»
Протокол б/н от 30 июня 2020 г.
Действует с 15.07.2020 г.
Версия 2.3

РЕГЛАМЕНТ
обслуживания клиентов
в системе «БАНК-КЛИЕНТ»
АО КИБ «ЕВРОАЛЪЯНС»

Оглавление

1. Термины, определения, сокращения.....	1
2. Общие положения.....	4
3. Порядок регистрации Клиента в Системе ДБО	7
4. Порядок проведения замены ключей ЭП Клиента в Системе ДБО	9
5. Порядок действий Клиента и Банка при компрометации ключа ЭП.....	9
6. Порядок блокирования работы в Системе ДБО и возобновления обслуживания Клиента в Системе ДБО.....	9
7. Подготовка платежных документов.....	11
8. Контроль, подписание, отправка и прием документов	13
9. Отказ от исполнения электронного документа.....	14
10. Обеспечение защиты информации от несанкционированного доступа	15
11. Права и обязанности Сторон	20
12. Услуга sms-информирования (sms-банкинг).....	24
13. Услуга Доверенный получатель	26
14. Сервис Центр финансового контроля (Сервис ЦФК).....	26
15. Контроль дополнительных параметров осуществления операций в Системе ДБО	26
16. Подтверждение платежных поручений	26
17. Аварийный режим работы	27
18. Ответственность сторон.....	27
19. Порядок разрешения споров.....	29
20. Прочие условия	32
Приложение №1	34
Приложение №2	35
Приложение №3	36
Приложение №3а.....	37
Приложение №4	38
Приложение №5	39
Приложение №6	40
Приложение №7	42
Приложение №8	43
Приложение № 9	44
Приложение №10	46
Приложение № 11	47
Приложение № 12	48
Приложение № 13	49
Приложение № 14	50
Приложение № 15	51

1. Термины, определения, сокращения

Регламент – настоящий Регламент обслуживания клиентов в системе «БАНК-КЛИЕНТ» АО КИБ «ЕВРОАЛЬЯНС».

Банк – АО КИБ «ЕВРОАЛЬЯНС».

Клиент (Организация) – юридическое лицо, индивидуальный предприниматель, в т.ч. физическое лицо, занимающееся частной практикой, который заключил с Банком договор банковского счета и Договор на обслуживание по Системе ДБО.

Стороны – Банк и Клиент.

Счет – счет, открытый Клиенту в Банке в соответствии с Договором банковского счета и другими договорами, заключенными между Клиентом и Банком.

Договор на обслуживание по Системе ДБО – документы в составе: 1) настоящий Регламент, 2) Заявление на подключение к Системе ДБО (Приложение №1 к настоящему Регламенту), надлежащим образом заполненное, подписанное Клиентом, принятое и согласованное Банком, либо заключенное Сторонами Дополнительное соглашение по предоставлению банковских услуг с использованием программно-технического комплекса «БАНК-КЛИЕНТ», 3) Тарифы Банка.

Автоматизированное рабочее место (АРМ) Клиента – программно-технический комплекс (компьютер, ноутбук), с помощью которого Клиент работает в системе дистанционного банковского обслуживания.

Мобильное устройство (МУ) – портативное электронное устройство, предназначенное для индивидуального пользования, в т.ч. планшет, коммуникатор, смартфон, мобильный телефон, позволяющее осуществлять переводы денежных средств, а также составлять/передавать/принимать/подтверждать электронные документы с использованием системы ДБО в соответствии с настоящим Регламентом.

Система дистанционного банковского обслуживания (Система ДБО), Система «БАНК-КЛИЕНТ» - совокупность программных средств, согласованно используемых Банком и Клиентом с целью предоставления Клиенту услуги дистанционного банковского обслуживания Счетов Клиента, открытых в Банке.

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Сертификат ключа проверки электронной подписи (Сертификат) - электронный документ или документ на бумажном носителе, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Владелец Сертификата ключа проверки электронной подписи (Владелец ключа ЭП) – уполномоченное лицо Клиента, которому выдан сертификат ключа проверки электронной подписи.

Блокировочное слово – уникальное слово, определяемое Клиентом при регистрации в Системе ДБО и используемое в телефонных переговорах с Банком для идентификации Клиента. Клиент имеет право на основании письменного заявления изменять свое блокировочное слово.

Доверенный получатель – контрагент Клиента, занесенный Клиентом в список Доверенных получателей в соответствии с разделом 13 настоящего Регламента.

Вредоносная программа (вредоносный код) – любое программное обеспечение, предназначенное для получения несанкционированного доступа к средствам вычислительной техники, оборудованию и другим устройствам или к информации, хранимой на них, с целью несанкционированного использования или причинения вреда (нанесения ущерба) владельцу информации и/или владельцу средств вычислительной техники, оборудования путем создания, копирования, искажения, удаления, блокирования, передачи или подмены информации, а также к созданию условий для указанных действий.

Компрометация ключа электронной подписи - получение доступа к ключу электронной подписи третьих лиц в результате утраты, хищения, несанкционированного копирования, использования третьими лицами, в т.ч. с применением средств удаленного администрирования и вредоносных программ, а также в результате любых других случаев, когда невозможно достоверно установить, что произошло с носителями, содержащими ключевую информацию.

Получатель (Получатель денежных средств) – юридические и физические лица, индивидуальные предприниматели, в том числе физические лица, занимающиеся частной практикой, банки, получающие переводы денежных средств на свои банковские счета, счета вкладов (депозитов) и переводы без открытия банковского счета.

Пользовательская документация – инструкции, руководства пользователя и другие документы, определяющие порядок работы Клиента с Системой ДБО, размещенные на официальном сайте Банка в сети Интернет www.euroalliance.ru. Пользовательская документация может быть изменена в одностороннем порядке Банком и/или разработчиком Системы ДБО.

Разработчик Системы ДБО – ООО «БИФИТ».

Тарифы Банка – тарифы Банка на расчетно-кассовое обслуживание Клиентов и оказание услуг, связанных с Системой ДБО, размещенные на сайте Банка.

Электронный документ (ЭД) - документ, в котором информация представлена в электронной форме, подписанный электронной подписью и имеющий равную юридическую силу с аналогичным документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным (при необходимости) оттиском печати.

Электронный платежный документ (ЭПД) – расчетный (платежный) документ Клиента в электронном виде, подписанный необходимым количеством ЭП сотрудников Клиента и являющийся основанием для совершения операций по Счетам Клиента.

Подтверждение подлинности электронной подписи в электронном документе - положительный результат проверки принадлежности электронной подписи в электронном документе Владельцу ключа ЭП и отсутствия искажений в подписанном данной электронной подписью электронном документе.

Исполнение электронного документа - последовательность действий сотрудника Банка с целью выполнения распоряжения Клиента, полученного в форме электронного документа, в соответствии с требованиями действующего законодательства РФ и нормативных актов Банка России.

Исходящие документы - финансовые документы, формируемые Клиентом с целью поручить Банку выполнить определенные действия в соответствии с данным документом.

Отчеты — сводные документы по Счетам, формируемые Клиентом для личного пользования.

Письма — информационные сообщения между Банком и Клиентом. Входящие письма — адресуемые Клиенту, исходящие письма — адресуемые Банку.

Справочники — регистры в Системе ДБО, содержащие информацию о реквизитах банков и корреспондентов, о кодах валют и другие данные, наиболее часто применяемые при заполнении документов. Используются для упрощения процедуры заполнения документов Клиентом.

Статус документа – стадия обработки документа Банком, отображаемая в Системе ДБО.

Электронное средство платежа (ЭСП) - средство (АРМ, МУ) и (или) способ, позволяющие Клиенту составлять, удостоверить и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, а также иных технических устройств.

Токен (USB-токен) – компактное персональное USB-устройство, предназначенное для формирования и безопасного хранения ключей шифрования и электронной подписи.

Sms-информирование (Sms-банкинг) – услуга Банка по передаче Клиенту информации об операциях и текущих остатках на Счетах Клиента, а также других событиях со Счетом Клиента посредством e-mail, sms-сообщений, push-сообщений.

Push-сообщение – сообщение с текстовыми и/или графическими материалами, представленное в электронно-цифровой форме, направленное Банком в Мобильное приложение Системы ДБО и/или в Мобильное приложение «Весточка».

Мобильное приложение «Весточка» – программа для ЭВМ, установленная на устройстве Клиента на базе ОС Android или iOS, посредством которой Клиент получает PUSH-сообщения от Банка.

Мобильное приложение Системы ДБО – приложение Системы ДБО, установленное на мобильное устройство Клиента.

2. Общие положения

2.1. Настоящий Регламент обслуживания клиентов в системе «БАНК-КЛИЕНТ» АО КИБ «ЕВРОАЛЬЯНС» в соответствии со статьей 428 Гражданского кодекса Российской Федерации является офертой Акционерного общества коммерческий инвестиционный банк «ЕВРОАЛЬЯНС» (ИНН 3702030072, КПП 370201001, 153000, г. Иваново, ул. Станко, д. 13) клиентам Банка - юридическим лицам и индивидуальным предпринимателям, в том числе физическим лицам, занимающимся частной практикой, открывшим Счет/Счета в Банке, о заключении Договора на обслуживание по Системе ДБО и о подключении к Системе ДБО.

2.2. Акцепт Клиентом настоящего Регламента осуществляется путем подписания и передачи в Банк Клиентом надлежащим образом оформленного и подписанного Заявления на подключение к Системе ДБО (Приложение №1 к настоящему Регламенту). Датой подключения Клиента к Системе ДБО и заключения Договора на обслуживание по Системе ДБО является дата согласования Банком Заявления на подключение к Системе ДБО. Клиенты, заключившие с Банком Дополнительное соглашение по предоставлению банковских услуг с использованием программно-технического комплекса «БАНК-КЛИЕНТ» (далее – Соглашение) после 01.01.2014 г., признаются акцептовавшими настоящий Регламент на основании пункта 10.2 Регламента обслуживания клиентов в системе «БАНК-КЛИЕНТ» (Приложение №1 к Соглашению), при этом датой заключения Договора на обслуживание по Системе ДБО является дата заключения Соглашения. Клиенты, заключившие с Банком Соглашение до 01.01.2014 г., в случае совершения операций через Систему ДБО после 22.04.2019 г. признаются фактически акцептовавшими настоящий Регламент путем совершения действий по выполнению условий Регламента, при этом датой заключения Договора на обслуживание по Системе ДБО является дата заключения Соглашения.

2.3. В случае изменения действующего законодательства Российской Федерации настоящий Регламент действует в части, не противоречащей законодательству Российской Федерации.

2.4. В случае расхождений в содержании настоящего Регламента и Соглашения, Соглашение действует в части, не противоречащей Регламенту.

2.5. Электронные документы создаются на основе подлинных экземпляров документов на бумажном носителе, заверенных подписями и печатью, или данных, являющихся результатом обработки платежных документов на вычислительной технике. Электронные документы и сообщения создаются, обрабатываются и хранятся на средствах вычислительной техники и могут передаваться по телекоммуникационным каналам.

2.6. Для создания электронного документа, эквивалентного подлинному документу на бумажном носителе с подписями Клиента и оттиском его печати, Клиент использует технические и программные средства, полученные от Банка, и собственные АРМ, МУ, а также программное обеспечение, необходимое для его функционирования.

2.7. При совершении операций с использованием системы «БАНК-КЛИЕНТ» Клиент может использовать следующие сервисы:

- **Сервис «Офлайн-Банк» (РС-Банкинг).** Предназначен для обслуживания Клиентов в режиме оффлайн. При использовании данного сервиса Клиент в соответствии с пользовательской документацией устанавливает специализированное программное обеспечение, с помощью которого на своем рабочем месте формирует электронные документы. Клиент работает с финансовыми документами локально, а обмен информацией с Банком (передача документов, обновление статусов документов, получение выписок) происходит в ходе синхронизации (сеанса связи) с Банком. При этом отсутствует необходимость поддерживать постоянное соединение с Банком в процессе работы. Данный сервис позволяет работать с Системой ДБО при низком или непостоянном качестве связи.
- **Сервис «Интернет-Банк» (Интернет-Банк).** Предназначен для работы с Банком в онлайн-режиме.
- **Сервис «Mobile-Банкинг» (Мобильный банк).** Предназначен для доступа Клиентов Банка к услугам электронного банкинга посредством мобильных устройств.

2.8. Пользовательская документация по работе с Системой «БАНК-КЛИЕНТ» размещается на сайте Банка www.euroalliance.ru.

2.9. Для подключения к Системе «БАНК-КЛИЕНТ» Клиент должен организовать автоматизированное рабочее место (АРМ) и/или настроить мобильное устройство (МУ) в соответствии с требованиями, изложенными в пользовательской документации.

2.10. В Системе ДБО возможны следующие режимы работы:

- **Информационный** – Клиенту доступен только просмотр документов,
- **Полнофункциональный** – Клиенту доступны создание всех видов документов, подтверждение документов, подписание документов электронной подписью.

2.11. Банк предоставляет Клиенту следующие услуги с использованием Системы ДБО:

- прием электронных документов на перевод денежных средств со Счетов Клиента и их исполнение Банком,
- прием от Клиента и предоставление Клиенту электронных документов валютного контроля в порядке, установленном валютным законодательством Российской Федерации,
- предоставление Клиенту информации, в том числе выписок, уведомлений об операциях, совершенных по Счетам Клиента,
- обмен информацией свободного формата между Клиентом и Банком,
- контроль дополнительных параметров осуществления операций в Системе ДБО, предоставление дополнительных услуг (сервисы проверки контрагентов, услуги sms-информирования, доверенные получатели и т.д.). Перечень дополнительных услуг может изменяться Банком в одностороннем порядке.

Перечень электронных документов, пересылаемых по Системе ДБО, приведен в Приложении №2 к настоящему Регламенту.

2.12. Банк осуществляет прием ЭД от Клиента круглосуточно, за исключением периодов технического обслуживания Системы ДБО.

2.13. Электронные платежные документы, а также электронные документы неплатежного характера исполняются Банком в следующие сроки:

- ЭД, поступившие в Банк в операционное время работы Банка, принимаются к исполнению в этот же день,
- ЭД, поступившие в Банк после окончания операционного времени работы Банка, принимаются к исполнению не позднее следующего рабочего дня.

Информация об операционном времени работы Банка размещается на информационных стендах в подразделениях Банка и/или на сайте Банка www.euroalliance.ru.

2.14. Наличные денежные средства выдаются на основании ЭД – Заявка на получение наличных денежных средств (далее – Заявка) в следующие сроки:

- по Заявкам, поступившим в Банк до 15-00 текущего дня, – на следующий рабочий день, либо в более позднюю дату, указанную в заявке,
- по Заявкам, поступившим в Банк после 15-00, на 2 рабочий день, либо в более позднюю дату, указанную в Заявке.

В случае сокращения операционного времени приема документов по системе Банк-Клиент, время приема к исполнению Заявок может быть сокращено.

2.15. ЭД, поступившие в Банк после окончания операционного времени работы Банка, принимаются к исполнению не позднее следующего рабочего дня.

2.16. В соответствии с Федеральным законом №161-ФЗ от 27.06.2011 г. «О национальной платежной системе» Банк информирует Клиента о совершении каждой операции с использованием Системы ДБО путем направления уведомления Клиенту в следующем порядке:

- в случае подключения Клиентом Услуги sms-банкинга – в виде sms-сообщений/push-сообщений и/или сообщений на e-mail, при этом Клиент самостоятельно настраивает в Системе ДБО параметры оповещений в соответствии с п. 12.1 настоящего Регламента,
- в случае, если Клиент в Системе ДБО указал адрес электронной почты (раздел Контактная информация о Клиенте) - в виде сообщений на электронную почту Клиента, при этом Банк самостоятельно определяет набор статусов, о которых направляет уведомления Клиенту,
- в виде предоставления информации о статусах документов в Системе ДБО, которые Клиент обязан самостоятельно просматривать не реже 1 раза каждый рабочий день,
- в виде промежуточной и/или окончательной выписки по Счету в Системе ДБО, которую(ые) Клиент обязан самостоятельно формировать и просматривать не реже 1 раза каждый рабочий день.

2.17. Окончательная выписка по Счетам за текущий операционный день предоставляется Клиенту с 9:00 московского времени следующего рабочего дня, что признается Сторонами надлежащим информированием Клиента о совершенных им операциях. Клиенту доступна также промежуточная

выписка, содержание которой может изменяться в соответствии с порядком прохождения документов, определенных учетной политикой Банка. Клиент обязан самостоятельно формировать и просматривать выписки по Счету в Системе ДБО не реже 1 раза каждый рабочий день.

Предоставление выписок по Счету на бумажном носителе осуществляется по Тарифам Банка.

2.18. Клиент обязан осуществлять в течение каждого рабочего дня не менее одного сеанса связи с Банком для получения выписок, возможных экстренных (технических) сообщений Банка и другой актуальной информации.

2.19. Банк считается уведомившим Клиента о совершении операций с использованием Системы ДБО с момента отправки Банком соответствующего уведомления, указанного в п. 2.14 настоящего Регламента. В случае, если от Клиента в течение дня, следующего за днем совершения операции, не поступило возражений по ней, совершенная банковская операция считается подтвержденной Клиентом.

2.20. По всем вопросам относительно работы Системы ДБО Клиенту необходимо обращаться по телефонам: (4932) 59-01-01, 41-25-79, 8 800 700 92 22.

2.21. Для обеспечения нормального функционирования клиентской части системы «БАНК-КЛИЕНТ» технические средства Клиента должны удовлетворять требованиям, изложенным в Пользовательской документации, размещенной на сайте Банка.

2.22. В случае обнаружения несовместимости технических и программных средств или выявления низкого качества связи, не позволяющего поддерживать работоспособность системы «БАНК-КЛИЕНТ», Банк предоставляет рекомендации по комплектации рабочего места Клиента. Клиент, следуя этим рекомендациям, принимает необходимые меры для создания возможностей установки и функционирования системы «БАНК-КЛИЕНТ».

2.23. При наличии сбоев в обмене информации, возникших в результате неисправности линий связи, отключения или перебоев в линии электропитания, неисправности аппаратных средств Банка или Клиента, проведение банковских операций осуществляется в соответствии с Договором банковского счета, заключенным между Сторонами.

2.24. Стоимость услуг, связанных с процедурой регистрации и эксплуатации программно-технического комплекса «БАНК-КЛИЕНТ» определяется действующими Тарифами Банка.

3. Порядок регистрации Клиента в Системе ДБО

3.1. Для начала работы в системе ДБО Клиент выполняет следующие действия:

3.1.1. Оформляет, подписывает уполномоченным лицом (руководителем или иным лицом по доверенности) и предоставляет в Банк Заявление на подключение к системе ДБО по форме Приложения №1 к настоящему Регламенту.

3.1.2. Оплачивает услуги Банка по подключению к Системе ДБО согласно Тарифам Банка.

3.1.3. Получает в Банке технические и программные средства, необходимые для подключения, регистрации и работы в системе ДБО (в соответствии с Приложениями №3, 3а), в том числе:

- устройство формирования и хранения ключей электронной подписи (USB-токен),

- средство криптографической защиты информации (в случае необходимости формирования файловых ключей).

3.1.4. Знакомится с Пользовательской документацией, правилами обеспечения безопасности при работе с Системой ДБО, обеспечивает выполнение требований к АРМ Клиента для работы с Системой ДБО.

3.1.5. В случае принятия решения о работе с сервисом РС-Банкинга скачивает с сайта Банка <https://ibank.euroalliance.ru/> и устанавливает программу, предназначенную для работы в данном сервисе Системы ДБО.

3.1.6. Используя установленное на АРМ программное обеспечение, создает Ключ ЭП и Сертификат ключа проверки ЭП по форме Приложения №4 к настоящему Регламенту. Сертификат следует распечатать в двух экземплярах, заверить собственноручной подписью Владельца сертификата ключа проверки ЭП, руководителя организации и оттиском печати, затем представить Сертификаты в Банк для проведения процедуры регистрации Клиента в Системе ДБО.

3.2. Сотрудник Банка при получении Сертификата от Клиента осуществляет проверку правильности его заполнения, а также проверку полномочий лиц, подписавших Сертификат, и передает Сертификат Администратору Системы «БАНК-КЛИЕНТ».

3.3. Администратор Системы «БАНК-КЛИЕНТ» проверяет соответствие данных в Сертификате данным в Системе «БАНК-КЛИЕНТ» и в случае положительного результата проверки не позднее следующего рабочего дня регистрирует Клиента в Системе ДБО. Один экземпляр Сертификата возвращается Клиенту.

3.4. Для использования сервиса **Мобильный банк** Клиенту необходимо:

- выполнить загрузку из Play Market или Apple Store и установку мобильного приложения Системы ДБО на мобильное устройство Клиента,
- выполнить инициализацию экземпляра мобильного приложения в соответствии с Пользовательской документацией (ввести номер мобильного телефона, код подтверждения из sms-сообщения, установить pin-код доступа к мобильному приложению или возможность входа с помощью отпечатка пальца),
- инициировать процесс генерации ключа ЭП и выпуск Сертификата ключа проверки ЭП.

Подключение и настройка услуги Мобильный банк производится Клиентом самостоятельно через АРМ Клиента в рамках сервиса Интернет-банк. Инструкция по регистрации в Мобильном банке размещена на сайте Банка www.euroalliance.ru.

3.5. Срок действия ключа ЭП Клиента устанавливается равным сроку действия полномочий Владельца ключа ЭП, но не может превышать 18 (восемнадцати) месяцев с даты начала действия ключа ЭП. В случае, если в течение срока действия ключа ЭП полномочия Владельца ключа ЭП прекращаются (например, в связи с досрочным отзывом полномочий Владельца ключа), Банк, после получения соответствующего уведомления от Клиента, блокирует возможность использования соответствующего ключа ЭП.

4. Порядок проведения замены ключей ЭП Клиента в Системе ДБО

4.1. За 30 календарных дней до истечения установленного срока действия ключа ЭП Клиента Система ДБО информирует Клиента при входе в Систему о необходимости произвести смену ключа ЭП.

4.2. Если Клиент соглашается произвести смену ключа ЭП, далее он осуществляет действия в соответствии с п. 3.1.6 настоящего Регламента.

4.3. В случае, если до истечения установленного срока действия ключа ЭП Клиент не произвел необходимые действия по замене ключей ЭП, с даты истечения срока возможность входа в Систему ДБО прекращается. Для возобновления работы в Системе ДБО Клиенту необходимо осуществить действия в соответствии с п. 3.1.6 настоящего Регламента и, при необходимости, предоставить в Банк документы, подтверждающие полномочия Владельца ключа ЭП.

4.4. Внеплановая замена ключей ЭП производится в случаях:

- Изменения ответственных сотрудников Клиента, указанных в карточке с образцами подписей формы № 0401026,
- компрометации Ключей ЭП,
- обращения Клиента с заявлением в письменной форме о смене ключей ЭП.

Смена ключей уполномоченных лиц Клиента производится в соответствии с п. 3.1.6 настоящего Регламента. ЭД, подписанный ЭП с использованием новых ключей, принимается Банком только после получения Сертификата ключа подписи и проведения процедуры регистрации ключей.

5. Порядок действий Клиента и Банка при компрометации ключа ЭП

5.1. Клиент обязан немедленно прекратить использование ключа ЭП и проинформировать Банк любым доступным способом в случае обнаружения факта/подозрения на факт компрометации ключа ЭП.

5.2. При получении сообщения Клиента о компрометации ключа ЭП Банк приостанавливает обработку ЭД Клиента, подписанных данным ключом ЭП, и блокирует учетную запись Клиента в Системе ДБО.

5.3. Не позднее следующего рабочего дня после обнаружения факта компрометации ключа ЭП Клиент должен предоставить в Банк Уведомление о компрометации ключа ЭП по форме Приложения №5 к настоящему Регламенту.

5.4. Банк на основании Уведомления о компрометации ключа ЭП отзывает Сертификат скомпрометированного ключа ЭП.

6. Порядок блокирования работы в Системе ДБО и возобновления обслуживания Клиента в Системе ДБО

6.1. Блокирование (прекращение или временное приостановление) работы в Системе ДБО может быть осуществлено по инициативе Банка или по инициативе Клиента.

6.2. Блокирование работы Клиента в Системе ДБО осуществляется Банком путем отключения возможности использования:

- *ключа ЭП*, после чего в Системе ДБО работа с данным ключом ЭП невозможна;

- *учетной записи Клиента*, после чего доступ в Систему ДБО становится невозможным.

6.3. По инициативе Клиента Банк обязан незамедлительно блокировать ключ ЭП и/или учетную запись Клиента в Системе ДБО вне зависимости от причин на основании соответствующего заявления Клиента, полученного Банком одним из следующих способов:

- письменного уведомления Клиента на бумажном носителе по форме Приложения №6 к настоящему Регламенту, а в случае компрометации ключа ЭП Клиента – по форме Приложения №5 к настоящему Регламенту. Данное уведомление может быть передано Клиентом по факсу с обязательным последующим предоставлением в Банк оригинала;
- информационного сообщения Клиента, полученного Банком по Системе ДБО и подписанного корректной ЭП, по форме Приложения №6 к настоящему Регламенту, а в случае компрометации ключа ЭП – по форме Приложения №5 к настоящему Регламенту.

6.4. По инициативе Банка (без предварительного уведомления Клиента) Банк вправе блокировать учетную запись Клиента в Системе ДБО и/или ключ ЭП Клиента в следующих случаях:

- 1) в случае нарушения Клиентом требований действующего законодательства Российской Федерации и нормативных актов Банка России,
- 2) в случае ненадлежащего исполнения Клиентом настоящего Регламента,
- 3) в случае возникновения разногласий и конфликтных ситуаций, а также в иных случаях, предусмотренных законодательством Российской Федерации или по усмотрению Банка,
- 4) в случае компрометации ключа ЭП Клиента и/или при возникновении у Банка подозрений в его компрометации,
- 5) при выявлении Банком нарушений Клиентом требований, предъявляемых к ЭСП, и требований по информационной безопасности (включая требования по защите от воздействия вредоносного кода),
- 6) в случае окончания сроков полномочий Владельца ключа ЭП Клиента и отсутствии у Банка информации об их продлении,
- 7) в случае выявления попыток несанкционированного доступа или работы в Системе ДБО третьих лиц от имени Клиента,
- 8) при выявлении поступивших на исполнение в Банк от имени Клиента ЭД, не характерных для данного Клиента или носящих признаков «сомнительных»,
- 9) при выявлении заражения ЭСП Клиента, используемого для работы в Системе ДБО, вредоносным кодом,
- 10) при выявлении признаков, указывающих на замену SIM-карты мобильного устройства, прекращении обслуживания или смены номера телефона Клиента,
- 11) при выявлении нетипичных для Клиента параметров операций и/или используемых устройств.

6.5. В случаях осуществления Банком блокирования ключа ЭП и/или учетной записи Клиента в Системе ДБО по собственной инициативе, Банк незамедлительно, но не позднее следующего рабочего дня с даты осуществления блокировки, по телефону или иным реквизитам Клиента, сообщает Клиенту о факте и причинах блокирования, а также о возможности осуществления операций по Счету на основании расчетных (платежных) документов, оформленных на бумажном носителе.

Блокирование Банком ключа ЭП в случаях отказа в предоставлении банковских услуг по Системе ДБО в соответствии с п. 9.2 Регламента осуществляется после предварительного уведомления, отправленного по Системе ДБО.

6.6. В случае блокирования работы в Системе ДБО по инициативе Клиента возобновление работы в Системе ДБО осуществляется на основании письменного заявления Клиента в произвольной форме, подписанного руководителем Клиента, при условии выполнения Клиентом требований к техническим средствам и требований информационной безопасности, изложенных в настоящем Регламенте.

6.7. В случае блокирования работы в Системе ДБО по инициативе Банка возобновление работы в Системе ДБО осуществляется после устранения Клиентом и Банком причин, приведших к блокировке, представления Клиентом (при необходимости) документов для устранения причин блокировки.

7. Подготовка платежных документов

7.1. В Системе ДБО используются следующие статусы исходящих документов:

Черновик. Присваивается при создании и сохранении нового документа или импорте документа, не прошедшего проверки на корректность заполнения полей. При исправлении всех ошибок в документе с таким статусом и последующем сохранении статус документа меняется на Новый. Документ со статусом Черновик не рассматривается и не обрабатывается на стороне Банка.

Новый. Присваивается при создании и сохранении нового документа, при редактировании и сохранении существующего документа, а также при импорте документа из файла. Документ со статусом Новый не рассматривается и не обрабатывается на стороне Банка.

Подписан. Присваивается в случае, если документ подписан, но число подписей под документом недостаточное для отправки в Банк документа. При внесении изменений в документ с таким статусом и его последующем сохранении статус документа меняется на Новый.

Требует подтверждения. Присваивается платежному поручению после получения необходимого количества подписей, до подтверждения ЭД Клиентом кодом подтверждения, полученным в SMS-сообщении или push-сообщении на номер Клиента, зарегистрированный в Банке.

Доставлен. Присваивается документу, когда число подписей под документом соответствует необходимому для рассмотрения документа Банком и ЭД прошел процедуру подтверждения Клиентом. Статус Доставлен является для Банка указанием начать обработку документа (исполнить или отвергнуть).

На обработке. Присваивается при принятии документа в Банке на обработку.

На исполнении. Присваивается при принятии документа в Банке на исполнение.

В картотеке. Присваивается документу при недостаточности средств на счете Клиента. При поступлении средств на счет Клиента денежные средства списываются в соответствии с очередностью платежа, установленной в соответствии с действующим законодательством. При этом для проведения таких списаний Банком формируются платежные ордера. Если была произведена частичная оплата, то статус «В картотеке» отображается на форме документа в виде ссылки, при нажатии на которую открывается диалог Частичная оплата.

Исполнен. Присваивается документу при исполнении документа Банком в полной сумме. Для документов в статусе **Исполнен** в разделе Настройки задается количество дней, за которое отображаются соответствующие документы.

Отвергнут. Присваивается документу, не принятому Банком к исполнению. При присвоении Банком документу статуса «Отвергнут» Клиент имеет возможность отредактировать и сохранить документ (статус изменится на **Новый**), или удалить документ (статус изменится на **Удален**).

Удален. Присваивается документу, удаленному Клиентом. Удалению подлежат только документы в статусе Черновик, Новый, Подписан или Отвергнут. Документы в статусе Черновик, Новый и Подписан удаляются безвозвратно.

На акцепт. Присваивается платежному поручению или заявлению на перевод в случаях нарушения правил контроля, заданных центром финансового контроля. Статус также присваивается, если установлено принудительное акцептование центром финансового контроля всех документов подчиненной компании.

7.2. Клиент готовит и передает в Банк только документы, определенные в перечне электронных документов, пересылаемых по Системе ДБО (Приложение №2 к настоящему Регламенту).

7.3. В Системе ДБО Клиент формирует электронный документ, эквивалентный документу на бумажном носителе, заполняемый в соответствии с требованиями Банка. Программным обеспечением может быть предусмотрена возможность заполнения отдельных полей в соответствии со встроенными Справочниками. Подробное описание процесса формирования документов содержится в Пользовательской документации. Клиент проверяет и несет ответственность за правильность заполнения полей и реквизитов каждого электронного документа, подготовленного для отправки в Банк.

7.4. Клиент имеет возможность подготовки электронных документов во внешних системах с последующей загрузкой этих документов в формате, поддерживаемом Системой ДБО.

7.5. Клиент может формировать и отправлять в Банк Заявку на получение наличных денежных средств по форме Приложения № 15 к настоящему Регламенту. Все поля данного документа являются обязательными к заполнению, в т.ч. поле «Дополнительная информация», куда вносится расшифровка направления выдачи. Подробное описание процесса формирования документа также содержится в Пользовательской документации.

7.6. Клиент может формировать и отправлять в Банк электронные сообщения произвольного формата, а также документы в виде вложенных файлов. Данные сообщения принимаются ответственным исполнителем Банка и передаются соответствующим службам Банка для последующей обработки.

8. Контроль, подписание, отправка и прием документов

8.1. Первоначальный контроль правильности реквизитов и заполнения происходит в Системе ДБО автоматически при заведении электронного платежного документа. При обнаружении ошибок, например, несоответствии расчетного счета получателя БИКу банка-получателя, Клиент немедленно получает сообщение о недопустимости операции и необходимости исправления ошибки.

8.2. Сформированный электронный документ заверяется электронными подписями в соответствии с Сертификатами в количестве и в соответствии с требованиями Банка, после чего документ приобретает статус «Подписан» и по шифрованному телекоммуникационному каналу связи передается в Банк.

8.3. Банк принимает от Клиента электронный документ, фиксирует время его фактического получения и обрабатывает.

8.4. В случае успешного приема документ проверяется на корректность ЭП. Если ЭП некорректна, электронный документ не принимается к обработке, и в адрес Клиента направляется сообщение об отказе в приеме документа по причине некорректности ЭП, а документ приобретает статус «Отвергнут». Если ЭП корректна, электронный документ принимается к обработке, в результате чего документ приобретает статус «На обработке».

8.5. Принятый к обработке документ проходит второй этап контроля. Проверке подвергаются правильность указания расчетного счета Клиента, корректность заполнения всех обязательных полей документа, платежные реквизиты Получателя, наличие средств на счете Клиента.

8.6. В случае выявления каких-либо ошибок или несоответствий, операции по данному электронному документу не проводятся, и он подлежит возврату Клиенту для повторного оформления, в результате чего документ приобретает статус «Отвергнут» с указанием причины возврата.

8.7. Электронный документ, успешно прошедший все стадии контроля, принимается Банком к исполнению, после исполнения ему присваивается статус «Исполнен».

8.8. В исполнении Заявки на получение наличных денежных средств Клиенту может быть отказано, а Заявка отвергнута по основаниям, предусмотренным настоящим Регламентом, Договором банковского счета и действующим законодательством.

О возможности выдачи наличных денежных средств в офисе Банка свидетельствует статус «Исполнено» на начало дня даты, указанной в Заявке.

8.9. Информацию о статусе документа Клиент может получить в Системе ДБО (в случае использования сервиса «Офлайн-Банк» - инициировав в Системе ДБО запрос о статусе документов). В случае, если направленный в Банк документ не имеет в течение часа статуса «Исполнен» или

«Отвергнут», Клиент обязан связаться с работником, обслуживающим счет Клиента, для уточнения информации и согласования дальнейших действий.

8.10. Клиент в любое время может получить информацию о состоянии своего счета и проведенных операциях (в случае использования сервиса «Офлайн-Банк» – инициировав запрос на получение выписки). Предоставление выписок по Счету на бумажном носителе осуществляется по Тарифам Банка.

8.11. Клиент имеет право отозвать документ, переданный в Банк, отправив запрос на отзыв документа в виде электронного сообщения по Системе ДБО с указанием причины отзыва. Сотрудник Банка обрабатывает данный запрос и в случае удовлетворения запроса предпринимает действия по отзыву документа, в результате чего статус документа изменяется на «Отозван». В случае невозможности отзыва документа в адрес Клиента высылается сообщение об отклонении запроса на отзыв документа с указанием причины.

9. Отказ от исполнения электронного документа

9.1. Основанием для отказа Банка от исполнения электронного документа служит:

- несоответствие содержимого документа требованиям защиты от несанкционированного доступа (отрицательный результат проверки ЭП);
- несоответствие реквизитов документа требованиям, установленным Банком России и Банком;
- недостаток денежных средств для проведения операций на счете Клиента (за исключением случаев предоставления овердрафта, оговоренных соответствующими договорами);
- несоответствие даты документа требованиям действующего законодательства РФ;
- иные причины, определенные требованиями действующего законодательства РФ, Банка России и внутренними документами Банка.

9.2. Банк вправе отказать клиенту в предоставлении банковских услуг по Системе ДБО в следующих случаях:

- выявления Банком подозрительной(-ых) операции(-й) и / или подозрительной деятельности, осуществляемой Клиентом с использованием Системы ДБО, в отношении которой (-ых) у Банка возникает подозрение в том, что такая(-ие) операция(-ии) / деятельность может осуществляться в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма;
- непредставления / несвоевременного предоставления / неполного представления Клиентом в установленный Банком срок по его требованию необходимых подтверждающих документов по проводимым операциям и сделкам, а также документов, подтверждающих необходимость получения наличных денежных средств;
- непредставления / несвоевременного предоставления / неполного предоставления Клиентом в установленный Банком срок актуальной информации (документов), необходимой(ых) для исполнения Банком требований Федерального закона от 7 августа 2001 г. N 115-ФЗ

"О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" (далее - Федеральный закон от 07.08.2001 №115-ФЗ) в части идентификации Клиента, представителя Клиента, выгодоприобретателя и бенефициарного владельца;

- выявления Банком факта отсутствия по своему местонахождению юридического лица, его постоянно действующего органа управления, иного органа или лица, которые имеют право действовать от имени юридического лица без доверенности.

После предварительного предупреждения расчетные документы Клиента не принимаются к исполнению по Системе ДБО и подлежат приему только на бумажном носителе.

9.3. В соответствии с требованиями действующего законодательства РФ при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, Банк приостанавливает использование Клиентом Системы ДБО.

При получении от Клиента подтверждения возобновления исполнения распоряжения, Банк обязан незамедлительно возобновить использование Клиентом Системы ДБО. При неполучении от Клиента подтверждения возобновления исполнения распоряжения, Банк возобновляет использование Клиентом Системы ДБО по истечении двух рабочих дней после дня приостановления использования Клиентом Системы ДБО.

9.4. При получении от Клиента уведомления, направляемого Банку в случае утраты электронного средства платежа и (или) его использования без согласия Клиента, после осуществления списания денежных средств со счета Клиента Банк обязан незамедлительно направить банку, обслуживающему получателя средств, уведомление о приостановлении зачисления денежных средств на банковский счет получателя средств по форме и в порядке, которые установлены нормативным актом Банка России. Далее Банк действует в соответствии с Федеральным законом от 27.06.2011 N 161-ФЗ «О национальной платежной системе».

9.5. Банк вправе отказать в исполнении электронного документа о совершении операции в случае истечения срока действия паспорта гражданина РФ лица, указанного в банковской карточке с образцами подписей и оттиска печати, имеющего право распоряжения денежными средствами Клиента по Счету, при достижении ими 20-ти или 45-тилетнего возраста, и непредставления Банку в качестве документа, удостоверяющего личность, временного удостоверения личности гражданина Российской Федерации, выдаваемого на период оформления паспорта гражданина Российской Федерации, а после выдачи нового паспорта – нового паспорта.

10. Обеспечение защиты информации от несанкционированного доступа

10.1. Защита информации в Системе является многоуровневой и задействует возможности операционной системы, прикладного программного обеспечения и специализированных программных и технических средств, организационных мер, организации хранения программного обеспечения, используемого в Системе.

10.2. Система комплексной защиты информации, состоящая из набора аппаратно-программных средств и административных мер, обеспечивает:

- создание ключей ЭП;
- формирование ЭП под документами;
- шифрование передаваемой информации по каналам связи;
- аутентификацию Клиентов и разграничение их прав;
- достоверность факта получения ЭД получателем;
- подтверждение авторства и целостности ЭД;
- выявление ошибок, сбоев и несанкционированных действий обслуживающего персонала;
- разбор конфликтных ситуаций.

Для разрешения возможных споров в Банке ведутся контрольные архивы ЭД, подписанных ЭП, а также архивы ключей электронной подписи. Хранение контрольных архивов ЭД осуществляется в течение 5 лет с момента проведения операции. При проверке подписи под документом используется соответствующий ключ ЭП владельца, подписавшего ЭД.

10.3. В целях выполнения требований информационной безопасности при работе с Системой ДБО Клиенту необходимо:

- определить список лиц, имеющих доступ к АРМ, на котором расположена Система ДБО; ограничить доступ этих лиц в соответствии с их служебными обязанностями,
- обеспечить защиту от несанкционированного доступа к Системе ДБО, носителям и ключам ЭП, средствам подтверждения ЭПД неустановленных лиц или лиц, не имеющих права доступа к защищаемой информации,
- обеспечить формирование безопасной среды выполнения на компьютере, где установлена Система ДБО. Для этих целей Клиент обязан использовать специально выделенное рабочее место, сертифицированное и поддерживаемое разработчиком программного обеспечения и оперативно обновлять системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. Клиент обязан использовать программное обеспечение в соответствии с требованиями пользовательской документации.
- обеспечить использование средств защиты от несанкционированного доступа из сети посредством установки межсетевых экранов, брандмауэров и т.п., а также применением политики безопасности. Вход в систему должен осуществляться под учетной записью с правами ограниченного доступа, не имеющей расширенные права администратора системы. Учетная запись "Гость" должна быть выключена. Учетные записи пользователей АРМ (в том числе, учетные записи администратора операционной системы) не должны содержать пустые или простые пароли. Пароли учетных записей пользователей должны содержать не менее 8 символов, включающих в себя строчные и прописные буквы и цифры, а также специальные символы. Должна производиться регулярная смена паролей пользователей.

- при первом входе в систему задать пароль доступа к ключу ЭП. Клиент обязан хранить пароль в недоступном месте, исключая несанкционированный доступ к нему других лиц. Должна производиться регулярная смена пароля доступа к ключу ЭП. Пароль доступа к ключу должен содержать не менее 8 символов, включающих в себя строчные и прописные буквы и цифры, а также специальные символы.
- никому и никогда не сообщать сведения о пароле, включая работников Банка. Банк никогда не запрашивает данную информацию у своих Клиентов.
- соблюдать правила безопасной работы в сети Интернет. Исключить посещение Интернет-сайтов с устройств, которые используются для доступа в Систему ДБО, за исключением сайтов банков и сайтов обновлений систем безопасности разработчиков системного, прикладного и антивирусного ПО. Применять для Интернет-браузера средние или высокие параметры безопасности и конфиденциальности. При установке соединения с сервером Системы ДБО Банка Клиент должен удостовериться, что в адресной строке установлен адрес <https://ibank.euroalliance.ru/> и выполнить отчет безопасности (замок в адресной строке), проверив соответствие сертификата сайта Банку. Злоумышленники могут использовать для совершения противоправных действий (фишинговых атак) похожие на первый взгляд сайты и адреса сайтов,
- в случае появления предупреждений Интернет – браузера при подключении к Системе ДБО о перенаправлении на другой сайт обратиться в Банк, исключив при этом совершение финансовых операций с использованием Системы ДБО,
- в случае сбоев в работе АРМ, его поломки во время работы с Системой ДБО или сразу после сеанса работы (проблемы с загрузкой операционной системы, выход из строя жесткого диска и т.п.), незамедлительно обратиться в Банк и убедиться, что от имени Клиента не производились несанкционированные переводы денежных средств. Необходимо провести диагностику компьютера и программного обеспечения, выполнить проверку на наличие вредоносного кода.
- обращать внимание на любые изменения в привычных процессах установления соединения с Системой ДБО. При возникновении любых сомнений в правильности функционирования Системы ДБО следует незамедлительно обратиться в Банк.
- не работать с системой ДБО через публичные сети (интернет-кафе, компьютерные салоны, иные общественные места). Запрещается использовать чужие электронные устройства.
- при наличии технической возможности АРМ, с которого осуществляется работа в Системе ДБО, не должно находиться в локальной сети (при ее наличии). При отсутствии технической возможности использования отдельного АРМ для работы в Системе ДБО, данное АРМ должно быть отделено от локальной сети аппаратным или программным межсетевым экраном, исключая несанкционированный доступ к АРМ со стороны внутренних или внешних пользователей.

- обеспечить постоянное функционирование и своевременное обновление средств защиты от вредоносного кода, регулярно проводить полную проверку АРМ на наличие вредоносного кода. При обнаружении вредоносного кода следует заблокировать Систему ДБО, направив соответствующее уведомление в Банк, отключить АРМ от сети и осуществить меры по удалению вредоносного кода, а в случае невозможности, переустановить системное и прикладное программное обеспечение. По окончании выполнения мер по предотвращению воздействия вредоносного кода необходимо выполнить генерацию новых ключей.
- исключить установку и использование средств отладки и декодирования программного кода, программ удаленного администрирования и удаленного доступа к данному АРМ.
- для предотвращения несанкционированного доступа в обязательном порядке использовать технические средства защиты (USB-токены). Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключен. Для авторизации Клиент обязан установить пароль доступа к ключу ЭП, отключать носители для хранения ключей ЭП в случаях, когда они не используются для работы в системе ДБО. В целях аутентификации при входе в систему или осуществлении переводов денежных средств использовать одноразовый код подтверждения, получаемый по альтернативному каналу связи посредством SMS либо PUSH сообщений, действительный на протяжении ограниченного времени, однозначно соответствующий подтверждаемому распоряжению.
- исключить передачу ключей ЭП и средств подтверждения ЭПД другим неуполномоченным лицам для проверки работы Системы ДБО, проверки настроек взаимодействия с Банком и т.п. При необходимости такие проверки осуществляет только Владелец ключа ЭП или уполномоченное лицо, в т.ч. подключение носителя ЭП к АРМ и ввод пароля доступа к ключу ЭП, исключая его подсматривание.
- при увольнении или изменении должностных обязанностей уполномоченного лица, имевшего доступ к ключу ЭП, незамедлительно обратиться в Банк с просьбой о временной блокировке Клиента в Системе ДБО, провести генерацию новых ключей ЭП и осуществить их регистрацию в Банке.
- в соответствии с пользовательской документацией выполнять требования по безопасности функционирования средств криптографической защиты информации (СКЗИ).
- установить средство контроля целостности установленного программного обеспечения Системы ДБО в соответствии с инструкцией по эксплуатации данного средства контроля, размещенной на сайте Банка.
- обеспечить неразглашение конфиденциальной информации, используемой в Системе ДБО.
- при возникновении любых подозрений на компрометацию ключа ЭП или компрометацию среды исполнения (наличие в АРМ или мобильном телефоне вредоносного кода)

незамедлительно заблокировать Систему ДБО и убедиться в отсутствии несанкционированных операций по счету.

10.4. Для обеспечения информационной безопасности при использовании мобильных устройств в работе с Системой ДБО Клиенту необходимо:

- установить пароль на разблокировку мобильного устройства,
- активировать защиту SIM-карты мобильного устройства PIN-кодом,
- если на мобильном устройстве реализована поддержка технологий Touch ID и Android Fingerprint Authentication (датчик отпечатка пальца), использовать ее для разблокировки и аутентификации в приложении,
- включить на мобильном устройстве шифрование данных, если данная функциональность не активирована,
- скачивать и устанавливать на мобильное устройство программное обеспечение из проверенных источников,
- скачивать и устанавливать на мобильное устройство приложение Мобильного банка только из официальных магазинов приложений Google Play, AppStore,
- установить на мобильном устройстве антивирусное программное обеспечение, обеспечивающее защиту от вредоносного кода, которое должно обновляться и осуществлять периодическое полное сканирование мобильного устройства,
- код доступа к приложению на мобильном устройстве, с которого осуществляется работа в мобильном приложении, должен находиться отдельно от мобильного устройства. Запрещается сообщать код доступа к Мобильному банку неуполномоченным лицам, в том числе сотрудникам Банка,
- при получении любых сообщений или писем, связанных с работой Мобильного банка, обращать внимание на отправителя. Подобные сообщения должны поступать только с официального сервисного номера или адреса электронной почты Банка,
- не переходить по ссылкам и не открывать вложения из писем от подозрительных или неизвестных отправителей,
- всегда выполнять выход из Мобильного банка после завершения работы с документами и банковскими счетами,
- исключить доступ к мобильному устройству неуполномоченных лиц,
- в случае поломки мобильного устройства и необходимости его ремонта в сервисном центре удалить с мобильного устройства приложение Мобильного банка. По окончании ремонта мобильного устройства необходимо проверить мобильное устройство на отсутствие вредоносного кода и программ из неизвестных источников, а затем инициировать процесс генерации нового ключа ЭП,

- при подозрении, что код доступа к Мобильному банку стал известен посторонним лицам или при получении уведомлений об операциях по счету, которые не совершались Клиентом, немедленно обратиться в Банк и заблокировать свою учетную запись,
- немедленно сообщить в Банк при утере мобильного устройства, смене SIM-карты и (или) абонентского номера,
- регулярно ознакомливаться с информацией о выявленных уязвимостях программного обеспечения, методах социальной инженерии, направленной на получение несанкционированного доступа к конфиденциальной информации, размещенной на сайте Банка.

11. Права и обязанности Сторон

11.1. Клиент имеет право:

- Составлять и направлять в Банк, а также получать от Банка ЭД в соответствии с настоящим Регламентом.
- Обращаться в Банк за консультациями и с запросами по вопросам работы Системы ЭДО и обмена ЭД.
- По своему усмотрению генерировать ключи ЭП и регистрировать их в Банке, досрочно прекращать и блокировать действие своих ключей ЭП в соответствии с требованиями настоящего Регламента.
- Принимать участие в работе разрешительной комиссии в случае возникновения спорных или конфликтных ситуаций, касающихся Системы ДБО.

11.2. Клиент обязуется:

- Соблюдать требования настоящего Регламента.
- Оплачивать услуги Банка в соответствии с Тарифами.
- Передавать в Банк электронные документы, подписанные ЭП уполномоченных лиц в соответствии с предоставленной в Банк карточкой с образцами подписей и оттиска печати, требованиями действующего законодательства Российской Федерации и Банка России.
- Выполнять требования по информационной безопасности, в т.ч. обеспечить безопасность и целостность среды исполнения на своем компьютере (отсутствие вирусов и других вредоносных программ).
- Обеспечивать сохранность, целостность и работоспособность Системы ДБО.
- Использовать Систему ДБО только в целях, установленных договором банковского счета и настоящим Регламентом, без права передачи третьим лицам и копирования.
- Обеспечивать конфиденциальность и сохранность паролей и ключевой информации, хранящейся на носителе Клиента.
- В случае утери, механического повреждения ключевого носителя, компрометации ключей или возникновения подозрения компрометации незамедлительно уведомить Банк в порядке, установленном настоящим Регламентом.

- Организовать внутренний режим функционирования рабочих мест уполномоченных лиц таким образом, чтобы исключить возможность использования Системы ДБО и ключей ЭП лицами, не имеющими допуска к работе с Системой ДБО.
- Производить своевременную замену ключей ЭП уполномоченных лиц в случаях, предусмотренных настоящим Регламентом.
- Не разглашать и не передавать третьим лицам информацию, связанную с работой Системы ДБО, за исключением случаев, предусмотренных действующим законодательством Российской Федерации, договором банковского счета, настоящим Регламентом.
- Хранить электронные платежные документы, подписанные ЭП, в течение сроков, установленных действующим законодательством РФ.
- При поступлении от Банка уведомления об обновлении программного обеспечения, полученного в виде информационного сообщения по Системе ДБО, принимать меры для своевременного получения и установки новой версии программы.
- Незамедлительно информировать Банк обо всех изменениях, подлежащих отражению в банковской карточке с образцами подписей и оттиска печати. Замена карточки является основанием для приостановки использования обмена электронными документами с помощью Системы ДБО и смены ключей ЭП.
- В случае истечения срока действия паспорта гражданина РФ лиц, указанных в банковской карточке с образцами подписей и оттиска печати, при достижении ими 20-ти или 45-тилетнего возраста, а также признания паспорта недействительным по любым основаниям Клиент обязан незамедлительно представить в Банк в качестве документа, удостоверяющего личность указанных лиц, временное удостоверение личности гражданина Российской Федерации, выдаваемое на период оформления паспорта гражданина Российской Федерации, а после выдачи нового паспорта – новый паспорт.
- При поступлении от Банка запроса на предоставление сведений о выгодоприобретателе по конкретному платежному документу, полученного в виде информационного письма по Системе ДБО, предоставить в течение 3-х рабочих дней данные сведения в формате, поддерживаемом Системой ДБО. В случае появления/изменения выгодоприобретателя(ей) по договору, расчеты по которому проходят через Банк, предоставить сведения о выгодоприобретателе(ях) в формате, поддерживаемом Системой ДБО.
- В случае поступления запроса Банка, предоставлять в установленный Банком срок подтверждающие документы по проводимым операциям и сделкам, в том числе документы, подтверждающие необходимость снятия наличных денежных средств.
- Предоставлять в установленный Банком срок актуальную информацию (документы), необходимые для исполнения Банком требований Федерального закона от 07.08.2001 №115-

ФЗ в части идентификации клиента, представителя клиента, выгодоприобретателя и бенефициарного владельца.

- В случае утраты электронного средства платежа и (или) его использования без согласия Клиента, Клиент обязан направить Банку уведомление в письменной форме незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия Клиента, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции. Уведомление может быть передано по факсу или Системе ДБО с обязательным последующим предоставлением оригинала уведомления в письменной форме не позднее 5 (Пяти) рабочих дней с даты передачи уведомления по факсу/Системе ДБО.
- Проводить проверку соответствия реквизитов исполненных ЭПД с реквизитами полученной выписки со Счета в день получения выписки и, в случае установления расхождений, направлять в Банк извещение в письменной форме или по Системе ДБО в течение 5 дней, содержащее информацию о выявленных расхождениях. Неполучение Банком указанного извещения в установленный срок является подтверждением Клиента правильности исполнения ЭПД, подтверждением совершенной операции и остатка средств на Счете.
- Незамедлительно информировать Банк любым доступным способом о неисправностях в работе Системы ДБО,
- Немедленно приостановить использование Системы ДБО и незамедлительно информировать Банк любым доступным способом при установлении возможности нарушения безопасности Системы ДБО, выявлении фактов или признаков таких нарушений.
- Предоставлять уполномоченным лицам Банка и членам разрешительной комиссии доступ в помещение, где размещается Система ДБО, для проведения проверок, а также в рамках работы разрешительной комиссии.
- После расторжения договора банковского счета или прекращения его действия прекратить использование и уничтожить программное обеспечение Системы ДБО.

11.3. Банк имеет право:

- Требовать от Клиента замены ключей ЭП при плановой смене ключей ЭП, при смене лиц, уполномоченных распоряжаться Счетом, при нарушениях требований информационной безопасности в процессе эксплуатации Системы ДБО, а также в иных случаях.
- Блокировать ключи ЭП Клиента в случаях, предусмотренных Регламентом.
- Отказать Клиенту в приеме от него распоряжений на проведение операций по Счетам, подписанных корректной ЭП, а также ограничить и приостановить применение Клиентом Системы ДБО, включая распоряжение Клиентом Счетом посредством Системы ДБО, в случае выявления в деятельности Клиента признаков необычных операций и сделок, ненадлежащего исполнения Клиентом своих обязательств по договору банковского счета и настоящему

Регламенту, в том числе при непредставлении сведений по запросам Банка или в случае выявления факта отсутствия по местонахождению юридического лица, его постоянно действующего органа управления, иного органа или лица, которые имеют право действовать от имени юридического лица без доверенности, с предварительным уведомлением Клиента, а также по требованию уполномоченных государственных органов в случаях и в порядке, предусмотренных законодательством Российской Федерации. В случае ограничения или приостановления Банком применения Клиентом Системы ДБО в части распоряжения Счетом, Клиент осуществляет распоряжение Счетом посредством распоряжений на бумажном носителе, оформленных и представленных Клиентом в Банк в соответствии с требованиями действующего законодательства Российской Федерации, нормативных актов Банка России, условий договора банковского счета, настоящего Регламента и Тарифов. При ограничении или приостановлении Банком применения Клиентом системы ДБО в части распоряжения счетом у Клиента сохраняется возможность передачи в Банк и получения от Банка ЭД, не предусматривающих распоряжения Счетом.

- Ввести ограничения или прекратить предоставление Клиенту услуг по Системе ДБО в случае возникновения признаков нарушения безопасности с использованием программно-аппаратных средств Клиента.
- В одностороннем порядке вносить изменения в Тарифы и настоящий Регламент в порядке, указанном в разделе 20.6 настоящего Регламента.
- Производить запись любых телефонных переговоров Клиента с Банком.

11.4. Банк обязуется:

- Передавать Клиенту и/или размещать на сайте Банка актуальные версии прикладного программного обеспечения Системы ДБО.
- Хранить эталонные программные средства, предназначенные для создания и проверки корректности ЭП, а также документацию на эти средства.
- Принимать к исполнению поступившие от Клиента ЭПД, оформленные и переданные в Банк в соответствии с условиями договора банковского счета и настоящего Регламента и подписанные корректной ЭП Клиента,
- Не исполнять поступившие от Клиента ЭПД, оформленные с нарушением требований действующего законодательства Российской Федерации, нормативных актов Банка России и условий настоящего Регламента, а также при отсутствии или некорректности ЭП Клиента,
- Осуществлять банковские операции на основе электронного документа Клиента в сроки, установленные Договором банковского счета и настоящим Регламентом.
- Предоставлять Клиенту в виде электронного документа информацию об операциях по Счетам Клиента, подключенным к Системе ДБО, в соответствии с настоящим Регламентом.

- По заявлению Клиента в согласованные сроки и в соответствии с Тарифами Банка проводить выезд специалиста Банка для оказания услуг, связанных с установкой и эксплуатацией Системы ДБО,
- В случае получения от Клиента сообщения о компрометации ключей или возникновения подозрения компрометации приостановить прием, отправку и исполнение электронных документов с момента получения соответствующего сообщения от Клиента до выяснения обстоятельств, уведомив об этом Клиента.
- Сообщать Клиенту об обнаружении попытки несанкционированного доступа к Системе ДБО, если это затрагивало операции Клиента незамедлительно с момента обнаружения факта,
- Своевременно информировать Клиента о всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих обмену ЭД,
- Сохранять конфиденциальность информации об операциях Клиента.
- Консультировать Клиента по вопросам работы Системы ДБО, предоставлять ему возможность использования дополнительных услуг, предоставляемых Банком.
- Вести архив электронных документов и протоколов проверки ЭП.
- Организовать внутренний режим функционирования в Банке таким образом, чтобы исключить возможность использования Системы ДБО и ключей ЭП лицами, не имеющими допуска к работе с Системой ДБО.
- При возникновении спорных или конфликтных ситуаций создать разрешительную комиссию с целью проведения мероприятий, способствующих досудебному решению данных вопросов.

11.5. Стороны обязуются:

- Поддерживать за свой счет в рабочем состоянии программно-технические средства, используемые при проведении электронного обмена информацией с помощью Системы ДБО.
- Ограничить доступ к программно-техническим средствам Системы ДБО, а также обеспечить доступ к работе с ключами ЭП и проведению операций в Систем ДБО только уполномоченных лиц.
- При компрометации или подозрении на компрометацию ключей ЭП или шифрования осуществлять внеплановую смену ключей с приостановкой использования электронного обмена информацией по Системе ДБО на время замены.
- Клиент делегирует Банку право создавать на основе электронного документа, заверенного корректной ЭП Клиента, копию соответствующего документа на бумажном носителе, заверенную Банком.

12. Услуга sms-информирования (sms-банкинг)

12.1. Банк по Заявлению Клиента, оформленному по форме Приложения №7 к настоящему Регламенту, может предоставлять Клиенту услугу информирования о состоянии его Счетов, подключенных к Системе ДБО, путем направления Клиенту PUSH-сообщений/SMS-сообщений

и/или электронных сообщений посредством электронной почты с необходимой информацией по событиям/условиям и/или запросам Клиента. Перечень событий и условий, производимых со Счетом, о которых Клиент желает получать информацию, а также номера телефонов и адреса электронной почты, на которые Банку следует направлять данную информацию, Клиент указывает самостоятельно в Системе ДБО. Документация по настройке сервиса «SMS-Банкинг» находится на сайте Банка (<http://www.euroalliance.ru>).

12.2. Установка Клиентом на своем мобильном устройстве мобильного приложения «Весточка» и выполнение Клиентом первого входа в указанное приложение, при котором осуществляется регистрация экземпляра приложения на сервере Сервиса «Весточка», означает акцепт Клиентом Соглашения об использовании сервиса «Весточка» по отправке PUSH-сообщений Банка в Мобильное приложение «Весточка», установленное на устройстве Клиента, а также согласие Клиента на отправку Банком и получение Клиентом посредством сервиса «Весточка» PUSH-сообщений. В этом случае Банк не направляет Клиенту SMS-сообщения, кроме исключительных случаев, указанных в Соглашении об использовании сервиса «Весточка», размещенном на сайте Банка.

12.3. В случае утраты Клиентом мобильного телефона или SIM-карты, несанкционированного доступа третьих лиц к электронной почте Клиент обязан незамедлительно уведомить Банк о данных событиях по телефонам: (4932) 59-01-01, (4932) 41-25-79, с последующим обязательным предоставлением соответствующего письма в адрес Банка в течение трех рабочих дней с момента наступления указанных событий. Банк не несет ответственность за нарушение конфиденциальности информации о состоянии счетов Клиента в случае утраты Клиентом мобильного телефона или SIM-карты, несанкционированного доступа третьих лиц к электронной почте Клиента, на которые Банк осуществляет рассылку информации о состоянии счетов Клиента посредством сервиса sms-информирования (sms-банкинг).

12.4. Банк не несет ответственность за задержки и сбои, возникающие в сетях сотовых операторов и сервисах провайдеров, в том числе в связи с неоплатой услуг связи Клиентом, которые могут повлечь за собой задержки или недоставку sms-сообщений/push-сообщений и электронной почты Клиенту.

12.5. Банк имеет право временно блокировать доступ к услугам сервиса «SMS-Банкинг» без предварительного уведомления Клиента, если, по мнению Банка, такая мера необходима для обеспечения безопасности системы до прекращения обстоятельств, послуживших основанием применения указанной меры.

12.6. Стоимость услуг пользования сервисом «SMS-Банкинг» рассчитывается согласно Тарифам Банка, информация о которых находится на информационном стенде в Банке, на сайте Банка.

12.7. Оплата услуг SMS-Банкинга производится Банком путем списания денежных средств с расчетного счёта Клиента в российских рублях в соответствии с Тарифами Банка, без распоряжения Клиента, то есть Клиент предоставляет Банку заранее данный акцепт на списание.

12.8. В случае отключения Клиента от Системы ДБО по какой-либо причине, услуги информирования посредством сервиса «SMS-Банкинг» не предоставляются.

13. Услуга Доверенный получатель

13.1. Клиент может воспользоваться услугой Доверенный получатель в рамках сервиса Интернет-банк, создавая список контрагентов, в пользу которых регулярно осуществляет платежи. Клиент может задавать индивидуальный лимит для суммы платежного поручения каждого доверенного получателя.

13.2. Факт занесения контрагента в список Доверенных получателей Клиент подтверждает с помощью sms или push-сообщений.

13.3. В дальнейшем при отправке платежей в адрес Доверенных получателей подтверждение платежей Клиентом не требуется.

14. Сервис Центр финансового контроля (Сервис ЦФК)

14.1. Сервис предназначен для поддержки сложных схем обслуживания крупных корпоративных клиентов с территориально удаленными подразделениями и дочерними предприятиями. Сервис поддерживает централизованное управление счетами нескольких предприятий, финансовый мониторинг и распределенное визирование документов. В рамках Сервиса ЦФК работа управляющей компании с несколькими контролируруемыми предприятиями осуществляется без необходимости переключаться между организациями, позволяя работать с документами и счетами нескольких предприятий в режиме "одного окна". Сотрудник управляющей компании с помощью Сервиса ЦФК работает со счетами и документами всех контролируемых предприятий, ведет мониторинг состояния их счетов (просматривает выписки и остатки по счетам). Подробный порядок работы сервиса изложен в Пользовательской документации на сайте Банка.

14.2. Для подключения к Сервису ЦФК Клиент оформляет Заявление по форме Приложения №8 к настоящему Регламенту.

15. Контроль дополнительных параметров осуществления операций в Системе ДБО

15.1. На основании заявления Клиента, составленного по форме Приложения №9 к настоящему Регламенту, Банк может устанавливать дополнительные параметры осуществления операций в Системе ДБО.

16. Подтверждение платежных поручений

16.1. Клиент уведомлен и согласен, что в Системе ДБО используется механизм адаптивного подтверждения платежных поручений, при котором необходимость подтверждения платежных поручений Клиента посредством одноразовых кодов из sms и push-сообщений определяется по результатам обработки соответствующего платежного поручения автоматизированной системой противодействия хищениям денежных средств (системой антифрода), используемой Банком. В случае необходимости подтверждения платежа, Клиенту по альтернативному Системе ДБО каналу связи (sms или push-сообщения) направляется сообщение, содержащее сведения о сформированном платежном поручении, включая сумму и получателя денежных средств, до подтверждения Клиентом указанного платежного поручения с использованием одноразового кода.

16.2. При выявлении операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента либо иных операций, которые по результатам обработки платежного поручения Клиента автоматизированной системой противодействия хищениям денежных средств (системой антифрода), используемой Банком, признаны подлежащими дополнительной проверке, исполнение платежного поручения Клиента приостанавливается, о чем Банк информирует Клиента по телефону, факсу и/или электронной почте. Возобновление исполнения платежного поручения производится Банком только после получения от Клиента заявления о подтверждении возобновления исполнения данного платежного поручения по форме Приложения № 13 к настоящему Регламенту, которое может быть передано Клиентом по факсу, электронной почте и/или непосредственно в письменном виде в любом офисе Банка, либо после получения подтверждения возобновления исполнения платежного поручения от Клиента по телефону с использованием Блокировочного слова.

16.3. Для подключения механизма расширенной аутентификации (подтверждения по своему выбору всех или части платежных поручений посредством одноразовых кодов из sms и push-сообщений) Клиент может оформить заявление по форме Приложения №12 к настоящему Регламенту.

16.4. Заявления на подключение расширенной аутентификации в системе ДБО, оформленные и переданные Клиентами в Банк ранее 02.09.2019 г., действуют в части, не противоречащей пункту 16.1 настоящего Регламента.

17. Аварийный режим работы

17.1. При возникновении неисправности технических или программных средств Банка и/или Клиента, других нештатных ситуаций Стороны обязаны незамедлительно предупредить друг друга, и осуществить действия для доставки в Банк надлежащим образом оформленных документов на бумажных носителях в сроки, установленные договором банковского счета.

18. Ответственность сторон

18.1. Банк и Клиент несут ответственность за выполнение условий настоящего Регламента в рамках действующего законодательства РФ и нормативных актов Банка России.

18.2. Банк и Клиент несут ответственность за достоверность информации, предоставляемой друг другу.

18.3. Банк несет ответственность за содержание ЭД, подписанного ЭП Банка. Клиент несет ответственность за содержание ЭД, подписанного ЭП Клиента.

18.4. Ответственность за ущерб, возникший вследствие нарушения конфиденциальности информации, нарушения установленных настоящим Регламентом требований информационной безопасности и защиты информации от воздействия вредоносного кода, несет Сторона, допустившая нарушение.

18.5. Стороны не отвечают за правильность заполнения и оформления ЭД другой Стороной.

18.6. Банк не несет ответственность:

- за ущерб, возникший вследствие разглашения уполномоченными лицами Клиента собственного ключа ЭП, его утраты или передачи, вне зависимости от причин, а также разглашения других кодов и паролей Системы ДБО;
- за последствия исполнения ЭПД, защищенного корректной ЭП Клиента, в т.ч. в случае использования ключей ЭП и Системы ДБО неуполномоченным лицом;
- за неработоспособность оборудования и программных средств Клиента и третьих лиц, повлекшую невозможность доступа Клиента к Системе ДБО и возникшие в результате задержки в осуществлении платежей Клиента, а также за возможное полное или частичное уничтожение информации, хранящейся на вычислительных средствах Клиента, подключенных к сети Интернет для обеспечения работы с Системой ДБО;
- в случаях задержек и сбоев в сетях операторов сотовой связи и сервисах провайдеров, которые могут повлечь за собой задержку или недоставку передаваемых Банком sms-сообщений/push-сообщений/сообщений по электронной почте;
- вследствие изменений в законодательстве Российской Федерации и нормативных документах Банка России, которые делают невозможным для Банка выполнение своих обязательств по предоставлению Клиентам услуг с использованием Системы ДБО;
- в случае, если в процессе использования Клиентом Системы ДБО информация об операциях по Счету Клиента станет известна третьим лицам не по вине Банка;
- вследствие нарушения и(или) ненадлежащего исполнения Клиентом правил безопасного функционирования АРМ и/или МУ с установленным СКЗИ, требований по информационной безопасности и защите информации от воздействия вредоносного кода и/или вследствие нарушений их работоспособности в результате воздействия на них вредоносного кода, в т.ч. за несанкционированные переводы денежных средств в результате такого воздействия;
- в результате телефонного мошенничества («социальной инженерии») или использования уполномоченными лицами Клиента ложных («фальсифицированных») ресурсов сети Интернет.

18.7. Ответственность за правильность оформления и своевременность отправки электронных документов полностью возлагается на Клиента. Банк не несет ответственности за допущенную задержку в исполнении распоряжений Клиента, вызванную несвоевременным предоставлением в Банк электронных документов или их несоответствием установленным требованиям.

18.8. Банк не несет ответственности за некорректную работу клиентской части Системы ДБО, возникшей при изменении Клиентом программно-аппаратной конфигурации Системы ДБО без согласования с Банком.

18.9. Стороны освобождаются от ответственности за полное или частичное неисполнение каких-либо обязательств, вытекающих из условий настоящего Регламента, если это неисполнение явилось следствием возникших обстоятельств непреодолимой силы, которые Сторона не могла ни предвидеть, ни предотвратить своими силами, например, наводнение, пожар, землетрясение, другие

стихийные бедствия, повреждения линий связи, забастовки, состояние войны, правительственные постановления или распоряжения государственных органов, препятствующие выполнению условий настоящего Регламента. Срок исполнения обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого будут действовать такие обстоятельства. Если такие обстоятельства будут продолжаться более тридцати календарных дней, то каждая из Сторон имеет право отказаться от дальнейшего исполнения обязательств по настоящему Регламенту, и в этом случае ни одна из Сторон не будет иметь права на возмещение возможных убытков. Сторона, у которой возникли обстоятельства непреодолимой силы, должна сообщить другой Стороне о наступлении и прекращении таких обстоятельств в письменной форме, а в случае запроса Банком Клиент обязан предоставить ему в назначенные сроки документы государственных органов, подтверждающие наступление обстоятельств непреодолимой силы.

19. Порядок разрешения споров

19.1. При возникновении разногласий и споров в связи с обменом ЭД с помощью Системы ДБО с целью установления фактических обстоятельств, послуживших основанием для их возникновения, а также для проверки целостности и подтверждения авторства ЭД, Стороны должны создать разрешительную комиссию (далее – Комиссию) и провести экспертизу в соответствии с порядком, указанным ниже. Споры, по которым не достигнуто соглашение Сторон после проведения экспертизы разрешительной комиссией, разрешаются в Арбитражном суде Ивановской области.

19.2. В состав Комиссии входят в равном количестве до 5 представителей Сторон. В случае необходимости могут привлекаться независимые эксперты в области криптографии, защиты информации, информатизации. Участие экспертов должно быть письменно согласовано обеими Сторонами. Эксперты не должны состоять в родственных, трудовых, гражданско-правовых отношениях со Сторонами, быть их аффилированными лицами.

19.3. Сторона, заявляющая разногласие (Сторона-инициатор), обязана направить другой Стороне заявление в письменной форме, подписанное уполномоченным должностным лицом, с указанием предмета спора, своих требований, обстоятельств, на которых заявитель основывает свои требования, перечня прилагаемых документов и предложением создать Комиссию. Заявление должно содержать фамилии представителей Стороны-инициатора, которые будут участвовать в работе комиссии, место, время и дату сбора комиссии (не позднее 5 рабочих дней со дня отправления заявления).

19.4. До подачи заявления Стороне-инициатору необходимо убедиться в целостности своего программного обеспечения, неизменности используемой ключевой информации, а также отсутствии несанкционированных действий со стороны персонала, обслуживающего собственное автоматизированное рабочее место обмена ЭД. Акт о проведенной работе по проверке целостности программного обеспечения, неизменности используемой ключевой информации, а также отсутствии несанкционированных действий со стороны персонала Стороны-инициатора должен быть приложен к заявлению.

19.5. На основании заявления Стороны-инициатора другая сторона не позднее дня, следующего за днем получения заявления, уведомляет Сторону-инициатора о получении заявления и согласовывает место и время работы Комиссии с указанием её состава со своей стороны.

19.6. Члены комиссии от каждой Стороны назначаются приказами Сторон.

19.7. Комиссия создается на срок до 5 рабочих дней. В исключительных случаях срок работы Комиссии по согласованию Сторон может быть продлен до 30 дней.

19.8. Стороны обязуются способствовать работе Комиссии и не допускать отказа от предоставления необходимых документов.

19.9. Стороны обязуются предоставить Комиссии возможность ознакомления с условиями и порядком работы на используемых в Системе ДБО ЭСП, предоставить информацию о состоянии и работоспособности данных ЭСП, информацию журналов работы и аудита Системы ДБО, в т.ч. информацию об отправленных на номер мобильного телефона Клиента sms-кодах/push-сообщениях с указанием даты и времени отправки, информацию о IP/MAC-адресах ЭСП Клиента, с которых осуществлялась работа в Системе ДБО, журналы работы системного, прикладного и антивирусного программного обеспечения, установленного на ЭСП Клиента, иную необходимую информацию.

19.10. В ходе работы Комиссии каждая Сторона обязана доказать, что она исполнила обязательства в соответствии с Регламентом надлежащим образом.

19.11. Работа Комиссии проходит в два этапа.

Первый этап - подготовительный.

Комиссия проверяет целостность программного обеспечения (ПО) АРМ обмена ЭД, установленного на АРМ у Клиента, и его контрольных характеристик. Полученные результаты сравниваются со значениями эталонного ПО, установленного на специализированном рабочем месте в Банке. В случае нарушения целостности ПО, установленного у Клиента, дальнейшее рассмотрение разногласий не проводится, а ответственность возлагается на Клиента. Если ПО Клиента совпадает с эталонным ПО, установленным на специализированном рабочем месте в Банке, оно принимается к использованию в работе Комиссии.

Ключи проверки ЭП Клиента, хранящиеся в Банке и у Клиента, сравниваются между собой. При положительном результате сравнения проверенные ключи принимаются к использованию в дальнейшей работе комиссии.

С помощью принятого комиссией к работе ПО проверяется целостность ключей, находящихся у Клиента.

При отрицательном результате сравнения, а также нарушении целостности ключей Клиента дальнейшее рассмотрение разногласий не проводится, а ответственность возлагается на Клиента.

Второй этап - проверка и анализ спорных документов.

Комиссией рассматриваются разногласия следующих типов:

1) Сторона-отправитель утверждает, что не направляла электронный платежный документ (ЭПД), а Сторона-получатель утверждает, что ЭПД был получен;

2) Сторона-получатель утверждает, что не получала ЭПД, а Сторона-отправитель утверждает, что ЭПД был направлен.

Разрешение 1-й спорной ситуации осуществляется в следующей последовательности.

- Сторона-получатель представляет ЭПД, оспариваемый Стороной-отправителем.
- Комиссия осуществляет подтверждение подлинности данного ЭПД путем проверки ЭП Стороны-отправителя с помощью принятого Комиссией к использованию ПО.
- Если в результате проверки будет установлена подлинность ЭПД, представленного Стороной-получателем, то Комиссией принимается решение о том, что Сторона-отправитель направляла ЭПД Стороне-получателю и должна нести за него ответственность.
- Если Сторона-отправитель настаивает на том, что данный ЭПД она не отправляла, Комиссия может вынести определение о компрометации секретного ключа ЭП Стороны-отправителя, что не снимает ответственности Стороны-отправителя за данный ЭПД.
- Если проверка ЭП Стороны-отправителя под оспариваемым ЭПД дает отрицательный результат, то Комиссией принимается решение о том, что Сторона-отправитель не направляла ЭПД Стороне-получателю и не должна нести за него ответственность. В этом случае ответственность за ЭПД несет Сторона-получатель.

Разрешение 2-й спорной ситуации осуществляется следующим образом.

- Сторона-отправитель предоставляет ЭПД, оспариваемый Стороной-получателем.
- Комиссия осуществляет подтверждение подлинности данного ЭПД путем проверки ЭП Стороны-отправителя с помощью принятого Комиссией к использованию ПО. Если подлинность ЭПД не подтверждена, Сторона-получатель не несет ответственность.
- Если в результате проверки будет установлена подлинность ЭПД, представленного Стороной-отправителем, далее Комиссия определяет соответствие фактического прохождения данного ЭПД схеме документооборота, установленной настоящим Регламентом. Если оспариваемым документом является не ЭПД, а протокол приема ЭПД и для этого протокола приема ЭПД не предусмотрено получение подтверждения о получении, подписанного ЭП, Комиссия ввиду отсутствия объективных доказательств получения ЭД Стороной-получателем не принимает к рассмотрению претензии по таким документам.

19.12. По итогам работы Комиссии составляется акт, содержащий:

- фактические обстоятельства, послужившие основанием возникновения разногласий;
- порядок работы членов Комиссии;
- вывод о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого ЭД и его обоснование.

19.13. Акт составляется не менее чем в 2 экземплярах, подписывается всеми членами Комиссии. Каждой из Сторон Комиссия направляет по одному экземпляру акта для принятия решения. Члены

Комиссии, не согласные с мнением большинства, подписывают акт с особым мнением, которое прикладывается к акту.

19.14. В случае, если на предложение Стороны-инициатора о создании Комиссии ответ другой Стороны не был получен или получен отказ от участия в работе Комиссии, или если другой Стороной создавались препятствия работе комиссии, Сторона-инициатор вправе составить акт в одностороннем порядке с указанием причины его составления. В акте приводится обоснование выводов о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого ЭД. Указанный акт составляется в двух экземплярах, подписывается уполномоченным должностным лицом, и один экземпляр направляется другой Стороне.

19.15. В случае разногласия членов Комиссии при составлении акта, Комиссией составляется акт с подробным изложением мнений членов Комиссии. Заинтересованная сторона на основании акта направляет другой стороне обоснованную претензию в письменном виде. Другая сторона рассматривает и дает ответ в письменном виде в течение 10 (десяти) дней с момента получения претензии. В случае не предоставления ответа на претензию в установленный настоящим Регламентом срок либо предоставления отрицательного ответа, спор подлежит рассмотрению в Арбитражном суде Ивановской области.

20. Прочие условия

20.1. Договор на обслуживание по Системе ДБО действует в течение неопределенного срока.

20.2. Клиент вправе расторгнуть Договор на обслуживание по Системе ДБО, уведомив Банк в письменной форме не менее чем за 15 дней до предполагаемой даты расторжения.

20.3. Действие Договора на обслуживание по Системе ДБО автоматически завершается в случае расторжения договора банковского счета между Банком и Клиентом.

20.4. Банк может расторгнуть Договор на обслуживание по Системе ДБО в одностороннем порядке, в случае нарушения Клиентом требований настоящего Регламента, а также в иных случаях по усмотрению Банка, уведомив Клиента в письменной форме не менее чем за 15 дней до предполагаемой даты расторжения.

20.5. Клиент самостоятельно устанавливает программное обеспечение, предоставленное Банком или полученное с сайта Банка, осуществляет смену ключей и обновление программ. При возникновении вопросов по эксплуатации или неисправностей в работе Системы ДБО Клиенту доступны консультации специалистов Банка по телефонам: (4932) 59-01-01, (4932) 41-25-79, 8 800 700 92 22. В случае невозможности самостоятельно устранить неисправности в работе Системы вызов специалиста Банка осуществляется на основании письменной заявки Клиента по форме Приложения №10 к настоящему Регламенту. Заявка может быть принята по факсу или электронным сообщением по адресу: banking@euroalliance.ru, с последующим направлением в Банк оригинала заявки. Выход специалиста Банка осуществляется в сроки по договоренности с Клиентом и оплачивается в соответствии с установленными Тарифами.

20.6. Внесение изменений в настоящий Регламент осуществляется Банком в одностороннем порядке.

20.7. Банк размещает на сайте www.euroalliance.ru и уведомляет Клиентов о вступлении в силу новой редакции Регламента не позднее 10 (Десяти) календарных дней до даты вступления в силу новой редакции одним или несколькими способами на усмотрение Банка:

- размещение информационных сообщений на сайте Банка,
- размещение информационных сообщений в офисах Банка,
- рассылка информационных сообщений Клиентам по Системе ДБО,
- рассылка информационных сообщений на адреса электронной почты Клиентов,
- рассылка информационных sms-сообщений Клиентам.

**ЗАЯВЛЕНИЕ
на подключение к Системе ДБО**

" ____ " _____ 20__ г.

Полное наименование юридического лица / ФИО индивидуального предпринимателя / ФИО физического лица, занимающегося частной практикой

ИНН (КИО): _____

Телефон: _____

E-mail: _____

просит подключить наш(и) Счет/Счета №№ _____
_____ к Системе ДБО.

Настоящим подтверждаем, что ознакомлены с действующим Регламентом обслуживания клиентов в системе «БАНК-КЛИЕНТ» АО КИБ «ЕВРОАЛЪЯНС», выражаем свое согласие с ним и обязуемся выполнять.

Обязуемся самостоятельно ознакомливаться с действующей редакцией Регламента обслуживания клиентов в системе «БАНК-КЛИЕНТ» АО КИБ «ЕВРОАЛЪЯНС» на сайте www.euroalliance.ru.

С тарифами Банка по установке и обслуживанию Системы ДБО ознакомлены и согласны.

Просим предоставить устройства генерации и хранения ключей ЭП:

USB – токен MS_KEY К – АНГАРА в количестве _____ штук.

В качестве получателей одноразовых паролей будут использоваться следующие номера мобильных телефонов:

+7 (_____) _____

+7 (_____) _____

Просим установить следующее Блокировочное слово: _____

Предоставляем Банку право списать со счета № _____, открытого в АО КИБ «ЕВРОАЛЪЯНС», без нашего распоряжения плату согласно тарифам, т.е. предоставляем заранее данный акцепт.

Наименование должности руководителя / _____ / _____
подпись *ФИО*

М.П.

Заполняется Банком

Заявление принято: « ____ » _____ 20__ г.

Сотрудник, принявший заявление: _____ / _____ /

Согласовано:

Руководитель банка /лицо, действующее на основании доверенности / _____ / _____
Подпись *ФИО*

Дата согласования заявления Банком: « ____ » _____ 20__ г.

ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ, ПЕРЕСЫЛАЕМЫХ ПО СИСТЕМЕ ДБО

Виды сообщений, которые Клиент передает в Банк по Системе ДБО:

Наименование ЭД	Вид сообщения
Платежные поручения по перечислению рублевых средств	Формализованное
Платежные требования	Формализованное
Инкассовые поручения	Формализованное
Отзыв документа	Свободный формат
Заявление об акцепте	Формализованное
Заявление на перевод (валютные документы)	Формализованное
Поручение на покупку иностранной валюты	Формализованное
Поручение на продажу иностранной валюты	Формализованное
Распоряжение на обязательную продажу иностранной валюты	Формализованное
Справка о валютных операциях	Формализованное
Справка о подтверждающих документах	Формализованное
Сведения о выгодоприобретателе – юридическом лице, физическом лице	Формализованное
Уведомление о зачислении валюты на транзитный счет	Формализованное
Сведения о валютных операциях	Формализованное
Заявление о постановке на учет контракта (кредитного договора)	Формализованное
Заявление о снятии с учета контракта (кредитного договора)	Формализованное
Заявление о внесении изменений в раздел I ведомости банковского контроля	Формализованное
Заявка на получение наличных денежных средств	Формализованное

Виды сообщений, которые Клиент получает по Системе ДБО из Банка:

Наименование ЭД	Вид сообщения
Выписки по рублевым счетам Клиента, включая остатки по счетам	Формализованное
Выписки по валютным счетам Клиента, включая остатки по счетам	Формализованное
Выписки по ссудным счетам Клиента	Формализованное
Выписки по счетам картотеки к расчетным счетам Клиента*	Формализованное
Уведомление о расторжении Соглашения	Свободный формат
Дополнительные соглашения	Свободный формат
Прочие сообщения	Свободный формат
Запрос о предоставлении сведений по выгодоприобретателю	Свободный формат
Предупреждение об отказе в приеме ЭД, подписанных ЭП	Формализованное

* Предоставляется по заявке Клиента (по форме Приложения №11) в режиме просмотра.

Перечень и формы ЭД могут меняться с учетом развития системы и услуг, предоставляемых Клиентам Банка при использовании Системы.

АКТ ПРИЕМА-ПЕРЕДАЧИ ключевого носителя

г. Иваново

“ ____ “ _____ 20__ г.

Акционерное общество коммерческий инвестиционный банк «ЕВРОАЛЬЯНС», именуемый
в _____
лице _____

действующего на основании _____, передал, а

менуемый в _____
лице _____

действующего на основании _____, принял:

USB-токен _____ №№ _____ в количестве ____ штук.

Настоящий Акт составлен в 2 (двух) экземплярах, по одному для каждой из сторон.

БАНК

КЛИЕНТ

Ответственный сотрудник ОКЗИ

(подпись)

(подпись)

М. П.

АКТ ПРИЕМА-ПЕРЕДАЧИ
средства криптографической защиты информации (СКЗИ)

г. Иваново

“ ____ “ _____ 20__ г.

Акционерное общество коммерческий инвестиционный банк «ЕВРОАЛЬЯНС», именуемый
в _____ дальнейшем «БАНК», в
лице _____
действующего на основании _____, передал, а
_____ именуемый в _____ «КЛИЕНТ», в
лице _____
действующего на основании _____, принял:
средство криптографической защиты информации _____ (на компакт-диске
регистрационный № ____):

Имя	Контрольная сумма	Описание
Программное обеспечение контроля целостности, утилита для удаления файлов		
Модуль СКЗИ		
Самораспаковывающийся архив		

Настоящий Акт составлен в 2 (двух) экземплярах, по одному для каждой из сторон.

БАНК

КЛИЕНТ

Ответственный сотрудник ОКЗИ

_____ (подпись)

_____ (подпись)

М. П.

**СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА
КЛИЕНТА В СИСТЕМЕ «БАНК-КЛИЕНТ» АО КИБ "ЕВРОАЛЬЯНС"**

1. Наименование организации _____

2. Юридический адрес _____

3. ОГРН _____ дата внесения в ЕГРЮЛ (ЕГРИП) «__» _____ г.

4. Тел. _____ 5. ИНН (КИО) _____ 6. КПП _____

7. Факс* _____ 8. E-mail* _____

9. Сведения о владельце ключа:

Фамилия, имя, отчество _____

Должность _____

Документ, удостоверяющий личность _____

серия _____ номер _____ дата выдачи " " 20__г.

кем выдан _____

10. Примечания*

* обязательно для заполнения

Настоящим подтверждаю согласие на обработку Банком моих персональных данных _____
подпись

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа проверки ЭП _____ Идентификатор устройства _____

Наименование криптосредств _____

Алгоритм _____ ID набора параметров алгоритма _____

Представление ключа проверки ЭП в шестнадцатеричном виде

Личная подпись владельца ключа проверки ЭП

Срок действия (заполняется Банком):

с " " _____ 20__г.

по " " _____ 20__г.

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках Регламента обслуживания клиентов в системе «БАНК-КЛИЕНТ» АО КИБ «ЕВРОАЛЬЯНС».

Достоверность приведенных данных подтверждаю

Руководитель организации

Уполномоченный представитель Банка

_____/_____/_____
подпись / ф.и.о.

_____/_____/_____
подпись / ф.и.о.

Оттиск печати

Оттиск печати

Дата приема сертификата
ключа проверки ЭП
«__» _____ 20__г.

Администратор безопасности Системы ДБО

_____/_____/_____
подпись / ф.и.о.

Дата регистрации сертификата ключа проверки ЭП
«__» _____ 20__г.

**Уведомление о компрометации
ключа электронной подписи (ЭП) Клиента**

" ____ " _____ 20__ г.

Полное наименование юридического лица / ФИО индивидуального предпринимателя / ФИО физического лица, занимающегося частной практикой

Адрес местонахождения, телефон, e-mail

ИНН (КИО): _____

уведомляет о компрометации ключей ЭП, принадлежащих следующим уполномоченным лицам

Клиента:

№ п/п	ФИО Владельца ключа ЭП (сотрудника Клиента)	Идентификатор ключа проверки ЭП	Обстоятельства компрометации ключа ЭП

Наименование должности руководителя

подпись

ФИО

М.П.

Заполняется Банком

Заявление принято: « ____ » _____ 20__ г. ____ часов ____ минут

Сотрудник, принявший заявление: _____ / _____ /

**Уведомление об отмене действия ключа ЭП/утрате электронного средства платежа и/или его
использования без согласия Клиента**

"__" _____ 20__ г.

Полное наименование юридического лица / ФИО индивидуального предпринимателя / ФИО физического лица, занимающегося частной практикой

Адрес местонахождения, телефон, e-mail

ИНН (КИО): _____

уведомляет (выбрать необходимое):

Об отмене действия ключа ЭП

№ п/п	ФИО Владельца ключа ЭП (сотрудника Клиента)	Идентификатор ключа проверки ЭП	Причина отмены действия ключа ЭП
1			
2			
3			

Об утрате (хищении) электронного средства платежа

№ п/п	Наименование устройства	Идентификатор устройства	Обстоятельства, в т.ч. дата и время обнаружения Клиентом, утраты (хищения)
1			
2			
3			

Об использовании электронного средства платежа без согласия Клиента

№ п/п	Наименование устройства	Идентификатор устройства	Обстоятельства, т.ч. дата и время обнаружения Клиентом, использования ЭСП без согласия Клиента

ЗАЯВЛЕНИЕ

о подключении сервиса sms-информирования (sms-банкинг)

"__" _____ 20__ г.

Полное наименование юридического лица / ФИО индивидуального предпринимателя / ФИО физического лица, занимающегося частной практикой

ИНН (КИО): _____

просит подключить наш Счет/Счета №№ _____

_____ к сервису sms-информирования (sms-банкинг).

Наименование должности руководителя

подпись

ФИО

М.П.

Заполняется Банком

Заявление принято: «__» _____ 20__ г.

Сотрудник, принявший заявление: _____ / _____ /

Подключение к сервису sms-информирования произведено: «__» _____ 20__ г.

Ответственный сотрудник: _____ / _____ /

**ЗАЯВКА
на подключение к сервису ЦФК**

Просим осуществить подключение к сервису ЦФК следующих организаций в качестве единой группы:

№ п/п	Наименование	№ расчетного счета	Подпись руководителя, печать
1.			
2.			
3.			
4.			
5.			

Сертификаты ключей для доступа к сервису ЦФК на __ лист __ прилагаются.

Наименование должности руководителя

подпись

ФИО

М.П.

Заполняется Банком

Заявление принято: «___» _____ 20__ г.

Сотрудник, принявший заявление: _____ / _____ /

Подключение к Сервису ЦФК произведено: «___» _____ 20__ г.

Ответственный сотрудник: _____ / _____ /

Заявление

на установление дополнительных параметров осуществления операций в Системе ДБО¹

Полное наименование юридического лица / ФИО индивидуального предпринимателя / ФИО физического лица, занимающегося частной практикой

ИНН (КИО): _____

просит установить следующие дополнительные параметры осуществления операций в Системе ДБО:

1) максимальная сумма перевода денежных средств:

за одну операцию _____ и/или *(нужное подчеркнуть)*

за день/месяц _____ *(нужное подчеркнуть)*.

2) перечень возможных получателей денежных средств *(наименование, реквизиты)*:

3) географическое местоположение устройств, с использованием которых может осуществляться подготовка и (или) подтверждение Клиентом электронных сообщений (доверенные регионы):

4) перечень идентификаторов устройств, с использованием которых может осуществляться подготовка и (или) подтверждение Клиентом электронных сообщений (ID USB-токена, IP-адреса, номер мобильного телефона):

5) перечень услуг, предоставляемых с использованием Системы ДБО:

¹ Устанавливаются Банком при наличии технической возможности

б) временной период, в который могут быть совершены переводы денежных средств с использованием Системы ДБО:

Наименование должности руководителя

подпись

ФИО

М.П.

Заполняется Банком

Заявление принято: « ____ » _____ 20__ г.

Сотрудник, принявший заявление: _____ / _____ /

Выполнено: « ____ » _____ 20__ г.

Комментарии:

Ответственный сотрудник: _____ / _____ /

ЗАЯВКА
на подключение дополнительных видов сообщений по Системе ДБО

" ___ " _____ 20__ г.

Полное наименование юридического лица / ФИО индивидуального предпринимателя / ФИО физического лица, занимающегося частной практикой

ИНН (КИО): _____

Просит предоставить право получения выписок по счету №
_____ без права распоряжения
вышеуказанным счетом.

Наименование должности руководителя *подпись* / _____ /
ФИО

М.П.

Заполняется Банком

Заявление принято: « ___ » _____ 20__ г.

Сотрудник, принявший заявление: _____ / _____ /

Выполнено: « ___ » _____ 20__ г.

Ответственный сотрудник: _____ / _____ /

**Заявление
на подключение/отключение расширенной аутентификации
в системе ДБО**

1. Настоящим _____
(наименование Клиента)

просит подключить/отключить (нужное подчеркнуть) механизм расширенной многофакторной аутентификации с использованием одноразовых паролей, получаемых посредством PUSH-сообщений/SMS-сообщений:

На сумму платежа, превышающую:

_____ (_____) рублей.
(сумма цифрами) (сумма прописью)

Независимо от суммы платежа.

Установка Клиентом на своем мобильном устройстве мобильного приложения «Весточка» и выполнение Клиентом первого входа в указанное приложение, при котором осуществляется регистрация экземпляра приложения на сервере Сервиса «Весточка», означает акцепт Клиентом оферты Банка по отправке PUSH-сообщений Банка в Мобильное приложение «Весточка», установленное на устройстве Клиента (далее – оферта), а также согласие Клиента на отправку Банком и получение Клиентом посредством сервиса «Весточка» PUSH-сообщений. В этом случае Банк не направляет Клиенту SMS-сообщения, кроме исключительных случаев, указанных в оферте.

2. В качестве получателей одноразовых паролей будут использоваться номера мобильных телефонов, указанные в Заявлении на подключение к Системе ДБО или в Заявлении на изменение/отключение номеров мобильных телефонов.

Мы поставлены в известность о том, что возможна задержка в доставке SMS-сообщения с одноразовым паролем по вине сотового оператора.

_____/_____
Наименование должности руководителя подпись ФИО

М.П.

Заполняется Банком

Заявление принято: «___» _____ 20__ г.

Сотрудник, принявший заявление: _____/_____

ЗАЯВКА НА ПОЛУЧЕНИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ

№ _____ от _____

Клиент _____

Банку _____

Списать со счета _____ и подготовить к выдаче _____
в отделении _____
(код отделения) (наименование)

Получатель _____
средств _____
Сумма _____

Назначение _____

Дополнительная _____
информация _____

М.П. _____
