УТВЕРЖДЕНЫ

Приказом АО «Ванта»

№4 от 6 февраля 2023 года

ПРАВИЛА УПРАВЛЕНИЯ РИСКАМИ, СВЯЗАННЫМИ С ОСУЩЕСТВЛЕНИЕМ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРА ФИНАНСОВОЙ ПЛАТФОРМЫ

Москва
2023

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. В настоящих Правилах применяются следующие термины, определения и сокращения:

- ***Агрегатор*** - владелец ресурса (сайта в информационно-телекоммуникационной сети «Интернет» и/или мобильного приложения) с информацией о товарах (услугах), привлекаемый Оператором для обеспечения размещения в соответствии с Правилами финансовой платформы информации о финансовых сделках, совершаемых с использованием Финансовой платформы.
- ***База данных о событиях операционных рисков, БДСОР*** - электронное хранилище информации о событиях операционного риска АО «Ванта».
- ***База данных рисков, БДР*** – реестр рисков, электронное хранилище информации о нефинансовых рисках АО «Ванта».
- ***ГСИБ*** - главный специалист по информационной безопасности - должностное лицо, осуществляющее управление рисками.
- ***Избегание риска*** - отказ от принятия/передачи/снижения отдельных видов риска, который должен повлечь за собой отказ от совершения каких-либо операций и оказания каких-либо услуг, которым присущ риск. Поскольку данные действия могут привести к уменьшению доходов, решение об избегании/удержании риска должно приниматься с учетом сравнения величины риска и размера дохода.
- ***Ключевой индикатор, КИ*** – показатель деятельности АО «Ванта» (в том числе статистический, финансовый), позволяющий осуществлять мониторинг масштабности и вероятности/возможности реализации риска.
- ***Контрольные процедуры*** - совокупность мер, направленных на снижение вероятности/возможности возникновения, уменьшение потенциального ущерба от реализации риска и устранение последствий события возникновения риска.
- ***Кредитный риск*** - риск возникновения убытков вследствие неисполнения, несвоевременного либо неполного исполнения контрагентом своих обязательств в соответствии с условиями договоров.
- ***Минимизация риска*** – деятельность, направленная на снижение вероятности/возможности возникновения риска, уменьшения потенциального ущерба от реализации риска или устранения негативных последствий события риска, за счет внедрения новых или оптимизации существующих контрольных процедур.
- ***Нефинансовые риски, риски*** – операционный риск, комплаенс, включая регуляторный риск, риск потери деловой репутации, стратегический риск.
- ***Нештатная ситуация, НС*** – обстоятельства, нестандартная ситуация, вызывающие и/или создающие предпосылки к возникновению сбоев (отказов) при эксплуатации подсистем программно-технического комплекса Платформы в процессе своей деятельности, и/или непосредственно препятствующие их нормальному (штатному) функционированию, и иные обстоятельства, которые:
  - повлекли или могут повлечь за собой нарушения порядков взаимодействия между Оператором Платформы и сторонами Платформы;
  - привели или могут привести к нарушению порядка и сроков проведения операций, порядка доступа Участников к Платформе, а также раскрытия и предоставления информации, установленных внутренними документами Оператора Платформы;

- ***Оператор финансовой платформы, Оператор Платформы, Оператор*** – Акционерное общество «Ванта» (АО «Ванта»), включенное Банком России в реестр операторов финансовых платформ в соответствии с Федеральным законом от 20 июля 2020 года № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы», оказывающее услуги, связанные с обеспечением возможности совершения Финансовых сделок между Потребителями финансовых услуг и Финансовыми организациями с использованием Финансовой платформы. Оператор финансовой платформы не является стороной Финансовых сделок, совершаемых с использованием Финансовой платформы.
- ***Операционный риск*** - риск возникновения последствий, влекущих за собой приостановление или прекращение оказания услуг в полном или неполном объеме, а также риском возникновения расходов (убытков) Оператора Платформы в результате сбоев и (или) ошибок программно-технических средств, и (или) во внутренних бизнес-процессах, ошибок работников и (или) в результате внешних событий, оказывающих негативное воздействие на Оператора Платформы.
- ***Передача риска*** - способ управления риском, предусматривающий передачу чистого риска полностью или частично на основе договора третьей стороне. Наиболее часто используемой формой передачи риска является передача части процессов на аутсорсинг, а также страхование рисков.
- ***Пользователи*** - посетители Сайта Оператора Платформы и (или) Приложения, являющиеся физическими лицами.
- ***Принятие риска*** - деятельность, с которой связан данный вид риска, продолжает осуществляться в неизменном виде. В случае принятия риска в обязательном порядке рассматривается необходимость установления системы мониторинга по различным показателям, характеризующим уровень риска. Процедура принятия риска закрепляется во внутренних документах.
- ***Регистратор финансовых транзакций, Регистратор, РФТ*** - Небанковская кредитная организация акционерное общество «Национальный расчетный депозитарий», ОГРН: 1027739132563; место нахождения: Российская Федерация, 105066, город Москва, ул. Спартаковская, дом 12.
- ***Риск*** – это событие или условие, которое в случае возникновения имеет негативное воздействие на бизнес-процессы, услуги и клиентов, а также которое приводит или может привести к потенциальным потерям, которые могут выражаться в недополучении доходов, появлении дополнительных расходов или в отрицательном влиянии на деловую репутацию.
- ***Риск-аппетит*** - представляет собой максимальный уровень риска, который Оператор Платформы готов принять для достижения стратегических целей.
- ***Санкционные риски*** – это вероятность, что в отношении контрагента, его учредителя, бенефициара или контролирующего лица будут введены американские или европейские санкции, что не позволит продолжить исполнение договора без ограничений.
- ***Комплаенс (регуляторный) риск*** - риск возникновения у Оператора Платформы расходов (убытков) и (или) иных неблагоприятных последствий в результате несоответствия деятельности требованиям федеральных законов и принятых в соответствии с ними нормативных актов, правилам Оператора финансовой платформы, учредительным и внутренним документам Оператора Платформы, а также в результате применения мер со стороны Банка России, других регулирующих или контрольных органов.
- ***Риск потери деловой репутации, РПДР*** - риск возникновения негативных последствий у Оператора Платформы в результате негативного восприятия Оператора Платформы со стороны Участников, контрагентов и клиентов, Банка России и иных лиц, которые могут

негативно повлиять на способность Оператора Платформы поддерживать существующие и (или) устанавливать новые деловые отношения и поддерживать на постоянной основе доступ к источникам финансирования.

- ***Система управления рисками, СУР*** - комплекс правил, документов и мероприятий по идентификации и оценке рисков, воздействию на риски, а также контролю за их состоянием с целью минимизации финансовых потерь вследствие неблагоприятного изменения факторов риска.
- ***Событие риска*** - событие, ситуация, обстоятельства, которые характеризуется реализацией (проявлением) риска и могут сопровождаться причинением компании убытков (возникновения расходов).
- ***Стороны*** - термин, используемый при совместном упоминании Оператора, Финансовой организации, Потребителя.
- ***Стратегический риск*** - риск возникновения расходов (убытков) у Оператора Платформы в результате принятия ошибочных решений в процессе планирования и управления, в том числе при разработке, утверждении и исполнении документов, определяющих направления развития, ненадлежащем исполнении принятых решений в процессе управления, неучете органами управления изменений внешних факторов, влияющих или способных повлиять на процесс управления Платформой.
- ***Участники финансовой платформы, Участники, Потребители*** - потребители финансовых услуг, присоединившиеся к договору об оказании услуг Оператора Платформы в целях совершения финансовых сделок с финансовыми организациями и эмитентами.
- ***Фактор риска*** - обстоятельство, обусловившее или способное обусловить возникновение события риска.
- ***Финансовая платформа, Платформа*** - информационная система (программно-технический комплекс), которая обеспечивает взаимодействие участников финансовой платформы посредством информационно-телекоммуникационной сети «Интернет» в целях обеспечения возможности совершения Финансовых сделок и доступ к которой предоставляется Оператором финансовой платформы с Сайта финансовой платформы и/или через Приложение Финансовой платформы.
- ***Финансовые организации*** - для целей Правил под финансовыми организациями понимаются кредитные и некредитные финансовые организации, присоединившиеся к Договору об оказании услуг Оператора финансовой платформы, условия которого установлены Правилами платформы, в целях совершения финансовых сделок с потребителями финансовых услуг.
- ***Чрезвычайная ситуация, ЧС*** – ситуация, которая может представлять собой угрозу прерывания нормальной деятельности, причиной которой может являться:
    - нарушение нормального функционирования автоматизированных систем, поддерживающих критичные процессы;
    - неработоспособность (недоступность) основных каналов связи, информационно-телекоммуникационной сети Интернет, других каналов связи с взаимодействующими организациями, необходимых для выполнения критичных процессов
    - отсутствие физической возможности нахождения работников, обеспечивающих деятельность Оператора Платформы, на рабочих местах вследствие пожара, наводнения, аварий, актов террора, диверсий, саботажа, стихийных бедствий и других обстоятельств непреодолимой силы;

- иные случаи, способные повлечь нарушение нормальной работы Платформы.

1.2. Термины и определения, не указанные в настоящих Правилах, используются в значениях, установленных в нормативных правовых актах Российской Федерации, нормативных и иных актах Банка России, в том числе, регламентирующих порядок деятельности оператора финансовой платформы, Правилах ЭДО и иных внутренних документах Оператора.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила управления рисками, связанными с осуществлением деятельности оператора финансовой платформы (далее - Правила), являются основополагающим документом, определяющим основные принципы организации системы управления рисками Оператора финансовой платформы АО «Ванта» (далее – *Оператор Платформы*), связанные с деятельностью финансовой платформы, и формируют основу для построения эффективно работающей системы управления рисками, связанными с осуществлением деятельности Оператора Платформы.

2.2. Правила разработаны на основании требований Федерального закона от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» (далее – Федеральный закон) в целях повышения качества управления рисками Оператора Платформы.

2.3. Правила подлежат ежегодной оценке на предмет актуальности и эффективности. Пересмотр правил осуществляется по мере необходимости.

2.4. Правила содержат общие положения, определяющие цели управления рисками, включая:

- основные методологические принципы и подходы к идентификации, оценке и мониторингу рисков;
- классификацию рисков, присущих деятельности Платформы;
- критерии существенности последствий, к которым может привести реализация рисков Оператора Платформы, в целях признания таких рисков значимыми, а также порядок сопоставления результатов оценки выявленных рисков с указанными критериями;
- порядок выявления, анализа и оценки рисков Оператора Платформы;
- порядок внесения рисков и результатов их оценки в реестр рисков, порядок осуществления оценки реестра рисков на предмет его актуальности;
- порядок и периодичность проведения идентификации угроз, которые могут привести к неработоспособности Оператора Платформы;
- порядок назначения отдельных должностных лиц, ответственных за реализацию мероприятий;
- порядок и сроки информирования органов управления, должностных лиц о рисках;
- порядок и периодичность составления и представления на рассмотрение органов управления отчетов и информации о результатах реализации процессов и мероприятий в рамках организации системы управления рисками;
- содержание отчетов и информации о результатах осуществления в рамках организации системы управления рисками и представляемых на рассмотрение органов управления;
- порядок принятия Оператором Платформы мер по предотвращению и урегулированию конфликта интересов, связанного со совмещением деятельности оператора финансовой платформы с иными видами деятельности с учетом ограничений, установленных Федеральным законом;
- перечень мер, предпринимаемых для обеспечения конфиденциальности и защиты информации о рисках, в том числе конфиденциальности отчетов о рисках;

- порядок обеспечения операционной надежности и поддержания непрерывности деятельности;
- порядок обеспечения контроля за выполнением процессов и мероприятий по управлению рисками;
- порядок и сроки проведения проверок эффективности управления рисками.

2.5. В рамках системы управления рисками организован непрерывный мониторинг нештатных ситуаций с оценкой степени их возможного воздействия на технологические процессы Оператора Платформы, а также обновляется система комплексного управления рисками в соответствии с принимаемыми решениями и правилами. Оператор Платформы осуществляет постоянное развитие и совершенствование системы управления рисками для снижения уязвимости бизнес-процессов и времени их восстановления, повышения уровня резервирования технологий.

2.6. Оператор Платформы обеспечивает хранение документов и информации, связанных с организацией системы управления рисками, в течение не менее чем пяти лет со дня их создания.

3. ОПИСАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ

3.1. Управление рисками осуществляется в соответствии с требованиями Федерального закона, нормативных документов Банка России и Уставом АО «Ванта».

3.2. Принципы управления рисками:

- Принцип комплексности предполагает выявление источников и объектов риска на основе всестороннего анализа всех существующих и планируемых к вводу бизнес-процессов, ИТ систем и продуктов;
- Принцип непрерывности предполагает проведение на регулярной основе необходимого набора упорядоченных, целенаправленных процедур, таких как оценка текущих рисков, анализ технологии и регламентов функционирования СУР, предоставление отчетности органам управления;
- Принцип открытости - выражается в предоставлении всей необходимой информации об организации СУР всем заинтересованным сторонам;
- Принцип существенности означает, что при внедрении различных элементов СУР следует исходить из сопоставления затрат на реализацию механизмов анализа, контроля и управления рисками с потенциальными результатами от этой реализации, а также с затратами на организацию и внедрение продуктов, услуг или сервисов, несущих оцениваемые риски;
- Принцип независимости оценок - означает, что оценка и управление рисками осуществляется ГСИБ, независимым от подразделений, генерирующих прибыль/финансовый результат;
- Принцип документированного оформления – означает, что порядок и работы системы управления рисками должны быть разработаны, пройти процедуру внутреннего согласования и быть утверждены соответствующими органами управления;
- Принцип консерватизма - предполагает, что выбор метода оценки и управления рисками базируется на разумном сочетании надежности СУР и рентабельности деятельности.

3.3. Целью функционирования СУР является ограничение принимаемых рисков по всем направлениям деятельности в соответствии с собственными стратегическими задачами и целями, обеспечение достаточности собственных средств на покрытие принимаемых рисков и обеспечение надежного функционирования бизнес-процессов Оператора Платформы.

3.4. Цель управления рисками достигается на основе системного, комплексного подхода, который подразумевает решение следующих задач:
- выявление, анализ, мониторинг, контроль, и снижение рисков (или их принятие/исключение) на постоянной основе;
- организация информационного обмена между структурными подразделениями в процессе выявления рисков;
- качественная и количественная оценка (измерение) рисков;
- установление порядка предоставления отчетности по вопросам управления рисками органам управления;
- осуществление контроля эффективности управления рисками;
- создание системы контрольных мероприятий по предупреждению событий риска, поддержанию приемлемого уровня риска (рисков), а также системы быстрого и адекватного реагирования для устранения последствий таких событий в случае их возникновения.

3.5. Полномочия и функции ГСИБ ответственного за организацию СУР:
- Для управления рисками Оператора Платформы назначено специальное должностное лицо - главный специалист по информационной безопасности (далее – ГСИБ).
- ГСИБ вправе требовать у работников и должностных лиц предоставления информации (документов), в том числе письменных объяснений, по вопросам, возникающим в ходе выполнения им своих обязанностей.
- Органы управления, иные структурные подразделения и должностные лица также могут быть вовлечены в процессы управления рисками.

3.6. В компетенцию ГСИБ входит, в том числе:
- разработка программ обучения (консультаций) работников по вопросам выявления, идентификации и оценки рисков, а также их контроля;
- разработка методологии и инструментов управления рисками;
- оценка нефинансовых рисков с учетом вероятности его наступления и влияния на деятельность Оператора Платформы;
- разработка рекомендации органам управления, должностным лицам, в том числе руководителям структурных подразделений, о мерах, которые необходимо предпринять для устранения того или иного риска Оператора Платформы;
- осуществление контроля выполнения мер, направленных на устранение рисков Оператора Платформы;
- предоставление информации о рисках Оператора Платформы коллегиальному исполнительному органу и единоличному исполнительному органу;
- принятие иных мер, направленных на организацию СУР, предусмотренных внутренними документами.

3.7. В компетенцию Общего собрания акционеров входит, в том числе, утверждение внутренних документов концептуального характера в области управления рисками.

3.8. Процесс управления рисками выстраивается таким образом, что каждый работник Оператора Платформы информирует ГСИБ об идентифицированных рисках, а также о событиях риска, и участвует в реализации мероприятий по контролю и минимизации риска в зоне своей ответственности.

4. ОСНОВНЫЕ РИСКИ, СВЯЗАННЫЕ С ОСУЩЕСТВЛЕНИЕМ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРА ПЛАТФОРМЫ

4.1. Платформа представляет собой информационную систему, использующую программно-технические средства, предназначенные для обеспечения удаленного взаимодействия между Платформой, Участниками и Финансовыми организациями в целях заключения сделок. Оператором Платформы является АО «Ванта».

4.2. Основные риски Оператора Платформы выражаются в нарушении функционирования информационной системы в результате сбоя программно-технических средств, невозможности подключения Участников и Финансовых организаций к Платформе с целью заключения сделок, невозможности выполнения Оператором Платформы своих обязательств перед Участниками и Финансовыми организациями по подключению и выполнению поручений по заключению сделок; а также комплаенс риски, связанные с идентификацией иностранных налогоплательщиков (FATCA/CRS).

4.3. Реализация рисков может приводить к сбоям в работе Платформы, задержкам расчётов, финансовым и иным потерям. К возможным случаям реализации рисков относятся ошибки и (или) задержки при обработке информации, перебои в работе систем, недостаточная пропускная способность, мошенничество, а также потеря и (или) утечка данных. Риск может возникать как из внутренних, так и из внешних источников.

4.4. Система управления рисками Оператора Платформы включает в себя следующие виды рисков:

4.4.1. Нефинансовые риски:

4.4.1.1. Операционный риск:

- Факторы возникновения:
  - не оптимально выстроенные, недостаточные и/или неэффективные контрольные процедуры в системах и процессах;
  - неадекватные действия работников (в том числе ошибки, внутреннее мошенничество);
  - несовершенство организационной структуры и внутренних документов в части распределения полномочий подразделений и работников, порядков и процедур совершения операций, их документирования и отражения в учете;
  - несоблюдение работниками установленных порядков и процедур;
  - неэффективность внутреннего контроля;
  - сбои в функционировании систем и оборудования;
  - неблагоприятные внешние обстоятельства, находящиеся вне контроля Оператора Платформы (включая внешнее мошенничество, хакерские и DdoS атаки, техногенные и природные катастрофы);
  - нарушение информационной безопасности.
- Этапы управления операционным риском:
  - выявление, анализ, мониторинг, контроль и снижение рисков (или их исключение) на постоянной основе;
  - организация информационного обмена между структурными подразделениями в процессе выявления рисков;
  - качественная и количественная оценка (измерение) рисков;
  - установление порядка предоставления отчетности по вопросам управления рисками органам управления;
  - осуществление контроля эффективности управления рисками;

- создание системы контрольных мероприятий по предупреждению событий риска, поддержанию приемлемого уровня риска (рисков), а также системы быстрого и адекватного реагирования для устранения последствий таких событий в случае их возникновения;
- эффективное распределение полномочий и ответственности между Общим собранием акционеров, ГСИБ и работниками по вопросам управления рисками.

- В рамках управления операционными рисками выделяют процесс управления рисками, связанными с оказанием поставщиками услуг внешних услуг и поставке оборудования в течение всего периода их оказания. Заключение договоров на оказание внешних услуг с поставщиками услуг сопряжено со следующими рисками:
  - не оказание услуги должным образом/непоставку оборудования;
  - не предоставление документов, подтверждающих факт выполнения договора;
  - нарушение иных условий договора поставщиком, включая нарушение соглашения о конфиденциальности, предоставление недостоверных сведений.
- В целях управления рисками, связанными с оказанием поставщиками услуг и оборудования, проводится оценка поставщиков, включая проверку достоверности сведений, предоставленных контрагентом, анализ и оценка его финансовой состоятельности, надежности и деловой репутации. По результатам проведенной проверки делается заключение о возможности заключения договора с представленным контрагентом.
- В рамках управления операционным риском Оператор Платформы выделяет управление рисками информационной безопасности (ИБ).

4.4.1.2. Комплаенс риск, включая регуляторный:

- Оператор Платформы рассматривает следующий минимальный перечень базовых комплаенс-рисков, подлежащих управлению:
  - Риск использования в целях легализации (отмывания) доходов, полученных преступным путем и финансирования терроризма (ПОД/ФТ);
  - Несоблюдение работниками норм профессиональной этики и/или совершение действий, которые могут привести к потере деловой репутации;
  - Нарушение требований в части идентификации иностранных налогоплательщиков (FATCA/CRS).
- К внутренним факторам, влияющим на величину комплаенс-рисков, относятся:
  - Несоблюдение законодательства, в том числе по противодействию ПОД/ФТ, по идентификации и изучению клиентов, контрагентов, противодействию коррупции, а также в сфере финансовых рынков, защиты прав и интересов клиентов, конфликта интересов;
  - Несоблюдение внутренних документов и процедур;
  - Несоблюдение профессиональных стандартов или норм деловой этики;
  - Резкие изменения в составе и количестве сотрудников;
  - Ускоренное развитие бизнеса;
  - Внедрение новых технологий;
  - Разработка новых продуктов или расширение в новые сферы бизнеса/новые рынки;

- Изменения в организационной структуре.

- К внешним факторам, влияющим на величину комплаенс-рисков, относятся:
  - Нахождение клиентов и контрагентов под юрисдикцией различных государств;
  - Недобросовестные действия клиентов/контрагентов;
  - Развитие схем внутреннего и внешнего мошенничества, вредительства и ухода от контроля;
  - Развитие рынка и технологий;
  - Существенные изменения в экономике и/или законодательстве (в том числе, иностранном).
- Процесс управления комплаенс-риском включает в себя выявление, оценку присущего уровня риска, определение стратегии реагирования на риск, разработку перечня мер по снижению риска, определение остаточного уровня риска и контроль за выполнением мероприятий по минимизации риска.
- Меры по минимизации комплаенс-риска:
  - Разработка внутренних нормативных документов, регламентирующих процессы и процедуры, связанные с управлением комплаенс-риском;
  - Автоматизация контроля;
  - Обучение персонала.

4.4.1.3. Риск потери деловой репутации (РПДР):

- Управление РПДР производится в целях снижения возможных убытков, сохранения и поддержания деловой репутации перед клиентами и контрагентами, учредителями (участниками), участниками финансового рынка, органами государственной власти, участником которых является Оператор Платформы.
- Оператор Платформы в рамках управления риском потери деловой репутации организует сбор и анализ отзывов о деятельности Оператора Платформы в средствах массовой информации, включая публикации и отзывы касательно случаев реализации операционных рисков, связанных с техническими проблемами на стороне Платформы и связанных с деятельностью организаций, участвующих в деятельности Платформы, в том числе с использованием специализированных автоматизированных информационных систем.
- Процесс управления РПДР включает идентификацию РПДР и событий РПДР, их оценку по установленным Оператором Платформы шкалам вероятности и влияния, разработку мер по минимизации РПДР, постоянный мониторинг РПДР и предоставление отчетности органам управления на периодической основе. Все события РПДР и риски РПДР систематизируются и хранятся в базе данных операционных рисков.

4.4.1.4. Стратегический риск:

- Основной целью управления стратегическим риском является формирование системы, обеспечивающей возможность принятия надлежащих управленческих решений в отношении деятельности Оператора Платформы по снижению влияния стратегического риска на деятельность Оператора Платформы в целом.
- Оператор Платформы в рамках управления стратегическим риском обеспечивает проведение оценки ГСИБ в целях выявления потенциальных источников возникновения рисков:
  - Разработка проектов изменений в порядок осуществления деятельности Оператора Платформы, предоставления дополнительных услуг, а также

иных организационных и (или) технологических изменений (далее -проекты изменений);

- Анализ целесообразности внедрения проектов изменений;
- Анализ эффективности реализованных проектов изменений по итогам их введения в деятельность;
- Мероприятия по планированию развития деятельности, в том числе, посредством разработки стратегии развития;
- Оценка стратегии развития на предмет определения возможности и целесообразности ее реализации, а также внесение изменений в стратегию развития в случае указанного решения.

4.4.1.5. Санкционный риск:

- Оператор Платформы рассматривает три основных источника санкционных рисков Платформы, подлежащих управлению:
  - Финансовые организации – Участники платформы;
  - Физические лица - Пользователи платформы;
  - Контрагенты Оператора платформы, в том числе осуществляющие поставку ИТ оборудования и ПО, необходимых для функционирования Платформы.
- Несоблюдение установленных требований в области санкций может привести к:
  - Блокировке активов за рубежом;
  - Распространение режима экономических ограничений на Оператора платформы и (либо) ее аффилированных лиц;
  - Преследованию Оператора платформы либо его аффилированных лиц в уголовном, либо административном порядке;
  - Существенным штрафам и иным санкциям со стороны регулирующих органов;
  - Принудительному надзору за действиями Оператора со стороны независимых и регулирующих органов других стран;
  - Требованию провести ретроспективную проверку деятельности организации за период до десяти лет и устранить выявленные нарушения;
  - Репутационному ущербу.
- Управление санкционным риском осуществляется в соответствии с настоящим документом, а также иными внутренними нормативными документами Оператора Платформы, устанавливающими принципы управления санкционным риском, и включает в себя мероприятия в рамках управления операционным риском, связанным с оказанием поставщиками услуг внешних услуг и поставке оборудования, а также следующие мероприятия :
  - Управление конфликтом локального и иностранного законодательства;
  - Определение объема проверок, осуществляемых в отношении финансовых организаций-участников Платформы, пользователей Платформы контрагентов и операций, осуществляемых посредством Платформы;
  - Использование юридических инструментов ограничения санкционных рисков;
  - Определение порядка действий в случае обнаружения потенциальных и фактических совпадений с санкционными списками;
  - Определение объема тестирования эффективности используемых автоматизированных решений;

- Выявление на стадии допуска пользователей и финансовых организаций – участников Платформы с высоким или неприемлемым уровнем санкционного риска;
- Определение необходимости и порядка прекращения отношений с пользователями Платформы, финансовыми организациями – участниками Платформы, контрагентами, а также ограничения предоставления отдельных услуг.

4.4.2. Финансовые риски:

4.4.2.1. ***Кредитный риск:***

- Основным источником кредитного риска в деятельности Оператора Платформы является риск неуплаты или несвоевременной уплаты комиссионных вознаграждений Финансовыми организациями.
- С целью управления кредитным риском ГСИБ проводит комплекс мер и процедур:
  - Осуществляет ежедневный мониторинг финансового положения и оценку уровня кредитного риска по отношению к контрагентам в соответствии с применяемой внутренней методикой;
  - Осуществляет оценку финансового положения контрагентов в рамках закупочной деятельности в целях снижения экономических, налоговых, и репутационных рисков;
  - Осуществляет оценку необходимости формирования резервов под ожидаемые кредитные потери.

4.5. Так как Оператор Платформы, в соответствии со своей бизнес- и юридической моделью не несет обязательств по сделкам, заключаемым на ней Пользователями, в случае неисполнения одной стороной по сделке своих обязательств перед другой, то иные финансовые риски в деятельности Платформы не выявлены.

4.6. Управление рисками включает в себя также выявление чрезвычайных ситуаций и проведения анализа обстоятельств их возникновения, ведения перечня потенциальных нештатных ситуаций.

4.7. Оператор Платформы обеспечивает непрерывное взаимодействие Потребителей финансовых услуг с Финансовыми организациями и эмитентами для совершения финансовых сделок, бесперебойного и непрерывного функционирования объектов информационной инфраструктуры, в том числе в случае реализации информационных угроз, а также восстановления предоставления услуг и работоспособности объектов информационной инфраструктуры в установленные в правилах Оператора Платформы сроки.

4.8. Оператор Платформы обеспечивает и постоянно поддерживает конфиденциальность, целостность и доступность своих защищаемых информационных активов путем реализации комплекса мероприятий по защите информационной безопасности, включая регулярную инвентаризацию и классификацию информационных активов, формирование и совершенствование системы управления информационной безопасности, внедрения и настройки средств защиты информации и обучения персонала, своевременного выявления и устранения уязвимостей активов и тем самым предупреждения возможности нанесения ущерба и нарушения нормального функционирования бизнес-процессов Оператора Платформы.

4.9. Оператор Платформы обеспечивает соблюдение целевых показателей операционной надежности исходя из требований Банка России, обеспечивая ее бесперебойность, а также конфиденциальность, целостность и сохранность данных, доступ к данным на постоянной основе.

4.10. Оператор Платформы устанавливает и пересматривает не реже одного раза в год пороговый уровень показателя бесперебойности с использованием результатов оценки рисков, а также с учетом развития новых технологий и совершенствования бизнес-процессов.

4.11. Оператор Платформы при предоставлении услуг по содействию в совершении финансовых сделок между Потребителями финансовых услуг и Финансовыми организациями обеспечивает реализацию мероприятий по достижению показателя доступности Финансовой Платформы не ниже установленного уровня.

4.12. Оператор Платформы в рамках реализации процессов обеспечения операционной надежности классифицирует все бизнес- и технологические процессы, реализующие виды деятельности Платформы, связанные с предоставлением услуг, в зависимости от степени влияния указанных процессов на предоставление услуг:

- Основные, выполнение которых напрямую связано с предоставлением услуг;
- Вспомогательные, выполнение которых косвенно связано с предоставлением услуг.

4.13. Оператор Платформы производит приоритизацию основных и вспомогательных бизнес- и технологических процессов с целью корректного установления параметров, характеризующих операционную надежность.

4.14. Планирование и реализация процессов обеспечения операционной надежности осуществляются Оператором Платформы начиная с этапа разработки и планирования внедрения бизнес- и технологических процессов, реализующих деятельность Платформы.

4.15. В рамках реализации процессов обеспечения операционной надежности Оператор Платформы обеспечивает функционирование системы обеспечения операционной надежности в отношении:

- Бизнес- и технологических процессов, реализуемых Оператором Платформы в целях предоставления услуг в рамках своей деятельности;
- Систем хранения данных, применяемых Оператором Платформы, в рамках реализации бизнес- и технологических процессов;
- Прикладного программного обеспечения автоматизированных систем и приложений, применяемых Оператором Платформы;
- Объектов информационной инфраструктуры, задействованных Оператором Платформы, в рамках реализации бизнес- и технологических процессов (включая управление мощностями и производительностью объектов информационной инфраструктуры);
- работников Оператора Платформы;
- планов обеспечения операционной надежности деятельности Оператора Платформы.

4.16. Оператор Платформы обеспечивает регламентацию, реализацию, контроль (мониторинг) требований по обеспечению операционной надежности по следующим направлениям:

- Управление изменениями;
- Управление конфигурациями и уязвимостями;
- Обеспечение операционной надежности на этапах жизненного цикла в отношении планирования обеспечения непрерывности выполнения бизнес- и технологических процессов, организации технического обслуживания, физической защиты и защиты окружения, закупки систем и сервисов, аудита и контроля за обеспечением операционной надежности.
- Предельный уровень (допустимый уровень) рисков Оператора Платформы, а также совокупный предельный размер рисков Оператора Платформы (риск-аппетита) описан в Методике определения контрольных показателей риск-аппетита. Методика устанавливает перечень показателей риск-аппетита, параметры их расчета и ограничений (пороговых значений), порядок их мониторинга и пересмотра, а также меры реагирования на пограничные значения.

5. ЭТАПЫ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ

5.1. Этапы управления рисками:

5.1.1. Выявление рисков – представляет собой сбор сведений о рисках (как внутренних, так и внешних), способных нанести Оператору Платформы ущерб, их факторах, о возможности/вероятности возникновения рисков в деятельности Оператора Платформы и о размере ущерба (ожидаемом, наихудшем, наиболее частом и т.д.).

5.1.2. Анализ и оценка рисков - осуществляются для получения информации о существенности того или иного риска в деятельности Оператора Платформы и последующего принятия решения о реагировании на данный риск.

5.1.3. Мониторинг, контроль и снижение рисков или их исключение, или принятие - система мероприятий, направленных на периодический сбор и анализ информации об изменении уровня риска. Мониторинг осуществляется с целью отслеживания изменений уровня риска, исследования причин данных изменений, а также для своевременного принятия действий, направленных на снижение уровня риска до приемлемого.

5.1.4. Планирование (принятие решения о реагировании на риск, разработка и реализация мер по контролю и минимизации риска). На этапе планирования принимается решение о реагировании на риск:

- принятие риска;
- избегание риска;
- передача риска;
- снижение (минимизация) риска.

В случае принятия решения о снижении риска, планируются мероприятия по внедрению контрольных мер и процедур, направленных на снижение данного риска.

5.1.5. Обмен информацией о рисках между подразделениями и органами управления;

5.1.6. Отчетность - призвана гарантировать полноту, достоверность и своевременность информации об уровне риска (рисков) в отношении всех направлений деятельности и реализуемых продуктов и услуг. Отчетность по рискам должна быть наглядной и содержать необходимую и достаточную информацию для принятия эффективных управленческих решений.

5.2. Основные подходы к управлению рисками:

5.2.1. Управление операционным риском предусматривает использование следующих механизмов выявления (идентификации) операционного риска:

- агрегирование в БДР и БДСОР информации о событиях и факторах операционного риска;
- агрегирование во внешней БДР информации о внешних событиях и факторах операционного риска;
- самооценка операционного риска. Самооценка проводится в формате интервью или анкетирования подразделений на регулярной основе, но не реже 1 раза в год. По результатам самооценки подготавливается отчет, содержащий информацию о выявленных рисках их присущих и остаточных уровнях с учетом оценки адекватности контролей и рекомендации по минимизации рисков;
- диагностика бизнес-процессов, анализ пересечений в полномочиях и ответственности подразделений и работников Оператора Платформы;
- анализ результатов внутреннего и внешнего аудита контролей/процедур/систем;
- анализ новых продуктов, процессов и систем (анализ всех нововведений, проводимых Оператором Платформы: изменения структуры и процедур, внедрение новых услуг и

технологий, в том числе с привлечением аутсорсинга, освоение новых направлений деятельности и т.п.).

5.3. Для анализа и оценки операционного риска используются, в том числе, следующие методы:
- сценарный анализ;
- статистическая и аналитическая обработка информации, содержащейся в БДР и внешней БДР, на базе которой производится оценка влияния рисков Оператора Платформы на ее финансовую устойчивость посредством оценки событий риска, наступление которых, в том числе с учетом вероятности их наступления и степени влияния, повлечет за собой возникновение убытков.

5.4. Для выявления (идентификации), анализа и оценки операционных рисков используется также стресс-тестирование программно-технических средств, используемых для осуществления деятельности Оператора Платформы с периодичностью, определенной внутренними документами Оператора Платформы.

5.5. В рамках идентификации рисков Оператора Платформы проводится также анализ потенциальных угроз, которые по оценке Оператора Платформы могут привести к ее неработоспособности.

5.6. Информация о каждом выявленном риске и результатах ее оценки вносится в реестр рисков (БДР), осуществляется регулярная оценка БДСОР на предмет его актуальности, а в случае выявления неактуальных сведений - пересмотр реестра рисков с периодичностью не реже 1 раза в год.

5.7. К основным методам управления (способам минимизации) операционным риском относятся:
- разработка организационной структуры, внутренних правил и процедур совершения операций, порядка разделения полномочий, утверждения (согласования) и подотчетности по проводимым операциям, позволяющих исключить (минимизировать) возможность возникновения факторов операционного риска;
- разработка контрольных мероприятий по итогам анализа статистических данных, осуществляемого с целью выявления типичных операционных рисков на основе повторяющихся событий операционного риска;
- контроль соблюдения установленных правил и процедур;
- развитие систем автоматизации технологий осуществляемых операций и защиты информации;
- страхование, включая как традиционные виды имущественного и личного страхования (страхование зданий, иного имущества от разрушений, повреждений, утраты в результате стихийных бедствий и других случайных событий, а также в результате действий третьих лиц, работников; страхование работников от несчастных случаев и причинения вреда здоровью), так и страхование специфических рисков профессиональной деятельности как на комплексной основе, так и применительно к отдельным видам рисков;
- разработка системы мер по обеспечению непрерывности финансово-хозяйственной деятельности при совершении операций, включая планы действий на случай непредвиденных обстоятельств (планы по обеспечению непрерывности и (или) восстановления финансово-хозяйственной деятельности).

5.8. Для мониторинга изменения уровня операционного риска используются, в том числе, ключевые индикаторы.

5.9. В случае заключения Оператором Платформы договора на оказание услуг с третьим лицом (далее - поставщик услуг) договоры с поставщиком услуг в связи с оказанием внешних услуг формируются с учетом анализа рисков, связанных с оказанием поставщиком услуг внешних услуг в течение всего периода их оказания.

6. ПРОЦЕССЫ И МЕРОПРИЯТИЯ ПО УПРАВЛЕНИЮ ОПЕРАЦИОННЫМИ РИСКАМИ

6.1. В рамках управления операционным риском Оператор Платформы обеспечивает осуществление следующих мероприятий:

- Принятие мер, направленных на предотвращение случаев дублирования (частичного дублирования) полномочий структурных подразделений;
- Определение перечня требующих защиты от противоправных действий программно-технических средств, сбои и (или) ошибки в функционировании которых способны повлечь за собой приостановление или прекращение оказания услуг в полном или неполном объеме и (или) оказать иное неблагоприятное воздействие на деятельность Оператора Платформы;
- Определение перечня и реализация мер по защите информации, осуществляемых в рамках соответствия требованиям законодательства;
- В целях управления рисками информационной безопасности Оператор Платформы обеспечивает сбор, актуализацию и хранение данных о случаях и попытках осуществления незаконных финансовых операций, в том числе сделок с использованием финансовой платформы без согласия потребителя финансовых услуг;
- Осуществление идентификации угроз, которые по оценке Оператора Платформы могут привести к ее неработоспособности, а также постоянного мониторинга текущего состояния систем, в том числе на предмет необходимости их обновления;
- Оценка рисков непрерывности бизнеса (далее — Оценка рисков) проводится следующим этапом по завершению Анализа воздействия на бизнес. При этом если Анализ воздействия на бизнес позволяет проанализировать влияние сбоев в процессах на бизнес Оператора Платформы, то Оценка рисков показывает, каким угрозам подвержен Оператор Платформы в текущий период и как реализация этих угроз может привести к сбоям в критичных процессах. Процесс Оценки рисков включает в себя:
    - Определение областей, в рамках которых организация может быть подвержена рискам непрерывности бизнеса;
    - Выделение угроз, реализация которых может привести к нарушению хода критичных процессов, определенных на этапе Анализа воздействия на бизнес; анализ степени влияния угроз на Оператора Платформы в случае их реализации, в т.ч. на работников, инфраструктуру, информационные активы Оператора Платформы, оценку вероятности реализации угрозы и (или) анализ существующих контрольных процедур;
    - В процессе Оценки рисков оценивается вероятность реализации угрозы, степень возможного влияния на Платформу, существующие организационно-технические мероприятия и контрольные процедуры, направленные на снижение рисков;
    - Оценка рисков проводится на регулярной основе, не реже одного раза в год, а также в случае существенных изменений внутренних и внешних факторов.
- Осуществление контроля прав доступа работников к программно-техническим средствам;
- Определение перечня и реализация мер, направленных на обеспечение предоставления Оператору Платформы Участниками, а также иными контрагентами информации о событиях операционного риска;
- Осуществление мониторинга использования Участниками технических средств Оператора Платформы;

- Определение перечня требований к программно-техническим средствам, используемым участниками при подключении к Платформе;
- Устранение недостатков в работе Платформы, выявленных в результате проведения испытательных работ (тестирования);
- Ведение базы данных о событиях операционного риска по следующим видам событий операционного риска с учетом критериев существенности последствий:
    - события, влекущие за собой приостановление или прекращение работоспособности Платформы (далее - критически важные процессы), в том числе чрезвычайные ситуации (далее - существенные события операционного риска или события высокого уровня влияния);
    - события операционного риска, не относящиеся к существенным событиям операционного риска, но оказывающие негативное влияние на порядок и условия осуществления критически важных процессов Оператора Платформы, в том числе на возможность подключения участников к Платформе и исполнения поручений Участников (далее - значимые события операционного риска или события среднего уровня влияния);
    - события операционного риска, не относящиеся к существенным событиям операционного риска и значимым событиям операционного риска (события низкого уровня влияния).
- Ведение базы данных о расходах (убытках), понесенных Оператором Платформы вследствие реализации событий операционного риска, содержащей следующую информацию в отношении каждого события операционного риска:
    - размер расходов (убытков), понесенных вследствие реализации события операционного риска;
    - дата реализации события операционного риска, повлекшего за собой возникновение расходов (убытков);
    - обстоятельства возникновения (выявления) события операционного риска, приведшего к расходам (убыткам).
- Обучение работников по вопросам выявления, оценки и снижения операционного риска;
- Осуществление мероприятий по замене или улучшению (обновлению) программно-технических средств

6.2. Оператор Платформы в рамках управления операционным риском разрабатывает систему мер, направленных на обеспечение условий для бесперебойного функционирования, а также для восстановления осуществляемой деятельности в случае реализации событий операционного риска, включающую в себя следующие мероприятия:

- Определение перечня критически важных процессов Оператора Платформы, приостановление или прекращение которых влечет за собой нарушение порядка осуществления Оператором Платформы своей деятельности;
- Выявление чрезвычайных ситуаций и проведение анализа обстоятельств возникновения чрезвычайных ситуаций;
- Обеспечение контроля за бесперебойным функционированием средств Платформы, в том числе посредством обеспечения контроля за недопущением превышения объема поступающих заявок участников частоты их поступления, в результате которого произойдет приостановление или прекращение оказания услуг Оператора Платформы в полном или неполном объеме;
- Определение перечня потенциальных чрезвычайных ситуаций исходя из оценки Оператором Платформы возможных расходов (убытков), а также иных его контрагентов

вследствие нарушения непрерывности осуществления деятельности, вероятности и времени возможного возникновения такого нарушения, а также характера и объема совершаемых операций;

- Проведение идентификации угроз, которые могут привести к неработоспособности Платформы;
- Распределение ответственности и полномочий между структурными подразделениями и их работниками в случае возникновения существенных событий операционного риска;
- Разработка и утверждение мероприятий в рамках Программы непрерывности деятельности;
- Создание резервных копий информации, содержащейся в реестрах, ведение которых Оператор Платформы осуществляет в соответствии с требованием законодательства, и хранение указанных копий в течение пяти лет со дня их создания;
- Проверка наличия и техническое обслуживание независимых генераторов электричества, предоставляющих мощность, обеспечивающую осуществление критически важных процессов Оператора Платформы в течение всего периода восстановления функционирования программно-технических средств основного комплекса технических средств Платформы.

7. ОТЧЕТНОСТЬ ПО РИСКАМ

7.1. Для обеспечения конфиденциальности информации о рисках, в том числе конфиденциальности отчётов о рисках устанавливается следующий порядок предоставления информации и отчетности по вопросам управления рисками работникам и органам управления:

- В ходе работ по идентификации, оценке, мониторингу, контролю рисков ГСИБ информирует работников о выявленных рисках, отнесённых к деятельности подразделений, работниками которых они являются, в объёме необходимом для эффективного участия работников в оценке риска и формировании планов мероприятий по их снижению и/или контролю.

Если иное не определено во внутренних документах:

- сроки информирования работников и предоставление отчётности структурным подразделениям и органам управления о рисках определяются ГСИБ на основе его профессионального суждения, формируемого с учётом оценки риска, потребностей Оператора Платформы, величины того или иного риска и принципа существенности;
- Общему собранию акционеров ГСИБ предоставляется полная и своевременная информация, в том числе отчётность по рискам в соответствии со сроками и порядком, определённым в данном разделе Правил.

7.2. Отчетность подразделяется на регулярную и внеочередную (оперативную).

- Регулярная отчётность по рискам предоставляется ГСИБ Общему собранию акционеров и Директору не реже 1 (одного) раза в квартал и в срок не позднее 30 (тридцати) дней с даты окончания очередного квартала;
- Регулярная отчетность по рискам состоит из утверждённых внутренними документами отчетных форм, а также аналитической части, в которой интерпретируются полученные результаты и даются рекомендации в отношении мероприятий по управлению рисками.

7.3. Предоставление отчетности другим пользователям осуществляется по решению органов управления, за исключением случаев, когда такое предоставление отчетности осуществляется

на основании федеральных законов и принятых в соответствии с ними нормативно-правовых актов федерального органа исполнительной власти в области финансовых рынков.

7.4. Регулярная отчетность включает в себя:
- оценку рисков по основным направлениям деятельности Оператора Платформы, ее обоснование, включая сведения о нарушениях Оператором Платформы требований нормативных правовых актов Банка России, Устава и внутренних документов;
- меры, принятые для устранения выявленных нарушений и снижения рисков;
- сведения о выполнении рекомендаций;
- иные сведения, предусмотренные внутренними документами.

7.5. Внеочередная (оперативная) отчетность формируется в случае выявления событий риска с высокими убытками, существенного изменения уровня риска, проведения дополнительных специальных программ оценки риска.

7.6. Информирование Общего собрания акционеров и Директора о выявленном событии риска с высокими убытками осуществляет ГСИБ в день обнаружения события.

7.7. Подробный отчет ГСИБ о выявленном событии риска с высокими убытками, существенном изменении уровня риска, проведении дополнительных специальных программ оценки риска предоставляется Общему собранию акционеров и Директору не позднее десяти дней с даты выявления соответствующего нарушения.

8. ОЦЕНКА ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ РИСКАМИ

8.1. В рамках процесса управления рисками не реже одного раза в год проводится оценка эффективности управления рисками посредством анализа результативности своей деятельности по выявлению нарушений ограничений рисков, их устранению и (или) осуществлению иных мероприятий в рамках снижения рисков или их исключения. Проведение оценки эффективности предусматривает формирование экспертного заключения ДОВКиК, в том числе, о соотношении достигнутых результатов и затраченных на внедрение инструментов управления рисками и реализацию мер по их снижению ресурсов, оценка которых даётся в качественных и количественных показателях. Оценка эффективности включается в регулярную отчетность по рискам за квартал, в котором была проведена соответствующая оценка эффективности.

8.2. Периодически в рамках оценки эффективности СУР могут проводиться внешние аудиты с привлечением независимых аудиторов и консультантов, регулирующих органов.

9. РАСКРЫТИЕ ИНФОРМАЦИИ О СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ

9.1. Оператор Платформы доводит до сведения акционеров, Участников, а также регулирующих органов, внешних аудиторов и других заинтересованных лиц информацию о действующей системе управления рисками Оператора Платформы.

9.2. Раскрытие информации осуществляется в следующих объемах:
- для акционеров, кредиторов, Участников - о текущем состоянии системы управления рисками:
  - краткая характеристика действующей системы управления рисками;
  - иная информация, доводимая до сведения акционеров, Участников в соответствии с требованиями регулирующих органов или внутренними документами.
- для регулирующих органов, с периодичностью и в объеме, установленном соответствующими нормативными документами;

- для внешних аудиторов, регулирующих органов в ходе проведения проверок, на основании распоряжения органов управления:
    - нормативные документы по управлению рисками;
    - аналитические отчеты по уровню отдельных видов риска;
    - по отдельному запросу - методики оценки рисков, параметры моделей.

9.3. Механизмами раскрытия информации являются:

- размещение информации на сайте в сети Интернет;
- предоставление отчетности, обозначенной во внутренних документах по управлению рисками.