АКЦИОНЕРНОЕ ОБЩЕСТВО «ФИНФОРТ МП»
(АО «ФИНФОРТ МП»)

КОММЕРЧЕСКАЯ ТАЙНА
АО «ФИНФОРТ МП»

УТВЕРЖДЕНЫ
Приказом № МП3/24ОД от «15» января 2024 года
Генерального директора АО «Финфорт МП»

Правила управления рисками, связанными с осуществлением деятельности оператора финансовой платформы АО «Финфорт МП»

(версия – 2.0)

Москва
2024

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила управления рисками, связанными с осуществлением деятельности оператора финансовой платформы (далее – Правила), являются основополагающим документом, определяющим цели, задачи и основные принципы организации системы управления рисками АО «Финфорт МП» как оператора финансовой платформы (далее – Оператор Платформы), связанными с деятельностью финансовой платформы, и формируют основу для построения эффективно работающей системы управления рисками, сопровождающей деятельность Оператора Платформы.

1.2. Правила содержат описание значимых рисков, описывают подходы к управлению ими.

1.3. Правила разработаны на основании требований Федерального закона от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» (далее – Федеральный закон).

1.4. Настоящие Правила разработаны в целях повышения качества управления рисками Оператора Платформы.

1.5. Правила являются частью системы внутреннего контроля Оператора Платформы.

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

1.7. Правила содержат общие положения, определяющие цели управления рисками, а также:

- основные методологические принципы и подходы к идентификации, оценке и мониторингу рисков;
- классификацию рисков, присущих деятельности Оператора 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 и периодичность проведения идентификации угроз, которые могут привести к нарушению деятельности Оператора Платформы;
- порядок и сроки информирования органов управления, должностных лиц и структурных подразделений 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 реализации процессов и мероприятий в рамках организации системы управления рисками, представляемых на рассмотрение органам управления Оператора Платформы;
- 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 распределения ответственности и полномочий между структурными подразделениями в случае реализации существенных событий риска, связанных с деятельностью Оператора Платформы;

–порядок обеспечения контроля за выполнением процессов и мероприятий по управлению рисками;

–порядок и сроки проведения проверок эффективности управления рисками.

1.8. 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.

1.9. Оператор Платформы осуществляет постоянное развитие и совершенствование системы управления рисками для снижения уязвимости бизнес-процессов и времени их восстановления, повышения уровня резервирования технологий на основе принципа разнесения и дублирования ресурсов.

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

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

–**База событий операционного риска (БСОР)** – электронное хранилище информации о событиях операционного риска компаний Оператора Платформы.

–**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.

–**Контрольные процедуры** – совокупность мер, направленных на снижение вероятности/возможности возникновения, уменьшение потенциального ущерба от реализации риска и устранение последствий события возникновения риска.

–**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-риск, включая регуляторный риск, риск потери деловой репутации, стратегический риск.

–**Нештатная ситуация (НС)** - 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 субъектами Платформы;

- привели или могут привести к нарушению порядка и сроков проведения операций, порядка доступа Участника или группы Участников к Платформе, а также раскрытия и предоставления информации, установленных внутренними документами Оператора Платформы.

–**Оператор финансовой платформы (Оператор Платформы)** – юридическое лицо, созданное в организационно-правовой форме акционерного общества в соответствии с законодательством Российской Федерации, оказывающее услуги, связанные с обеспечением возможности совершения финансовых сделок между финансовыми организациями или эмитентами и потребителями финансовых услуг с использованием финансовой платформы, и включенное Банком России в реестр операторов финансовых платформ. Оператор Платформы не является стороной финансовых сделок, совершаемых с использованием финансовой платформы. Оператором Платформы является Акционерное общество «Финфорт МП» (ОГРН: 1217700630751, место нахождения: Российская Федерация, 119285, город Москва, вн.тер.г. Муниципальный округ Раменки, км мжд Киевское 5-Й, д.1, стр.1. Возможности финансовой платформы могут быть реализованы посредством сайта Оператора Платформы и/или посредством мобильного приложения Оператора

–**Операционный риск** – риск возникновения последствий, влекущих за собой приостановление или прекращение оказания услуг в полном или неполном объеме, а также риск 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** – метод управления риском, при котором деятельность продолжает осуществляться, при этом в нее вносятся изменения, в результате которых риск полностью или частично передается 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) мобильного приложения, являющиеся физическими лицами.

–**ПО** – программное обеспечение.

–**Принятие риска** – метод управления риском, при котором 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.

–**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 международные санкции, что не позволит продолжить исполнение договора без ограничений.

–Регуляторный (комплаенс) 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.

–СВК – Служба внутреннего контроля.

–СУР – Служба управления рисками.

–СОР – событие операционного риска.

–Система управления рисками – 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.

–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 финансовых услуг, присоединившиеся к договору об оказании услуг Оператора Платформы в целях совершения финансовых сделок с финансовыми организациями и эмитентами.

–Финансовая платформа Оператора платформы (Платформа) – информационная система, которая обеспечивает взаимодействие финансовых организаций или эмитентов с участниками финансовой платформы посредством информационно-телекоммуникационной сети «Интернет» в целях обеспечения возможности совершения финансовых сделок и доступ к которой предоставляется Оператором Платформы.

–Финансовые организации – для целей Правил под финансовыми организациями понимаются организации, присоединившиеся к договору об оказании услуг оператора финансовой платформы, условия которого установлены Правилами платформы.

Термины, специально не определенные в Правилах, используются в значениях, определенных во внутренних документах Оператора платформы, а также законами и иными нормативными актами Российской Федерации.

3. ОПИСАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ

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

3.1. **Принципы управления рисками**

3.1.1. Система управления рисками строится в соответствии со следующими принципами:

1. Принцип комплексности предполагает выявление источников и объектов риска на основе всестороннего анализа всех существующих и планируемых к вводу бизнес-процессов, информационных систем и продуктов.
2. Принцип непрерывности предполагает проведение на регулярной основе необходимого набора упорядоченных, целенаправленных процедур, таких как оценка текущих рисков, анализ технологии и регламентов функционирования системы управления рисками, предоставление отчетности органам управления.
3. Принцип открытости выражается в предоставлении всей необходимой информации об организации системы управления рисками всем заинтересованным сторонам.
4. Принцип существенности означает, что при внедрении различных элементов системы управления рисками 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.
5. Принцип независимости оценок означает, что оценка и управление рисками осуществляется подразделениями, независимыми от подразделений, генерирующих прибыль/финансовый результат.
6. Принцип консерватизма предполагает, что выбор метода оценки и управления рисками базируется на разумном сочетании надежности системы управления рисками и рентабельности деятельности.

3.2. **Цели и задачи управления рисками**

3.2.1. Целью функционирования системы управления рискам 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.

3.2.2. 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;
– эффективное распределение полномочий и ответственности между органами управления, исполнительными органами, структурными подразделениями и работниками по вопросам управления рисками.

3.3. **Полномочия и функции в области организации системы управления рисками и управления рисками**

3.3.1. Для управления рисками Оператора Платформы сформировано отдельное структурное подразделение, ответственное за организацию системы управления рисками – СУР, руководство которым осуществляет Руководитель СУР. Управление отдельными видами рисков в рамках организации системы управления рисками может осуществляться отдельными структурными подразделениями.

3.3.2. Руководитель СУР и руководители отдельных структурных подразделений, указанные в п. 3.3.1 настоящих Правил не осуществляют функции, которые не связаны с управлением рисками и при исполнении своих обязанностей не зависят от других должностных лиц и структурных подразделений.

3.3.3. Руководитель СУР, работники структурных подразделений, указанные в п. 3.3.1 настоящих Правил, вправе требовать у работников и должностных лиц предоставления информации (документов), в том числе письменных объяснений, по вопросам, возникающим в ходе выполнения им (ими) своих обязанностей.

3.3.4. Органы управления, иные структурные подразделения и должностные лица также могут быть вовлечены в процессы управления рисками.

3.3.5. В компетенцию Руководителя СУР 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 их 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 единоличному исполнительному органу (Генеральному директору) Оператора Платформы;
– принятие иных мер, направленных на организацию системы управления рисками, предусмотренных внутренними документами.

3.3.6. Управление отдельными видами рисков в рамках организации системы управления рисками Оператора Платформы осуществляется:
– СУР – в части операционного (кроме риска информационной безопасности, риска информационных систем, риска операционной надежности, правового риска), стратегического риска, риска потери деловой репутации, санкционного риска;
– Юридический отдел – в части правового риска;
– СВК – в части регуляторного (комплаенс) риска в соответствии с утвержденными документами;
– Руководитель /подразделение по информационной безопасности – в части риска информационной безопасности, риска операционной надежности;
– Отдел системного обеспечения - в части риска информационных систем.
– В целях организации управления рисками в компетенцию Генерального директора входит, в том числе:
– распределение полномочий и ответственности по управлению рисками между руководителями подразделений в целях соблюдения основных принципов по управлению рисками;
– создание и поддержание эффективной системы управления рисками;
– обеспечение организации процесса управления рисками, включая, при необходимости, образование рабочих органов, в том числе комитетов, комиссий, определение их компетенции, утверждение положений о них.

3.3.7. Процесс управления рисками выстраивается таким образом, что каждый работник Оператора Платформы информирует руководителя подразделения и/или Руководителя СУР об идентифицированных рисках, а также о событиях риска, и участвует в реализации мероприятий по контролю и минимизации риска в зоне своей ответственности.

3.3.8. Полномочия подразделений в области управления рисками определяются внутренними документами.

4. ОСНОВНЫЕ РИСКИ, СВЯЗАННЫЕ С ОСУЩЕСТВЛЕНИЕМ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРА ФИНАНСОВОЙ ПЛАТФОРМЫ

4.1. **Основные понятия**

4.1.1. 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 «Финфорт МП»

4.1.2. 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 регуляторные (комплаенс) риски.

4.1.3. Реализация рисков может приводить к сбоям в работе Платформы, задержкам расчетов, 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.

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

– нефинансовые риски:

- регуляторный (комплаенс) риск;
- риск потери деловой репутации;
- стратегический риск;
- санкционный риск;
- операционный риск.

4.1.5. Основными факторами возникновения операционных рисков в деятельности Оператора Платформы являются:

– не оптимально выстроенные, недостаточные и/или неэффективные контрольные процедуры в системах и процессах;

– неадекватные действия работников (в том числе ошибки, внутреннее мошенничество);

– совершение операций с использованием Оператора Платформы без согласия участников;

– 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 программно-аппаратных средств, 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.

4.1.6. Управление операционным риском представляет собой цикличный процесс, который включает в себя следующие этапы:

– 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 между исполнительным органом, СУР, структурными подразделениями и работниками по вопросам управления рискам.

4.1.7. 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:
– неоказание услуги должным образом/непоставку оборудования;
– непредоставление документов, подтверждающих факт выполнения договора;
– нарушение иных условий договора поставщиком, включая нарушение соглашения о конфиденциальности, предоставление недостоверных сведений.

4.1.8. В целях управления рисками, связанными с оказанием поставщиками услуг и поставке 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.

4.1.9. В рамках управления операционным риском Оператор Платформы выделяет управление рисками информационной безопасности (ИБ), мероприятия по управлению которыми описаны, в том числе в Правилах.

4.2. **Риск потери деловой репутации (РПДР)**

4.2.1. 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.

4.2.2. Оператор Платформы в рамках управления РПДР 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.

4.2.3. 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 событий операционных рисков.

4.3. **Стратегический риск**

4.3.1. 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.

4.3.2. Оператор Платформы в рамках управления стратегическим риском обеспечивает проведение оценки СУР 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. **Регуляторный (комплаенс) риск**

4.4.1. Возникновение регуляторного (комплаенс) риска может быть обусловлено следующими причинами:

- несоблюдение Оператором Платформы законодательства и нормативных актов Банка России;
- несоответствие внутренних документов Оператора Платформы законодательству и нормативным актам Российской Федерации, несвоевременная актуализация внутренних документов или их несовершенство;
- несоблюдение работниками Оператора Платформы установленных внутренних порядков и процедур;
- неэффективная организация внутреннего контроля, приводящая к нарушению Правил, норм и стандартов вследствие действий работников и органов управления Оператора Платформы;
- несовершенство организационной структуры Оператора Платформы в части распределения полномочий подразделений и работников;
- возникновение конфликта интересов;
- недостаточная проработка Оператором Платформы вопросов при разработке и внедрении продуктов, бизнес-процессов, условий осуществления финансовых сделок на предмет наличия потенциального регуляторных рисков при их дальнейшей реализации.

4.4.2. Оператор Платформы рассматривает следующий минимальный перечень базовых регуляторных рисков, подлежащих управлению:

- риск использования в целях легализации (отмывания) доходов (ОД), полученных преступным путем и финансирования терроризма (ФТ);

–несоблюдение работниками норм профессиональной этики и/или совершение действий, которые могут привести к потере деловой репутации.

4.4.3. Процесс управления регуляторным (комплаенс) риском включает в себя:

– выявление, (идентификация) регуляторного (комплаенс) риска и учет событий, связанных с регуляторным (комплаенс) риском;

–оценка регуляторного (комплаенс) риска;

–мониторинг регуляторного (комплаенс) риска;

–определение стратегии реагирования на риск, разработку перечня мер по снижению риска и контроль за выполнением мероприятий по минимизации риска.

4.4.4. Меры по минимизации регуляторного (комплаенс) риска Оператора Платформы могут включать в себя следующие:

–разработку внутренних нормативных документов, регламентирующих процессы и процедуры, связанные с управлением регуляторным риском;

–автоматизацию контролей;

–обучение персонала.

4.5. **Санкционный риск**

4.5.1. Оператор Платформы рассматривает три основных источника санкционных рисков Оператора Платформы, подлежащих управлению:

–финансовые организации – участники платформы;

–физические лица – пользователи платформы;

–контрагенты Оператора платформы, в том числе осуществляющие поставку информационно-технологического оборудования и ПО, необходимых для функционирования Платформы.

4.5.2. Несоблюдение установленных требований в области санкций может привести к:

–распространению режима экономических ограничений на Оператора Платформы и (либо) его 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 Платформы со стороны независимых и регулирующих органов других стран;

–требованию провести проверку деятельности организации и устранить выявленные нарушения;

–репутационному ущербу.

4.5.3. Управление санкционным риском осуществляется в соответствии с настоящим документом, а также иными внутренними документами Оператора Платформы, устанавливающими принципы управления санкционным риском, и включает в себя мероприятия в рамках управления операционным риском, связанным с оказанием поставщиками 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.

4.6. **Нештатные и чрезвычайные ситуации**

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

4.6.2. Для целей настоящих Правил чрезвычайная и нештатная ситуации определены следующим образом:

1. 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.

   По решению уполномоченного органа, осуществляющего координацию действий по урегулированию сложившейся ситуации, ЧС может быть признана Нештатной ситуацией.
2. 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 субъектами Платформы;
- привели или могут привести к нарушению порядка и сроков проведения операций, порядка доступа Участника или группы Участников к Платформе, а также раскрытия и предоставления информации, установленных внутренними документами Оператора Платформы.

4.6.3. Для управления ЧС и НС определяются порядок обнаружения ЧС и НС, порядок принятия решения во время ЧС или НС, порядок по коммуникациям, порядок восстановления и урегулирования последствий ЧС и НС.

4.6.4. Управление рисками непрерывности деятельности Оператора Платформы осуществляется в рамках внутренних документов Оператора Платформы, регламентирующих управление непрерывностью, в которых определяется порядок действий в случае ЧС и НС.

4.6.5. 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.

4.6.6. Оператор Платформы обеспечивает и постоянно поддерживает конфиденциальность, целостность и доступность своих защищаемых информационных активов путем реализации комплекса мероприятий по информационной безопасности, включая регулярную инвентаризацию и классификацию информационных активов, формирование и совершенствование системы управления информационной безопасностью, 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.

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

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

4.6.9. В рамках реализации процессов обеспечения операционной надежности Оператор Платформы обеспечивает учет и мониторинг элементов критичной инфраструктуры, а именно:

- технологических процессов, реализуемых непосредственно Оператором Платформы;
- технологических процессов, реализуемых внешними контрагентами, оказывающими услуги в сфере информационных технологий (далее – поставщики услуг);

– структурных подразделений Оператора Платформы, ответственных за разработку технологических процессов, поддержание их выполнения, реализацию технологических процессов;
– технологических участков (этапов) технологических процессов;
– программно-аппаратных средств Оператора Платформы, задействованных при выполнении каждого технологического процесса;
– работников Оператора Платформы или иных лиц, осуществляющих физический и/или логический доступ, или программных сервисов, осуществляющих логический доступ к программно-аппаратным средствам (далее – субъекты доступа), задействованных при выполнении каждого технологического процесса;
– взаимосвязей и взаимозависимостей между Оператором Платформы, Участниками, регистратором финансовых транзакций, а также поставщиками услуг в рамках выполнения технологических процессов, в том числе взаимосвязей и взаимозависимостей между их программно-аппаратными средствами;
– программно-аппаратных средств поставщиков услуг, задействованных при выполнении технологических процессов;
– каналов передачи информации, обрабатываемой и передаваемой в рамках технологических процессов участниками технологического процесса при взаимодействии с работниками Оператора Платформы.

4.6.10. Оператор Платформы обеспечивает регламентацию, реализацию, контроль (мониторинг) требований по обеспечению операционной надежности по следующим направлениям:
– контроль соблюдения целевых показателей операционной надежности;
– идентификация элементов критичной инфраструктуры;
– управление изменениями критичной архитектуры;
– выявление, регистрация, реагирование на инциденты операционной надежности и восстановление выполнения технологических процессов и функционирования программно-аппаратных средств после реализации таких инцидентов;
– организация надежного взаимодействия с поставщиками услуг;
– тестирование операционной надежности технологических процессов;
– управление риском несанкционированного доступа работников Оператора Платформы или работников поставщиков услуг, обладающих полномочиями доступа к программно-аппаратным средствам;
– обеспечение осведомленности об актуальных информационных угрозах;
– управление риском возникновения зависимости обеспечения операционной надежности от субъектов доступа, обладающих уникальными знаниями, опытом и компетенцией, а также защиту критичной архитектуры от возможной реализации информационных угроз при организации дистанционной работы работников.

4.6.11. В целях реализации требований к операционной надежности Оператор Платформы:
– моделирует информационные угрозы в отношении критичной архитектуры;
– планирует применение организационных и технических мер, направленных на реализацию требований к операционной надежности, на основе результатов

оценки риска реализации информационных угроз в рамках системы управления рисками;

– обеспечивает реализацию требований к операционной надежности на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации программно-аппаратных средств;

– обеспечивает контроль соблюдения требований к операционной надежности в отношении элементов критичной архитектуры.

4.6.12. Оператор Платформы информирует Банк России:

– о выявленных инцидентах операционной надежности, включенных в перечень типов инцидентов операционной надежности, размещаемый Банком России на официальном сайте Банка России в сети «Интернет», а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный Оператором Платформы или Банком России инцидент операционной надежности;

– о планируемых мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети «Интернет», в отношении инцидентов операционной надежности не позднее одного рабочего дня до дня проведения мероприятия.

4.6.13. Оператор Платформы устанавливает и пересматривает не реже одного раза в год целевые показатели операционной надежности с использованием результатов оценки рисков, а также с учетом развития новых технологий и совершенствования технологических процессов.

4.6.14. Порядок выполнения Оператором Платформы требований законодательства Российской Федерации к операционной надежности приведен в Положении об операционной надежности, в том числе:

– определение и описание состава процедур, направленных на выполнение требований к операционной надежности;

– определение организационной структуры Оператора Платформы, задействованной в выполнении требований к операционной надежности, в том числе обеспечивающее установление функций структурных подразделений, ответственных за разработку технологических процессов, поддержание их выполнения, реализацию технологических процессов (в том числе в части принятия решений с учетом исключения конфликта интересов), и контроль за выполнением требований к операционной надежности в рамках порядка организации и осуществления Оператором Платформы внутреннего контроля;

– выделение ресурсного обеспечения для выполнения требований к операционной надежности;

– порядок утверждения и условия пересмотра процедур, направленных на выполнение требований к операционной надежности.

4.6.15. Перечень контрольных показателей, устанавливающих предельный (допустимый) уровень рисков Оператора Платформы, параметры их расчета и ограничений (например, пороговые значения), порядок их мониторинга и пересмотра, а также меры реагирования на пограничные значения в соответствующих внутренних и/или организационно-распорядительных документах Оператора Платформы.

5. ЭТАПЫ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ

5.1. Управление рисками представляет собой цикличный процесс, который включает в себя следующие этапы:

- выявление рисков;
- анализ и оценка рисков;
- мониторинг, контроль и снижение рисков или их исключение или принятие;
- планирование (принятие решения о реагировании на риск, разработка и реализация мер по контролю и минимизации риска).
- обмен информацией о рисках между подразделениями и органами управления;
- отчетность.

5.2. Выявление риска 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.).

5.3. Существенную важность представляет выявление рисков в новых продуктах/процессах/системах Оператора Платформы.

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

5.5. На этапе планирования принимается решение о реагировании на риск. В ходе этого этапа может быть принято одно из следующих решений:

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

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

5.7. Мониторинг – 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.

5.8. Система отчетности по рискам 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.

5.9. Основные подходы к управлению рисками:

5.9.1. Управление нефинансовыми рисками (за исключением регуляторного риска) осуществляется аналогично управлению операционным риском, описание которого приведено в настоящих Правилах и в Положении по управлению операционным риском.

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

– агрегирование в БСОР информации о событиях и факторах операционного риска;
– самооценка операционного риска. Самооценка проводится в формате интервью или анкетирования ответственных 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.).

5.10. Для анализа и оценки операционного риска используются, в том числе, следующие методы:
– сценарный анализ;
– статистическая и аналитическая обработка информации, содержащейся в БСОР, 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.

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

5.12. К основным методам управления (способам минимизации) операционным риском относятся:
– разработка организационной структуры, внутренних правил и процедур совершения операций, порядка разделения полномочий, утверждения (согласования) и под ности 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);
– мониторинг изменения уровня операционного риска, для чего используются, в том числе, контрольные показатели.

5.13. 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 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:

6.1.1. Принятие мер, направленных на предотвращение случаев дублирования (частичного дублирования) полномочий структурных подразделений.

6.1.2. 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.

6.1.3. Определение перечня мер, направленных на исполнение требований законодательства Российской Федерации по защите информации, и их реализация.

6.1.4. В целях управления рисками информационной безопасности Оператор Платформы осуществляет выявление операций по финансовым сделкам без волеизъявления Участников, в том числе:
– применяет полученную от Банка России информацию о случаях и попытках осуществления операций по финансовым сделкам без волеизъявления Участников;
– осуществляет мероприятия по выявлению атак на объекты информационной инфраструктуры Оператора Платформы и/или Участников, которые могут привести к случаям и/или попыткам осуществления операций по финансовым сделкам без волеизъявления Участников;
– осуществляет сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Оператора Платформы, Участников, а также сбор сведений об обращении Участников в правоохранительные органы;
– предоставляет условия для направления Участникам уведомления о совершении финансовых сделок без их волеизъявления;
– применение Оператором Платформы мер защиты информации, а также ограничений по параметрам операций по финансовым сделкам, устанавливаемых на основании заявления Участников.

6.1.5. 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.

6.1.6. 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.

6.1.7. Осуществление контроля прав доступа работников к программно-техническим средствам.

6.1.8. Определение перечня мер, направленных на обеспечение предоставления Оператору Платформы Участниками и иными контрагентами информации о событиях операционного риска, и их реализация.

6.1.9. Определение перечня требований к программно-техническим средствам, используемым участниками при подключении к Платформе.

6.1.10. Устранение недостатков в работе Платформы, выявленных в результате проведения испытательных работ (тестирования).

6.1.11. Ведение БСОР, содержащей следующую информацию в отношении каждого события операционного риска:

- причины СОР (обстоятельства возникновения (выявления) СОР, приведшее к расходам (убыткам);
- вид риска;
- степень влияния;
- оценка значимости;
- меры, направленные на устранение риск-события;
- размер расходов (убытков), понесенных вследствие реализации события операционного риска;
- мероприятия по устранению, минимизации и передаче риска;
- срок исполнения мероприятия;
- фамилия, имя, отчество работника, ответственного за исполнение мероприятия;
- тип нарушения;
- сведения об источнике информации о нарушении;
- перечень нарушенных норм;
- дата нарушения;
- вид деятельности;
- описание нарушения.

6.1.11.1. События операционного риска классифицируются с учетом степени их влияния на деятельность Оператора Платформы:

- «Существенные» – для СОР, приведших к прерыванию совершения одной или нескольких значимых финансовых сделок с потребителями финансовых услуг и финансовыми организациями;
- «Значимые» – для СОР, не приведших к прерыванию оказания значимых услуг, но негативно повлиявших на деятельность свыше 15 процентов потребителей финансовых услуг, эмитентов и финансовых организаций, совершающих

финансовые сделки с потребителями финансовых услуг пользователей информационной системы Оператора Платформы от общего числа потребителей финансовых услуг, эмитентов и финансовых организаций, присоединившихся к договору об оказании услуг оператора финансовой платформы;

– «Несущественные» – для СОР, не относящимся к «существенным» или «значимым» событиям операционного риска (события низкого уровня влияния».

6.1.12. Обучение работников по вопросам выявления, оценки и снижения операционного риска.

6.1.13. 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:

6.2.1. Определение перечня критически важных процессов Оператора Платформы, приостановление или прекращение которых влечет за собой нарушение порядка осуществления Оператором Платформы своей деятельности. Данный процесс регламентируется внутренними документами по операционным рискам и непрерывности бизнеса.

6.2.2. Выявление чрезвычайных ситуаций и проведение анализа обстоятельств возникновения чрезвычайных ситуаций. Данный процесс регламентируется внутренними документами по операционным рискам и непрерывности бизнеса.

6.2.3. 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.

6.2.4. 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.

6.2.5. Проведение идентификации угроз, которые могут привести к неработоспособности Платформы.

6.2.6. Распределение ответственности и полномочий между структурными подразделениями и их работниками в случае возникновения существенных событий операционного риска.

6.2.7. Разработка и утверждение мероприятий в рамках Плана обеспечения непрерывности деятельности.

6.2.8. Организация функционирования резервного комплекса средств, функционально дублирующего основной комплекс технических средств.

6.2.9. Контроль работоспособности и техническое обслуживание основного и резервного комплексов технических средств, поддержание их состояния на уровне, обеспечивающем возможность функционирования всех критически важных процессов Оператора Платформы в случае возникновения чрезвычайной ситуации.

7. ОТЧЕТНОСТЬ ПО РИСКАМ

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

7.1.1. В ходе работ по идентификации, оценке, мониторингу, контролю рисков СУР информирует работников о выявленных рисках, отнесенных к деятельности подразделений, работниками которых они являются, в объеме 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 отчетности структурным подразделениям и органам управления о рисках определяются Руководителем СУР (в части нерегулярной отчетности), на основе его профессионального суждения, формируемого с учетом оценки риска, потребностей Оператора Платформы, величины того или иного риска и принципа существенности;
- сроки и форма предоставления информации работниками, определяется в соответствующих запросах СУР.

7.1.2. Органам управления Руководителем СУР предоставляется полная и своевременная информация, в том числе отчетность по рискам в соответствии со сроками и порядком, определенным в данном разделе Правил, а также в иных внутренних нормативных документах Оператора Платформы.

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

7.2.1. Регулярная отчетность по рискам предоставляется Генеральному директору.

7.2.2. Регулярная отчетность по рискам состоит из утвержденных внутренними документами отчетных форм, а также аналитической части, в которой интерпретируются полученные результаты и даются рекомендации в отношении мероприятий по управлению рисками.

7.2.3. 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.

7.2.4. 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.

7.2.5. Внеочередная (оперативная) отчетность формируется в случае выявления событий риска с высокими убытками, существенного изменения уровня риска.

8. ОЦЕНКА ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ РИСКАМИ

8.1. В рамках процесса управления рисками не реже одного раза в год проводится самооценка 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, в том числе, о соотношении достигнутых результатов и затраченных на внедрение инструментов управления рисками и реализацию мер по их снижению ресурсов, оценка которых дается в качественных и количественных показателях. Оценка эффективности включается в регулярную отчетность по рискам за квартал, в котором была проведена соответствующая оценка эффективности.

8.2. Оценка эффективности системы управления рисками может проводиться внешними аудиторами с привлечением независимых аудиторов и консультантов.

9. РАСКРЫТИЕ ИНФОРМАЦИИ О СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ

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

9.2. Предоставление информации осуществляется в следующих объемах:

–для акционеров:

- текущее состояние системы управления рисками:
- краткая характеристика действующей системы управления рисками;
- иная информация, доводимая до сведения акционеров, в соответствии с требованиями регулирующих органов и (или) внутренних документов Оператора Платформы;

–для регулирующих органов:

- с периодичностью и в объеме, установленном соответствующими нормативными документами;

–для внешних аудиторов, регулирующих органов в ходе проведения проверок:

- нормативные документы по управлению рисками;
- аналитические отчеты по уровню отдельных видов риска;
- по отдельному запросу – методики оценки рисков.