Утверждены
Приказом № RP-23/П-09 от 25.08.2023 г.
Директора ТОО «RocketPay»
Терзиева Д.О.

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ ТОО «RocketPay»

2023 г.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ. ОПИСАНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

Настоящие Правила осуществления деятельности платежной организации ТОО «RocketPay» (далее – «**Правила**») разработаны в соответствии с положениями Закона Республики Казахстан от 26 июля 2016 года № 11-VI «О платежах и платежных системах», Правил организации деятельности платежных организаций, утвержденных постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215, Устава ТОО «RocketPay» и другими нормативными правовыми актами Республики Казахстан и определяют порядок организации деятельности ТОО «RocketPay» в качестве платежной организации (далее – «**Платежная организация**»).

Согласно учетной регистрации, проведенной Национальным Банком Республики Казахстан, Платежная организация оказывает услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам (далее – «**Платежные услуги**»).

Платежные услуги оказываются посредством системы обработки электронных платежей (далее – «**Система RocketPay**»), в которой Платежная организация выступает в качестве ее оператора, другими ее участниками являются:

Клиент - физическое лицо, держатель платежной карточки, получатель Платежных услуг, плательщик, совершающий посредством Системы RocketPay платежи за товары, работы, услуги, иные платежи, вытекающие из гражданско-правовых отношений, пожертвования, членские взносы, платежи в бюджет т.п.

Партнер - банк второго уровня, организация, осуществляющая отдельные виды банковских операций, с которым/которой Платежная организация заключила договор сотрудничества в целях оказания Платежных услуг.

Поставщик услуг – заключившее с Платежной организацией договор об оказании Платежных услуг юридическое лицо, индивидуальный предприниматель, реализующие товары (работы, услуги), юридическое лицо, принимающее пожертвования, членские взносы, а также лицо, осуществляющее деятельность, не относящуюся к предпринимательской, имеющие право в соответствии с законодательством Республики Казахстан принимать платежи.

В настоящих Правилах могут быть использованы термины и определения, не определенные Правилами, в таком случае их толкование определено документами, образующими договор между участниками Системы RocketPay и/или законодательством Республики Казахстан.

Документы, договоры, которые могут быть опубликованы Платежной организацией на своем официальном сайте и/или применяться для регулирования деятельности Платежной организации, установления форм партнерских взаимоотношений, порядка оказания Платежных услуг, являются составными частями настоящих Правил.

Условия Правил, включая определения, предусмотренные Правилами, превалируют над условиями договоров и определениями в них, и в случае противоречий отдельных положений такого договора Правилам, преимущественную силу имеют Правила.

В случае, если отношения, возникающие между участниками Системы RocketPay прямо не урегулированы Правилами, договором или выходят за пределы их норм, применяются нормы законодательства Республики Казахстан.

Несоблюдение Правил может явиться одним из оснований для прекращения участия в Системе RocketPay участника, допустившего подобное несоблюдение.

Платежная организация по мере необходимости имеет право вносить изменения в настоящие Правила путем разработки, утверждения и публикации новой редакции Правил.

Актуальная редакция Правил публикуется на официальном сайте Платежной организации в сети интернет.

ГЛАВА 2. ИНФОРМАЦИЯ О ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ

ТОО «RocketPay», БИН 220340012049;
Регистрационный номер в реестре платежных организаций, прошедших учетную регистрацию в Национальном Банке Республики Казахстан - № 02-22-123 от 01.06.2022 года;
Адрес местонахождения: г. Алматы, 050043, ул. Жандосова, д.98, оф. 406;
Официальный сайт: https://rocketpay.kz;
Телефонный номер: +7 707 512-89-61;
Электронная почта: info@rocketpay.kz.

ГЛАВА 3. ПОРЯДОК И СРОКИ ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ КЛИЕНТАМ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ

Оказание Платежных услуг (прием платежей) осуществляется в следующем порядке:
Шаг 1. Клиент с целью инициирования платежа с использованием платежной карточки в пользу Поставщика услуг переходит со страницы интернет - ресурса Поставщика услуг на платежную форму Платежной организации и вводит в платежную форму реквизиты платежной карточки (имя держателя платежной карточки, номер платежной карточки, срок действия платежной карточки, CVV).
Шаг 2.
Клиент знакомится с порядком предоставления Платежной организацией Платежных услуг, условиями взимания и размером комиссии и соглашается с условиями Правил и договора, размещенными на официальном сайте Платежной организации. Использование Клиентом Платежных услуг свидетельствует об ознакомлении и согласии Клиента с порядком предоставления Платежной организацией Платежных услуг, условиями взимания и размером комиссии, условиями Правил и договора.
Шаг 3.
Платежная организация обеспечивает прием платежа, инициированного Клиентом и последующую передачу реквизитов платежа в адрес Партнера.
Шаг 4.
Партнер исполняет поручение Клиента, переданное через Систему RocketPay в электронной форме, в следующем порядке: производит списание денег с платежной карточки Клиента, осуществляет перевод платежа в пользу Поставщика услуг, указанного в поручении Клиента с учетом вознаграждения Платежной организации и комиссионного вознаграждения Партнера (при их наличии).

Движение денежных средств при положительно обработанной операции в рамках вышеуказанного порядка приема платежей выглядит следующим образом:

- Эмитент[1] осуществляет списание денежных средств с платежной карточки Клиента;
- Эмитент осуществляет платеж в пользу Партнера, обеспечивающего эквайринг;
- Партнер, обеспечивающий эквайринг перечисляет денежные средства (за исключением своей комиссии) на специальный (транзитный) счет Партнера рамках соответствующего договора с Платежной организацией;
- После зачисления платежей на такой специальный (транзитный) счет Платежная организация передает Партнеру электронные реестры платежей с указанием суммы и реквизитов Поставщика услуг, которому необходимо зачислить платежи, а Партнер осуществляет соответствующий перевод платежей на указанный счет Поставщика услуг.

[1] Эмитент - банк или Национальный оператор почты, осуществивший выпуск платежных карточек.

При оказании Платежных услуг в зависимости от конкретной категории сервисов, предоставляемых Поставщиком услуг могут производится выплаты (перевод денег): со специального (транзитного) счета (способ 1) или с корпоративной платежной карточки Поставщика услуг (способ 2):

По способу 1 оператором перевода выступает Партнер в рамках заключенного договора между Платежной организацией и Партнером и предусматривается следующий порядок действий:

Шаг 1. Платежная организация принимает запрос на выплату (перевод денег) от Поставщика услуг.

Шаг 2. Платежная организация по факту запроса передает Партнеру информацию о списании денег со специального (транзитного) счета Партнера и зачислении денег на платежную карточку Клиента.

Шаг 3. Партнер по получению информации от Платежной организации осуществляет перевод денег со специального (транзитного) счета Партнера на платежную карточку Клиента.

По способу 2 следующий порядок действий:

Шаг 1. Платежная организация принимает запрос на выплату (перевод денег) от Поставщика услуг.

Шаг 2. Платежная организация по факту запроса передает Партнеру информацию о списании денег с корпоративной платежной карточки Поставщика услуг и зачислении денег на платежную карточку Клиента.

Шаг 3. Партнер по получению информации от Платежной организации осуществляет перевод денег одной платежной карточки на другую.

Условия оплаты и/или получения выплат посредством Системы, предусмотрены договором.

Сроки оказания Платежной услуги - в течение 3 (трех) операционных дней, следующих за днем приема платежа.

ГЛАВА 4. СТОИМОСТЬ ПЛАТЕЖНЫХ УСЛУГ (ТАРИФЫ)

Тарифы Платежной организации по Платежным услугам состоят из следующих комиссий:

- с каждой транзакции на прием платежей по Платежным карточкам Visa и Mastercard – от 5 % и ниже, минимальная сумма комиссия – 0 тенге.
- с каждой транзакции на выплаты на Платежные карточки Visa и Mastercard – от 5% и ниже, минимальная сумма комиссия – 0 тенге.

Платежная организация вправе изменять действующие тарифы с учетом специфики вида деятельности Поставщика услуг, предполагаемого количества транзакций, в том числе, отнесения и/или принадлежности его к определенному уровню риска, и т. п., а также в случае изменения тарифов Партнерами. Действующие стандартные тарифы на платежные услуги размещаются на сайте Платежной организации в сети интернет по адресу https://rocketpay.kz и/или устанавливаются условиями договора.

ГЛАВА 5. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ С УЧАСТНИКАМИ СИСТЕМЫ ROCKETPAY

Основанием взаимодействия Платежной организации с участниками Системы RocketPay является договор.

Платежной организацией с участниками Системы RocketPay заключаются следующие виды договоров:

- с Партнером - договор о взаиморасчетах и информационно-техническом взаимодействии и иные договора в рамках сотрудничества;

• с Клиентом - договор об оказании Платежных услуг, заключенный путем совершения конклюдентных действий Клиента (пользование Платежными услугами) в ответ на оферту, размещенную на официальном сайте Платежной организации;
• с Поставщиком услуг - договор об оказании Платежных услуг, заключенный путем присоединения Поставщика услуг к публичному договору, на основании анкеты, при условии его акцепта Платежной организацией или путем заключения индивидуального договора.
Далее по тексту каждый из указанных видов договоров именуются вместе и по отдельности «договор».

5.1. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ С ПОСТАВЩИКАМИ УСЛУГ

Платежная организация до заведения нового Поставщика услуг в Систему RocketPay, осуществляет предварительный экономический анализ его деятельности, по результатам которого, в случае положительного решения о дальнейшем сотрудничестве, Платежная организация переходит к запросу документов, перечень которых определен условиями договора и необходим в рамках проведения оценки на соответствие требованиям законодательства Республики Казахстан и анализа возможности заключения деловых отношений (далее «**онбординг**»).
Порядок проведения онбординга предусмотрен внутренними документами Платежной организации.
Платежной организацией к взаимодействию рассматриваются Поставщики услуг, зарегистрированные и осуществляющие свою деятельность на территории Республики Казахстан и в соответствии с законодательством Республики Казахстан или на территории иностранного государства, работающие посредством интернета – ресурсов.
К интернет – ресурсу Поставщика услуг, Платежной организацией устанавливаются следующие обязательные требования, не исчерпывающие:
• интернет – ресурс должен быть рабочим (интернет-ресурс, который находится в стадии разработки не принимается к рассмотрению);
• интернет – ресурс должен принадлежать Поставщику услуг. В случае принадлежности интернет - ресурса учредителю, руководителю и/или иным лицам, Поставщик услуг обязан предоставить документ, подтверждающий право на использование интернет – ресурса от его правообладателя;
• наличие на сайте актуальной справочной информации о Поставщике услуг. Обязательным условием является наличие наименования юридического лица, индивидуального предпринимателя, данные юридического адреса, а также контактных телефонов, по которым Клиент может связаться со службой поддержки интернет – ресурса/Поставщиком услуг;
• перечень продаваемых товаров, оказываемых услуг, производимых работ с отражением стоимости, и иных характеристик, в случае, когда лицо, осуществляет деятельность, не относящуюся к предпринимательской в соответствии с законодательством Республики Казахстан и принимающее иные платежи, вытекающие из гражданско-правовых отношений, пожертвования, членские взносы, платежи в бюджет т.п. с отражением или без отражения их размеров, в том случае, если инициатива платы на стороне Клиента;
• договор оферты с условиями сделки, включая обмен/возврат/отмену заказа;
• политика конфиденциальности;
• условия и варианты оплаты с использованием платежных карточек (условия могут входить в состав условий договора оферты или быть размещены самостоятельно в отдельных вкладках интернет – ресурса).

Иные требования могут предусматриваться условиями договора либо могут быть затребованы Платежной организацией в зависимости от конкретной категории сервисов, предоставляемых Поставщиком услуг.
В случае положительного результата онбординга между Платежной организацией и Поставщиком услуг заключается договор.
После заключения договора, Платежная организация и Поставщик услуг осуществляют интеграцию с Системой «RocketPay».
Первоначально Платежная организация устанавливает для Поставщика услуг тестовый режим проведения операций, после настройки параметров обработки операций Платежная организация активирует возможность перехода Поставщика услуг на «боевой режим» проведения операций в Системе «RocketPay».
По запросу Поставщика услуг после положительного онбординга но до заключения договора, между Платежной организацией и Поставщиком услуг могут проводится мероприятия тестовой интеграции информационных систем и технологического взаимодействия для оценки возможности дальнейшего взаимодействия сторон.

5.2. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ С ПАРТНЕРАМИ

Платежная организация вправе привлекать любое количество Партнеров с целью обеспечения оказания Платежных услуг.
Договор взаимодействия Платежной организации с Партнером должен содержать, по меньшей мере, но не ограничиваясь, следующую информацию:

- общее описание оказываемых Платежных услуг, включая порядок и максимальный срок их оказания;
- размеры взимаемых сборов и комиссий, а также порядок их взимания;
- порядок расчетов с Платежной организацией и Поставщиком услуг;
- порядок предъявления претензий и разрешения споров.

К взаимодействию Платежной организацией рассматриваются Партнеры соответствующие следующим критериям:

- общая финансовая устойчивость;
- осуществление мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- наличие необходимых лицензий (разрешений) на осуществление деятельности Банка в соответствии с требованиями применимого законодательства;
- обеспечение информационной защиты и банковской тайны;
- регистрация Платежной организации в Системе Партнера. Для целей такой регистрации Платежная организация осуществляет реализацию интерфейса подключения (API) к системе Партнера.

В рамках взаимодействия/договора Платежная организация и Партнер обязуются передавать друг другу информацию о каждом обработанном платеже непосредственно в период обработки платежа на основе предоставленных Клиентом данных, проводить сверку по успешно обработанным платежам.

5.3. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ С ТРЕТЬИМИ ЛИЦАМИ, ОБЕСПЕЧИВАЮЩИМИ ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

В рамках законодательства Республики Казахстан Платежная организация вправе уполномочивать третьих лиц на оказание информационно-технологической поддержки для целей оказания Платежных услуг.

Подключение информационных систем третьего лица к Системе RocketPay осуществляется при условии и на основании заключенного договора на оказание информационных и (или) технологических услуг, который обязательно включает в себя следующие условия:
•ответственность третьего лица и его обязательства по поддержанию требуемого уровня информационной безопасности;
•необходимость оперативного уведомления Платежной организации о случаях нарушения информационной безопасности и об угрозах таких нарушений;
•соглашение о конфиденциальности (неразглашении информации), устанавливающего режим конфиденциальности информации, ее охраны и неразглашения.

ГЛАВА 6. СВЕДЕНИЯ О СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ, ИСПОЛЬЗУЕМОЙ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ

Основной задачей управления рисками в Платежной организации является обеспечение эффективного, надежного и безопасного функционирования.
Достижение такой задачи осуществляется посредством реализации следующих задач:
- обеспечения стабильного функционирования Платежной организации;
- обеспечение бесперебойности и надежности оказания Платежных услуг;
- обеспечения и поддержания рисков на приемлемом уровне;
- предотвращение перерастания отдельных рисков в системный риск.

Процесс управления рисками включает следующие этапы:
- идентификация риска, представляющая собой процесс выявления рисков и их основных источников, обнаружения событий, источников их возникновения и возможных последствий, исследования и описания рисков;
- измерение и оценка риска представляет собой процесс исследования сущности риска и определения его уровня, на основании чего оценивается риск и принимаются решения о реагировании на него. Также оценка включает сравнение уровня риска, выявленного в процессе измерения, на основании которого определяется дальнейшее отношение к риску.

Реагирование на риск предусматривает принятие мер по результатам выявления (идентификации) и измерения (оценки) риска, представляющих собой одно или несколько из следующих действий:
- ограничение (снижение) риска (уменьшение вероятности возникновения риска и (или) размеров возможного ущерба при наступлении неблагоприятных событий);
- сохранение риска, (принятие риска либо при необходимости его увеличение до величины, не превышающей допустимого уровня);
- уклонение от риска посредством отказа от начала либо продолжения деятельности, в результате которой возникает риск.

Мониторинг, контроль и корректировка тактики управления рисками в Платежной организации.
Оценка тактики управления рисками осуществляется посредством сопоставления ее и полученного результата. Если цели управления рисками достигнуты либо полученные показатели превышают ожидаемые, результат считается положительным, если цели не достигнуты или достигнуты частично, — отрицательным. При получении отрицательного результата проводится детальный анализ подходов к управлению рисками, по итогам которого разрабатываются корректирующие мероприятия либо новая тактика управления рисками.
Управление рисками в Платежной организации определяются такими способами как:
- осуществление операций в пределах, лимитах, установленных Платежной организацией и/или Партнером;
- осуществление операций в пределах, лимитах находящихся денежных средств на платежной карточке;

- другими допустимыми способами управления рисками.

ГЛАВА 7. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ И РАЗРЕШЕНИЯ СПОРОВ С КЛИЕНТАМИ

В случае возникновения у Клиента какой-либо претензии к Платежной организации, связанной с оказанием Платежных услуг, Клиент вправе направить Платежной организации соответствующее обращение, составленное в произвольной форме с описанием возникшей спорной ситуации и указанием предпочтительного способа обратной связи (далее – «Претензия»).

К любой Претензии, направляемой Клиентом Платежной организации, должны быть приложены надлежащим образом оформленные документы, подтверждающие изложенные в ней факты, а также документы, удостоверяющего личность Клиента.

Претензия может направлена одним из следующих способов:

- почтовым отправлением по адресу – Казахстан, город Алматы, 050043, улица Жандосова, д.98, оф. 406; и/или
- на электронную почту: info@rocketpay.kz.

Платежная организация обязуется рассмотреть и направить ответ Клиенту на полученную Претензию в срок, не превышающий 10 (десять) рабочих дней со дня получения Претензии.

При необходимости Платежная организация вправе запрашивать у Клиента дополнительные документы (или их копии), объяснения и иные сведения.

Клиент по запросу Платежной организации обязан предоставить запрашиваемые сведения и документы (их копии).

Платежная организация на основании полученных сведений и разъяснений для формирования полного ответа на Претензию составляет и направляет мотивированный ответ Клиенту на Претензию в установленный выше срок.

Любой спор, если он не был разрешен мирным путем в досудебном порядке, подлежит окончательному разрешению в судебном порядке в соответствии с законодательством Республики Казахстан.

ГЛАВА 8. ПОРЯДОК СОБЛЮДЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Платежная организация обеспечивает создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления рисками Платежной организации, предназначенной для управления процессом обеспечения информационной безопасности.

Платежная организация и Поставщики услуг соблюдают требования стандарта безопасности данных, включающего в себя требования международных платежных систем (далее – «**МПС**») к обеспечению информационной безопасности — PCI DSS и иные требования МПС.

Система управления информационной безопасностью Платежной организации обеспечивает защиту информационных активов, допускающую минимальный уровень потенциального ущерба для своих бизнес-процессов.

Основными мерами защиты конфиденциальности, целостности и доступности информационных активов Платежной организации являются:

- управление сетевой безопасностью;
- управление уязвимостями и политиками безопасности;
- управление безопасностью конечных устройств;
- управление идентификацией и доступом;
- управление инцидентами информационной безопасности;
- управление криптографическими средствами защиты;
- управление антивирусными средствами защиты;

- обеспечение физической безопасности информационных активов;
- обеспечение безопасности при взаимодействии с контрагентами;
- обучение и повышение осведомленности персонала в вопросах информационной безопасности;
- обеспечение безопасности интернет-ресурсов.

Платежная организация разрабатывает внутренние процедуры по созданию, сбору, хранению и обработке информации в своих информационных системах.

Платежная организация осуществляет мониторинг за процессами создания, хранения и обработки информации и доступа к ней с помощью механизмов информационных систем и технических средств обеспечения безопасности.

ГЛАВА 9. ОПИСАНИЕ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ И ОБОРУДОВАНИЯ, НЕОБХОДИМОГО ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖНЫХ УСЛУГ

Соответствие требованиям к программно-техническим средствам Платежной организации и системе управления информационной безопасностью.

Для целей обеспечения надежного хранение информации применяется дублирование систем хранения данных, а также наличием холодного резерва комплектующих к ним.

Защиту от несанкционированного доступа обеспечивает:

- использование сетевого оборудования отвечающими характеристикам с показателями не ниже:

Характеристика	**Показатель**
Пропускная способность в режиме Firewall (App-ID enabled)	940 Mbps
Пропускная способность в режиме защиты от угроз	610 Mbps
Пропускная способность IPSec VPN	400 Mbps
Максимальное число одновременно поддерживаемых сессий	128 000
Максимальное количество «новых» сессий	8 300/c
Максимальное количество туннелей VPN/туннельных интерфейсов	1000
Максимальное количество зон безопасности	30
Максимальное число правил безопасности	1 500

- использование программного обеспечения на сетевом оборудовании:

Threat Prevention – включает функциональные возможности IPS, Antivirus, Anti-Bot, Anti-Spyware;

URL-Filtering – фильтрация URL-запросов пользователей по категориям;

Global Protect – предоставляет возможность подключения пользователей к ресурсам локальной сети через межсетевой экран Palo Alto Networks, также позволяет задействовать возможность проверки удаленного хоста на соответствие определенным правилам безопасности такие как наличие на клиентском устройстве антивируса, актуальной версии ОС со всеми актуальными обновлениями;

WildFire –возможность использовать публичное облако специализированных компаний, оказывающих услуги в области информационной безопасности, для сканирования подозрительных файлов на вредоносную активность.

Обеспечение целостности баз данных и полную сохранность информации в электронных архивах и базах данных при полном или частичном отключении электропитания в любое время на любом участке оборудования обеспечивается:

- хранением информации с использованием системы управления базой данных Microsoft SQL Server версии не ниже Standard Edition выпуска не старше 2016;

• использованием технологии SQL Server AlwaysOn, решения высокого уровня доступности и аварийного восстановления, включающая в себя в том числе следующие функции:
распределение метаданных и уведомлений - метаданные служб и размещенных приложений, конфигурации и состояния хранятся на каждом узле кластера, изменения в метаданных или состоянии узла автоматически распространяются на другие узлы кластера;
управление ресурсами - отдельные узлы в кластере могут предоставлять физические ресурсы, например, подключаемое напрямую хранилище, сетевые интерфейсы и доступ к общему дисковому хранилищу.
мониторинг работоспособности - определение исправности основного узла и исправности между узлами осуществляется за счет сочетания сетевых соединений по типу тактовых импульсов и мониторинга ресурсов;
координацию отработки отказа - каждый ресурс настроен для размещения на основном узле, и каждый может быть перенесен автоматически или вручную на один или несколько второстепенных узлов. Политика отработки отказа в зависимости от исправности управляет автоматическим переносом ресурсами между узлами кластера. Узлы и размещенные приложения получают уведомления об отработке отказа, что позволяет им продолжить выполнять возложенные на них функции без прерывания в работе и потери данных;
расположение оборудования, использующегося для обработки и хранения баз данных в центрах обработки данных, отвечающих требованиям:
- гарантированное электропитание;
- обеспечение необходимого климатического режима;
- круглосуточный мониторинг и техническое обслуживание;
- автоматический комплекс газового пожаротушения;
- круглосуточно охраняемая территория;
- системы видеонаблюдения;
- разграничение физического доступа и организационные процедуры контроля доступа во все помещения;
- порт выхода в сеть интернет на скорости от 100 Мбит в секунду.

Доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предоставляется пользователям в соответствии с «Матрицей владельцев и администраторов информационных систем».
Требования к учетным записям пользователей:

• учетные записи, включая системные и сервисные, в системном и прикладном программном обеспечении, а также системы и средства защиты информации (включая доступ к управлению межсетевыми экранами и антивирусным программным обеспечением) защищены стойкими методами аутентификации;

• каждому пользователю информационной системы назначается уникальный идентификатор (имя учётной записи);

• недопустимость использования разделяемых между несколькими пользователями учётных записей, групповых и общих учётных записей, паролей и других средств аутентификации.

В используемых формах ввода данных используется контроль полноты вводимых данных либо справочники полей обязательных к заполнению, необходимых для проведения и регистрации операций, в случае выполнения функций или операций без полного заполнения всех полей программа может обеспечивать запись соответствующее записи в журнал и\или выдачу соответствующего уведомления.
Программное обеспечение, используемое для проведения и регистрации операций, обеспечивает поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по

доступным параметрам, а также возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе.
Обработка информации и ее хранение осуществляется по дате и времени.
В информационных системах используется автоматизированное формирование журналов внутреннего учета средствами используемой операционной системы, дополнительно критичные события фиксируются в программном инструменте Zabbix для мониторинга элементов ИТ-инфраструктуры:

- локальная вычислительная сеть;
- физические сервера;
- виртуальные сервера;
- прикладное программное обеспечение: сервисы обработки операций, системы управления базами данных;
- облачные сервисы.

При этом обеспечивается сбор и отображение основных метрик состояния, событий, а также формирование журнала\отчета событий за определенный диапазон дат или полностью.
Информационные системы, задействованные в проведении и хранении операций, обеспечивают автоматизированное формирование форм отчетов, представляемых операторами систем электронных денег в Национальный банк, а также отчетов о проведенных операциях.
Резервированное копирование и восстановления данных, хранящихся в учетных системах, обеспечивается средствами используемых системой управления базой данных, а также Microsoft Data Protection Manager - систем непрерывного резервного копирования/восстановления. Контроль выполнения процедур резервного копирования осуществляется путем:

- оповещения ответственного сотрудника при удачном\неудачном резервном копировании
- тестирования восстановления баз данных информационных систем не реже 1 (одного) раза в год.

Программное обеспечение реализует возможность вывода выходных документов на экран, принтер или в файл.
Программное обеспечение реализует возможность обмена электронными документами.
Регистрацию и идентификацию происходящих в информационной системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события, результат выполнения события фиксируется средствами используемых системой управления базой данных, в том числе:

- модуль для сбора событий.
- модуль для анализа и управления событиями и потоками сети из устройств, конечных точек, серверов, антивирусов, брандмауэров и различных систем предотвращения вторжений.