УТВЕРЖДЕНЫ

решением Наблюдательного совета ПАО
Московская Биржа
от 01.08.2025 г. (Протокол № 4).

ПРАВИЛА УПРАВЛЕНИЯ РИСКАМИ, СВЯЗАННЫМИ С ОСУЩЕСТВЛЕНИЕМ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРА ФИНАНСОВОЙ ПЛАТФОРМЫ

Москва, 2025 г.

Оглавление

1. Общие положения

1.1. Настоящие Правила управления рисками, связанными с осуществлением деятельности оператора финансовой платформы (далее - Правила), являются основополагающим документом, определяющим основные принципы организации системы управления рисками ПАО Московская Биржа 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 о от 20.07.2020 N 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, включая:

1.7.1. основные методологические принципы и подходы к идентификации, оценке и мониторингу рисков, описанные в пункте 3.2 и главе 4 настоящих Правил;

1.7.2. классификацию рисков, присущих деятельности Платформы, описанную в пункте 4.4. настоящих Правил;

1.7.3. 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, описанные в пункте 6.1.11. настоящих Правил;

1.7.4. порядок выявления, анализа и оценки рисков Оператора Платформы, описанный в разделе 5 настоящих Правил;

1.7.5. порядок внесения рисков и результатов их оценки в реестр рисков, порядок осуществления оценки реестра рисков на предмет его актуальности, описанный в пункте 5.12. настоящих Правил;

1.7.6. порядок и периодичность проведения идентификации угроз, которые могут привести к неработоспособности Оператора Платформы, описанный в пунктах 5.11 и 6.1.5. настоящих Правил;

1.7.7. порядок назначения отдельных должностных лиц, ответственных за реализацию мероприятий, и порядок их взаимодействия со структурным подразделением, ответственным за организацию системы управления рисками (СУР), описанный в пункте 3.4. настоящих Правил;

1.7.8. порядок и сроки информирования органов управления, должностных лиц и структурных подразделений о рисках, описанные в пунктах 7.6. и 7.1. настоящих Правил соответственно;

1.7.9. 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, описанные в пункте 7.8. настоящих Правил;

1.7.10. содержание отчетов и информации о результатах осуществления в рамках организации системы управления рисками и представляемых на рассмотрение органов управления, описанное в пунктах 7.4. и 7.5. настоящих Правил;

1.7.11. 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, описанный в пункте 3.4.3 настоящих Правил;

1.7.12. перечень мер, предпринимаемых для обеспечения конфиденциальности и защиты информации о рисках, в том числе конфиденциальности отчетов о рисках, описанный в пункте 4.14 настоящих Правил;

1.7.13. порядок обеспечения операционной надежности и поддержания непрерывности деятельности, описанные в пунктах 4.17-4.20 и пункте 4.12. настоящих Правил;

1.7.14. порядок распределения ответственности и полномочий между структурными подразделениями в случае реализации существенных событий риска, связанных с деятельностью Оператора Платформы, описанный в пункте 6.2.6. настоящих Правил;

1.7.15. порядок обеспечения контроля за выполнением процессов и мероприятий по управлению рисками, описанный в пункте 3.9. настоящих Правил;

1.7.16. порядок и сроки проведения проверок эффективности управления рисками, описанные в разделе 8 настоящих Правил.

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, повышения надежности систем взаимодействия между самим Оператором Платформы и компаниями Группы «Московская Биржа».

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 данных о событиях операционных рисков (БДСОР) - электронное хранилище информации о событиях операционного риска компаний Группы «Московская Биржа».

База данных рисков (БДР) – реестр рисков, электронное хранилище информации о нефинансовых рисках компаний Группы «Московская биржа».

ДВКиК- Департамент по внутреннему контролю и комплаенсу.

УОР ДОРИБиНБ – Управление операционных рисков Департамента операционных рисков, информационной безопасности и непрерывности бизнеса.

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 риска (КИР) – количественный показатель, направленный на измерение и контроль операционного риска в определенный момент времени.

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 (далее - риски) – операционный риск, комплаенс, включая регуляторный риск, риск потери деловой репутации, правовой, стратегический риск.

Нештатная ситуация (далее НС) — обстоятельства, нестандартная ситуация, вызывающие и/или создающие предпосылки к возникновению сбоев (отказов) при эксплуатации подсистем программно-технических комплексов, в Группе «Московская Биржа» 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 другими компаниями Группы «Московская Биржа», Банком России и субъектами Платформы (Оператором Платформы, Участниками и Финансовыми организациями);

— привели или могут привести к нарушению порядка и сроков проведения операций, порядка доступа участника или группы участников к Платформе, а также порядка 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 Публичное акционерное общество «Московская Биржа ММВБ-РТС» (ОГРН: 1027739387411, место нахождения: Российская Федерация, 125009, город Москва, Большой Кисловский переулок, дом 13. Возможности финансовой платформы могут быть реализованы посредством сайта Оператора Платформы, а также посредством мобильного приложения финансовой платформы «Финуслуги».

Операционный риск - риск нарушения деятельности Оператором Платформы в результате несовершенства внутренних бизнес-процессов Оператора Платформы и (или) действий или бездействия работников Оператора Платформы, ошибок в функционировании программно-технических средств Оператора Платформы, а также в результате внешних событий и (или) действий или бездействия третьих лиц.

Передача риска - 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.

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.

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 - 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 (далее - РПДР).

СВА - Служба внутреннего аудита.

СВК – Служба внутреннего контроля.

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.

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.

УФР - Управление финансовых рисков.

Финансовая платформа «Московская Биржа» (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 присоединившиеся к договору об оказании услуг оператора финансовой платформы, условия которого установлены Правилам платформы, кредитные организации, страховые организации, Эмитенты и Агенты по размещению Облигаций.

Термины, специально не определенные в Правилах, используются в значениях, определенных во внутренних документах компаний Группы «Московская Биржа», а также законами и иными нормативными актами Российской Федерации.

3. Описание системы управления рисками

3.1. Управление рисками осуществляется в соответствии с требованиями Федерального закона, нормативных документов Банка России и Уставом ПАО Московская Биржа.

3.2. **Принципы управления рисками**

Система управления рисками строится в соответствии со следующими принципами:

- 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 подразделениями, независимыми от подразделений, генерирующих прибыль/финансовый результат.
- Принцип документированного оформления – означает, что порядок и работы системы управления рисками должны быть разработаны, пройти процедуру внутреннего согласования с подразделениями, участвующими в процессе оценки и управления рисками, 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. Цели и задачи управления рисками

3.3.1. 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.

3.3.2. 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.

3.4. Полномочия и функции структурного подразделения, ответственного за организацию СУР, и органов управления в области организации СУР и управления рисками:

3.4.1. Для организации системы управления рисками, в том числе, рисками Оператора Платформы сформировано отдельное структурное подразделение, ответственное за организацию СУР - Департамент операционных рисков, информационной безопасности и непрерывности бизнеса (далее - ДОРИБиНБ), ДОРИБиНБ возглавляет должностное лицо, в функциональные обязанности которого входит руководство ДОРИБиНБ (далее - Директор ДОРИБиНБ). Управление отдельными видами рисков в рамках организации СУР осуществляется структурными подразделениями, указанными в п. 3.6 Правил.

3.4.2. Директор ДОРИБиНБ и руководители отдельных структурных подразделений, указанные в п. 3.6 Правил, осуществляют функции, которые обеспечивают процесс управления рискам и при исполнении своих обязанностей не зависят от других должностных лиц и структурных подразделений.

3.4.3. ПАО Московская Биржа совмещает деятельность оператора финансовой платформы с деятельностью организатора торговли и оператора обмена цифровых финансовых активов. В рамках системы мер по минимизации риска, связанного с совмещением деятельности, Оператор Платформы принимает меры, направленные на выявление конфликта интересов, связанного с таким совмещением, предотвращение негативных последствий данного конфликта интересов, выражающегося в нарушении прав и законных интересов потребителей финансовых услуг, а также на минимизацию риска этих последствий, используя следующие механизмы и методы:

• разделение программно-технических комплексов Оператора Платформы с программно-техническими комплексами, обеспечивающими иные виды деятельности ПАО Московская Биржа, на уровне, достаточном для исключения взаимного влияния нештатных ситуаций;

• разделение служебных обязанностей работников структурных подразделений Оператора Платформы в соответствии с их должностными инструкциями;

• установление требований по обеспечению защиты информации ограниченного доступа от несанкционированного доступа;

• обеспечение доступа к сведениям, относящимся к категориям ограниченного доступа, только тем работникам Оператора Платформы, которым в соответствии со своими должностными обязанностями должен быть предоставлен в установленном порядке допуск к работе с такой информацией;

• установление дисциплинарных мер ответственности за неправомерное использование и предоставление информации ограниченного доступа работниками структурных подразделений, совмещающими деятельность по организации торгов и оператора финансовой платформы.

Меры, направленные на предотвращение конфликта интересов, устанавливаются в утвержденном Перечне мер, направленных на

предотвращение конфликта интересов, связанного с совмещением деятельности оператора финансовой платформы с иными видами деятельности с учетом ограничений, установленных Федеральным законом.

В целях управления данным видом риска проводятся регулярные оценки не реже одного раза в год, с целью выявления иных рисков, связанных с совмещением деятельности оператора финансовой платформы с иными видами деятельности, выявленные риски подлежат обработке в соответствии с настоящими Правилами.

3.4.4. Директор ДОРИБиНБ и руководители отдельных структурных подразделений, указанные в п. 3.6 Правил, могут входить в состав создаваемых комитетов и комиссий, не являющихся структурными подразделениями Оператора Платформы.

3.4.5. Директор ДОРИБиНБ, сотрудники структурных подразделений, указанные в пункте 3.6 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.

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

3.5. В компетенцию Директора ДОРИБиНБ 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;
- принятие иных мер, направленных на организацию СУР, предусмотренных внутренними документами.

3.6. Управление отдельными видами рисков в рамках организации СУР Оператора Платформы осуществляется:

- УОР ДОРИБиНБ – в части операционного, стратегического риска, риска потери деловой репутации;
- УФР – в части кредитного риска;
- СВК – в части регуляторных рисков в соответствии с утвержденными документами;
- ДВКиК – в части комплаенс, санкционных рисков.

3.7. В компетенцию Наблюдательного совета входит, в том числе, утверждение внутренних документов концептуального характера в области управления рисками.

3.8. В целях организации выполнения решений Наблюдательного совета в соответствии с утвержденными им внутренними документами в области управления рисками, в компетенцию исполнительных органов управления 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 образование рабочих органов, в том числе комитетов, комиссий, определение их компетенции, утверждение положений о них;

3.9. Процесс управления рисками выстраивается таким образом, что каждый работник Оператора Платформы информирует руководителя подразделения и/или Директора ДОРИБиНБ и/или отдельное структурное подразделение, ответственное за управление рисками, об идентифицированных рисках, а также о событиях риска, и участвует в реализации мероприятий по контролю и минимизации риска в зоне своей ответственности.

3.10. Полномочия подразделений в области управления рисками определяются внутренними документами, в том числе, Положениями о подразделениях.

4. Основные риски, связанные с осуществлением деятельности оператора финансовой 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 ПАО Московская биржа.

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 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:

Нефинансовые риски:

- операционный риск;
- комплаенс риск, включая регуляторный;

- риск потери деловой репутации;
- стратегический риск;
- правовой риск;
- санкционный риск.

Также Оператор Платформы выделяет финансовый риск - кредитный.

4.5. **Операционный риск**

4.5.1. 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[1];
- неблагоприятные внешние обстоятельства, находящиеся вне контроля Оператора Платформы (включая внешнее мошенничество, хакерские и DDoS атаки, техногенные и природные катастрофы);
- нарушение информационной безопасности.

4.5.2. 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;
- организацию 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

[1] Подробнее в Политике обеспечения непрерывности бизнеса ПАО Московская Биржа и Порядке обеспечения операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг ПАО Московская биржа.

быстрого и адекватного реагирования для устранения последствий таких событий в случае их возникновения;

- эффективное распределение полномочий между Наблюдательным советом, исполнительными органами, структурными подразделениями и работниками по вопросам управления рискам.

4.5.3. 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.

4.5.4. 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.

4.5.5. В рамках управления операционным риском Оператор Платформы выделяет управление рисками информационной безопасности (ИБ), мероприятия по управлению которыми описаны в п.4.13 Правил.

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

4.6.1. 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.

4.6.2. 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.

4.6.3. 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 данных операционных рисков.

4.7. **Стратегический риск**

4.7.1. 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.

4.7.2. Оператор Платформы в рамках управления стратегическим риском обеспечивает проведение оценки УОР ДОРИБиНБ в целях выявления потенциальных источников возникновения рисков:

4.7.2.1. Разработка проектов изменений в порядок осуществления деятельности Оператора Платформы, предоставления дополнительных услуг, а также иных организационных и (или) технологических изменений (далее - проекты изменений).

4.7.2.2. Анализ целесообразности внедрения проектов изменений.

4.7.2.3. Анализ эффективности реализованных проектов изменений по итогам их введения в деятельность.

4.7.2.4. Мероприятия по планированию развития деятельности, в том числе, посредством разработки стратегии развития.

4.7.2.5. Оценка стратегии развития на предмет определения возможности и целесообразности ее реализации, а также внесение изменений в стратегию развития в случае указанного решения.

4.8. **Правовой риск**

4.8.1. Правовой риск – риск возникновения убытков в результате неэффективной организации правовой работы, приводящей к правовым ошибкам в деятельности Биржи вследствие действий работников или органов управления; нарушения Биржей, а также клиентами и контрагентами Биржи условий договоров; наличия в договорах положений, не отвечающих правам и интересам Биржи; несовершенства правовой системы; нахождения Биржи, ее клиентов и контрагентов под юрисдикцией различных государств.

4.8.2. Целью управления правовым риском является поддержание принимаемого Биржей риска на уровне, определенном Биржей в соответствии со стратегическими задачами. Приоритетным является обеспечение максимальной сохранности активов и капитала на основе уменьшения (исключения) возможных убытков, в том числе в виде выплат денежных средств на основании постановлений (решений) судов и надзорных органов.

4.9. **Комплаенс риск**

4.9.1. Оператор Платформы рассматривает следующий минимальный перечень базовых комплаенс-рисков, подлежащих управлению:

4.9.1.1. Риск использования в целях легализации (отмывания) доходов (ОД), полученных преступным путем и финансирования терроризма (ФТ);

4.9.1.2. Несоблюдение работниками норм профессиональной этики и/или совершение действий, которые могут привести к потере деловой репутации;

4.9.1.3. нарушение требований в части идентификации иностранных налогоплательщиков (FATCA/CRS)

4.9.2. К внутренним факторам, влияющим на величину комплаенс-рисков, относятся:

4.9.2.1. несоблюдение законодательства, в том числе по противодействию ОД/ФТ, по идентификации и изучению клиентов, контрагентов, противодействию коррупции, а также в сфере финансовых рынков, защиты прав и интересов клиентов, конфликта интересов;

4.9.2.2. несоблюдение внутренних документов и процедур;

4.9.2.3. несоблюдение профессиональных стандартов или норм деловой этики;

4.9.2.4. резкие изменения в составе и количестве сотрудников;

4.9.2.5. ускоренное развитие бизнеса;

4.9.2.6. Внедрение новых технологий;

4.9.2.7. Разработка новых продуктов или расширение в новые сферы бизнеса/новые рынки;

4.9.2.8. изменения в организационной структуре.

4.9.3. К внешним факторам, влияющим на величину комплаенс-рисков, относятся:

4.9.3.1. нахождение клиентов и контрагентов под юрисдикцией различных государств;

4.9.3.2. недобросовестные действия клиентов/контрагентов;

4.9.3.3. развитие схем внутреннего и внешнего мошенничества, вредительства и ухода от контроля;

4.9.3.4. развитие рынка и технологий;

4.9.3.5. существенные изменения в экономике и/или законодательстве (в том числе иностранном).

4.9.4. 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.

4.9.5. Меры по минимизации комплаенс риска Оператора Платформы могут включать в себя следующие:

4.9.5.1. Разработку внутренних нормативных документов, регламентирующих процессы и процедуры, связанные с управлением комплаенс-риском;

4.9.5.2. автоматизацию контролей;

4.9.5.3. обучение персонала.

4.10. **Санкционный риск**

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

4.10.1.1. финансовые организации – участники платформы;

4.10.1.2. физические лица- пользователи платформы;

4.10.1.3. контрагенты Оператора платформы, в том числе осуществляющие поставку ИТ оборудования и ПО, необходимых для функционирования Платформы.

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

•блокировке активов за рубежом;

• распространение 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 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.

4.10.3. 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 согласно пп.4.5.3.и 4.5.4. Правил, 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.

4.11. **Кредитный риск**

4.11.1. Основным источником кредитного риска в деятельности Оператора Платформы является риск неуплаты или несвоевременной уплаты комиссионных вознаграждений пользователями Платформы.

4.11.2. С целью управления кредитным риском УФР 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 соответствии с Положением о проявлении должной осмотрительности при выборе контрагента в целях снижения экономических, налоговых, и репутационных рисков;
- осуществляет оценку необходимости формирования резервов под ожидаемые кредитные потери.

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

4.12. **Нештатные и чрезвычайные ситуации**

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

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

4.13.1.1. 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.

4.13.1.2. 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, отвечающие критериям нештатных ситуаций, определенным в соответствии с Регламентом действий подразделений ПАО Московская Биржа в нештатных ситуациях, возникших при осуществлении деятельности оператора финансовой платформы.

4.13.2. 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.

4.13.3. Управление рисками непрерывности деятельности Оператора Платформы описывается в Приложении №1 к Правилам управления рисками, связанными с осуществлением деятельности оператора финансовой платформы

4.14. 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.

4.15. 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.

4.16. 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

4.17. 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.

4.18. Оператор Платформы при предоставлении услуг по содействию в совершении финансовых сделок между потребителями финансовых услуг и финансовыми организациями (эмитентами) обеспечивает реализацию мероприятий по достижению показателя доступности финансовой платформы не ниже установленного уровня.

4.19. 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:

4.19.1. основные, выполнение которых напрямую связано с предоставлением услуг;

4.19.2. вспомогательные, выполнение которых косвенно связано с предоставлением услуг.

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

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

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

4.22.1. бизнес- и технологических процессов, реализуемых Оператором Платформы в целях предоставления услуг в рамках своей деятельности (далее – бизнес- и технологические процессы);

4.22.2. систем хранения данных, применяемых Оператором Платформы, в рамках реализации бизнес- и технологических процессов;

4.22.3. прикладного программного обеспечения автоматизированных систем и приложений, применяемых Оператором Платформы;

4.22.4. объектов информационной инфраструктуры, задействованных Оператором Платформы, в рамках реализации бизнес- и технологических процессов (включая управление мощностями и производительностью объектов информационной инфраструктуры);

4.22.5. работников Оператора Платформы;

4.22.6. планов обеспечения операционной надежности деятельности Оператора Платформы.

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

4.23.1. управление изменениями;

4.23.2. управление конфигурациями и уязвимостями;

4.23.3. 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.

4.24. 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 ПАО Московская Биржа.

4.24.1. 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. 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);

5.1.1. обмен информацией о рисках между подразделениями и органами управления;

5.1.2. 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 других компаний Группы «Московская Биржа» 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.

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

5.6. 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.

5.7. Система отчётности 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.

5.8. Основные подходы к управлению рисками.

5.8.1. Управление финансовыми рисками описано в Политике по управлению финансовыми рисками. Управление нефинансовыми рисками (за исключением регуляторного риска) осуществляется аналогично управлению операционным риском, описание которого приведено в Главах 5 пп.5.8.2-5.15 и 6 Правил и в Политике управления операционным риском.

5.8.2. 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 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.).

5.9. 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.

5.10. 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.

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

5.12. 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.

5.13. 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).

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

5.15. 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 помимо процессов и мероприятий, описанных в Главе 5 Правил, 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 и реализация мер по защите информации, осуществляемых в рамках соответствия требованиям законодательства.

6.1.4. 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.

6.1.5. 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.

6.1.5.1. 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.

6.1.5.2. В процессе Оценки рисков оценивается вероятность реализации угрозы, степень возможного влияния на Платформу, существующие организационно-технические мероприятия и контрольные процедуры, направленные на снижение рисков.

6.1.5.3. Оценка рисков проводится на регулярной основе, не реже одного раза в год, а также в случае существенных изменений внутренних и внешних факторов.

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

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

6.1.8. Осуществление мониторинга использования Участниками технических средств Оператора Платформы.

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 базы данных о событиях операционного риска по следующим видам событий операционного риска с учетом критериев существенности последствий:

6.1.11.1. события операционного риска, приведшие к прерыванию совершения одной или нескольких значимых финансовых сделок с потребителями финансовых услуг и финансовыми организациями, эмитентами на финансовой платформе (далее - существенные события операционного риска или события высокого уровня влияния);

6.1.11.2. события операционного риска, не приведшие к прерыванию оказания значимых услуг, но негативно повлиявшие на деятельность свыше 15 процентов потребителей финансовых услуг, эмитентов и финансовых

организаций, присоединившихся к договору об оказании услуг оператора финансовой платформы (далее - значимые события операционного риска или события среднего уровня влияния);

6.1.11.3. события операционного риска, не относящиеся к существенным событиям операционного риска и значимым событиям операционного риска (события низкого уровня влияния).

6.1.12. 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).

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

6.1.14. 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[2], 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

[2] Подробнее в Политике обеспечения непрерывности бизнеса ПАО Московская Биржа и Порядке обеспечения операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг ПАО Московская биржа.

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 Платформы (далее - резервный офис), удовлетворяющего следующим требованиям:

- расположение резервного офиса в отдельном здании (вне основного комплекса);
- территориальное удаление резервного офиса от основного комплекса на расстояние, обеспечивающее возможность работников продолжить работу в резервном офисе в течение двух часов с момента возникновения чрезвычайной ситуации;
- проведение мероприятий по поддержанию постоянного функционирования резервного офиса и возможности переключения управления на него в случае невозможности осуществления критически важных процессов Платформы в основном комплексе средств.

6.2.9. 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.

6.2.10. Проверка наличия и техническое обслуживание независимых генераторов электричества в основном комплексе и в резервном офисе, предоставляющих мощность, обеспечивающую осуществление критически важных процессов Оператора Платформы в течение всего периода восстановления функционирования программно-технических средств основного комплекса технических средств Платформы.

6.2.11. Создание и поддержание технического оснащения резервного офиса на уровне, обеспечивающем восстановление критически важных процессов.

6.2.12. Мероприятия, обеспечивающие возможность оказания услуг, необходимых для функционирования основного комплекса средств и резервного офиса, как минимум двумя независимыми поставщиками телекоммуникационных услуг.

6.2.13. Поддержание резервного офиса на уровне, обеспечивающем возможность функционирования всех критически важных процессов Оператора Платформы, и поддержание таких процессов в течение не менее одного месяца с момента возникновения чрезвычайной ситуации.

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 УОР ДОРИБиНБ, 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 Директором ДОРИБиНБ (в части нерегулярной отчетности), на основе его профессионального суждения, формируемого с учётом оценки риска, потребностей Оператора Платформы, величины того или иного риска и принципа существенности;
  - сроки и форма предоставления информации работниками, определяется в соответствующих запросах Директора ДОРИБиНБ;
- Органам управления Директором ДОРИБиНБ 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).

7.2.1. Регулярная отчётность по рискам включена в регулярную отчетность по рискам Группы и предоставляется Правлению Биржи и Комиссии по управлению рисками Наблюдательного совета, Наблюдательному Совету.

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 может включать 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.

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 Директора ДОРИБиНБ, 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. СВА в рамках своих полномочий проводит независимую оценку эффективности системы управления рисками Платформы в целом или отдельных ее элементов в соответствии с Планом проверок СВА.

8.3. Периодически в рамках оценки эффективности СУР могут проводиться внешние аудиты с привлечением независимых аудиторов и консультантов

8.4. Оценка эффективности включается в регулярную отчетность по рискам за квартал, в котором была проведена соответствующая оценка эффективности, и предоставляется Правлению, на Комиссии по рискам Наблюдательного совета, Комиссии по аудиту при Наблюдательном Совете и Наблюдательному Совету.

9. Раскрытие (предоставление) 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. Предоставление и 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:
  - нормативные документы по управлению рисками;
  - аналитические отчеты по уровню отдельных видов риска;
  - по отдельному запросу - методики оценки рисков, параметры моделей.

9.3. Механизмами раскрытия и предоставления информации являются:

- размещение информации на сайте в сети Интернет;

- предоставление обязательной отчетности, установленной нормативными документами Банка России, а также иной отчетности, обозначенной во внутренних документах по управлению рисками.

Приложение №1

к Правилам управления рисками,
связанными с осуществлением деятельности
оператора финансовой платформы.

Программа непрерывности деятельности Оператора платформы

Основными этапами программы непрерывности деятельности являются:

- поддержание способности Оператора Платформы выполнять принятые на себя обязательства перед клиентами и партнерами, предупреждение и предотвращение возможного нарушения режима повседневного функционирования Оператора платформы;
- обеспечение соответствия всех требований государственных органов РФ, а также требованиям нормативно-правовых актов;
- снижение тяжести последствий нарушения режима повседневного функционирования Оператора Платформы (в том числе, размера материальных потерь, потерь информации, потери деловой репутации);
- восстановление функционирования Оператора Платформы в рамках установленного времени и определенного объема в случае возникновения ЧС;
- сохранение уровня управления Оператора Платформы, позволяющего обеспечить условия для принятия обоснованных и оптимальных управленческих решений, их своевременную и полную реализацию;

Требования всех заинтересованных сторон постоянно отслеживаются, осуществляется их анализ для осуществления текущей деятельности. При планировании развития Оператора платформы именно требования всех заинтересованных сторон являются основанием для осуществления изменений и развития функционала, ввода новых услуг.

В программе непрерывности деятельности Оператора Платформы предусматриваются следующие сценарии возможных ЧС:

- Полная/ частичная потеря здания;
- Потеря ИТ-инфраструктуры;
- Невозможность доступа в здание;
- Существенная потеря/недоступность работников;
- Проблемы на стороне поставщиков / отказ поставщиков от предоставления товаров/услуг.

Основная цель программы непрерывности деятельности Оператора Платформы — это выполнение всех принятых на себя обязательств в случае возникновения чрезвычайной ситуации. Оператор Платформы предлагает множество различных услуг и в случае активации программы сосредоточится на восстановлении и поддержании в краткосрочной перспективе самых критически важных бизнес-процессов, в среднесрочной перспективе - некритичных процессов и в долгосрочном плане - всех процессов.

Активация программы непрерывности деятельности возможна только при возникновении чрезвычайной ситуации. Хотя весьма затруднительно предусмотреть исчерпывающий список угроз, которые могут повлечь за собой активацию плана, но к ним, к примеру, могут быть отнесены различные события - от природных катаклизмов до террористических атак. Таким образом, как только Оператор Платформы начинает испытывать трудности в

поддержке критичных бизнес систем из-за сбоя, атак, других инцидентов, немедленно активируется план обеспечения непрерывности бизнеса.

АЛЬТЕРНАТИВНЫЕ ПЛОЩАДКИ

У Оператора Платформы есть альтернативные площадки, которые активируются при недоступности основных площадок. Альтернативные площадки повторяют инфраструктуру основного офиса, где все оборудование уже настроено и готово к эксплуатации в любой момент. Наличие географически распределенных резервных площадок позволяет не прерывать предоставление ИТ- сервисов Оператора Платформы

ПРОЦЕСС

При реализации программы непрерывности деятельности Оператора Платформы используется методика международного стандарта в области обеспечения непрерывности ISO 22301:2012 и модель «Plan-Do-Check-Act» - «Планирование-Действие-Проверка-Корректировка». Основными элементами этого подхода являются:

- 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).
- 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.

КРИЗИСНОЕ УПРАВЛЕНИЕ (РЕЖИМ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ)

В режиме ЧС общей задачей являются деятельность по минимизации последствий ЧС и скорейшее возобновление нормальной деятельности.

Кризисное управление регламентирует следующее:

- порядок эскалации информации о возможности возникновения инцидента, который потенциально может привести к недоступности любого офиса / недоступности основного ЦОД / существенному воздействию на персонал;
- критерии признания инцидента и объявления Чрезвычайной ситуации в случае возникновения критичного инцидента непрерывности деятельности;
- порядок действий при обработке инцидента;
- порядок оповещения работников, входящих в задействованные команды восстановления;
- порядок оповещения заинтересованных лиц;

В рамках кризисного управления подключаются МКЦ (Малый Кризисный Центр) и БКЦ (Большой Кризисный Центр), рассматривающие вопросы, связанные с возникновением нештатных ситуаций и принимающие решения по таким вопросам.