Платежная Система «QIWI Wallet»

Операционные правила

(v.2, dated 01/06/2014)

СОДЕРЖАНИЕ

1. Общие положения

Операционные правила Платежной Системы «QIWI Wallet» (далее – «Операционные правила») является нормативным документом Системы, регулирующим правила осуществления Субъектами Системы деятельности в рамках Платежной Системы «QIWI Wallet».

Операционные правила определяют:

- порядок использования электронных денег;
- порядок осуществления расчетов с использованием электронных денег;
- технологию управления рисками в Системе;
- порядок урегулирования споров Субъектов Системы между собой, а также между Субъектами Системы и лицами, не входящими в Систему;

2. Использование электронных денег

Под «использованием электронных денег» в рамках Платежной Системы «QIWI Wallet» понимается деятельность Банка-Эмитента, связанная с выпуском, реализацией и погашением электронных денег, а также проведением расчетов с использованием электронным денег
Договор, заключаемый Банком-Эмитентом с физическим лицом – потенциальным владельцем электронных денег, разрабатывается Банком-Эмитентом самостоятельно, при условии соблюдения общих Правил Системы.
Договор, заключаемый Банком-Эмитентом с юридическим лицом – потенциальным Агентом Банка-Эмитента, разрабатывается Банком-Эмитентом самостоятельно, при условии соблюдения общих Правил Системы.

2.1. Общие вопросы выпуска электронных денег

В рамках Платежной Системы «QIWI Wallet» Банк-Эмитент вправе осуществлять выпуск электронных денег.

Выпуск электронных денег осуществляется Банком-Эмитентом в пределах суммы денежных средств, предварительно внесенных Агентом Банка-Эмитента или физическим лицом Банку-Эмитенту, в соответствии с условиями заключенного между Банком-Эмитентом и таким Агентом Банка-Эмитента/физическим лицом договора.

Выпуская электронные деньги, Банк-Эмитент принимает на себя денежные обязательства, заменяющие в процессе их обращения требования Торгово-сервисных предприятий и/или Владельцев электронных денег по оплате товаров или услуг, а также требования Членов Системы и/или Владельцев электронных денег по погашению кредитных обязательств Владельцев электронных денег перед Членом Системы (здесь и далее – «Погашение кредитных обязательств»), и в том числе денежные обязательства, составленные в электронной форме.

Выпуск электронных денег производится в валюте страны, резидентом которой является Эмитент и на территории которой им осуществляется выпуск электронных денег.

2.2. Общие вопросы реализации электронных денег

В рамках Платежной Системы «QIWI Wallet» Банки-Эмитенты вправе осуществлять реализацию электронных денег как самостоятельно, так и с привлечением агентов на основании соответствующего договора между Банком-Эмитентом и Агентом Банка-Эмитента (если это не противоречит Применимому законодательству).

Реализация электронных денег осуществляется путем внесения физическим лицом Банку-Эмитенту (либо его Агенту) наличных денежных средств, либо путем перечисления денежных средств в безналичном порядке на соответствующий счет Банка-Эмитента.

В момент реализации электронных денег владельцу электронных денег выдается квитанция или иной документ, подтверждающий факт приобретения физическим лицом электронных денег. Форма и способы выдачи квитанции при реализации электронных денег устанавливается соответствующим договором, заключаемым между Банком-Эмитентом и физическим лицом – потенциальным владельцем электронных денег. Содержание квитанции должно полностью соответствовать требованиям Применимого законодательства.

Допускается реализация электронных денег Агентами Банка-Эмитента через электронные терминалы, позволяющие совершать операции по приему наличных денежных средств, пункты приема наличных денежных средств и иными способами, не противоречащими Применимому законодательству на основании договора, заключенного между Банком-Эмитентом и Агентами Банка-Эмитента.

Электронные деньги считаются реализованными Владельцу электронных денег с момента отражения информации о доступном остатке электронных денег в электронном кошельке Владельца электронных денег.

2.3. Общие вопросы погашения электронных денег

В рамках Платежной Системы «QIWI Wallet» Банки-Эмитенты вправе осуществлять погашение электронных денег, если это не противоречит Применимому законодательству.

Погашение электронных денег осуществляется Банком-Эмитентом при их предъявлении Владельцем электронных денег к погашению. Банк-Эмитент погашает электронные деньги путем выдачи предъявившему их лицу наличных денежных средств либо путем перевода денежных средств на банковский счет, указанный Владельцем электронных денег.

При погашении электронных денег сумма денежных средств, выдаваемых (переводимых) Владельцу электронных денег, предъявившему электронные деньги к погашению, должна соответствовать сумме электронных денег, предъявленных к погашению.

Электронные деньги считаются погашенными Банком-Эмитентом с момента выдачи Владельцу, предъявившему электронные деньги к погашению, соответствующей суммы наличных денежных средств или зачисления соответствующей суммы денежных средств на банковский счет, указанный Владельцем электронных денег.

3. Расчеты с использованием электронных денег

3.1. Общие вопросы осуществления операций с использованием электронных денег

Операции с использованием электронных денег осуществляются Банком-Эмитентом в соответствии с положениями настоящих Операционных правил, условиями договоров, заключенных Банками-Эмитентами с Агентом Банка-Эмитента, торгово-сервисными предприятиями, и нормами Применимого законодательства.

Операция с использованием электронных денег осуществляется на основании распоряжения Владельца электронных денег, переданного с использованием технических средств и методов, определенных Банком-Эмитентом.

Для обеспечения безопасности совершения операций с использованием электронных денег Банк-Эмитент обязан использовать только те технические средства и методы, право на использование которых предоставлено ему Оператором Системы в момент присоединения Банка-Эмитента к Платежной Системе «QIWI Wallet».

Распоряжение Владельца электронных денег о совершении операции с использованием электронных денег должно содержать указание на сумму операции, конечного получателя электронных денег и иные реквизиты, установленные Банком-Эмитентом в договоре, заключенном с Владельцем электронных денег.

Операция с использованием электронных денег осуществляется путем списания электронных денег с электронного кошелька Владельца электронных денег, направившего соответствующего распоряжение, и их передачи указанному таким Владельцем электронных денег получателю.

Осуществление операции с использованием электронных денег сопровождается выдачей Владельцу электронных денег, направившему распоряжение о совершении соответствующей операции, документа, подтверждающего факт осуществления операции с использованием электронных денег. Форма и способы выдачи такого подтверждающего документа устанавливаются соответствующим договором, заключаемым между Банком-Эмитентом и Владельцем электронных денег. Содержание документа, подтверждающего совершение операции с использованием электронных денег, должно полностью соответствовать требованиям Применимого законодательства.

По запросу Владельца электронных денег Банк-Эмитент обязан предоставить ему отчет, содержащий информацию обо всех операциях, совершенных Владельцем электронных денег по своему электронному кошельку. Формат и сроки предоставления отчета определяются договором, заключенным между Эмитентом и Владельцем электронных денег.

3.2. Оплата товаров (работ, услуг), погашение кредитных обязательств.

3.2.1. Общие вопросы оплаты товаров (работ, услуг), погашения кредитных обязательств.

Операции оплаты товаров (работ, услуг), погашения кредитных обязательств с использованием электронных денег могут совершаться в торгово-сервисном предприятии, осуществляющем реализацию товаров (работ, услуг).

Операции оплаты товаров (работ, услуг) осуществляются в пределах лимитов, устанавливаемых Банком-Эмитентом.

3.2.2. Требования к совершению операций оплаты товаров (услуг), погашения кредитных обязательств в ТСП

При совершении операции оплаты товаров (услуг) ТСП, Субъекты Системы обязаны обеспечить выполнение следующих требований:

- выполнение проверки совершаемой операции на соответствие ограничениям, накладываемым Банком-Эмитентом лимитами;
- выполнение авторизации операции, планируемой к совершению с использованием электронных денег;
- формирование первичного документа по совершенной операции в электронной форме;
- предоставление Владельцу электронных денег подтверждающего документа, оформленного согласно требованиям Применимого законодательства, по результатам осуществленной операции, на бумажном носителе.

4. Управление рисками

4.1. Общие положения управления рисками

Основными функциями Оператора Системы при обеспечении безопасности операций, осуществляемых Субъектами Системы в связи с выпуском, реализацией и погашением электронных денег, являются:

- идентификация угроз и уязвимости автоматизированных информационных систем;
- оценка рисков информационной безопасности автоматизированных информационных систем;
- обработка рисков информационной безопасности автоматизированных информационных систем.

Настоящий раздел Операционных правил определяет порядок проведения оценки рисков информационной безопасности для автоматизированных информационных систем, а также методику обработки выявленных рисков.

Порядок распространяется на всех Субъектов Системы и их автоматизированные информационные системы, и является обязательной к исполнению Субъектами Системы.

4.2. Идентификация угроз и уязвимостей

Идентификация угроз и уязвимостей автоматизированных информационных систем проводится коллегиально, с участием представителей Оператора Системы, Банка-Эмитента, чьи автоматизированные информационные системы проходят проверку, а также иных Субъектов Системы, взаимодействующие с автоматизированными информационными системами проверяемого Банка-Эмитента.

Идентификация угроз и уязвимостей автоматизированных информационных систем проводится по мере выявления новых угроз и уязвимостей автоматизированных информационных систем, но не реже одного раза в год.

При идентификации угроз и уязвимостей обязательно должны быть учтены:

- сведения об инцидентах информационной безопасности, произошедших в автоматизированных информационных системах Банка-Эмитента;
- результаты выполнения утвержденных в Системе процедур проверок (сканирование уязвимостей, тесты на проникновение, мониторинг событий информационной безопасности и прочие);
- мнения заинтересованных Субъектов Систем;
- информация внешних специализированных баз знаний (новостные ленты и прочие).

По результатам процесса идентификации угроз и уязвимостей проверяемый Банк-Эмитент создает реестр выявленных угроз и уязвимостей.

4.3. Оценка рисков информационной безопасности

Оценка рисков информационной безопасности проводится комиссией по оценке рисков (далее – «Комиссия по оценке рисков») не реже одного раза в год, а также при возникновении существенных изменений, влияющих на результаты предыдущей оценки.

Комиссия по оценке рисков формируется из представителей Оператора Системы, Банка-Эмитента, а также иных Субъектов Системы, использующих и/или взаимодействующих с проверяемыми автоматизированными информационными системами, из числа специалистов, обладающих достаточной осведомленностью о ключевых используемых автоматизированных информационных системах, основных процессах и рисках.

Организацию работы, подготовку исходной информации, модерирование работы и председательство в Комиссии по оценке рисков осуществляет полномочный представитель Оператора Системы (далее – «Председатель Комиссии по оценке рисков»).

Оценка рисков информационной безопасности автоматизированных информационных систем производится в соответствии с процедурой, описанной в Приложении № 1 к настоящим Операционным правилам.

Работа Комиссии по оценке рисков завершается формированием Отчета об оценке рисков, утверждаемого Председателем Комиссии по оценке рисков, который включает в себя рекомендации Комиссии по оценке рисков о доработках автоматизированных информационных систем Банков-Эмитентов в части предотвращения угроз и устранения уязвимостей таких систем в части информационной безопасности.

4.4. Обработка рисков информационной безопасности

Значение приемлемого уровня риска информационной безопасности автоматизированных информационных систем Субъектов Системы устанавливается Оператором Системы.

Возможные варианты действий с выявленными рисками, прошедшими оценку:

- выбор и применение защитных мер, направленных на снижение рисков до приемлемого уровня;
- предотвращение рисков, путем исключения рискованных действий и/или оптимизации работы автоматизированных информационных систем;
- перенос рисков на третьих лиц, не являющихся Субъектами Системы (например, страхование рисков информационной безопасности);
- принятие рисков, если их значение не превышает приемлемый уровень;
- принятие рисков, если стоимость реализации защитных мер превышает вероятный ущерб от реализации соответствующей угрозы.

При рассмотрении Отчета об оценке рисков Комиссия по оценке рисков принимает решение об обработке рисков: риски, не превышающие приемлемые уровни, принимаются; остальные снижаются, предотвращаются или переносятся.

На основании решения Комиссии по оценке рисков Оператор Системы разрабатывает, в отношении рисков, требующих проведения мероприятий, План обработки рисков информационной безопасности.

Разработанный и согласованный План обработки рисков подлежит выполнению Субъектом(ами) Системы в течение установленного Оператором Системы срока. По итогам выполнения Плана обработки рисков проводится повторная идентификация угроз и уязвимостей автоматизированных информационных систем соответствующего Субъекта Системы.

5. Урегулирование споров

5.1. Претензия Субъекта Системы

В случае возникновения у Субъекта Системы каких-либо претензий к Оператору Системы и/или иным Субъектам Системы по любой спорной ситуации, связанной с осуществлением Субъектом Системы деятельности в рамках Платежной Системы «QIWI Wallet», Субъект Системы вправе направить Оператору Системы соответствующую претензию в письменной форме.

В случае если претензия Субъекта Системы связана с опротестованием совершенных с использованием электронных денег операций в Системе, такая претензия может быть подана Субъектом Системы только в одном из следующих случаев:

- операция с использованием электронных денег не была осуществлена по вине одного из Субъектов Системы;
- операция с использованием электронных денег была заблокирована Оператором Системы в связи с подозрением на незаконность такой операции.

К направляемой Субъектом Системы претензии должны быть приложены документы, содержащие доказательства обстоятельств, послуживших поводом для направления претензии.

Претензия может быть направлена Субъектом Системы любым из следующих способов:

- в электронном виде, посредством электронного документооборота;
- заказным почтовым отправлением с уведомлением и описью вложения;
- нарочным, с проставлением отметки уполномоченного представителя Оператора Системы о получении претензии.

5.2. Рассмотрение претензии

Рассмотрение претензии Субъектом Системы осуществляется Оператором Системы в течение 10 (Десяти) рабочих дней с даты поступления к Оператору Системы соответствующей претензии Субъектом Системы.

По результатам рассмотрения претензии Субъекта Системы Оператор Системы производит одно из следующих действий:

- в случае установления правомерности требований Субъекта Системы, заявленных в претензии (полностью или в части), предпринимает действия, направленные на удовлетворение требований Субъекта Системы по спорной ситуации;
- в случае установления неправомерности требований Субъекта Системы, заявленных в претензии, направляет Субъекту Системы, от которого получена претензия, разъяснительную информацию в отношении спорной операции.

5.3. Согласительная комиссия

В случае несогласия Субъекта Системы, направившего претензию, с разъяснительной информацией, полученной от Оператора Системы, Субъект Системы, направивший претензию, вправе потребовать рассмотрения спорной ситуации Согласительной комиссией. Требование о передаче спора на рассмотрение Согласительной комиссии может быть заявлено Субъектом Системы, направившим претензию,в течение 5 (Пяти) рабочих дней с даты получения разъяснений Оператора Системы по претензии Субъекта Системы.

Согласительная комиссия формируется из представителей Оператора Системы, Субъекта Системы, направившего претензию, а также иных Субъектов Системы, участвовавших в спорной операции (операциях). Формирование Согласительной комиссии обеспечивается Оператором Системы и должно быть завершено в течение 10 (Десяти) рабочих дней с

даты получения Оператором Системы соответствующего требования Субъекта Системы, направившего претензию.

Рассмотрение спорной ситуации Согласительной комиссией осуществляется в порядке и по правилам, установленным в Приложении № 2 к настоящим Операционным правилам.

В течение 5 (Пяти) рабочих дней с даты завершения рассмотрения спорной ситуации Согласительной комиссией, решение Согласительной комиссии направляется Оператором Системы с соответствующими разъяснениями и указаниями (в случае признания требований Субъекта Системы, направившего претензию правомерными полностью или в части) всем заинтересованным Субъектам Системы.

5.4. Арбитраж

В случае несогласия кого-либо из Субъектов Системы, интересы которого затронуты решением Согласительной комиссии, с решением Согласительной комиссии, такой Субъект Системы в течение 30 (Тридцати) календарных дней после получения решения Согласительной комиссии вправе уведомить Оператора Системы о своем несогласии. В таком уведомлении о несогласии должны быть указаны спорные вопросы и причины несогласия.

Ни одна из сторон спорной ситуации не имеет права начинать судебное разбирательство в отношении любого спора, если не было представлено уведомление о несогласии с решением Согласительной комиссии, как описано выше.

Если ни одна из сторон спорной ситуации не представила уведомления о несогласии с решением Согласительной комиссии в пределах 30 (Тридцати) календарных дней после получения соответствующего решения Согласительной комиссии, то решение Согласительной комиссии становится окончательным и имеет обязательную силу для всех заинтересованных Субъектов Системы.

Если Оператором Системы от какой-либо из сторон спорной ситуации будет получено уведомление о несогласии, заинтересованные Субъекты Системы обязаны попытаться мирным путем урегулировать спор до начала судебного разбирательства. Однако если Сторонами не согласовано иначе, судебное разбирательство может быть начато по истечении 45 (Сорока пяти) календарных дней с момента представления уведомления о несогласии, даже если не было предпринято попыток урегулировать спор мирным путем.

Любой спор, решение Согласительной комиссии по которому не стало окончательным и обязательным для всех заинтересованных Субъектов Системы, и если спорная ситуация не разрешена мирным путем, такая спорная ситуация подлежит окончательному разрешению в судебном порядке в соответствии с Применимым законодательством путем передачи спора на рассмотрение в Международный коммерческий арбитражный суд при Торгово-промышленной палате России в соответствии с действующим Регламентом.

При этом, ни один из Субъектов Системы в ходе судебного разбирательства не может быть ограничен представлением доказательств или аргументов, которые ранее выдвигались Согласительной комиссии для вынесения ею решения, или причинами несогласия, указанными в уведомлении о несогласии. Любое решение Согласительной комиссии может быть предъявлено в суде в качестве подтверждения или доказательства.

6. Приложения к настоящим Операционным правилам

6.1. Приложение № 1: Процедура Оценки рисков информационной безопасности автоматизированных информационных систем

Исходной информацией для проведения оценки рисков являются:

- перечень информационных систем, процессов и прочих активов, для которых проводится оценка рисков;
- актуальный Реестр угроз и уязвимостей;
- результаты предыдущей оценки рисков информационной безопасности.

В ходе проведения Оценки рисков информационной безопасности члены Комиссии по оценке рисков определяют набор угроз и уязвимостей, применимых к каждому из активов, и проводят их оценку с точки зрения степени вероятности реализации и степени тяжести последствий, основываясь на знаниях о реализованных защитных мерах и ценности актива. Отчетным документом по результатам собрания является Отчет об оценке рисков информационной безопасности.

Под определением степени вероятности реализации (СВР) нарушения информационной безопасности подразумевается значение в соответствии со шкалой ниже, определяющее потенциальную вероятность реализации угрозы для данного актива с учетом реализованных защитных мер.
Для выполнения оценки СВР угроз информационной безопасности проводится анализ возможности потери каждого из свойств информационной безопасности для информационных активов в результате воздействия выделенных источников угроз.

Основными факторами для оценки СВР угроз информационной безопасности являются:

- информация соответствующих моделей угроз, в частности:
- данные о расположении источника угрозы относительно соответствующих типов объектов среды;
- информация о мотивации источника угрозы (для источников угроз антропогенного характера);
- предположения о квалификации и (или) ресурсах источника угрозы;
- статистические данные о частоте реализации угрозы ее источником в прошлом;
- информация о способах реализации угроз информационной безопасности;
- информация о сложности обнаружения реализации угрозы рассматриваемым источником;
- данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих априорных защитных мер.

Для оценки СВР угроз информационной безопасности используется следующая качественная шкала степеней:

- крайне маловероятно – «1»;
- маловероятно – «2»;
- потенциально возможно – «3»;
- высокая вероятность реализации – «4»;
- реализуемо – «5».

При привлечении к оценке отдельных СВР угроз информационной безопасности нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку СВР угроз информационной безопасности принимать равной экспертной оценке, определяющей наибольшую СВР угрозы информационной безопасности.

Для угроз, источником которых является человек, простота реализации угрозы путем эксплуатации уязвимости прямо пропорциональна необходимой для ее реализации квалификации злоумышленника.

Для определения степени тяжести последствий (СТП) нарушения информационной безопасности проводится анализ последствий потери каждого из свойств информационной безопасности для каждого из типов информационных активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз.

Основными факторами для оценки СТП нарушения информационной безопасности являются:

- степень влияния на непрерывность деятельности;
- степень влияния на деловую репутацию;
- объем финансовых и материальных потерь;
- объем финансовых и материальных затрат, необходимых для восстановления свойств информационной безопасности для информационных активов рассматриваемого типа и ликвидации последствий нарушения информационной безопасности;
- объем людских ресурсов, необходимых для восстановления свойств информационной безопасности для информационных активов рассматриваемого типа и ликвидации последствий нарушения информационной безопасности;
- объем временных затрат, необходимых для восстановления свойств информационной безопасности для информационных активов рассматриваемого типа и ликвидации последствий нарушения информационной безопасности;
- степень нарушения законодательных требований и (или) договорных обязательств;
- степень нарушения требований регулирующих и контролирующих (надзорных) органов в области информационной безопасности;
- объем хранимой, передаваемой, обрабатываемой, уничтожаемой информации, соответствующей рассматриваемому типу объекта среды;
- данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих апостериорных защитных мер.

Для оценки СТП нарушения информационной безопасности вследствие реализации угроз информационной безопасности используется следующая качественная шкала степеней:

- незначительная – «1»;
- небольшая – «2»;
- существенная – «3»;
- серьезная – «4»;
- критическая – «5».

При привлечении к оценке отдельных СТП нарушения информационной безопасности нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку СТП нарушения информационной безопасности принимать равной экспертной оценке, определяющей наибольшую СТП нарушения информационной безопасности.

Каждый член Комиссии оглашает собственную субъективную оценку СВР и СТП угроз для рассматриваемого скоупа оценки рисков.

Результирующие оценки рассчитываются по формуле:

$$V_R = (V_1 + V_2 + \ldots + V_n) / n$$, **где:**

VR – результирующая оценка;
Vi – оценка, выданная i-ым членом Комиссии;
n – общее количество членов Комиссии.

Результирующие оценки фиксируются Председателем Комиссии в Отчете об оценке рисков информационной безопасности.

Риски активов рассчитываются по следующей формуле:

$$R = СВР \times СТП$$, **где:**

R – оцениваемый риск;

СВР – степень вероятности реализации угрозы нарушения ИБ
СТП – степень тяжести последствий реализации угрозы нарушения ИБ;

Риски могут принимать значение от 1 до 25.
Полученный Отчет об оценке рисков в рабочем порядке проходит согласование со всеми членами Комиссии, и утверждается Оператором Системы.

6.2. Приложение № 2: Порядок и правила работы Согласительной комиссии

1. Срок рассмотрения спорной ситуации Согласительной комиссией составляет 45 (Сорок пять) календарных дней с момента завершения формирования состава Согласительной комиссии.

2. Решение по спору считается принятым Согласительной комиссией, в случае если оно принято всеми арбитрами единогласно.

3. В ходе рассмотрения спора Согласительной комиссией, Субъекты Системы обязаны представлять в Согласительную комиссию копии любых документов, имеющих отношение к предмету спора, которые может запросить Согласительная комиссия. Копии всех документов переписки между Согласительной комиссией и Субъектами Системы должны отправляться всем Субъектам Системы.

4. Согласительная комиссия обязана действовать в соответствии с положениями настоящих Правил. Согласительная комиссия обязана:
   - поступать справедливо и беспристрастно при разрешении спора между Субъектами Системы, предоставляя каждому из них разумную возможность изложить свои доводы и ответить на доводы иных Субъектов Системы, участвующих в разбирательстве;
   - применять процедуры, приемлемые для каждого конкретного спора, избегая ненужной задержки или расходов.

5. Согласительная комиссия вправе созвать слушанье по рассмотрению спорного вопроса. В этом случае Согласительная комиссия принимает решение о дате и месте проведения такого слушанья и вправе потребовать от Субъектов Системы документацию и аргументы в письменном виде до или в процессе заседания. При этом уведомление о созыве слушанья подлежит направлению Согласительной комиссией Субъектам Системы через Оператора Системы не позднее, чем за 10 (Десять) календарных дней до даты проведения такого слушанья.

6. Согласительная комиссия обладает полномочиями по утверждению процедуры расследования, отказу в допуске на слушанье любых лиц, кроме представителей заинтересованных Субъектов Системы, и ведению слушанья в отсутствие представителя любого из Субъектов Системы, которым Оператор Системы направил уведомление о проведении слушанья.

7. Согласительная комиссия обладает (наряду с иными) следующими полномочиями:
   - устанавливать приемлемую процедуру решения спора;
   - самостоятельно устанавливать для себя сферу полномочий и определять, в какой степени тот или иной спор относится к ней;
   - проводить слушанья так, как представляется необходимым, руководствуясь исключительно порядком и правилами, предусмотренными в нормативных документах Системы;
   - проявлять инициативу для выяснения фактов и обстоятельств, необходимых для принятия решения;
   - использовать собственные специальные знания, если таковые имеются.

8. Согласительная комиссия в ходе слушанья не должна выражать какое-либо мнение по поводу весомости любых аргументов, выдвинутых Субъектами Системы, участвующими в спорной ситуации.

9. Согласительная комиссия должна принять решение и уведомить о нем всех заинтересованных Субъектов Системы через Оператора Системы в письменном виде, в течение 10 (Десяти) календарных дней с даты принятия решения.