УТВЕРЖДАЮ:

Председатель Правления

РНКО «Платежный Центр» (ООО)

_____

Г.М. Мац

Редакция №9 от «24» марта 2023 г.

ПРАВИЛА РАБОТЫ СЕРВИСА

«Финансовые операции в торговых сетях»

Настоящие Правила работы сервиса «Финансовые операции в торговых сетях» (далее – «Правила», «Сервис») определяют правила работы Сервиса, порядок и условия его использования Участниками. Текст действующих Правил размещается в сети Интернет по адресу rnko.ru.

Присоединение Участника к условиям Правил осуществляется путём заключения с Организатором сервиса соглашения, согласно условиям которого Участник присоединяется к условиям настоящих Правил, либо путём подачи Организатору сервиса заявления / заявки, предусмотренных настоящими Правилами, Правилами BeSafe, Правилами ЦФТ ID. Участник приобретает все права и обязанности, предусмотренные Правилами, с даты вступления такого соглашения в силу, либо с даты принятия Организатором сервиса указанных заявок / заявлений.

Настоящие Правила действуют в рамках правил электронного документооборота корпоративной информационной системы «BeSafe» (далее – Система BeSafe), текст которых представлен в сети Интернет по адресу www.besafe.ru (далее – Правила BeSafe), а также Правил электронного документооборота корпоративной информационной системы ЦФТ ID (далее – Система ЦФТ ID), текст которых представлен в сети Интернет по адресу: service.cft.ru (далее – Правила ЦФТ ID). Присоединение Участника к условиям настоящих Правил означает также присоединение Участника к Правилам BeSafe и Правилам ЦФТ ID. Под Участником в настоящих Правилах понимается Клиент в терминах Правил BeSafe и Правил ЦФТ ID.

Присоединение Участника к условиям Правил возможно исключительно в случае, если Участник полностью согласен с настоящими Правилами, Правилами BeSafe и Правилами ЦФТ ID, условиями присоединения к Сервису, Системе BeSafe и Системе ЦФТ ID, удовлетворяет содержащимся в Правилах Сервиса, Правилах BeSafe и Правилах ЦФТ ID критериям.

Обратившемуся лицу может быть отказано в присоединении к настоящим Правилам с направлением соответствующего уведомления, без указания причин отказа.

1. Предмет регулирования настоящих Правил

Предметом регулирования настоящих Правил является:

1.1. Определение основных принципов организации и проведения электронного документооборота между Участниками и Организатором сервиса (далее – Стороны) в рамках заключенных между ними договоров;

1.2. Установление прав, обязанностей и ответственности Сторон в результате указанной в п.1.1 Правил деятельности.

1.3. В связи с тем, что в рамках данных Правил Стороны действуют во исполнение заключенных между ними договоров, для достижения взаимных интересов, никаких дополнительных финансовых обязательств в результате исполнения прав и обязанностей, установленных данными Правилами, между Сторонами не возникает (если иное не предусмотрено настоящими Правилами).

2. Термины и определения

Владелец сертификата ключа проверки ЭП (Владелец сертификата) – физическое или юридическое лицо, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки электронной подписи и которое владеет соответствующим Ключом ЭП.

Ключ электронной подписи (Ключ ЭП, Закрытый ключ) – последовательность символов, известная Владельцу сертификата и предназначенная для создания в Электронных документах Электронной подписи с использованием Средств ЭП, а также расшифровывания Электронных сообщений.

Ключ проверки электронной подписи (Ключ проверки ЭП, Открытый ключ) – последовательность символов, соответствующая Ключу ЭП, предназначенная для подтверждения (проверки)

с использованием Средств ЭП подлинности Электронной подписи в Электронном документе, а также зашифровывания Электронных сообщений, предназначенных Владельцу сертификата ключа проверки ЭП.

Организатор сервиса – Расчетная небанковская кредитная организация «Платежный Центр» (общество с ограниченной ответственностью), лицензия Банка России № 3166-К, имеющая в Системе BeSafe статус Организатора сервиса «Финансовые операции в торговых сетях», а в Системе ЦФТ ID статус Организатора ассоциированного сервиса «Финансовые операции в торговых сетях», и осуществляющая в рамках Системы BeSafe, Системы ЦФТ ID и Сервиса функции информационного электронного обслуживания Участников, участвующих в работе Сервиса, привлечение Участников к работе в Системе BeSafe, Системе ЦФТ ID и Сервисе. В рамках Правил BeSafe Расчетная небанковская кредитная организация «Платежный Центр» (общество с ограниченной ответственностью) имеет также статус «**Агент Удостоверяющего Центра (далее – Агент УЦ)»**, позволяющий организовывать выдачу Участникам либо их уполномоченным лицам Сертификатов, созданных Удостоверяющим Центром.

Пароль – набор символов, состоящий из двух частей, сгенерированный Организатором и единый для всех точек обслуживания Участника.

Простая Электронная подпись (далее – Простая ЭП) – реквизит Электронного документа, предназначенный для защиты Электронного документа от подделки, позволяющий подтвердить факт формирования Простой ЭП определенным уполномоченным лицом Участника.

Средства электронной подписи (Средства ЭП) – аппаратные и/или программные средства, являющиеся частью средств криптографической защиты информации и реализующие хотя бы одну из следующих функций при организации Электронного документооборота: создание Электронной подписи в Электронном документе с использованием Ключа ЭП; подтверждение подлинности Электронной подписи, содержащейся в Электронном документе, с использованием Ключа проверки ЭП; создание Ключей ЭП и Ключей проверки ЭП.

Сертификат ключа проверки электронной подписи (далее – Сертификат) –Электронный документ с Электронной подписью уполномоченного лица Удостоверяющего центра, который включает в себя Ключ проверки ЭП и который выдается Удостоверяющим центром Владельцу сертификата для подтверждения подлинности Ключа проверки ЭП и идентификации Владельца сертификата ключа проверки ЭП.

Смарт-ключ – компактное программно-аппаратное устройство, предназначенное для хранения Ключа проверки ЭП, Ключа ЭП, Сертификата, а также другой электронно-цифровой информации. Смарт-ключ имеет защищенную память, чтение записанных в память Смарт-ключа данных или копирование памяти Смарт-ключа невозможно.

Удостоверяющий Центр – Удостоверяющий Центр AUTHORITY, созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов», который осуществляет изготовление цифровых сертификатов для юридических и физических лиц для возможности осуществления электронного документооборота в рамках корпоративной информационной системы «BeSafe».

Усиленная неквалифицированная Электронная подпись (далее – Электронная подпись, ЭП) – реквизит Электронного документа, предназначенный для защиты Электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием Средств ЭП и Ключа ЭП, позволяющий идентифицировать Владельца сертификата ключа проверки ЭП, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в электронном документе информации.

Сервис – сервис «Финансовые операции в торговых сетях», организованный Организатором сервиса в рамках Системы BeSafe и Системы ЦФТ ID, предназначенный для организации и осуществления Электронного документооборота и информационного обмена между Организатором сервиса и Участниками.

Электронный документооборот – обмен Электронными документами в рамках Сервиса в соответствии с настоящими Правилами.

Электронный документ (ЭД) – электронное сообщение, заверенное ЭП / Простой ЭП, в котором информация представлена в электронно-цифровой форме и соответствует установленному Организатором сервиса формату.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного ЭД.

Термины, не определенные в настоящих Правилах, имеют значение, придаваемое им Правилами BeSafe и Правилами ЦФТ ID.

3. Общие принципы электронного документооборота в рамках Сервиса

3.1. Все ЭД в рамках Сервиса проходят проверку принадлежности ЭП в ЭД уполномоченным лицам Сторон и отсутствия искажений в данном ЭД.

3.2. Электронный документооборот, а именно отправка, передача и получение ЭД между Сторонами (их уполномоченными лицами) осуществляется посредством электронных каналов связи, с использованием средств информационной системы Организатора сервиса (далее по тексту - Система) и/или адресов электронной почты. Если иные адреса электронной почты не определены основными договорами между

Участниками и Организатором сервиса для конкретных ЭД, Участники и Организатор сервиса принимают к обработке ЭД, подписанные ЭП / Простыми ЭП уполномоченных лиц Сторон, направленные с использованием средств Системы.

3.3. Участники и Организатор сервиса признают, что:

- внесение изменений в ЭД после его подписания ЭП дает отрицательный результат проверки ЭП;
- каждый Участник несет ответственность за обеспечение сохранности Ключей ЭП / Закрытых ключей / Идентификационных и Аутентификационных данных своими уполномоченными лицами и за действия своего персонала при работе в Системе и/или посредством электронных адресов электронной почты;
- Электронные документы юридически эквивалентны документам на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц с проставлением оттиска печати.

3.4. В рамках Системы BeSafe для создания Ключей ЭП и Ключей проверки ЭП, подписания ЭД, проверки ЭП, зашифровывания и расшифровывания Электронных сообщений в Системе, а также в случаях передачи ЭД с использованием адресов электронной почты Участники используют только совместимые Средства криптографической защиты информации (далее – СКЗИ), и признают их достаточными для Подтверждения подлинности Электронной подписи в Электронном документе, для защиты от несанкционированного доступа, а также для обеспечения конфиденциальности, авторства и подлинности информации, содержащейся в пересылаемых ЭД. Список совместимых (разрешенных к использованию) СКЗИ представлен в Приложении №2 к Правилам «BeSafe».

3.5. Стороны принимают на себя все риски, связанные с работоспособностью своего оборудования, каналов связи, программного обеспечения, установленного на своих программно-аппаратных комплексах.

3.6. Стороны обязуются своевременно информировать друг друга обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих обмену ЭД. В случае обнаружения возможных угроз безопасности ЭД Стороны обязуются своевременно извещать друг друга о них для принятия согласованных мер по защите.

3.7. Участники строго выполняют требования технической и эксплуатационной документации на Систему, предоставляемую Организатором сервиса, а также на средства защиты информации, применяемые в Системе, которые поставляются Организатором сервиса или приобретаются Участником самостоятельно.

3.8. Участники организовывают внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность использования Системы и/или адресов электронной почты лицами, не имеющими допуска к работе с ней, а также исключить возможность использования паролей доступа и Ключей ЭП, а также Идентификационных и Аутентификационных данных Пользователей не уполномоченными на то лицами.

3.9. Участники принимают необходимые меры для исключения обмена ЭД, содержащими компьютерные вирусы и/или иные вредоносные программы.

3.10. Участники признают в качестве единой шкалы времени время часового пояса г. Новосибирска. Участники обязуются поддерживать системное время аппаратных средств, обеспечивающих работоспособность Системы в соответствии с текущим астрономическим временем с точностью до пяти минут. При возникновении разногласий эталонным считается время, установленное на аппаратных средствах Организатора сервиса.

3.11. Участники организуют архивное хранение ЭД, подписанных ЭП / Простыми ЭП, в течение срока действия аналогичных документов, оформленных на бумажных носителях.

3.12. Организатор сервиса вправе при осуществлении Электронного документооборота привлекать на основании договора организации, оказывающие Организатору сервиса услуги информационно-технологического обслуживания.

4. Особенности Электронного документооборота в рамках Системы «BeSafe»

4.1. Порядок выдачи и регистрации Сертификата ключа проверки электронной подписи Участника.

4.1.1. Лицо, уполномоченное без доверенности действовать от имени Участника, или лицо, действующее от имени Участника-юридического лица на основании доверенности (далее - уполномоченное лицо Участника), самостоятельно изготавливает Ключ электронной подписи, Ключ проверки электронной подписи, сохраняя их в памяти своего персонального компьютера или на Смарт-ключах, и направляет Агенту УЦ заявление о создании Сертификата ключа проверки электронной подписи. Для этого соответствующее уполномоченное лицо Участника, при необходимости, устанавливает требуемое программное обеспечение, заходит на сайт Удостоверяющего Центра по ссылке, указанной в пункте 4.3 Правил (соответствующая ссылка определяется в зависимости от Класса Сертификата ключа проверки электронной подписи), заполняет отображаемую форму Заявления на выдачу Сертификата ключа проверки электронной подписи и отправляет заявление. Заявление формируется в виде Электронного документа и направляется Агенту УЦ с использованием программно-аппаратных средств Участника, подключенных через каналы связи к программно-техническим средствам Агента УЦ. После отправки заявления в электронном виде Участник предоставляет его Агенту УЦ в бумажном виде с собственноручной подписью уполномоченного лица Участника, действующего на основании учредительных документов (с заверением печатью Участника, если имеется) или доверенности, с приложением документов, подтверждающих личность и полномочия

уполномоченного лица Участника (в доверенности должны быть обязательно указаны ФИО и должность/паспортные данные уполномоченного лица Участника; при указании должности одновременно с доверенностью должна быть представлена заверенная копия документа о назначении на должность с указанием паспортных данных)..

4.1.2. В течение 3 (Трёх) дней с момента получения заявления в бумажном виде Агент УЦ направляет Участнику изготовленный Удостоверяющим Центром Сертификат в электронном виде, либо мотивированный отказ от его выдачи. Участник направляет Агенту УЦ Акт приёма-передачи Сертификата ключа проверки электронной подписи в бумажном виде за подписью уполномоченного лица Участника, указанного в п. 4.1.1 Правил.

4.1.3. Создание Сертификата осуществляется Удостоверяющим центром в соответствии с Правилами работы Удостоверяющего Центра «AUTHORITY», размещенными на сайте www.authority.ru (далее – Правила Удостоверяющего Центра). Срок действия Сертификата – 1 (один) год.

4.1.4. После получения Сертификата Участник передает Организатору сервиса полученный Сертификат, который содержит в себе Ключ проверки электронной подписи.

4.1.5. Участник направляет Организатору сервиса в бумажном виде заявку о регистрации в Сервисе Сертификата ключа проверки электронной подписи. Сертификат ключа проверки электронной подписи Класса 3 регистрируется в Сервисе в соответствующей роли, (перечень ролей для Сертификата Класса 3 представлен в п. 4.1.7. Правил). Сертификат ключа проверки электронной подписи Класса 2 регистрируется в Сервисе в роли уполномоченного лица Участника для обмена ЭД, предусмотренными договором между Участником и Организатором сервиса. Заявка должна быть заполнена в строгом соответствии с утвержденными формами (Приложение №1 Правил) и подписана уполномоченным лицом Участника.

4.1.6. Сертификат может быть зарегистрирован в Сервисе только при условии наличия у Организатора сервиса всего пакета оригиналов документов на бумажном носителе и в надлежащей форме, а именно: Заявления на выдачу Сертификата, Акта приема-передачи Сертификата, Заявки на регистрацию Сертификата, доверенности, подтверждающей полномочия уполномоченных лиц Участника (при необходимости). Доверенность может быть предоставлена в копии, если она заверена надлежащим образом.

В исключительных случаях, а также при регистрации Сертификата ключа проверки электронной подписи Класса 3 в ролях, предусмотренных пп. 2) – 6) п.4.1.7. настоящих Правил, Организатор сервиса вправе зарегистрировать Сертификат в Сервисе на основании поступивших в электронном виде в систему учета заявок http://jira.korona.net сканированных копий указанного пакета документов при условии поступления оригиналов документов течение 1 (одного) месяца с даты регистрации Сертификата. В случае непоступления оригиналов пакета документов, Организатор сервиса вправе заблокировать возможность использования Сертификата в Сервисе до поступления оригиналов. При этом Участник несет ответственность за все операции, совершенные с использованием Сертификата, зарегистрированного на основании поступивших сканированных копий, в любом случае.

В целях обеспечения конфиденциальности при передаче сканированных копий документов в электронном виде, такие файлы могут быть зашифрованы Участником при помощи криптографических средств защиты информации.

Для выполнения криптографических операций резидентам необходимо использовать сертифицированное СКЗИ «КриптоПро CSP», нерезидентам – средство для шифрования информации GNU Privacy Guard (GPG).

Для резидентов публичный ключ РНКО для зашифровывания файлов размещен по ссылке http://rnko.ru/accounts/sertificate/Documents/sign.7z, для нерезидентов - по ссылке http://rnko.ru/accounts/sertificate/Documents/RNKO%20Platezhnyjj%20Centr%202018.zip.

4.1.7. Участник и соответствующий Сертификат ключа проверки электронной подписи Класса 3 регистрируется в одной или нескольких из представленных ролей:

1) уполномоченный работник Участника (сертификат Агента);
2) оператор точки обслуживания;
3) бухгалтер;
4) администратор ключей точки обслуживания;
5) оператор информационного центра;
6) аудитор безопасности;
7) уполномоченное лицо по получению сертификатов

4.1.8. В связи с истечением срока действия Сертификата уполномоченное лицо Участника должно изготовить и получить новые: Ключ электронной подписи, Ключ проверки электронной подписи и Сертификат ключа проверки электронной подписи в порядке, установленном п. 4.1.1 настоящих Правил.

4.2. Допускается регистрировать также Сертификат Участника, ранее полученный им в рамках Системы BeSafe. Порядок такой регистрации аналогичен изложенному в п. 4.1.5-4.1.6 настоящих Правил.

4.3. В целях создания Сертификата ключа проверки электронной подписи Класса 3 используется следующая ссылка: https://ca.faktura.ru/ca/new-certificate?agentId=1084&class=3.

В целях создания Сертификата ключа проверки электронной подписи Класса 2 используется следующая ссылка: https://secure.authority.ru/auth/1st_class.jsp?class=2&type=1&f=fin&agentId=1084.

4.4. Участник обязуется обеспечивать конфиденциальность своих Ключей электронных подписей, в частности не допускать использование кем-либо принадлежащих Участнику Ключей электронных подписей без его согласия.

При компрометации/аннулировании (отзыве) Ключа электронной подписи Участника, Участник обязан незамедлительно сформировать и направить Организатору сервиса уведомление о компрометации/аннулировании Ключа электронной подписи в соответствии с утвержденной в Приложении №3 Правил формой в электронном виде в систему учета заявок https://jira.korona.net с последующей отправкой в бумажном виде. В течение 24 (Двадцати четырёх) часов с даты получения уведомления в электронном виде Организатор сервиса блокирует Сертификат, однозначно связанный со скомпрометированным\аннулированным Ключом электронной подписи в Сервисе. До момента блокировки Сертификата в Сервисе Электронные документы, направленные с использованием скомпрометированного\аннулированного Ключа электронной подписи, считаются направленными Участником, и Участник несет всю полноту ответственности за совершенные с использованием такого Сертификата действия.

4.5. При изменении уполномоченного лица Участника или его данных, отзыва полномочий такого лица, Участник обязуется направить Организатору сервиса уведомление об аннулировании Ключа электронной подписи в порядке, аналогичном п. 4.4 Правил.

4.6. Удостоверяющий Центр, Организатор сервиса (Агент УЦ) не несут ответственности за несанкционированное использование Сертификатов, а также за ущерб, причиненный Участнику или уполномоченному лицу Участника таким использованием до истечения срока для блокировки Сертификата, установленного п. 4.4. Правил.

4.7. В рамках настоящих Правил Электронные документы признаются полученными с момента получения Электронного документа получателем Электронного документа.

4.8. В рамках настоящих Правил действуют Сертификаты ключей проверки электронной подписи Класса 2 и Класса 3, а также Технологический сертификат, предусмотренные Правилами работы Удостоверяющего Центра.

4.9. В рамках настоящих Правил Участник не вправе осуществлять отзыв отправленных Электронных документов.

4.10. Участник несет полную ответственность по всем операциям, подтвержденным любым Сертификатом, зарегистрированным Участником в Сервисе, вне зависимости от зарегистрированной для соответствующего Сертификата роли.

4.11. Организатор сервиса получает и регистрирует Сертификаты на свое имя и на своих уполномоченных лиц в том же порядке, что предусмотрен настоящими Правилами для Участника.

5. Особенности Электронного документооборота, действующие вне Правил Системы Besafe.

5.1. Для доступа Участника к Системе Организатора сервиса в рамках заключенного между Участником и Организатором сервиса основного договора и работы в ней, а также для создания и подтверждения запросов и сообщений, не требующих подписания Усиленной неквалифицированной Электронной подписью, Участник вправе совершить одно или несколько из следующих действий по согласованию с Организатором сервиса:

5.1.1. Зарегистрировать Работника Клиента для работы с Простой электронной подписью в соответствии с Правилами ЦФТ ID,

5.1.2. Получить Пароль, направив посредством средств Системы Организатора сервиса запрос на получение Пароля. Срок действия Пароля составляет 4 (четыре) года.

5.1.3. Получить Технологический сертификат в следующем порядке:

5.1.3.1. Для получения Технологического сертификата (сертификата точки обслуживания Участника) Участник оформляет заявление по ссылке https://www.authority.ru/auth/1st_class.jsp?class=5&type=2&f=fin&agentId=3802. Сертификат точки обслуживания Участника является технологическим сертификатом, создаваемым в соответствии с Правилами Удостоверяющего Центра. Заявление формируется в виде Электронного документа и направляется Агенту УЦ. После отправки заявления в электронном виде Участник направляет его Агенту УЦ в бумажном виде с собственноручной подписью уполномоченного лица Участника, с приложением документов, подтверждающих личность и полномочия уполномоченного лица Участника.

5.1.3.2. В течение 3 (Трёх) дней с момента получения заявления в бумажном виде Агент УЦ направляет Участнику изготовленный Удостоверяющим Центром Сертификат в электронном виде, либо мотивированный отказ от его выдачи. Участник направляет Агенту УЦ акт приёма-передачи Сертификата в бумажном виде за подписью уполномоченного лица Участника. Участник регистрирует указанный сертификат в Сервисе, направив заявку в бумажном виде (форма представлена в Приложении №2 к настоящим Правилам) Организатору сервиса. Срок действия Сертификата точки обслуживания Участника составляет 4 (Четыре) года.

5.1.3.3. Выдача и регистрация сертификатов точки обслуживания Участника может также происходить путем формирования работником Участника, Сертификат которого зарегистрирован в Сервисе

в роли «Администратор ключей точки обслуживания», соответствующих заявлений. «Администратор ключей точки обслуживания», используя АРМ «Администратор», создает и подписывает заявление на получение сертификата точки обслуживания Участника своей электронной подписью.

5.2. Участник регистрирует у Организатора сервиса свои точки обслуживания/терминалы (устройства) самообслуживания, в которых осуществляется Электронный документооборот, путем направления заявки на регистрацию точек обслуживания или терминала (устройства) самообслуживания Участника любым из следующих способов:

5.2.1. В виде документа на бумажном носителе по форме Приложения №4 к настоящим Правилам.

5.2.2. В виде реестра, содержащего следующие данные точек обслуживания/терминалов (устройств) самообслуживания: внутренний идентификатор, наименование (не обязательно), режим работы, адрес (населенный пункт, улица, дом, код ФИАС), телефон, IP-адрес. Заявка на регистрацию точек обслуживания/терминалов (устройств) самообслуживания в виде реестра передается Организатору сервиса по электронной почте с использованием адресов, указанных Участником в бумажном документе, указанном в п.5.2.1 Правил, либо через АРМ «Администратор» работником Участника, зарегистрированным в роли «Администратор ключей точки обслуживания» в рамках Системы BeSafe или в качестве Администратора в рамках Системы ЦФТ ID. Участник также может блокировать/возобновлять работу определенных точек обслуживания в рамках Сервиса посредством направления соответствующих заявок через АРМ «Администратор» или по электронной почте в аналогичном порядке.

5.3. В согласованных с Организатором сервиса случаях Участнику необходимо получить Смарт-ключи в целях работы по настоящим Правилам.

6. Порядок внесения изменений и дополнений в настоящие Правила.

6.1. Настоящие Правила утверждаются Организатором сервиса. Изменения в Правила вносятся Организатором сервиса в одностороннем порядке путём размещения новой редакции Правил на сайте www.besafe.ru и www.rnko.ru не позднее, чем за 15 (Пятнадцать) календарных дней до даты вступления в силу новой редакции Правил.

7. Переходные положения.

7.1. Заявки, оформленные Участником по формам, представленным в приложениях к настоящим Правилам до даты вступления в силу действующей редакции Правил, считаются надлежащими, создающими соответствующие права и обязанности в рамках действующих Правил.

7.2. Сертификаты, зарегистрированные Участником в Сервисе в порядке, предусмотренном ранее действующей редакцией Правил, сохраняют свою силу, считаются надлежащими, создающими соответствующие права и обязанности в рамках действующих Правил.