

ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

г. Москва

Действуют с 16.08.2019 г.

1. ИСПОЛЬЗУЕМЫЕ ПОНЯТИЯ И ТЕРМИНЫ

Договор – настоящий договор присоединения в соответствии со статьей 428 Гражданского кодекса РФ, заключенный между ООО «НКО «Вестерн Юнион ДП Восток», ОГРН 1037739616122, ИНН 7727067410, расположенным по адресу 125171, Россия, г. Москва, Ленинградское шоссе, дом 16А, строение 1, лицензия Банка России № 2726-С от 08.05.2013 г. (далее – «НКО») и Клиентом, состоящий из настоящих Правил дистанционного банковского обслуживания (далее – «Правила») с приложениями, в том числе Заявления о присоединении к Правилам дистанционного банковского обслуживания (далее – «Заявление о присоединении»), Тарифов НКО. Правила с приложениями, в том числе Заявление о присоединении, Тарифы НКО размещаются НКО на официальном сайте НКО в сети Интернет www.wumte.ru.

Клиент – кредитная организация - участник Платежной Системы Вестерн Юнион, заключившая с НКО договор об установлении корреспондентских отношений и порядке открытия и ведения корреспондентского счета в российских рублях и/или иностранной валюте, присоединившийся к Договору в установленном порядке, с целью проведения расчетных операций по банковскому счету Клиента, открытому в НКО, на основании электронных платежных документов, подписанных электронной подписью Клиента, с использованием Системы ДБО и СИКЮЛ.

Система дистанционного банковского обслуживания (далее – «Система ДБО») – корпоративная информационная Система НКО, представляющая собой совокупность программно-аппаратных средств, устанавливаемых у Клиента и у НКО с целью организации электронного документооборота с возможностью автоматизации расчетов посредством обработки ЭД, подписания их ЭП и проверки ЭП.

Система «Интернет клиент для юридических лиц» (далее – «СИКЮЛ») – элемент Системы ДБО, представляющий собой программный комплекс «InterBank RS» и использующая для соединения с НКО сеть Интернет (минимальная скорость передачи данных не ниже 128 Kbps), клиентское программное обеспечение которой функционирует через веб-браузеры (URL-адрес сайта СИКЮЛ <https://dbo.westernunion.ru>).

Работа клиентского программного обеспечения СИКЮЛ обеспечивается в операционных средах и КриптоПро ЭЦП Browser plug-in обеспечивается в операционных средах, поддерживаемых разработчиком СКЗИ (более подробно на сайте разработчика <http://cryptopro.ru/products/cades/plugin>) при использовании лицензионного программного обеспечения и настройке операционной системы, дополнительных компонентов, политики безопасности в соответствии с требованиями пользовательской документации. Версия операционной системы Windows должна быть не ниже 7. Обязательно наличие устройства для подключения ключевого носителя - порта USB не ниже 2.0.

Под обработкой ЭД понимается отправка ЭД Клиентом, отправка подтверждений на принятие Банком ЭД Клиента, вывод ЭД на печать и др.

Безопасность информации – состояние информации, информационных ресурсов и информационных систем, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, копирования, блокировки, нарушения конфиденциальности, доступности, достоверности и т.п.; состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних и внешних угроз.

Достоверность информации – состояние информации, информационных ресурсов и информационных систем, при котором обеспечивается отсутствие искажения, модификации, подделки, и иного изменения информации лицами, не имеющими соответствующих полномочий.

Электронный документ (далее – «ЭД») – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. В СИКЮЛ под электронными документами понимаются оформленные в соответствии с требованиями Центрального банка РФ платежные документы и согласованные Сторонами документы, необходимые для расчетно-кассового обслуживания и валютного контроля.

Электронная подпись (далее – «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. В соответствии с видами электронной подписи, установленными Федеральным законом от «6» апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – «Закон») в настоящих Правилах под ЭП понимается и используется в системе электронных расчетов усиленная неквалифицированная электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после его подписания; создается с использованием средств электронной подписи.

Удостоверяющий центр (далее – «УЦ») – НКО, осуществляющая функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Администратор Удостоверяющего центра (далее – «Администратор УЦ») – уполномоченный представитель Удостоверяющего центра, ответственный за выполнение операций по регистрации пользователей, изготовлению и обслуживанию сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего Центра.

Администратор безопасности – уполномоченное Клиентом лицо на осуществление регистрации пользователей Клиента в УЦ.

Средства УЦ – программные и (или) аппаратные средства, используемые для реализации функций УЦ.

Средство криптографической защиты информации (далее – «СКЗИ») – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средства ЭП – СКЗИ, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка (подтверждение) ЭП, создание секретного ключа ЭП и ключа проверки ЭП.

Владелец сертификата ключа проверки ЭП – лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки ЭП.

Ключевой носитель – машинный носитель информации (USB токен), содержащий секретный ключ ЭП.

Ключ ЭП (секретный ключ ЭП) – уникальная последовательность символов, предназначенная для создания ЭП.

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с секретным ключом ЭП и предназначенная для проверки подлинности ЭП.

Генерация ключа – операция, предусмотренная СКЗИ, результатом которой является выработка секретного ключа ЭП, ключа проверки ЭП.

Реквизиты персонального пароля – уникальные последовательности символов (логин, пароль и идентификатор), генерируемые для каждого Пользователя Клиента, благодаря которым становится возможным вход Пользователя в СИКЮЛ и самостоятельная генерация Пользователем секретного ключа ЭП.

Сертификат ключа проверки ЭП – электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП Владельцу сертификата ключа проверки ЭП; включает в себя ключ проверки ЭП, информацию о Владельце сертификата, сведения об УЦ, выдавшем сертификат, дополнительные атрибуты (расширения), определяемые требованиями использования сертификата ключа проверки ЭП в защищенной системе и др.

Подтверждение подлинности ЭП (далее – «проверка ЭП») – положительный результат проверки средством ЭП с использованием сертификата ключа проверки ЭП принадлежности ЭП в электронном документе Владельцу сертификата ключа проверки ЭП и отсутствия искажений (изменений) в подписанном данной ЭП электронном документе, с указанием лица, с использованием ключа ЭП которого подписан проверяемый ЭД.

Компрометация секретных ключей ЭП – нарушение конфиденциальности секретных ключей ЭП, утрата доверия к тому, что используемый ключ ЭП обеспечивает безопасность информации; констатация Владельцем сертификата ключа проверки ЭП обстоятельств, при которых возможно несанкционированное использование его ключа ЭП неуполномоченными лицами.

Информационный сервис – сервис доступа Клиента к СИКЮЛ с возможностью просмотра выписки по подключенным к системе счетам Клиента, а также возможность запроса выписки (наличие USB-порта, крипто-компонент, использование ключей ЭП не требуются). При этом возможность совершать Клиентом расходные операции по банковскому счету, а также обмениваться информацией с НКО документами посредством СИКЮЛ отсутствует.

Пользователь – уполномоченное лицо Клиента, состоящее с Клиентом в трудовых отношениях, которому на основании предоставленного в НКО Заявления о присоединении на подключение Клиента к СИКЮЛ (Приложение 1) предоставлен доступ к СИКЮЛ.

Сторона – НКО или Клиент.

Стороны – НКО и Клиент.

Официальный сайт НКО в сети Интернет – www.wumte.ru.

2. ПРЕДМЕТ ДОГОВОРА

- 2.1. НКО предоставляет Клиенту на возмездной основе доступ к Системе дистанционного банковского обслуживания НКО «Интернет клиент для юридических лиц» (СИКЮЛ) с целью передачи Клиентом в НКО подписанных электронной подписью Клиента распоряжений на проведение расчетных операций по корреспондентскому счету Клиента, открытому в НКО для целей осуществления расчетов в рамках Платежной Системы Вестерн Юнион.
- 2.2. К Системе дистанционного банковского обслуживания НКО «Интернет клиент для юридических лиц» (СИКЮЛ) могут быть подключены несколько корреспондентских счетов Клиента, открытых в НКО.
- 2.3. Настоящим Договором Стороны признают юридическую силу ЭД, подписанных ЭП соответствующей Стороны с использованием Средств ЭП, созданных в соответствии с действующим законодательством об электронной подписи и средствах криптографической защиты информации.
- 2.4. В СИКЮЛ принимаются к исполнению распоряжения о переводе денежных средств, оформленные в соответствии с действующим законодательством и необходимые для проведения операций по счетам Клиента. Для проведения операций по счету Клиента, открытому в НКО, используются электронные документы, содержащие все реквизиты платежного документа на бумажном носителе.
- 2.5. При обслуживании в СИКЮЛ валютных счетов Клиента, Сторонами допускается обмен электронными документами, оформляемыми при совершении валютных операций в соответствии с банковским законодательством и законодательством о валютном регулировании и валютном контроле.
- 2.6. В Системе ДБО НКО не принимаются к исполнению ЭД, направленные на возникновение, прекращение, изменение между НКО и Клиентом иных обязательств, не оговоренных настоящими Правилами.
- 2.7. Время приема к исполнению электронных документов Клиента и форматы электронных документов, регламентируются договорами и соглашениями, заключенными между Клиентом и НКО.
- 2.8. Используемый в СИКЮЛ сертификат ключа проверки ЭП должен быть создан исключительно средствами ЭП, используемыми в данной СИКЮЛ (для обеспечения программной и технологической совместимости).
- 2.9. Стороны признают, что средства УЦ и средства ЭП, применяемые в СИКЮЛ, при их использовании в соответствии с мерами по обеспечению безопасности информации, предусмотренными в настоящих Правилах, не нарушают достоверность информации, обрабатываемой с их помощью.
- 2.10. Стороны признают, что правом подписания электронных документов, обрабатываемых в СИКЮЛ, наделены лица, включенные в карточку с образцами подписей и оттиска печати Клиента, предоставленную ранее Клиентом НКО при открытии банковского (банковских) счета (счетов), с учетом сочетания подписей согласованных Клиентом и НКО.
- 2.11. Стороны признают, что правом формировать и обрабатывать электронные документы в СИКЮЛ могут быть наделены лица, не включенные в карточку образцов подписей и оттиска печати Клиента, при условии, что данные лица наделены таким правом в соответствии с доверенностью (Приложение 5).
- 2.12. Передача реквизитов персонального пароля производится Администратору безопасности Клиента, указанному в заявке на подключение Клиента к СИКЮЛ. Обладание одним физическим лицом – уполномоченным представителем Клиента несколькими секретными ключами ЭП с правом подписи ЭД не допускается.

Уровень возможных прав доступа:

Роль подписи	Права	Комментарий
Пользователь без права подписи	Сотрудник Клиента без ЭП	Просмотр, создание, редактирование, выгрузка, платежных поручений; просмотр, создание писем.
Пользователь	Сотрудник Клиента (единственная подпись)	Просмотр, создание, редактирование, выгрузка, отправка и отзыв платежных поручений; просмотр, создание, отправка писем.
Единоличный исполнительный орган Клиента, его заместитель, член коллегиального исполнительного органа, или иное лицо, которому Клиент предоставил право 1-й подписи	1-я подпись Клиента	Просмотр, создание, редактирование, выгрузка, отправка и отзыв платежных поручений; просмотр, создание, отправка писем. Если Клиентом задана схема подписания – сочетание двух подписей, то каждый направляемый ЭД снабжается двумя подписями .
Главный бухгалтер клиента, его заместитель или иное лицо, которому Клиент предоставил право 2-й подписи	2-я подпись Клиента	

2.13. Формирование секретных ключей ЭП Клиента производится исключительно самим Клиентом, таким образом, что единственным владельцем секретного ключа ЭП является лицо, его сформировавшее. Сведения о секретном ключе ЭП в НКО отсутствуют. Ключи проверки ЭП, хранящиеся в НКО, не могут быть использованы для подписи ЭД или восстановления (вычисления) сгенерированных Клиентом секретных ключей ЭП.

2.14. Подключение банковских счетов/счета Клиента к СИКЮЛ производится на основании Заявки на подключение Клиента к СИКЮЛ.

3. ПОРЯДОК ЗАКЛЮЧЕНИЯ ДОГОВОРА

3.1. Заключение с Клиентом Договора осуществляется в соответствии со статьей 428 Гражданского кодекса РФ путем присоединения Клиента к Договору на основании подачи в НКО подписанного Клиентом Заявления о присоединении (Приложение 1).

3.2. Для заключения Договора Клиент представляет в НКО подписанное Заявление о присоединении и, по запросу НКО, дополнительные документы. Дополнительные документы могут быть запрошены с целью проведения НКО внутренней процедуры приема Клиента. Заявление о присоединении и дополнительные документы представляются Клиентом в НКО:

- на бумажном носителе (в одном экземпляре) при личной явке уполномоченного Клиентом лица в НКО;
- курьерской или почтовой службой с описью вложения, позволяющей установить дату и время отправления и получения корреспонденции.

3.3. Копия Заявления о присоединении с отметками НКО о принятии передается НКО Клиенту и является документом Клиента, подтверждающим факт заключения Договора.

3.4. Обязательным условием для заключения Договора является открытие Клиентом корреспондентского счета в НКО для осуществления расчетных операций в рамках участия Клиента в Платежной Системе Вестерн Юнион. В случае, если Клиент уже имеет корреспондентский счет в НКО, открытие дополнительного счета не требуется.

3.5. Присоединение Клиента к Договору осуществляется по месту открытия корреспондентского счета Клиенту в НКО.

4. ОБЯЗАТЕЛЬСТВА И ПРАВА СТОРОН

4.1. НКО обязуется:

4.1.1. Предоставлять Клиенту возможность проведения расчетных операций по банковскому счету Клиента, открытому в НКО, на основании электронных платежных документов, подписанных электронной подписью Клиента, посредством Системы ДБО и СИКЮЛ в соответствии с действующим законодательством, нормативными актами Банка России и Договором.

4.1.2. Передать Клиенту по Акту приема-передачи при подключении Реквизиты персонального пароля.

4.1.3. Хранить в течение срока деятельности УЦ материалы по предмету Договора для разрешения споров, в том числе:

4.1.3.1. Файлы ЭД, полученные от Клиента.

4.1.3.2. Сертификат ключа проверки ЭП в форме электронного документа.

4.1.4. Принимать к исполнению ЭД, подлинность которых подтверждена положительным результатом проверки ЭП Клиента, за исключением случаев, оговоренных в пункте 4.3. настоящих Правил.

4.1.5. Немедленно сообщать Клиенту о факте неподтверждения подлинности его ЭП посредством уведомления в СИКЮЛ.

4.1.6. Информировать Клиента о проведенных по счету операциях, в том числе с использованием ЭД, по СИКЮЛ не позднее операционного дня, следующего за днем передачи ЭД в НКО, после 10:00:00 часов по московскому времени.

4.1.7. Информировать Клиента путем размещения на официальном сайте НКО в сети Интернет информации об условиях и о порядке использования ЭП и средств электронной подписи, информацией о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

4.2. Клиент обязуется:

4.2.1. Выполнять условия Договора.

4.2.1.1. Предоставить в НКО документы согласно пункту 3.2. Договора одновременно с Заявлением о присоединении. В случае внесения изменений и дополнений в предоставленные ранее документы, представить в НКО новые документы и/или документы, подтверждающие внесение изменений и дополнений.

4.2.1.2. Обеспечить предоставление физическими лицами, в том числе Пользователями, чьи персональные данные содержатся в представляемых Клиентом в НКО документах, согласия на обработку НКО таких персональных данных (Приложение 4) с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), трансграничную передачу, обезличивание, блокирование, удаление, уничтожение персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в целях исполнения Сторонами договорных обязательств по настоящему Договору, на срок действия Договора. Клиент обязуется незамедлительно информировать НКО в письменной форме о случаях отзыва физическими лицами и Пользователями согласия на обработку персональных данных.

4.2.1.3. Своевременно оплачивать установленную НКО плату за предоставление Клиенту доступа к Системе дистанционного банковского обслуживания НКО «Интернет клиент для юридических лиц» (СИКЮЛ). Условия и порядок оплаты установлены Договором.

4.2.1.4. До расторжения Договора погасить задолженность перед НКО по оплате доступа к Системе дистанционного банковского обслуживания НКО «Интернет клиент для юридических лиц» (СИКЮЛ).

4.2.2. Знакомиться с изменениями и дополнениями, внесенными в настоящие Правила и приложения к Правилам, Тарифы НКО, актуальной эксплуатационной документацией Системы ДБО, условиями и о порядке использования ЭП и средств электронной подписи, информацией о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки. Регулярно, но не реже одного раза в календарном месяце, обращаться в НКО или на официальный сайт НКО в сети Интернет www.wumte.ru для получения информации о внесенных изменениях в указанные в настоящем пункте Договора документы.

4.2.3. Соблюдать установленные НКО форматы ЭД.

4.2.4. Соблюдать регламент отправки ЭД.

4.2.5. Исключить доступ к ключевому носителю и Реквизитам персонального пароля неуполномоченных лиц.

4.2.6. Не передавать, не копировать, не разглашать секретный ключ ЭП третьим лицам.

4.2.7. Самостоятельно осуществлять установку и настройку СИКЮЛ, а также последующую генерацию секретного ключа ЭП на принадлежащем ему оборудовании, согласно пользовательской документации.

4.2.7.1. Доступ к документации СИКЮЛ осуществляется посредством сайта <https://dbo.westernunion.ru>

4.2.8. Обновлять компоненты СИКЮЛ.

4.2.9. Принять меры по обеспечению безопасности информации, обрабатываемой посредством составляющих СИКЮЛ, расположенных на его территории, не противоречащие действующему законодательству и положениям настоящих Правил, достаточные для недопущения и (или) нейтрализации последствий рисков, указанных в пункте 7.3. Договора.

4.2.10. Рассматривать всю информацию, полученную от НКО в ходе исполнения Договора (за исключением сведений, доступ к которым не может быть ограничен в соответствии с законодательством) как конфиденциальную и не использовать ее в целях иных, чем определено условиями Договора.

4.2.11. Обязательства по сохранению конфиденциальности имеют силу в течение срока действия Договора и в течение последующих 5 (пяти) лет после истечения его срока действия Договора ли его досрочного расторжения.

4.2.12. При неподтверждении подлинности ЭП на полученных из НКО ЭД сохранить эти документы с одновременным сообщением об этом в НКО.

4.2.13. При возникновении споров, связанных с использованием СИКЮЛ, предоставлять по письменному запросу НКО все необходимые документы.

4.2.14. Немедленно уведомить НКО о прекращении полномочий владельца сертификата ключа проверки ЭП и не осуществлять отправку в НКО ЭД, подписанных ЭП владельца сертификата ключа проверки ЭП, полномочия которого прекращены.

4.2.15. Не реже одного раза в течение рабочего дня проверять исполнение НКО платежных ЭД и проведение операций по счету в соответствии с информацией, представленной НКО в соответствии с пунктом пунктом 4.1.6. Договора или содержащейся в самостоятельно запрашиваемой Клиентом выписке в СИКЮЛ.

4.2.16. Не передавать клиентское программное обеспечение СИКЮЛ и права по Договору третьим лицам.

4.2.17. В случае компрометации секретных ключей ЭП, а также при возникновении подозрений о возможном нарушении безопасности СИКЮЛ:

4.2.17.1. Немедленно сообщить об этом в УЦ по телефону +7(495)7829800 и по электронной почте путем направления сообщения на адрес Moscow.infosec@westernunion.ru с адреса электронной почты Администратора безопасности Клиента. Любая информация, переданная Клиентом по СИКЮЛ с использованием скомпрометированных секретных ключей ЭП, НКО игнорируется.

4.2.17.2. Представить в НКО письменное уведомление, содержащее изложение обстоятельств, относящихся к случаю компрометации ключей ЭП или подозрений о возможном нарушении безопасности СИКЮЛ, а также заявление на аннулирование сертификата ключа проверки ЭП в соответствии с регламентом УЦ.

4.2.18. Клиент обязуется использовать средства ЭП и обеспечить выполнение Пользователями правил пользования ключами ЭП и положений Договора, а также принимать меры по обеспечению безопасности информации при работе в СИКЮЛ в соответствии с Приложением 2 к настоящим Правилам. Клиент обязуется обеспечить выполнение указанных правил и требований уполномоченными Пользователями.

4.2.19. При расторжении Договора Клиент обязуется уничтожить все принадлежащие ему ключи ЭП и пароли, относящиеся к настоящему Договору, не передавать их третьим лицам. Все другие конфиденциальные сведения хранятся и уничтожаются Сторонами в соответствии с действующим законодательством, нормативными актами Банка России и Договором.

4.2.20. Не осуществлять в отношении клиентского программного обеспечения, его модулей и подсистем, а также СКЗИ:

4.2.20.1. Декомпилирование и/или изучение кода, его модификацию или улучшение.

4.2.20.2. Использование не в составе соответствующей Системы ДБО.

4.2.20.3. Передачу третьим лицам каких-либо прав не в составе соответствующей Системы ДБО.

4.2.20.4. Не использовать каким-либо образом компоненты, модули и подсистемы программного обеспечения Системы ДБО в других программах для ЭВМ, а также одновременно (без деинсталляции) на нескольких ЭВМ.

4.2.21. Проводить плановую замену ключей ЭП и соответствующих им ключей проверок ЭП один раз в год.

4.3. Права НКО:

4.3.1. В одностороннем порядке вносить изменения в условия Договора, в том числе Тарифы НКО, с предварительным уведомлением Клиента не менее чем за 15 (пятнадцать) календарных дней до даты вступления в силу изменений путем размещения изменений на официальном сайте НКО в сети Интернет.

4.3.2. Отказать Клиенту в доступе к СИКЮЛ, в случаях:

4.3.2.1. Наличия задолженности перед НКО по оплате доступа к Системе дистанционного банковского обслуживания НКО «Интернет клиент для юридических лиц» (СИКЮЛ) за период, превышающий 30 (тридцать) дней с даты образования задолженности.

4.3.2.2. Закрытия Клиентом единственного/последнего корреспондентского счета в НКО.

4.3.3. Дополнять и изменять перечень документов, представляемых Клиентом одновременно с Заявлением о присоединении (если применимо).

4.3.4. Расторгнуть Договор в одностороннем порядке, если в процессе исполнения Договора НКО выявлены признаки сомнительных операций и сделок, а также при непредъявлении Клиентом дополнительной информации НКО, в том числе объясняющей экономический смысл проводимых операций и сделок.

4.3.5. НКО вправе не принимать к исполнению ЭД или не исполнить принятый ЭД в случаях:

4.3.1.1. Наличии сомнений в полномочиях владельца сертификата ключа проверки ЭП.

4.3.1.2. При получении сообщения о возможной компрометации ключей ЭП в соответствии с пунктом 4.2.17. настоящих Правил.

4.3.1.3. При несоответствии ЭД формату, установленному НКО.

4.3.1.4. В иных случаях, предусмотренных действующим законодательством и заключенными Сторонами Договорами и Соглашениями.

4.3.6. Запрашивать у Клиента документы при возникновении спорных ситуаций при исполнении Договора.

4.3.7. Расторгнуть в одностороннем порядке Договор при нарушения Клиентом условий настоящих Правил.

4.3.8. Обновлять компоненты СИКЮЛ.

5. ПОРЯДОК ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

5.1. Проверка ЭП в ЭД, передаваемых Сторонами в СИКЮЛ, является обязательной и осуществляется средствами ЭП автоматически при поступлении новых ЭД. Результат проверки ЭП хранится в лог-файле СИКЮЛ.

5.1.1. В СИКЮЛ проверка ЭП проводится автоматически, результат проверки ЭП можно получить, воспользовавшись функцией просмотра наложенных подписей для конкретного ЭД.

5.2. Исходными данными для процедуры проверки ЭП являются:

5.2.1. ЭД, переданный одной из Сторон в формате Системы ДБО и подписанный ее ЭП.

5.2.2. Сертификат ключа проверки ЭП Стороны, подписавшей ЭД.

5.3. ЭП в электронных документах, передаваемых Сторонами в СИКЮЛ, признается действительной при одновременном соблюдении следующих условий:

5.3.1. Сертификат ключа проверки ЭП заверен УЦ НКО.

5.3.2. Сертификат ключа проверки ЭП действителен на момент подписания ЭД.

5.3.3. Положительный результат проверки принадлежности сертификата ключа проверки ЭП Клиенту - участнику СИКЮЛ.

5.3.4. Подтверждено отсутствие изменений, внесенных в ЭД, после его подписания.

5.4. Проверка ЭП должна осуществляться средствами ЭП в соответствии с правилами пользования ими.

6. УСЛОВИЯ И ПОРЯДОК ОПЛАТЫ

6.1. За предоставление доступа к Системе дистанционного банковского обслуживания НКО «Интернет клиент для юридических лиц» (СИКЮЛ) НКО с Клиента взимается плата согласно действующим Тарифам НКО, размещенным на официальном сайте НКО в сети Интернет.

6.2. Оплата Клиентом за обслуживание в СИКЮЛ происходит путем списания НКО комиссии в последний рабочий день отчетного месяца с рублевого банковского счета Клиента, открытого в НКО, в российских рублях. При подключении к Системе СИКЮЛ нескольких счетов, ежемесячная абонентская плата не увеличивается.

6.3. Настоящим Клиент предоставляет НКО согласие (акцепт) на списание без его распоряжения денежных средств со счета, указанного в пункте 6.2. настоящей статьи, на условиях и в порядке, установленных Договором. Согласие (акцепт) Клиента на списание НКО денежных средств со счета, указанного в настоящей статье 6 Договора, является заранее данным акцептом.

7. ФОРС-МАЖОР (ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ) И РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ЭП

7.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств, если это неисполнение явилось следствием обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих или препятствующих осуществлению Сторонами своих обязательств по Договору, в том числе, связанных с запретительными и ограничительными мерами со стороны государственных органов в стране нахождения банков-корреспондентов Сторон и иных обстоятельств, не зависящих от волеизъявления Сторон, Стороны по Договору освобождаются от ответственности за неисполнение или ненадлежащее исполнение принятых на себя обязательств по Договору.

7.2. Сторона, ссылающаяся на форс-мажорные обстоятельства, обязана в течение 5 (пяти) рабочих дней письменно проинформировать другую Сторону о наступлении таких обстоятельств с указанием на характер таких обстоятельств и ожидаемый срок прекращения действия таких обстоятельств.

7.3. При прекращении указанных выше обстоятельств Сторона должна без промедления, но не позднее 5 (пяти) рабочих дней, известить об этом другую Сторону в письменной форме.

7.4. Клиент несет все возможные неблагоприятные последствия (риски), связанные с использованием электронной подписи, в том числе:

7.4.1. Риски, возможные при хищении или утере секретного ключа ЭП.

7.4.2. Риски, возможные при получении доступа третьих лиц к информационным системам, в которых используется секретный ключ ЭП.

7.4.3. Риски, возможные при нецелевом использовании сертификата ключа проверки ЭП при подписании электронной подписью документов Клиента.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. Стороны несут ответственность за ненадлежащее исполнение своих обязанностей в соответствии с законодательством РФ и условиями Договора.

8.2. Ответственность за содержание, полноту и правильность оформления ЭД несет Сторона, составившая и подписавшая указанный документ своей ЭП. Ответственность за действия (бездействие), в результате которых ключевой носитель (секретный ключ ЭП) стал известен неуполномоченным лицам и последствия таких действий (бездействия), несет владелец сертификата ключа проверки ЭП.

8.3. Клиент несет ответственность за действия в СИКЮЛ уполномоченных им Пользователей.

8.4. Клиент несет ответственность перед НКО за ущерб и расходы, понесенные НКО в результате нарушения Клиентом положений Договора, законодательных или нормативных актов.

8.5. Клиент несет ответственность в соответствии с законодательством РФ за несвоевременную оплату (неоплату) услуг НКО.

8.6. НКО не несет ответственности в случае невыполнения Клиентом условий Договора.

8.7. НКО не несет ответственности за техническое состояние компьютерного оборудования Клиента, возможные технические помехи в телефонных линиях, сбои в работе почты, Интернета и иных сетей связи Клиента, прекращение использования СИКЮЛ из-за отключения электроэнергии и/или возникновения перерывов в связи, возникших по техническим причинам, не зависящим от НКО, а также за последствия, которые являются следствием неприменения Клиентом мер по обеспечению информационной безопасности при работе с СИКЮЛ.

8.8. НКО не несет ответственность за убытки, возникшие у Клиента вследствие непринятия к исполнению или при отказе в исполнении ЭД.

8.9. НКО не несет ответственность за любые косвенные убытки Клиента (включая упущенную выгоду), связанные с исполнением, изменением или прекращением настоящего Договора.

9. ПРОЧИЕ УСЛОВИЯ

9.1. Разногласия, возникающие по Договору и неразрешенные Сторонами путем переговоров, рассматриваются Сторонами в претензионном порядке. Срок рассмотрения претензии – 15 (пятнадцать) календарных дней с даты получения претензии. При недостижении согласия или неполучении ответа на претензию в течение 30 (тридцати) календарных дней с даты отправки претензии спор подлежит разрешению в суде.

9.2. Все споры, разногласия или требования, возникающие из Договора или в связи с ним и неразрешенные в претензионном порядке, в том числе касающиеся его вступления в силу, заключения, изменения, исполнения, нарушения, прекращения или действительности, подлежат рассмотрению в Международном коммерческом арбитражном суде при Торгово-промышленной палате Российской Федерации в соответствии с его применимыми правилами и положениями.

10. СРОК ДЕЙСТВИЯ И ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА

10.1. Настоящий Договор действует без ограничения срока.

10.2. В случае закрытия всех счетов Клиента, подключенных к СИКЮЛ, реорганизации Клиента либо отзыва лицензии Клиента на осуществление банковских операций настоящий Договор считается расторгнутым.

10.3. Любая из Сторон вправе расторгнуть Договор в любое время, предупредив об этом другую Сторону письменно не менее чем за 30 (тридцать) календарных дней до предполагаемой даты расторжения Договора. До даты расторжения Договора Клиент обязан оплатить задолженность перед НКО, возникшую вследствие исполнения Договора.

11. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ К ПРАВИЛАМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

- 11.1. Приложение 1 «Заявления о присоединении к Правилам дистанционного банковского обслуживания»
- 11.2. Приложение 2 «Правила использования СКЗИ и ЭП»
- 11.3. Приложение 3 «Акт приема-передачи»
- 11.4. Приложение 4 «Заявление Пользователя о согласии на обработку персональных данных» (образец)
- 11.5. Приложение 5 «Доверенность» (образец)
- 11.6. Приложение 6 «Тарифы НКО»

в ООО «НКО «Вестерн Юнион ДП Восток»

Данная форма отменяет все действующие формы разрешенного доступа

ЗАЯВЛЕНИЕ

о присоединении к Правилам дистанционного банковского обслуживания

Наименование организации (Клиента), реквизиты
лицензии Банка России

ИНН _____ ОГРН _____ ОКПО _____
БИК _____ КПП _____ ОКАТО _____

Прошу оказывать услуги с использованием СИКЮЛ при осуществлении операций по счетам, открытым в ООО «НКО «Вестерн Юнион ДП Восток» на дату подписания настоящего Заявления, по следующим счетам:

№ _____	от _____	№ _____	от _____
№ _____	от _____	№ _____	от _____
№ _____	от _____	№ _____	от _____

Перечень сотрудников, уровень прав доступа

1. АРМ Клиента будет установлено на рабочем месте

(должность, подразделение, фамилия, имя, отчество полностью, уровень прав доступа)

2. АРМ Клиента будет установлено на рабочем месте

(должность, подразделение, фамилия, имя, отчество полностью, уровень прав доступа)

3. АРМ Клиента будет установлено на рабочем месте

(должность, подразделение, фамилия, имя, отчество полностью, уровень прав доступа)

Контакты Клиента

1. Обязанности Администратора безопасности возложены на

(должность, подразделение, фамилия, имя, отчество полностью)

Адрес электронной почты _____ Телефон (в т.ч. код) _____

2. По финансовым вопросам обращаться к

(должность, подразделение, фамилия, имя, отчество полностью)

Адрес электронной почты _____ Телефон (в т.ч. код) _____

3. IP адреса с которых будет происходить соединение:

(перечень IP адресов)

Настоящим Клиент в соответствии со статьей 428 Гражданского кодекса Российской Федерации присоединяется к Правилам дистанционного банковского обслуживания (Договору) в действующей редакции Правил дистанционного банковского обслуживания (Договора) и подтверждает, что:

- ознакомился с Правилами дистанционного банковского обслуживания (Договором), понимает их текст, выражает свое согласие с ними и обязуется их выполнять;

- настоящее Заявление является документом, подтверждающим факт заключения Договора (Правил дистанционного банковского обслуживания) между НКО и Клиентом.

Тарифы НКО, условия, правила работы с подключаемой СИКЮЛ известны Клиенту и принимаются Клиентом безоговорочно.

«__» _____ 20__ г.

[должность Руководителя Клиента]
[наименование Клиента]

М.П.

Фамилия И.О.

ОТМЕТКИ НКО

ООО «НКО «Вестерн Юнион ДП Восток», ОГРН 1037739616122, ИНН 7727067410, расположенное по адресу 125171, Россия, г. Москва, Ленинградское шоссе, дом 16А, строение 1, лицензия Банка России № 2726-С от 08.05.2013 г., подтверждает заключения Договора № _____ от «__» _____ 20__ г. с [наименование Клиента] о дистанционном банковском обслуживании посредством Системы «Интернет клиент для юридических лиц» (СИКЮЛ).

Должность сотрудника НКО, оформившего Заявление

подпись

Фамилия, И.О.

Правила использования СКЗИ и ЭП

1. Общие положения

Средства криптографической защиты информации (СКЗИ) предназначены для подписи файлов электронной подписью (ЭП) с целью подтверждения подлинности информации и ее авторства (данные СКЗИ называются также средствами ЭП).

По истечении срока действия ключей ЭП Клиент обязан обратиться в УЦ НКО для их замены.

Переданные в рамках Договора средства ЭП и СКЗИ не предназначены для обработки сведений, составляющих государственную тайну и не подлежат использованию для их обработки.

Клиент обязуется осуществлять использование СКЗИ в соответствии с эксплуатационно-технической документацией к нему.

2. Работа со средствами ЭП и СКЗИ

Для работы со средствами ЭП и СКЗИ привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации-Клиента. Должностные лица, уполномоченные данным приказом и эксплуатирующие СКЗИ, использующие секретные ключи ЭП (далее - Пользователи), несут персональную ответственность за: сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы со средствами ЭП и СКЗИ; сохранение в тайне содержания закрытых ключей СКЗИ и средств ЭП; сохранность ключевых носителей и других документов, выдаваемых с ключевыми носителями.

Клиент должен обеспечить условия хранения и использования ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования информации ключевого носителя и паролей.

Не допускается:

а) Разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным, выводить содержимое ключевых носителей на дисплей и принтер, или копировать его на другие носители;

б) Вставлять ключевой носитель в компьютер при проведении работ, не являющихся штатными процедурами использования ключей (шифрование и (или) расшифровывание информации, проверка ЭП и т.д.), а также в другие компьютеры, не предназначенные для работы с Системой ДБО;

в) Записывать на ключевой носитель постороннюю информацию;

г) Вносить какие-либо изменения в программное обеспечение (далее ПО) СКЗИ и средств ЭП;

д) Использовать бывшие в работе ключевые носители для записи посторонней информации;

2.1. Правила эксплуатации и хранения ключевых носителей.

а) Оберегайте носитель от механических воздействий (падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения; все это может привести к его поломке.

б) Не прилагайте излишних усилий при подсоединении устройства к порту компьютера.

в) Не допускайте попадания на носитель (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема примите меры для их очистки. Для очистки корпуса и разъема устройства используйте сухую ткань. Использование органических растворителей недопустимо.

г) Не разбирайте носитель! Такие действия могут привести к поломке корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие, к ненадежной работе или выходу из строя самого устройства.

д) Разрешается подключать носитель только к исправному оборудованию. Параметры USB порта должны соответствовать спецификации для USB.

е) Запрещается использовать длинные переходники или USB хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для носителя, может подаваться несоответствующее напряжение.

ж) Запрещается извлекать носитель из порта компьютера, если происходит работа с данным устройством - прерывание работы может негативно сказаться как на данных, так и на работоспособности носителя.

з) Запрещается оставлять носитель подключенным к компьютеру во время перезагрузки, ухода в спящий или ждущий режимы, поскольку в это время возможны перепады напряжения на USB порту и, как следствие, выход устройства из строя.

и) Запрещается оставлять носитель подключенным к компьютеру, когда необходимость в работе с ЭП и СКЗИ отсутствует.

к) Рекомендуется отключать другие USB устройства на время работы с носителем. Большое количество USB устройств может приводить к значительным изменениям в режимах питания USB портов компьютера и, как следствие, к выходу из строя устройств.

л) В случае неисправности или неправильного функционирования носитель следует заменить.

3. Обеспечение информационной безопасности на рабочем месте

Клиент обязан обеспечивать безопасное функционирование СКЗИ в соответствии с переданной ему документацией СКЗИ и следующими требованиями по безопасности:

С целью защиты от угроз, связанных с появлением в сети Интернет ложных (фальсифицированных) ресурсов, имитирующих программный интерфейс Системы ДБО, необходимо осуществлять доступ к ней только по указанному в Договоре URL-адресу.

Защита информации от несанкционированного доступа (далее НСД) должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором безопасности.

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку.

При размещении технических средств с установленным СКЗИ:

а) Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.

б) Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

При установке программного обеспечения СКЗИ следует:

а) На технических средствах, предназначенных для работы с СКЗИ использовать только лицензионное ПО фирм-изготовителей.

б) На ЭВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности.

При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ и приложений, использующих СКЗИ, а также для просмотра кода и памяти СКЗИ и приложений, использующих СКЗИ, в процессе обработки СКЗИ защищаемой информации и/или при загруженной ключевой информации.

в) Предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатавания системного блока и разъемов ЭВМ).

г) ПО, устанавливаемое на ЭВМ с СКЗИ, не должно содержать возможностей, позволяющих: модифицировать содержимое произвольных областей памяти; модифицировать собственный код и код других подпрограмм; модифицировать память, выделенную для других подпрограмм; передавать управление в область собственных данных и данных других подпрограмм; несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске; повышать предоставленные привилегии; модифицировать настройки операционной системы (далее ОС); использовать недокументированные фирмой-разработчиком функции ОС.

д) Рекомендуется периодически проверять на отсутствие аппаратных закладок аппаратуру, на которой устанавливается и работает СКЗИ. Необходимость таких проверок определяется решением руководства эксплуатирующей организации.

При организации работ по защите информации от НСД необходимо учитывать следующие требования:

а) Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN и т.д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

- личный пароль пользователь не имеет права сообщать никому;

- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

б) Средствами BIOS должна быть исключена возможность работы на ЭВМ с СКЗИ, если во время ее начальной загрузки не проходят встроенные тесты. Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

в) Не использовать нестандартные, измененные или отладочные версии ОС.

г) Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.

д) Исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек.

е) На ЭВМ должна быть установлена только одна операционная система.

ж) Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.

з) ОС должна быть настроена только для работы с СКЗИ. Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).

и) Режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень.

к) Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

л) Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части): системный реестр; файлы и каталоги; временные файлы; журналы системы; файлы подкачки; кэшируемая информация (пароли и т.п.); отладочная информация.

м) Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

н) Необходимо организовать и использовать комплекс мероприятий антивирусной защиты (включающий в себя установку антивирусного программного обеспечения).

о) Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.

п) При использовании СКЗИ на ЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

4. Действия в случае компрометации ключей ЭП

Клиент самостоятельно определяет факт компрометации принадлежащего ему секретного ключа ЭП. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, обрабатываемой с помощью средств СКЗИ и ЭП в информационных системах, принадлежащих Клиенту, организует сам Клиент.

При компрометации секретного ключа ЭП Клиент должен немедленно прекратить все работы, связанные с передачей документов в электронном виде по каналам связи, и сообщить в НКО о факте компрометации. Информация о компрометации может передаваться по телефону или непосредственно уполномоченному лицу УЦ НКО. Не позднее 1 часа после поступления сообщения о компрометации ключа НКО блокирует электронные документы в Системе ДБО, подписанные скомпрометированным секретным ключом ЭП Клиента. Разблокировка будет произведена только после замены скомпрометированных ключей.

Для получения новых ключей ЭП владелец сертификата ключа проверки ЭП, у которого были скомпрометированы ключи ЭП, должен направить в соответствии с Регламентом УЦ запрос на изготовление сертификата ключей проверки ЭП.

С настоящими Правилами использования СКЗИ и ЭП ознакомлен(а), их содержание мне понятно:

«__» _____ 20__ г.

_____ /
подпись

Фамилия, И.О. Пользователя

АКТ ПРИЕМА-ПЕРЕДАЧИ

г. Москва

«__» _____ 20__ г.

ООО НКО «Вестерн Юнион ДП Восток», именуемое в дальнейшем «**НКО**», в лице Президента Зюбановой Евгении Витальевны, действующей на основании Устава, с одной стороны, и [**Наименование Клиента**], именуемое в дальнейшем «**Клиент**», в лице [должность, ФИО руководителя полностью], действующего на основании [указать], с другой стороны, составили настоящий акт о том, что НКО «__» _____ 20__ г. произведено подключение Клиента к Системе дистанционного банковского обслуживания «Интернет клиент для юридических лиц» (СИКЮЛ) на основании Заявления Клиента о присоединении к Правилам дистанционного банковского обслуживания от «__» _____ 20__ г. (далее – «Заявление»).

Регистрация Пользователя(ей) Клиента в Системе дистанционного банковского обслуживания «Интернет клиент для юридических лиц» (СИКЮЛ) НКО произведена в соответствии перечнем лиц, указанных Клиентом в Заявлении.

Реквизиты персонального пароля для всех зарегистрированных Пользователей Клиента переданы НКО Администратору безопасности Клиента, Клиентом получены.

Стороны претензий друг к другу не имеют.

Принял:

Передал:

[должность Руководителя Клиента]

Президент

[Наименование Клиента]

ООО НКО «Вестерн Юнион ДП Восток»

_____ [ФИО руководителя]

_____ Зюбанова Е.В.

М.П.

М.П.

ОБРАЗЕЦ

В _____
(наименование Клиента)

(Ф.И.О. Руководителя Клиента)
от _____
(Ф.И.О. Пользователя (полностью))

Заявление Пользователя о согласии на обработку персональных данных

Настоящим я, _____ (фамилия, имя, отчество (при наличии) полностью), дата рождения: _____, зарегистрированный/проживающий (пребывающий) (нужное подчеркнуть) по адресу: _____, гражданство: _____, документ, удостоверяющий личность на территории РФ: _____ (указать), серия _____, номер _____, выдан «__» _____ г., орган выдачи: _____,

действуя свободно, своей волей и в своем интересе, в соответствии с положениями Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» даю согласие Обществу с ограниченной ответственностью «Небанковская кредитная организация «Вестерн Юнион ДП Восток» (ОГРН 1037739616122), зарегистрированному и расположенному по адресу: 125171, Российская Федерация, город Москва, Ленинградское шоссе, дом 16А, строение 1, совершать любые действия (операции) или совокупность действий (операций), с использованием средств автоматизации или без использования таких средств с моими персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), включая трансграничную передачу, обезличивание, блокирование, удаление, уничтожение моих персональных данных, для цели исполнения мной полномочий Пользователя в рамках Правил дистанционного банковского обслуживания (Договора) на срок действия Правил дистанционного банковского обслуживания (Договора).

Настоящее согласие на обработку персональных данных может быть отозвано в письменной форме. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

_____ «__» _____ 20__ г.
Ф.И.О. полностью подпись дата

ОБРАЗЕЦ

(Оформляется на фирменном бланке Клиента)

ДОВЕРЕННОСТЬ

[Дата, место выдачи доверенности]

_____ (далее – «Доверитель»)
(полное наименование юридического лица с указанием местонахождения, ОГРН, ИНН)

В лице _____
(должность, фамилия, имя и отчество)

Действующего на основании _____
(наименование документа)

Настоящим уполномочивает _____
(должность, фамилия, имя и отчество, дата и место рождения)

Паспорт серия _____ № _____, выдан «____» _____ г.

_____ (орган выдачи паспорта, код подразделения)

формировать, обрабатывать, подписывать электронной подписью от имени Доверителя и отправлять и принимать электронные документы в рамках Договора № _____ от «__» _____ 20__ г. с ООО «НКО «Вестерн Юнион ДП Восток» при использовании Системы дистанционного банковского обслуживания «Интернет клиент для юридических лиц» (СИКЮЛ), распоряжаться денежными средствами на счетах Доверителя, открытых в ООО «НКО «Вестерн Юнион ДП Восток», путем использования СИКЮЛ.

Настоящая Доверенность выдана сроком на _____ с запретом на передоверие полномочий третьим лицам.

[должность Руководителя Клиента]
[наименование Клиента]

М.П.

Фамилия, И.О.

ТАРИФЫ
на обслуживание банковских счетов в российских рублях и долларах США для Клиентов за использование Системы дистанционного банковского обслуживания «Интернет клиент для юридических лиц» (СИКЮЛ)

Наименование услуги	Порядок начисления	Тариф
Обслуживание в Системе дистанционного банковского обслуживания «Интернет клиент для юридических лиц» (СИКЮЛ)	Ежемесячно ¹	1 000 рублей ² , НДС не облагается

¹ Комиссия взимается вне зависимости от наличия оборотов по банковским счетам в течение отчетного месяца, начиная с даты присоединения Клиента к Договору. Комиссия взимается как за полный, так и за неполный месяц оказания услуги.

² Списание комиссии осуществляется в последний рабочий день отчетного месяца с корреспондентского счета в российских рублях.