УТВЕРЖДЕНЫ

решением Наблюдательного совета
ПАО Московская Биржа
от 18.11.2022 г. (Протокол № 10)

ПРАВИЛА УПРАВЛЕНИЯ РИСКАМИ, СВЯЗАННЫМИ С ОСУЩЕСТВЛЕНИЕМ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАТОРА ТОРГОВЛИ И ОПЕРАТОРА ОБМЕНА ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ

Москва, 2022 г.

Содержание

1 Термины и определения, используемые в настоящих Правилах

База данных о событиях операционных рисков (БДСОР) – электронное хранилище информации о событиях операционного риска Биржи и инцидентах (событиях), связанных с операционным риском, но не имевших последствий и не оказавших негативного влияния на процессы Биржи.

База данных рисков (БДР) – реестр рисков, электронное хранилище информации о нефинансовых рисках Биржи.

Бизнес-владелец риска – единоличный или коллегиальный орган Биржи или руководитель структурного подразделения Биржи, ответственные за процессы (выполняемые ими и/или находящиеся в зоне их компетенции), на которые реализация операционного риска оказывает негативное влияние и может привести к возникновению убытков или нарушению бесперебойности функционирования систем/сервисов Биржи. Бизнес-владелец риска несёт ответственность за принятие решения о реагировании на событие операционного риска, риски, мониторинг рисков и контроль внедрения контрольных процедур в рамках деятельности вверенного ему структурного подразделения.

Биржа – ПАО Московская Биржа, Организатор торговли, Оператор обмена цифровых финансовых активов

Владелец риска – руководитель структурного подразделения, бизнес-процесса или его этапа, в ходе осуществления которого проявляются обстоятельства, обуславливающие возможную реализацию операционного риска, как у самого Владельца риска, так и у Бизнес-владельца риска. Должностное лицо, ответственное за разработку, внедрение и поддержание в работоспособном состоянии процесса, а также за разработку контрольных процедур.

Внешняя база данных о событиях операционных рисков (внешняя БДСОР) – электронное хранилище информации о внешних событиях операционного риска, которые произошли вне ПАО Московская Биржа.

ВПТС – внешние программно-технические средства проведения торгов.

Группа – Группа компаний ПАО Московская Биржа, состоящая из ПАО Московская Биржа, НКО АО НРД, НКО НКЦ (АО), ООО «ММВБ-Финанс», АО НТБ, «ООО МБ Инновации» и ООО «МБ Защита информации».

Деловая репутация – качественная оценка участниками гражданского оборота деятельности Биржи, а также действий его акционеров и аффилированных лиц.

ДОД – Дежурный операционный Директор.

Заключение о рисках – профессиональное суждение работников подразделений риск-менеджмента, СВК и ДВКиК установленной формы в отношении рисков продукта - возможных финансовых и нефинансовых событий, которые могут негативно повлиять на экономическую эффективность продукта проекта, репутационные риски, риски утраты доверия клиентов.

Информационная безопасность– безопасность, связанная с угрозами в информационной сфере.

Информационная инфраструктура (ИТ-инфраструктура) – совокупность систем обработки информации и обрабатываемых данных, используемая для обеспечения деятельности Биржи.

Информационные угрозы – источник реализации события риска информационной безопасности (в результате компьютерной атаки).

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Ключевой индикатор риска (КИР) – показатель деятельности Биржи (в том числе статистический, финансовый), позволяющий осуществлять мониторинг масштабности и вероятности/возможности реализации риска.

Комплаенс риск – риск возникновения убытков из-за несоблюдения законодательства, внутренних документов, стандартов саморегулируемых организаций (если такие стандарты или правила являются обязательными), а также в

результате применения санкций и (или) иных мер воздействия со стороны надзорных органов. Для описания комплаенс-рисков используется термин «регуляторный риск», который, является одной (но не единственной) из составляющих комплаенс-рисков Биржи.

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

Конфликт интересов – ситуация, при которой косвенная или прямая личная заинтересованность, фактическая или потенциальная выгода работника Биржи влияет или может повлиять на добросовестное и эффективное исполнение ими должностных обязанностей и может привести к неблагоприятным последствиям для Биржи, его клиентов и партнеров при осуществлении деятельности по проведению организованных торгов.

Кредитный риск – риск возникновения убытков вследствие неисполнения, несвоевременного либо неполного исполнения контрагентом своих обязательств в соответствии с условиями договоров.

Снижение риска- минимизация риска, деятельность продолжает осуществляться в измененном виде, в частности, за счет внедрения новых или оптимизации существующих контрольных процедур.

Нештатная ситуация (НС) – обстоятельства, вызывающие и/или создающие предпосылки к возникновению сбоев (отказов) при эксплуатации подсистем программно-технического комплекса Биржи 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 ПАО Московская Биржа и другими компаниями Группы «Московская Биржа», Банком России, Государственной корпорацией «Банк развития и внешнеэкономической деятельности (Внешэкономбанк)», Государственным

учреждением - Пенсионный фонд Российской Федерации и Федеральным казначейством на одном из рынков;

- привели или могут привести к нарушению порядка и сроков проведения операций, порядка доступа участника или группы участников к торгам, а также раскрытия и предоставления информации, установленных внутренними документами Биржи для соответствующего рынка.

Нефинансовые риски – операционный риск (включая риск нарушения информационной безопасности и непрерывности бизнеса), риск потери деловой репутации, стратегический риск, проектный риск, правовой риск, комплаенс-риск, включая регуляторный.

Объект информатизации - совокупность объектов и ресурсов доступа, средств и систем обработки информации, в том числе автоматизированные системы, используемых для обеспечения информатизации бизнес-процессов и (или) технологических процессов Биржи, используемых для предоставления финансовых услуг.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Операционная надежность – способность обеспечить непрерывность функционирования критически важных процессов с учетом соблюдения целевых показателей операционной надежности.

Операционный риск – риск возникновения последствий, влекущих за собой приостановление или прекращение оказания услуг по проведению организованных торгов в полном или неполном объеме, а также риск возникновения расходов (убытков) Биржи в результате сбоев и (или) ошибок программно-технических средств Биржи, включая программно-технические средства и информационно-коммуникационные средства связи, с помощью которых обеспечивается проведение организованных торгов, и (или) во внутренних бизнес-процессах Биржи, ошибок работников и (или) в результате внешних событий, оказывающих негативное воздействие на деятельность Биржи.

Ответственный за план - работник, ответственный за координацию деятельности по минимизации/закрытию риска.

Отказ от риска (уклонение от риска) – отказ от принятия/передачи 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 Биржи, решение об избегании/удержании риска должно приниматься с учетом сравнения величины риска и размера дохода.

Передача риска – деятельность продолжает осуществляться, при этом в нее вносятся изменения, в результате которых риск полностью или частично передается третьей стороне.

План обеспечения непрерывности и восстановления деятельности (далее – План ОНиВД) - внутренний документ Биржи, определяющий цели, задачи, порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования Биржи (подразделений), вызванного непредвиденными обстоятельствами (возникновением ЧС или иным событием, наступление которого возможно, но трудно предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению Биржей принятых на себя обязательств).

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.

Предельный уровень риска (риск-аппетит) – это максимальный уровень риска, который Биржа готова принять для достижения стратегических целей.

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 Биржи. Процедура принятия операционного риска свыше установленного размера риск-аппетита в отдельных случаях должна сопровождаться мотивированным суждением о достаточности средств на покрытие потерь от реализации событий такого риска, рассчитанных на основе исторических данных за предшествующие года (не менее 10 лет) при наличии данных и модели для проведения расчетов.

Проект - Ограниченная во времени деятельность для создания новых (уникальных) продуктов, услуг или результатов, представляющая ценность для Группы «Московская Биржа», а также для третьих лиц

ПТК ТЦ - Программно-технический комплекс Технического центра Биржи.

Риск – 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 – предельный уровень риска, который Биржа готов принять для достижения стратегических задач, выраженный в виде системы контрольных количественных и качественных показателей, ограничивающих уровень принимаемых рисков.

Риск-менеджер – работник структурного подразделения, ответственного за организацию системы управления рисками (ДОРИБиНБ).

Риск продукта - возможные финансовые и нефинансовые события, которые могут негативно повлиять на экономическую эффективность продукта проекта, репутационные риски, риски утраты доверия клиентов. Фиксируются в

консолидированном Заключении и рисках продукта, формируемом подразделениями риск-менеджмента.

Регуляторный риск – риск возникновения у ПАО Московская Биржа расходов (убытков) и (или) иных неблагоприятных последствий в результате несоответствия деятельности, осуществляемой Биржей на основании лицензии биржи на осуществление деятельности по проведению организованных торгов, деятельности оператора финансовой платформы, осуществляемой на основании включения ПАО Московская Биржа в реестр операторов финансовых платформ, требованиям законодательства Российской Федерации, регулирующего деятельность ПАО Московская Биржа, правилам организованных торгов, правилам финансовой платформы, учредительным и иным внутренним документам ПАО Московская Биржа по управлению регуляторными рисками, и (или) в результате применения мер в отношении ПАО Московская Биржа со стороны надзорных органов Биржи

Риск информационной безопасности – риск, связанный с возможностью утраты свойств информационной безопасности (конфиденциальности, целостности, доступности) информационных активов Биржи в результате реализации угроз информационной безопасности. К возможным последствиям от реализации риска информационной безопасности относятся:

- возникновение потерь Биржи, его клиентов, контрагентов;
- нарушение непрерывного предоставления Биржи финансовых и (или) информационных услуг в условиях реализации информационных угроз;
- невыполнение обязательств по обеспечению защиты интересов клиентов Биржи в случае их потерь в результате событий, связанных с реализацией информационных угроз;
- несоблюдение требований законодательства Российской Федерации в области защиты информации и т.д.

Риск потери деловой репутации – риск возникновения последствий, влекущих за собой расходы (убытки) Биржи или иные негативные последствия в результате негативного восприятия Биржи со стороны контрагентов Биржи, участников торгов и их клиентов, акционеров Биржи, Банка России и иных лиц, которые могут негативно

повлиять на способность Биржи поддерживать существующие и (или) устанавливать новые деловые отношения и поддерживать на постоянной основе доступ к источникам финансирования (далее - РПДР).

Риск проекта (проектный риск) - возможное событие или условие, наступление которого может отрицательно сказаться на параметрах проекта (срок, содержание, бюджет/лимит финансирования проекта).

Риск реализации информационных угроз - возможность реализации информационных угроз (в совокупности с последствиями от их реализации), которые обусловлены недостатками процессов обеспечения операционной надежности и защиты информации, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности ПАО Московская Биржа

Система защиты информации - совокупность мер защиты информации, применение которых направлено на непосредственное обеспечение защиты информации, процессов применения указанных мер защиты информации, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты информации.

Событие риска – событие, ситуация, обстоятельство, которые характеризуются реализацией (проявлением) риска и могут сопровождаться причинением Бирже убытков (возникновения расходов), в терминах Правил события нефинансовых рисков, т.е. события операционного, репутационного, стратегического и регуляторного (комплаенс), правового, проектного риска.

Событие операционного риска (СОР) – событие, ситуация, обстоятельства, которые характеризуются реализацией (проявлением) операционного риска и могут приводить к убыткам[1].

[1] К СОР относится также событие риска реализации информационных угроз (включая киберриск и другие виды риска реализации информационных угроз), в случае если событие привело к нарушению бизнес-процессов.

Совокупный предельный уровень рисков – это максимальная величина потенциальных убытков, которые Биржа может понести в случае реализации рисков, предусмотренных ее риск-аппетитом.

СОИ - Система оперативного информирования.

Стратегический риск – риск возникновения расходов (убытков) Биржи в результате принятия ошибочных решений в процессе управления Биржей, в том числе при разработке, утверждении и исполнении документов, определяющих направления развития Биржи, ненадлежащего исполнения принятых решений в процессе управления Биржей, не учёте органами управления Биржи изменений внешних факторов, влияющих или способных повлиять на процесс управления Биржей.

Стресс-тестирование нефинансовых рисков – это моделирование различных негативных сценариев реализации нефинансовых рисков, влекущих финансовые и нефинансовые последствия для Биржи. Одним из стресс-сценариев операционных рисков является нагрузочное тестирование - оценка устойчивости программно-технических средств, используемых для осуществления деятельности по организации торгов, к существенным изменениям, исключительным, но правдоподобным событиям, связанным с нарушением бизнес-процессов и внешней средой.

Сценарный анализ нефинансовых рисков (сценарный анализ) – это специальным образом структурированный прогноз потерь и наступления событий операционного и (или) иного нефинансового риска, которые его вызывают, основанный на знаниях экспертов в той области, риски которой подлежат оценке. Сценарный анализ включает в себя прогноз возникновения события операционного риска, вероятность его возникновения, оценку размера возможных потерь в рамках анализируемого сценария. Сценарный анализ может проводиться на основе собранных данных о внутренних и внешних событиях операционного риска, на основе экспертных оценок, результатов количественного и качественного анализа, а также результатов самооценки рисков и контрольных процедур, постоянного операционного контроля, значений ключевых индикаторов риска, внутренних и внешних проверок аудита и проверок внешних надзорных органов.

ТКС - торгово-клиринговые системы Биржи.

Угроза информационной безопасности – угроза нарушения свойств информационной безопасности (доступности, целостности или конфиденциальности) информационных активов Биржи.

Фактор риска – обстоятельство, обусловившее или способное обусловить возникновение события риска.

Фактор нарушения режима нормального функционирования - ситуация, которая может представлять собой угрозу прерывания нормальной деятельности. Например:

- нарушение нормального функционирования автоматизированных систем, поддерживающих критичные процессы Биржи;
- неработоспособность (недоступность) основных каналов связи, в том числе корпоративной сети Биржи, информационно-телекоммуникационной сети Интернет, других каналов связи с взаимодействующими организациями, необходимых для выполнения критичных процессов Биржи;
- отсутствие физической возможности нахождения работников Биржи 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 Биржи.

Целевой уровень риска – тот уровень риска, к которому стремится Биржа при планировании мероприятий по управлению риском.

Цифровой финансовый актив - цифровые финансовые активы, которые выпускаются и учитываются в Информационной системе[2].

Чрезвычайная ситуация (ЧС) – это внешние воздействия, способные нарушить режим нормального функционирования Биржи и ее способность выполнять принятые на себя обязательства, вследствие чего Биржа может понести убытки. При этом, под внешним

[2] Под Информационной системой в целях настоящего абзаца понимается распределенный реестр, совокупность баз данных, тождественность содержащейся информации в которых обеспечивается на основе установленных алгоритмов (алгоритма), с помощью которого осуществляется выпуск и обращение цифровых финансовых активов и оператором которого является Небанковская кредитная организация акционерное общество «Национальный расчетный депозитарий» (НКО АО НРД).

воздействием понимается обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, распространения заболевания, представляющего опасность для окружающих, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Перечень возможных ЧС: крупномасштабные нестандартные и чрезвычайные ситуации, сопоставимые по длительности и силе воздействия, размерам возможных материальных потерь и негативным последствиям нематериального характера с чрезвычайной ситуацией муниципального характера, межмуниципального, регионального или межрегионального характера, следствием которых является наступление факторов нарушения режима нормального функционирования Биржи.
Эксперт – работник подразделения, принимающего участие в самооценке, владелец процессов, подверженных самооценке.

ДВКиК – Департамент по внутреннему контролю и комплаенсу.

ДК - Департамент по коммуникациям.

ДКП - Департамент клиентской поддержки.

ДОД - дежурный операционный директор. Сотрудник, осуществляющий организацию и координацию работы кризисных центров.

ДОРИБиНБ – Департамент операционных рисков, информационной безопасности и непрерывности бизнеса. Относится к подразделениям риск-менеджмента.

ДС – Департамент стратегии.

ДСТиВС - Департамент сопровождения торговых и вспомогательных систем.

КПП- Комитет по проектам и продуктам - Совещательный орган при Правлении, основными задачами которого являются:

- Формирование единого подхода в области управления общегрупповыми проектами (в том числе, контроль проектов, входящих в портфель проектов, выработка рекомендаций в отношении стратегических решений по проектам и программам проектов и т. п.);
- Повышение качества проработки проектов и продуктов за счет их всестороннего анализа, в том числе со стороны специалистов по управлению рисками в составе Комитета;
- Обеспечение взаимодействия между компаниями Группы «Московская Биржа» при принятии решений по проектам и продуктам за счет включения в состав Комитета представителей Группы.

ОД – Операционный департамент.

ПО – проектный офис

СВА – Служба внутреннего аудита.

СВК – Служба внутреннего контроля.

УФР – Управление финансовых рисков. Относится к подразделениям риск-менеджмента.

ЮД – Юридический департамент.

DR-тестирование (Disaster recovery test) - тестирование аварийного восстановления- тестирование программно-технических средств и сетевых коммуникаций Группы Московская Биржа, находящихся в основном и резервном центрах обработки данных.

NIST - National Institute of Standards and Technology (SP 800-30 «Guide for Conducting Risk Assessments»).

NPV - Net Present Value.

OSSTMM - Open Source Security Testing Methodology Manual.

OWASP - Open Web Application Security Project.

PTES - Penetration Testing Execution Standard.

TCO - Total Cost of Ownership.

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

2 Общие положения, определяющие цели управления рисками

2.1. Настоящие Правила управления рисками, связанными с осуществлением деятельности Организатора торговли и Оператора обмена цифровых финансовых активов (далее - Правила), являются основополагающим документом, определяющим основные принципы организации системы управления рисками в ПАО Московская Биржа (далее – Биржа), связанными с организацией торгов, обменом цифровых финансовых активов (далее – ЦФА), а также с осуществлением операций с собственным имуществом (далее при совместном упоминании - риски Биржи), и формируют регулятивную основу для построения эффективно работающей системы управления рисками, соответствующей масштабам деятельности Биржи.

2.2. Правила разработаны на основании требований:

- Федерального закона от 21.11.2011 г. №325-ФЗ «Об организованных торгах» (далее – Закон об организованных торгах);
- Федерального закона от 31.07.2020 N 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации";
- Положения Банка России от 17 октября 2014 г. №437-П «О деятельности по проведению организованных торгов»;
- Положения от 15 ноября 2021 г. №779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального Закона от 10 июля 2002 года №86-ФЗ "О Центральном банке Российской Федерации Банке России", в целях

обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)»;

- Указания Банка России от 07 мая 2018 г. №4791-У «О требованиях к организации организатором торговли системы управления рисками, связанными с организацией торгов, а также с осуществлением операций с собственным имуществом, и к документам организатора торговли, определяющим меры, направленные на снижение указанных рисков и предотвращение конфликта интересов»;
- Указания Банка России от 07 мая 2018 г. №4792-У «О требованиях к порядку осуществления организатором торговли внутреннего контроля и внутреннего аудита».
- Национальный стандарт ГОСТ Р 57580.1-2017 Российской Федерации «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

2.3. Цели управления рисками.

Целями управления рисками Биржи являются: 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 Биржи.

Цели управления рисками достигаются 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 Биржи в процессе выявления рисков;
- качественная и количественная оценка (измерение) рисков;

- установление порядка предоставления отчетности по вопросам управления рисками органам управления Биржи;
- 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;
- распределение полномочий и ответственности между структурными подразделениями и работниками по вопросам управления рисками.

2.4. Биржей сформировано отдельное структурное подразделение, ответственное за организацию системы управления рисками - Департамент операционных рисков, информационной безопасности и непрерывности бизнеса (далее - ДОРИБиНБ), руководство которым осуществляет Директор ДОРИБиНБ.

3 Критерии существенности последствий, к которым может привести реализация рисков Биржи, в целях признания Биржей таких рисков (за исключением операционного риска Биржи) значимыми, а также порядок сопоставления результатов оценки выявленных рисков Биржи с указанными критериями

Риск может быть признан значимым в случае, если негативные последствия от реализации данного риска оказывает существенное (значительное) влияние на один или несколько показателей:

- финансовый результат,
- репутацию,
- соблюдение требований регулирующих органов,
- информационную безопасность.

К значимым рискам, в любом случае, относятся риски, признаваемые значимыми, согласно требованиям указания Банка России №4791-У.

ПАО Московская Биржа определяет для себя следующие критерии существенности последствий, в целях признания таких рисков значимыми:

- нарушение требований законодательства Российской Федерации с применением штрафных санкций надзорными органами виде штрафов, в сумме за год превышающих 700 тыс. руб.;
- возможное приостановление отдельных операций, приостановление деятельности;
- всплеск негативных отзывов со стороны клиентов/контрагентов в размере, превышающем 70% от среднего значения количества негативных публикаций за предыдущий год;
- Негативная информация в прессе в отношении руководства Биржи;
- Финансовый убыток, превышающий предельное, установленное на текущий год значение для соответствующего вида риска;
- Нарушение работоспособности ключевых систем Биржи;
- Нарушение сроков реализации ключевых стратегических направлений на срок 12 и более месяцев;
- Существенное увеличение стоимости реализации ключевых стратегических направлений;
- Существенное снижение доходности реализуемых стратегических направлений;
- Существенное снижение доходности по ключевым продуктам Биржи;
- Существенные утечки информации, успешные атаки на ключевые системы Биржи;
- Иные последствия, способные оказать существенное негативное влияние на деятельности Биржи.

Для сопоставления результатов оценки выявленных рисков Биржи с указанными критериями Биржа придерживается следующего порядка:

- Реализует в течение календарного года мероприятия, направленные на выявление рисков;
- Проводит оценку факторов и потенциальных последствий выявленных рисков;
- Проводит моделирование возможных и вероятных исходов реализации выявленных рисков;
- Осуществляет анализ и измерение потенциального влияния последствий реализации выявленных рисков;

- Сопоставляет полученные результаты с критериями существенности последствий, приведенными в настоящих Правилах.

- Если результат оценки выявленных рисков демонстрирует соответствие критериям существенности последствий, принимается решение о признании рисков значимыми.

4 Методика определения предельного размера рисков (допустимого уровня рисков) Биржи, а также совокупного предельного размера рисков Биржи

В целях определения предельного уровня риска, а также совокупного предельного размера рисков Биржа использует следующие подходы:

4.1. Оценка размера реализации риска на исторических данных и установление предельных показателей на уровне средних значений за несколько предшествующих лет. Оценка размера реализации риска на исторических данных базируется на серии последовательно взятых в определенном периоде годовых показателях, в качестве такого временного периода используется период равный 10 годам.

4.2. Проведение сценарного анализа по наиболее вероятным сценариям реализации риска и установление показателей на уровне полученных значений;

4.3. Проведение оценки влияния потенциальных убытков на финансовые результаты Биржи и установление предельных показателей исходя из размера потенциального убытка, при котором отсутствует влияние на реализацию стратегических инициатив Биржи;

4.4. Проведение стресс-тестирований риска, с целью установления предельных ожидаемых убытков от реализации риска;

4.5. Для определения совокупного предельного размера риска используется подход, при котором используются реалистичные сценарии оценки потерь от совместной реализации одного или нескольких выявленных рисков. При этом реализация рисков не должна приводить к нарушению финансовой устойчивости Биржи.

Предельные показатели риска устанавливаются Наблюдательным советом Биржи на каждый календарный год.

5 Порядок выявления нарушений ограничений рисков

Для выявления нарушений ограничений рисков осуществляется мониторинг соблюдения установленных уровней количественных и качественных показателей риск-аппетита, которые рассчитываются ежемесячно подразделениями, ответственными за управление отдельными видами рисков, и консолидируются ДОРИБиНБ. Выявление нарушений ограничений рисков происходит в следующем порядке:

- Работник структурного подразделения, ответственного за управление риском, проводит анализ случаев реализации риска по факту их обнаружения, оценивает уровень риска, наличие нарушений пороговых значений, причины нарушений и последствия;
- В случае выявления нарушений установленных ограничений рисков работник инициирует разработку планов и мероприятий по снижению негативных последствий совместно с ответственными подразделениями, а также по снижению уровня риска или исключению риска, или пересмотру установленных ограничений;
- В случае превышения установленных ограничений (пороговых значений) риск-аппетита информация выносится на заседание Наблюдательного совета Биржи.

По результатам мониторинга риск-аппетита формируется отчет, представляемый Директором ДОРИБиНБ на рассмотрение Правления ежемесячно и Комиссии по управлению рисками Наблюдательного совета ежеквартально. Отчет содержит информацию о перечне показателей риск-аппетита, уровне риска на отчетную дату, информацию о выявленных нарушениях ограничений риска и мероприятиях по их устранению и снижению уровня риска (при необходимости).

По факту реализации рисков, влияющих на пороговые значения риск-аппетита, принимаются решения в отношении мер, необходимых для снижения отдельных рисков, оказывающих влияние на уровень рисков Биржи.

6 Порядок осуществления мероприятий по устранению выявленных нарушений ограничений рисков и (или) иных мероприятий в отношении рисков Биржи в рамках снижения таких рисков Биржи или их исключения

При выявлении нарушения ограничения риска, а также в рамках снижения или исключения рисков, работники подразделения, ответственного за управление рисками Биржи, придерживаются следующего порядка:

6.1. Определяют причину нарушения ограничения риска или определяют факторы, которые могут способствовать реализации выявленного риска;

6.2. Определяют возможные последствия, которые могут возникнуть вследствие реализации такого риска;

6.3. Определяют работников Биржи, ответственных за область возникновения факторов риска и за область последствий реализации риска;

6.4. Разрабатывают с работниками, указанными в предыдущем пункте, набор мероприятий, направленных на устранение факторов риска, либо мероприятий, направленных на снижение тяжести последствий реализации риска, либо мероприятий, направленных на исключение риска;

6.5. Согласовывают с руководителями структурных подразделений Биржи ответственных и сроки реализации указанных мероприятий;

6.6. Осуществляют регулярный контроль за сроками и фактом выполнения назначенных мероприятий;

6.7. При необходимости формируют отчетность по статусу выполнения мероприятий для коллегиальных органов управления Биржи.

7 Порядок осуществления процессов и мероприятий по выявлению, анализу, мониторингу риска, и обмену информацией между подразделениями и органами управления Биржи, а также порядок осуществления процессов и мероприятий, осуществляемых Биржей в рамках управления отдельными видами рисков Биржи

7.1. Выявление рисков Биржи.

Порядок выявления рисков:

- Каждый работник Биржи обязан информировать о рисках ДОРИБиНБ в момент их обнаружения;
- ДОРИБиНБ осуществляет сбор сведений о рисках (как внутренних, так и внешних), способных нанести Бирже ущерб, их факторах, о возможности/вероятности возникновения рисков в деятельности Биржи и о размере ущерба (ожидаемом, наихудшем, наиболее частом и т.д.);
- ДОРИБиНБ может привлекать УФР, ЮД, СВК, ДВКиК и иные структурные подразделения для определения видов риска;
- ДОРИБиНБ осуществляет самооценку операционного риска. Самооценка проводится в формате интервью или анкетирования ответственных подразделений на регулярной основе, но не реже одного раза в год;
- ДОРИБиНБ осуществляет диагностику бизнес-процессов, анализ пересечений в полномочиях и ответственности подразделений и работников Биржи;
- Различными структурными подразделениями проводится анализ результатов внутреннего и внешнего аудита контролей/процедур/систем;
- Подразделениями риск-менеджмента проводится анализ новых продуктов, процессов, систем, проектов и непроектных задач (анализ всех нововведений, проводимых Биржей: изменения структуры и процедур, внедрение новых услуг и технологий, освоение новых направлений деятельности и т. п.);

- Подразделениями риск-менеджмента проводится анализ рисков новых стратегий и изменений в действующих.

7.2. Анализ и оценка рисков Биржи.

Для анализа и оценки рисков используются, в том числе, следующие методы:

- сценарный анализ. В рамках сценарного анализа проводится идентификация угроз, которые по оценке Биржи могут привести в том числе к неработоспособности средств проведения торгов;
- статистическая и аналитическая обработка информации, содержащейся в БДР и внешней БДСОР, на базе которой производится оценка влияния рисков Биржи на его финансовую устойчивость посредством оценки событий риска, наступление которых, в том числе с учетом вероятности их наступления и степени влияния, повлечет за собой возникновение убытков;

- для выявления (идентификации), анализа и оценки операционных рисков используется также стресс-тестирование программно-технических средств, используемых для осуществления деятельности по Организации торгов и обмену цифровых финансовых активов, с периодичностью, определенной внутренними документами Биржи, но не реже одного раза в 6 месяцев.

Порядок оценки:

- выявление факторов и источников риска, определение видов риска;
- анализ сведений о риске (как внутренних, так и внешних), способных нанести Бирже ущерб, о возможности/вероятности возникновения риска в деятельности Биржи, о размере ущерба/убытка (убытков) (ожидаемом, наихудшем, наиболее частом и т. д.);
- сопоставление результатов оценки выявленных рисков с установленными критериями существенности в соответствии с п.3 настоящих Правил;
- установление предельного размера рисков, а также совокупного предельного размера рисков в соответствии с п.4 настоящих Правил;
- анализ сведений о применяемых контролях на основе экспертного суждения работников структурных подразделений Биржи в рамках выполняемых ими функций и задач;
- оценка рисков продукта осуществляется при открытии проекта на всех последующих фазах жизненного цикла проекта. Оценка рисков продуктов является обязательным этапом запуска любого проекта и осуществляется по нефинансовым и финансовым рискам в отношении всех проектов, и включает в себя:

  - описание влияния будущего продукта на рискозащищенность Биржи, на которую он оказывает воздействие по полному списку финансовых и нефинансовых рисков;
  - оценку нефинансовых рисков и стоимостную оценку рисков будущего продукта;
  - оценку влияния рисков на деятельность Биржи;
  - оценку размера возможных потерь по видам присущих продукту рисков;

- оценку доходности продукта с учетом принимаемых рисков в отношении доходных проектов. Результатом оценки является Заключение о рисках продукта, которое принимается во внимание Правлением при принятии решений в отношении продукта проекта.

7.3. Мониторинг, контроль и снижение рисков Биржи или их исключение.

Мониторинг - система мероприятий, направленных на периодический сбор и анализ информации об изменении уровня риска.

Порядок мониторинга рисков Биржи включает:

- отслеживание изменений уровня риска в подразделениях Биржи;
- оперативное реагирование на изменения уровня риска в подразделениях Биржи с целью снижения уровня риска;
- своевременное осуществление действий, направленных на снижение уровня риска до приемлемого.

Биржа в рамках мониторинга, контроля и снижения рисков или их исключения выполняет следующие мероприятия:

- определяет уровень рисков Биржи, в том числе на предмет соответствия установленным Биржей ограничениям рисков;
- разрабатывает и осуществляет мероприятия по устранению выявленных нарушений ограничений рисков и мероприятия по снижению рисков или их исключению. Биржа в отношении значимых рисков разрабатывает внутренние документы, содержащие план мероприятий по снижению рисков или их исключению. Данные мероприятия, а также статусы исполнения по ним регулярно доводятся до уполномоченных органов управления Биржи:
  - мероприятия в отношении рисков проекта,продукта, стратегий доводятся до сведения Правления;
  - мероприятия по снижению рисков, связанных с нарушением риск-аппетита, доводятся до Правления, Комиссии по управлению рисками Наблюдательного совета,Наблюдательного совета;

- мероприятия в рамках существенных событий риска доводятся до единоличного исполнительного органа, Правления и Комиссии по управлению рисками Наблюдательного совета и могут быть доведены до Наблюдательного совета по усмотрению руководителя Комиссии по управлению рисками Наблюдательного совета.

Для осуществления мониторинга рисков Биржи внедрены ключевые индикаторы риска - показатели деятельности Биржи (в том числе статистические, финансовые), посредством которых осуществляется учет событий операционного и иных видов риска, установлены пороговые для этих показателей значения, по которым проводится оценка вероятности повторного возникновения указанных событий.

Ключевыми индикаторами риска (далее - КИР) являются:

- показатели, характеризующие частоту и уровень влияния событий операционного и иных видов рисков, произошедших в течение отчётного периода;
- показатели, которые позволяют осуществлять мониторинг результативности установленных процедур контроля в бизнес-процессах и оценивать связанные с этим риски;
- показатели, которые позволяют оценить масштаб того или иного направления деятельности Биржи или отдельного бизнес-процесса, в целях определения уровня/степени их подверженности рискам.

Для каждого КИР определяются пороговые значения - численные показатели, отражающие предельно допустимые значения индикатора, отклонение от которых может указывать на рост возможности реализации события риска, что указывает на необходимость предпринять организационные меры по контролю и/или меры, направленные на минимизацию возможности реализации риска. Порядок мониторинга риска посредством КИР включает в себя следующие действия:

- разработка реестра КИР (включая описание, ответственных лиц, периодичность мониторинга);
- установление пороговых значений в реестре КИР;
- сбор данных по КИР за отчетный период и анализ полученных значений;

- формирование отчета органам управления Биржи, содержащего предложения по разработке мероприятий, основываясь на текущих показателях КИР (в случае необходимости);
- отслеживание выполнения мероприятий по снижению риска (в случае необходимости);
- периодический пересмотр реестра КИР.

Контроль рисков осуществляется ДОРИБиНБ и подразделениями, ответственными за управление отдельными видами рисков, путем реализации следующих мер:

- на ежедневной основе контролируется общий уровень риска и своевременность выполнения мероприятий по реагированию ответственными лицами посредством их мониторинга;
- ДОРИБиНБ на ежегодной основе контролирует реализацию мероприятий в рамках выявленных и/или реализовавшихся операционных рисков;
- СВК проводит регулярные тематические проверки;
- УФР осуществляет контроль казначейских лимитов и иных показателей уровня финансовых рисков, выполняет предварительные согласования и проверки при принятии на обслуживание клиентов, заключении соглашений с контрагентами, допуске к торгам ценных бумаг, запуске новых продуктов/услуг, а также в ряде других случаев;
- ДВКиК выполняет предварительные согласования и проверки при принятии на обслуживание клиентов, заключении соглашений с контрагентами, допуске к торгам ценных бумаг, запуске новых продуктов/услуг, а также в ряде других случаев, организует автоматизированные контроли, в том числе для проверки лиц по спискам комплаенс, обеспечивает наличие политик и процедур, проводит обязательное обучение;
- ЮД – осуществляет всесторонний анализ причин возникновения правового риска, а также обеспечивает предупреждение возникновения событий правового риска, реализации факторов возникновения риска.
- ДК изучает и анализирует показатели деятельности Биржи; осуществляет мониторинг жалоб и претензий к компании, в том числе относительно качества обслуживания клиентов и контрагентов, соблюдения обычаев делового

оборота; а также позитивных и негативных отзывов и сообщений в СМИ об акционерах и аффилированных лицах.

- ДС разрабатывает проекты изменений в порядок осуществления деятельности по проведению организованных торгов или связанной с проведением организованных торгов деятельности, предоставления дополнительных услуг, допуска к организованным торгам новых финансовых инструментов, а также иных организационных и (или) технологических изменений;
- осуществляет анализ целесообразности внедрения проектов изменений;
- оценивает стратегию развития Биржи на предмет определения возможности и целесообразности ее реализации, а также внесение изменений в стратегию развития Биржи в случае принятия Биржей указанного решения.
- ПО обеспечивает анализ возможных событий или условий, наступление которых может отрицательно сказаться на параметрах проекта (срок, содержание, бюджет/лимит финансирования проекта), разрабатывает мероприятия по предотвращению реализации риска.
- независимый контроль за реализацией всех мероприятий по управлению рисками осуществляется СВА с периодичностью не реже, чем раз в три года и (или) внепланово, а также внешними аудиторами и регулирующими органами.

Снижение рисков осуществляется путем реализации мероприятий:

- страхование;
- автоматизация контрольных процедур и процессов;
- реализация контроля полномочий в рамках управления риском информационной безопасности;
- реализация принципа «четырех глаз»;
- регламентация внутренних процессов;
- установление системы лимитов и их мониторинга;
- резервирование информации;
- обучение персонала и применение мотивационных программ.

Исключение рисков Биржи заключается в отказе от совершения определенного вида деятельности и/или проекта, создающего риск.

Биржа может принимать риски в своей деятельности, т. е. реализовывать свою деятельность по ряду направлений, не предпринимая мер по минимизации и (или) исключению риска. Решение о принятии риска принимает уполномоченный орган управления Биржи и (или) руководители структурных подразделений в рамках своих полномочий.

Мероприятия по финансовым рискам в рамках данных направлений отражены в Политике по финансовым рискам.

7.4. Обмен информацией о рисках Биржи между подразделениями Биржи, между подразделениями Биржи и органами управления Биржи.

Обмен информацией о рисках Биржи между подразделениями Биржи и органами управления Биржи осуществляется путем предоставления регулярных и внеплановых (оперативных) отчётов о рисках.

Биржей установлен следующий порядок предоставления информации по вопросам управления рисками работникам Биржи:

- В отношении анализа событий риска, оценки уровня риска и статусов выполнения мероприятий по минимизации риска проводятся совещания в рамках рабочих групп с обязательным участием в следующем порядке:

  - Работник ДОРИБиНБ назначает встречи с периодичностью не реже одного раза в месяц работникам и руководителям структурных подразделений, задействованных в процессе реализации мероприятий по минимизации риска;
  - Проводится анализ и обсуждение произошедших за отчетный месяц событий операционного риска;
  - Осуществляется анализ статуса выполнения мероприятий по событиям, идентифицированным в предыдущих периодах;
  - Отчет о результатах проведенного нагрузочного тестирования предоставляется ДОРИБиНБ ответственным структурным подразделениям Блока информационных технологий в срок не позднее 10 дней с даты формирования отчета.

Если иное не определено во внутренних документах Биржи:

- сроки информирования работников и предоставление отчётности структурным подразделениям Биржи о рисках определяются Директором ДОРИБиНБ, на основе его профессионального суждения, формируемого с учётом оценки риска, потребностей Биржи, величины того или иного риска и принципа существенности;

- сроки и форма предоставления информации работниками Биржи определяются в соответствующих запросах Директора ДОРИБиНБ.

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

Меры включают в себя мероприятия, перечисленные в «Порядке принятия Организатором торговли мер по предотвращению и урегулированию конфликта интересов, возникающего у Биржи в связи с совмещением им своей деятельности с иными видами деятельности», а также анализ бизнес-процессов, проводимый ДОРИБиНБ, в рамках самооценки рисков.

7.6. Определение перечня требующих защиты от противоправных действий программно-технических средств Биржи, сбои и (или) ошибки в функционировании которых способны повлечь за собой приостановление или прекращение оказания услуг по проведению организованных торгов в полном или неполном объеме и (или) оказать иное неблагоприятное воздействие на деятельность Биржи.

Порядок определения перечня включает следующие мероприятия:

1) Перечень программно-технических средств Биржи составляется с учетом критичности систем и времени, необходимого для восстановления, в случае сбоя и/или ошибки;
2) Все программно-технические средства Биржи подразделяются на несколько групп в зависимости от уровня требований к надежности их функционирования;
3) Определяются следующие группы надежности:
    - Группа А – критичные:

- 1А – торговые системы и иные системы, как системы реального времени;
- 2А – основные системы обработки данных;
- 3А – прочие критичные системы обработки данных с более низкими требованиями к временным параметрам восстановления.

- Группа В – ответственные;
- Группа С – некритичные (офисные системы, системы разработки ПО ТКС, игровые, обучающие системы и др.).

4) Отнесение системы обработки данных (входящей в ее состав задачи) к группе надежности осуществляется по методике, основанной на анализе бизнес-процессов, и утверждается решением Архитектурного комитета. Системе (входящей в ее состав задачи), по тем или иным причинам не отнесенной к группе надежности по умолчанию присваивается группа С.
5) Определение характеристик группы надежности, которыми являются:

- Коэффициент доступности входящих в группу прикладных систем;
- Требования к изоляции и оснащению контуров, входящих в группу прикладных систем;
- Временные показатели восстановления входящих в группу прикладных систем, определяемые по программе обеспечения непрерывности деятельности, а именно:
  - Целевое время восстановления;
  - Допустимый диапазон потери данных.

6) Для каждой из групп систем устанавливаются коэффициенты доступности. Для обеспечения высокой доступности функциональных систем Биржи широко применяется резервирование, реализованное на всех уровнях структурной иерархии, начиная с физических компонентов, серверов, сетей и систем хранения и кончая резервированием на уровне прикладного программного обеспечения, сетевой инфраструктуры и системы Центра обработки данных Биржи (далее – ЦОД).

7.7. Определение перечня и реализация мер по защите информации.

Деятельности Биржи свойственен операционный риск, связанный с нарушением безопасности информации, что является объективной реальностью, и понизить этот

риск можно лишь до определенного остаточного уровня. Для управления операционным риском, связанным с безопасностью информации, Биржа обеспечивает:

- идентификацию и учет объектов информатизации;
- применение на различных уровнях информационной инфраструктуры, выбранных Биржей, мер защиты информации, направленных на непосредственное обеспечение защиты информации;
- применение выбранных Биржей мер защиты информации, обеспечивающих приемлемые для Биржи полноту и качество защиты информации, входящих в систему организации и управления защитой информации;
- применение выбранных Биржей мер защиты информации, направленных на обеспечение защиты информации на всех стадиях жизненного цикла автоматизированных систем;
- оценку остаточного уровня операционного риска, вызванного неполным или некачественным выбором и применением мер защиты информации, и обработку указанного риска;

Вышеперечисленный перечень мер, предпринимается Биржей также для обеспечения конфиденциальности и защиты информации о рисках Биржи, а также информации, предоставляемой Биржей поставщику услуг.

Снижение операционного риска, связанного с нарушением информационной безопасности, обеспечивается путем надлежащего выбора, повышения полноты и качества применения соответствующих мер защиты информации. Полнота и качество применения мер защиты информации достигается планированием, реализацией, проверкой и совершенствованием процессов управления рисками информационной безопасности, а также применением мер защиты информации на этапах жизненного цикла автоматизированных систем и приложений.

Оценка остаточного операционного риска, связанного с неполным или некачественным применением мер защиты информации, входящих в систему защиты информации, осуществляется в соответствии с процедурой, определенной требованиями законодательства, на основе оценки показателей соответствия реализации системы защиты информации Биржи требованиям Национального

стандарта Российской Федерации «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

Порядок определения перечня и реализация мер по защите информации, осуществляемых в рамках соответствия требованиям законодательства, включает следующие мероприятия:

- ДОРИБиНБ совместно с ответственными структурными подразделениями разрабатывает и утверждает внутренние документы, предусматривающие осуществление контрольных мероприятий по защите информации;
- ДОРИБиНБ совместно с ответственными структурными подразделениями внедряет средства защиты информации и осуществляет контрольные мероприятия, направленные на обеспечение средствами защиты информации.

  Перечень мер по защите информации включает:
- повышение вовлеченности и осведомленности работников Биржи в вопросах выявления нарушений требований по защите информации и противодействия реализации информационных угроз;
- обеспечение защиты информации при управлении доступом и регистрацией;
- обеспечение защиты информации на этапах жизненного цикла автоматизированных систем;
- обеспечение защиты информации средствами антивирусной защиты;
- обеспечение защиты информации при использовании ресурсов информационно-телекоммуникационной сети «Интернет», обеспечение защиты вычислительных сетей в целом;
- контроль целостности и защищенности информационной инфраструктуры;
- предотвращение утечек информации;
- обеспечение процедур безопасности и контроля (криптография, кодирование, защита от несанкционированного доступа во время передачи или хранения информации, ограничивающее доступ к данным программное обеспечение, аутентификация и авторизация участников и пользователей) в том числе при удаленной работе;
- обеспечение защиты информации при назначении и распределении ролей;

- регламентация и документирование деятельности по обеспечению защиты информации, включая порядок регистрации и хранения информации;
- обнаружение инцидентов информационной безопасности, в том числе инцидентов в отношение критичной архитектуры, и реагирование на них;
- мониторинг и анализ обеспечения защиты информации, проведение анализа причин и последствий реализации инцидентов;
- своевременное совершенствование средств обеспечения защиты информации, использование информации об актуальных сценариях реализации информационных угроз для цели обеспечения операционной надежности Биржи;
- обеспечение долгосрочного планирования информационных и компьютерных систем, спецификации требований к ним, выбора поставщиков и контроля за проектами создания систем и технологий обработки и передачи данных для Биржи;
- организацию взаимодействия Биржи и причастных сторон, в том числе клиентов Биржи при обмене информацией об актуальных сценариях реализации информационных угроз;
- обеспечение доступа персонала только к сведениям, необходимым для выполнения прямых служебных обязанностей в пределах предоставленных полномочий;
- ограничение доступа путем использования возможностей программного обеспечения;
- наличие систем разграничения доступа к разным уровням баз данных и операционной среды на уровне локальной сети;
- обеспечение процедур бесперебойного функционирования программно-технических средств Биржи, используемых для осуществления деятельности по организации торгов, и процедур восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов, в том числе:
  - наличие полностью резервированной архитектуры вычислительного комплекса, не содержащей нерезервированных точек отказа и обладающей устойчивостью к некратным аппаратным отказам любого

типа компонентов, способных обеспечить функционирование основных электронных систем, используемых Биржей;

- наличие резервных каналов связи;
- наличие поддерживаемого в актуальном состоянии плана действий при возникновении необходимости использования резервных мощностей и компонентов вычислительного центра и регулярной практической отработки мероприятий, предусмотренных этим планом;
- порядок восстановления работоспособности нарушенных внутренних процессов и систем и возврата к режиму нормальной работы;
- наличие встроенных в прикладные системы решений, обеспечивающих распределение нагрузки и взаимное дублирование на уровне серверов доступа и основных серверов обработки данных;
- использование в качестве платформы для наиболее критичных задач высоко доступных кластеров со встроенным дублированием основных компонентов;
- использование телекоммуникационных устройств со штатным дублированием основных блоков;
- использование для хранения баз данных и другой критичной информации устройств хранения данных с полностью резервированной архитектурой;
- наличие и неукоснительное выполнение процедур регулярного (не реже 1 раза в сутки) резервного копирования всех критичных данных, предусматривающих хранение и регулярное обновление резервных копий;
- наличие регламентированных процедур восстановления;
- наличие резервных универсальных рабочих мест;
- наличие в помещении вычислительного центра автоматической системы пожаротушения;
- наличие круглосуточного мониторинга состояния вычислительных и телекоммуникационных ресурсов, помещений вычислительного центра Биржи;
- перераспределение функций, полномочий и обязанностей подразделений и работников;

- меры по поддержанию адекватного информационного обеспечения, оценку готовности к чрезвычайной ситуации внешних поставщиков информационных услуг.

- организация взаимодействия между подразделениями Биржи, а также между Биржей и Банком России, причастными сторонами в рамках реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов.

Применяемые Биржей меры по определению политики управления риском информационной безопасности обеспечивают:

- установление структуры и организации системы управления риском информационной безопасности, а также распределение функций, ролей и ответственности в рамках управления риском информационной безопасности;
- управления риском информационной безопасности;
- участие Наблюдательного совета ПАО Московская Биржа и исполнительных органов Биржи в решении вопросов управления риском информационной безопасности.

Применяемые Биржей меры по оценке риска информационной безопасности обеспечивают:

- идентификацию критичной архитектуры;
- идентификацию риска информационной безопасности;
- выявление и моделирование информационных угроз;
- оценку риска информационной безопасности.

Применяемые Биржей меры по разработке мероприятий, направленных на уменьшение негативного влияния риска информационной безопасности, обеспечивают:

- выбор и применение способа реагирования на риск информационной безопасности;

- разработку мероприятий, направленных на снижение степени вероятности реализации риска информационной безопасности;
- разработку мероприятий, направленных на ограничение степень тяжести последствий реализации риска информационной безопасности.

Применяемые Биржей меры по защите от реализации риска информационной безопасности обеспечивают:

- защиту информации Биржи;
- Операционную надежность;
- управление риском реализации риска информационной безопасности при взаимодействии с поставщиками услуг;
- управление риском внутреннего нарушителя;
- управление риском информационной безопасности в финансовой экосистеме.

Применяемые Биржей меры по организации ресурсного (кадрового и финансового) обеспечения обеспечивают:

- организацию ресурсного (кадрового и финансового) обеспечения процессов системы управления риском информационной безопасности;
- организацию ресурсного (кадрового и финансового) обеспечения функционирования ДОРИБиНБ.

В случае возникновения в информационной инфраструктуре Биржи зафиксированных нештатных ситуаций (аварий или существенного снижения функциональности компонентов информационной инфраструктуры), при которых временно отсутствует техническая возможность применения всех мер защиты информации, входящих в систему защиты информации, Биржа предусматривает осуществление работниками Биржи действий, направленных на выполнение своих служебных обязанностей в условиях отсутствия применения отдельных мер защиты информации, а также должный контроль указанных действий.

Меры защиты информации, входящие в систему защиты информации, реализуются в том числе для обеспечения защиты:

- резервных копий ресурсов доступа, баз данных и архивных хранилищ информации;
- информации, обрабатываемой на виртуальных машинах, а также при реализации технологии виртуализации.

При хранении и обработке информации и документов, связанных с организацией торгов на рабочих станциях и серверах функционирует система разграничения доступа, позволяющая предоставлять доступ к данным только авторизованным работникам и препятствовать несанкционированному доступу со стороны всех остальных работников и посторонних лиц. Эта система функционирует как на уровне системных и сетевых средств, так и в приложениях, используемых Биржей.

Биржей определены, выполняются, регистрируются и контролируются правила и процедуры мониторинга доступа к информации, анализа и хранения данных о действиях и операциях работников, направленные на реализацию мер, предусмотренных процессом «Обеспечение защиты информации при управлении доступом» ГОСТ Р 57580.1-2017.

Биржей реализовано ведение журналов действия и операций автоматизированных рабочих мест, серверного и сетевого оборудования, межсетевых экранов с целью их использования при реагировании на инциденты с информацией и документами.
Процедуры мониторинга информации и анализа данных о действиях и операциях используют зафиксированные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга и анализа применяются на регулярной основе ко всем выполненным действиям и операциям.

7.8. Осуществление контроля прав доступа работников Биржи к программно-техническим средствам Биржи.

Порядок осуществления контроля прав доступа работников Биржи к программно-техническим средствам:

- Мониторинг прав доступа пользователей к Информационной системе (далее - ИС) проводится регулярно, но не реже одного раза в 12 месяцев;
- Внеплановый мониторинг прав доступа к ИС Биржи может проводиться в случае возникновения инцидента ИБ и иных обстоятельств, требующих

пересмотра предоставленных прав доступа по инициативе работника ДОРИБиНБ;

- Мониторинг прав доступа пользователей к ИС осуществляется в следующем порядке:
  - работник ДОРИБиНБ запрашивает у администраторов соответствующих ИС список всех существующих в ИС незаблокированных учетных записях и их правах доступа;
  - из полученного списка учетных записей каждой из проверяемых ИС, работник ДОРИБиНБ случайным образом выбирает несколько учетных записей для дальнейшей проверки их прав доступа. В указанную выборку должны попадать только те учетные записи, которые еще не подвергались проверке в предыдущие периоды;
  - работник ДОРИБиНБ запрашивает у администраторов системы регистрации заявок на предоставление прав доступа заявки, имеющиеся в данной системе, на предоставление прав доступа пользователям из указанной выборки;
  - работник ДОРИБиНБ проверяет предоставленные данные с целью выявления наличия прав доступа, не подтвержденных соответствующими заявками;
  - в случае выявления нарушений работник ДОРИБиНБ инициирует процесс изучения их причин и выбора соответствующих корректирующих мер. Кроме того, по всем фактам несоответствия проводится служебное расследование в соответствии с внутренними документами по информационной безопасности;
  - работник ДОРИБиНБ, проводивший мониторинг, документирует его результаты.

7.9. Определение перечня и реализация мер, направленных на обеспечение предоставления Бирже участниками торгов и их клиентами, а также иными контрагентами Биржи информации о событиях операционного риска участников торгов и их клиентов, связанных с их участием в организованных торгах.

Порядок определения мер, направленных на обеспечение предоставления Бирже участниками торгов и их клиентами, а также иными контрагентами Биржи информации

о событиях операционного риска участников торгов и их клиентов, связанных с их участием в организованных торгах:

- Биржа организует горячую линию для участников торгов и принимает обращения в техническую поддержку в случае технических сбоев, возникающих на стороне участников торгов;
- Биржа оказывает поддержку по восстановлению работы средств проведения торгов в случае проблем на стороне участников торгов;
- Биржа эскалирует ситуацию в случае, если проблемы представляются признаком технического сбоя на стороне Биржи;
- Биржа инициирует последующее обсуждение, подтверждение мер, направленных на недопущение повторения технических проблем на Информационно-технологическом комитет.

  Перечень мер, направленных на обеспечение предоставления Бирже участниками торгов и их клиентами, а также иными контрагентами Биржи информации о событиях операционного риска участников торгов и их клиентов, связанных с их участием в организованных торгах:
- Включение в регламентные документы определенных требований к ВПТС, сопрягаемым с системами Биржи, положения о необходимости оперативного информирования о случаях реализации рисков;
- Поддержание каналов взаимодействия и оперативного информирования с участниками торгов, их клиентами и контрагентами в целях организации сбора информации по факту выявленных событий операционного риска и мерах, предпринимаемых в целях снижения степени негативного влияния риска;

7.10. Осуществление мониторинга использования участниками торгов средств проведения торгов.

Порядок осуществления мониторинга использования участниками торгов средств проведения торгов включает следующее:

- Мониторинг ТКС в целом и отдельных ее элементов, включая параметры подключения клиентов. Процесс восстановления системы мониторинга ТКС идентичен процессу восстановления самой системы;

- В случае, если количество клиентов резко меняется, работник ответственного подразделения, именуемый как Вспомогательный Дежурный работник, по соответствующей системе следует специальным инструкциям, которые разработаны в разрезе каждого класса проблем. Инструкции подлежат постоянному обновлению по результатам текущей эксплуатации, анализа разноплановых ситуаций и т.д;
- Прохождение сертификации любой ВПТС;
- Мониторинг количества соединений и поведения участника торгов на наличие большого количества ошибочных транзакций;
- Если зафиксирована нештатная ситуация, которая не соответствует нормальному поведению участника торгов, то она эскалируется Дежурным работником по соответствующей системе на ДОДа и ДКП, которые совместно решают возникшую проблему. ДКП, в свою очередь, связывается с клиентом для разъяснения проблемы. ДСТиВС имеет право инициировать процедуру отключения торгов для данного клиента в соответствии с Правилами допуска к участию в организованных торгах ПАО Московская Биржа, если не получилось связаться с клиентом или, если после разъяснения проблемы клиенту, проблема не решилась.
- Если зафиксирована потеря соединения, которая не входит в рамки торгового режима, то происходит анализ количества потерянных соединений и оценивается необходимость приостановки торгов (в случае если количество потерянных соединений составляет более 50% от их общего числа). Данная проблема эскалируется подразделениям, ответственным за ее разрешение, разрабатывается план действий;
- Мониторинг качества соединения участников торгов к ВПТС, который осуществляется на стороне провайдера.

7.11. Определение перечня требований к программно-техническим средствам, используемым участниками торгов и их клиентами при подключении к средствам проведения торгов.

К подключению к промышленной среде допускаются только ВПТС участников торгов, прошедшие на тестовом контуре сертификацию на соответствие предъявляемым

требованиям к функционалу систем, а также соответствующие требованиям к подключению к программно-техническому комплексу Биржи.

7.12. Устранение недостатков в работе средств проведения торгов, выявленных в результате проведения испытательных работ (тестирования) средств проведения торгов.

- По итогу проведения испытательных работ (тестирования) средств проведения торгов составляется Протокол испытательных работ с указанием результатов его проведения и выявленных недостатков;
- В случае выявления недостатков они фиксируются в систему Jira с присвоением им тикета. Тикет назначается на тот или иной релиз, либо не назначается и выносится backlog. Ответственность за сбор backlog лежит на Руководителе разработки соответствующей системы;
- Выявленные недостатки в работе средств проведения торгов ранжируются по уровню критичности: critical, high, major, minor и недостатки с отсутствием влияния;
- Присвоенные уровни согласовываются с командой разработки, которая далее принимает решение по плану действий для каждого выявленного недостатка и определения приоритетности их устранения. Недостатки, которым были присвоены уровни critical и high, устраняются в первую очередь;
- В случае если недостатки с уровнем critical были выявлены на этапе тестирования, то релиз не выводится до момента их устранения. В таком случае может быть принято решение о невключении в релиз задачи, которая содержит в себе недостатки с уровнем critical, либо перенесении срока релиза на дату, когда соответствующие недостатки будут устранены. Все критические недостатки докладываются на Ресурсном комитете (далее – РК);
- Статус хода тестирования рассматривается на каждом РК на еженедельной основе;
- Также при выявлении недостатков в ВПТС и/или средствах мониторинга данные инциденты эскалируются ДОРИБиНБ и входят в состав отчетности в качестве события операционного риска, статус по которым отслеживается на ежемесячной основе.

7.13. Ведение базы данных о событиях операционного риска Биржи осуществляется по следующим видам событий операционного риска Биржи:

- события, влекущие за собой приостановление или прекращение осуществления процессов Биржи, приостановление или прекращение которых вызывает нарушение порядка осуществления Биржей деятельности по организации торгов, в том числе приостановление или прекращение организованных торгов, как в отношении отдельного финансового инструмента, иностранной валюты, товара, так и в отношении всех указанных инструментов (далее - критически важные процессы Биржи), в том числе чрезвычайные ситуации (далее - существенные события операционного риска);
- события операционного риска, не относящиеся к существенным событиям операционного риска, но по оценке Биржи оказывающие негативное влияние на порядок и условия осуществления критически важных процессов Биржи, в том числе на подачу заявок, возможность заключения договоров на организованных торгах в отношении более чем пятнадцати процентов участников торгов или их клиентов от общего числа зарегистрированных на соответствующей торговой (биржевой) секции участников торгов или их клиентов соответственно (далее - значимые события операционного риска);
- события операционного риска, не относящиеся к существенным событиям операционного риска и значимым событиям операционного риска (далее-события низкого уровня влияния).

Помимо этого в БДСОР содержатся события, которые не являются событиями операционного риска, подпадающими под определения существенных, значимых событий или событий низкого уровня влияния, и не оказывают влияния на деятельность Биржи, но потенциально способных привести к реализации событий операционного риска.

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

- Все новые работники Биржи перед тем, как приступить к работе, проходят обучение по вопросам выявления, оценки и снижения операционного риска в обязательном порядке;
- Директор ДОРИБиНБ проводит углублённое обучение работников Биржи по вопросам управления операционным риском, адаптированное для конкретных фокус-групп (в зависимости от функций подразделения);
- Обязательным для отдельных работников Биржи является прохождение электронных курсов, которые являются всегда доступными на общем корпоративном портале;
- ДОРИБиНБ осуществляет мониторинг статистики прохождения обучения с периодичностью не реже одного раза в месяц.

7.15. Осуществление мероприятий по замене или улучшению (обновлению) программно-технических средств Биржи в случае выявления их несоответствия характеру и объему совершаемых Биржей операций.

С целью выявления необходимости замены и/или улучшения (обновления) программно-технических средств Биржи на ежегодной основе проводятся нагрузочные тестирования, по итогу которых в случае выявления несоответствия реализуется набор мер, заключающихся в оценке необходимости обновления ПО и реализации мероприятий по его обновлению.

Порядок осуществления мероприятий по замене или улучшению (обновлению) программно-технических средств Биржи в случае выявления их несоответствия характеру и объему совершаемых Биржей операций включает:

- Регулярный мониторинг работоспособности программно-технических средств Биржи;
- Ежегодное нагрузочное тестирование программно-технических средств Биржи;
- Анализ и мониторинг и реализация мер по обновлению программно-технических средств Биржи. При обнаружении несоответствия характеру и объему совершаемых Биржей операций осуществляется доработка или закупка программно-технических средств.

7.16. Биржа в рамках управления операционным риском разработала систему мер, направленных на обеспечение условий для бесперебойного функционирования программно-технических средств Биржи, а также для восстановления осуществляемой Биржей деятельности в случае реализации событий операционного риска Биржи, включающую в себя следующие мероприятия:

- Определение перечня критически важных процессов Биржи, а также процессов участников торгов и (или) контрагентов Биржи, приостановление или прекращение которых влечет за собой нарушение порядка осуществления Биржей деятельности по организации торгов, в том числе приостановление или прекращение организованных торгов, как в отношении отдельного финансового инструмента, иностранной валюты, товара, так и в отношении всех указанных инструментов;
- При составлении Планов обеспечения непрерывности бизнеса каждое подразделение указывает перечень критически важных процессов, возникающих при взаимодействии с контрагентами, включая процессы взаимодействия с участниками торгов. Подобное взаимодействие оценивается в рамках программы обеспечения непрерывности деятельности;
- Определение плана мероприятий по реагированию на НС, возникающие по критически важным процессам Биржи, а также процессам участников торгов и (или) контрагентов Биржи;
- Периодическое тестирование адекватности и достаточности мероприятий по реагированию на НС.

Определение перечня критически важных процессов Биржи включает следующие мероприятия:

- Перечень критически важных процессов Биржи определяется ДОРИБиНБ совместно с руководителями структурных подразделений;
- Перечень критически важных процессов Биржи описывается в Планах ОНиВД структурных подразделений непосредственно структурными подразделениями совместно с ДОРИБиНБ;

- ДОРИБиНБ совместно с руководителями структурных подразделений регулярно проводит анализ текущего воздействия внешней среды на бизнес;
- ДОРИБиНБ совместно с руководителями структурных подразделений определяет перечень критически важных процессов подразделения;
- Перечень критически важных процессов обновляется не реже, чем раз в год.

7.17. Выявление чрезвычайных ситуаций и проведение анализа обстоятельств возникновения чрезвычайных ситуаций.

Порядок управления ЧС:

- Постоянный мониторинг средств проведения торгов и штатного функционирования всех процессов Биржи с целью своевременного выявления аномалий и отклонения от нормальной работы процессов Биржи;
- Оперативное информирование любым работником всех заинтересованных лиц подразделений Биржи в случае выявления аномалий и отклонения от нормальной работы процессов Биржи;
- По решению уполномоченного органа, осуществляющего координацию действий по урегулированию сложившейся ситуации, ЧС может быть признана НС;
- Проведение анализа обстоятельств возникновения ЧС/НС;
- Активация планов реагирования на ЧС/НС;
- Разработка и последующая реализация мероприятий по снижению негативных последствий реализации НС и предотвращению повторения НС, улучшение планов реагирования на ЧС/НС;
- Ведение перечня потенциальных НС с целью поддержания в актуальном состоянии планов реагирования на ЧС/НС.

7.18. Обеспечение контроля за бесперебойным функционированием средств проведения торгов, в том числе посредством обеспечения контроля за недопущением превышения объема поступающих заявок участников торгов и частоты их поступления, в результате которого произойдет приостановление или прекращение оказания услуг по проведению организованных торгов в полном или неполном объеме.

Биржа обеспечивает контроль за бесперебойным функционированием средств проведения торгов, в том числе посредством обеспечения контроля за недопущением превышения объема поступающих заявок участников торгов и частоты их поступления, в результате которого произойдет приостановление или прекращение оказания услуг по проведению организованных торгов в полном или неполном объеме. Порядок осуществления контроля включает в себя:

- Мониторинг ТКС в целом и отдельных ее элементов, включая параметры подключения клиентов. Процесс восстановления системы мониторинга ТКС идентичен процессу восстановления самой системы;
- В случае, если количество клиентов резко меняется, Дежурный работник по соответствующей системе следует специальным инструкциям, которые разработаны в разрезе каждого класса проблем;
- Прохождение сертификации любой ВПТС;
- Мониторинг количества соединений и поведения участника торгов на наличие большого количества ошибочных транзакций.

7.19. Определение перечня потенциальных чрезвычайных ситуаций исходя из оценки Биржей возможных расходов (убытков) Биржи, участников торгов и их клиентов, а также иных его контрагентов вследствие нарушения непрерывности осуществления деятельности Биржи, вероятности и времени возможного возникновения такого нарушения, а также характера и объема совершаемых Биржейопераций.

Идентификация угроз, которые могут привести к неработоспособности средств проведения торгов, осуществляется в рамках управления непрерывностью деятельности с периодичностью не реже одного раза в год. Кроме того, перечень потенциальных угроз может быть пересмотрен внеочередным порядком, в связи с меняющейся международной обстановкой (санкции), внутриполитическими проблемами, экономическими, техногенными и эпидемиологическими ситуациями и их влияния на финансовую устойчивость Биржи. Также могут быть пересмотрены приоритеты потенциальных угроз, уже включенных в указанный перечень в связи с изменением указанных обстоятельств.

7.20. Разработка и утверждение документа, определяющего меры, принимаемые Биржей в чрезвычайных ситуациях и направленные на обеспечение непрерывности осуществления деятельности по организации торгов и обмена ЦФА (далее - План непрерывности бизнеса).

Биржей разработан и утверждён План непрерывности бизнеса, определяющий меры, принимаемые Биржей в чрезвычайной ситуации (далее – ЧС) для обеспечения непрерывности осуществления деятельности по организации торгов и обмена ЦФА.

План непрерывности бизнеса– внутренний документ Биржи, определяющий цели, задачи, порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования Биржи (подразделений), вызванного непредвиденными обстоятельствами (возникновением ЧС или иным событием, наступление которого возможно, но трудно предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению Биржей принятых на себя обязательств).

План непрерывности бизнеса является консолидацией документации, в области управления непрерывностью деятельности Биржи. Для каждого структурного подразделения Биржи разработан и внедрен свой План обеспечения непрерывности и восстановления деятельности (План ОНиВД). Меры по обеспечению непрерывности, разработанные для подразделений, объединяются, группируются, приоритезируются и являются основанием для рабочих инструкций и последовательных действий персонала Биржи в условиях ЧС.

В Плане непрерывности бизнеса описываются процессы функционирования и определяются приоритеты деятельности Биржи от момента объявления ЧС до момента перехода к нормальному функционированию и впоследствии отмены действия режима ЧС, рассматривается наихудший из возможных сценариев (недоступность основного офиса; недоступность основного центра обработки данных; недоступность основного офиса и недоступность основного центра обработки данных).

Целью Плана непрерывности бизнеса является обеспечение реагирования на существенные инциденты, он включает в себя оценку возможных последствий

инцидента на деятельность Биржи, принятие решений об активации планов реагирования структурных подразделений, поддержание способности Биржи выполнять принятые на себя обязательства перед клиентами, предупреждение и предотвращение возможного нарушения режима повседневного функционирования Биржи, обеспечение способности Биржи осуществлять расчетные и клиринговые операции, в соответствии с принятыми на себя обязательствами, сохранение уровня управления Биржи, позволяющего обеспечить условия для принятия обоснованных и оптимальных управленческих решений, их своевременную и полную реализацию.

В рамках управления рисками непрерывности деятельности определяются порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования Биржи, вызванного непредвиденными обстоятельствами (возникновением ЧС или иным событием, наступление которого возможно, но трудно предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению Биржей принятых на себя обязательств).

7.21. Оценка плана непрерывности бизнеса в целях определения достаточности, содержащихся в нем мер для обеспечения непрерывности осуществления деятельности по организации торгов исходя из характера осуществляемой Биржей деятельности и объема совершаемых операций, в случае выявления недостаточности указанных мер для обеспечения непрерывности осуществления деятельности по организации торгов - осуществление пересмотра плана непрерывности бизнеса.

Биржа обеспечивает осуществление следующих мероприятий:

- В целях определения достаточности, содержащихся в Плане непрерывности бизнеса мер для обеспечения непрерывности осуществляется пересмотр Плана непрерывности бизнеса с периодичностью не реже одного раза в два года;
- В случае выявления недостаточности указанных мер для обеспечения непрерывности деятельности по организации торгов – осуществление пересмотра плана непрерывности бизнеса.

Выявление недостаточности указанных мер и основание для регулярного или внеочередного пересмотра Планов ОНиВД структурных подразделений и консолидированного Плана непрерывности бизнеса происходит в случаях и на основании:

- результатов тестирования Планов ОНиВД и учений по действиям в условиях ЧС;
- изменения структуры подразделений, их наименования, штата, физического расположения офиса, области деятельности или функционала, ответственности и полномочий работников и персонала;
- изменение дислокации оборудования, состава оборудования и ПО, находящегося под управлением или необходимого для деятельности подразделения;
- реализовавшейся угрозы и наступления события ЧС, по результатам анализа действий структурных подразделений и Биржи в целом и выполнения мер Плана непрерывности в условиях конкретной ЧС.

7.22. Организация функционирования резервного комплекса средств проведения торгов, функционально дублирующего основной комплекс средств проведения торгов (далее - резервный офис), удовлетворяющего следующим требованиям:

- расположение резервного офиса в отдельном здании (вне основного комплекса средств проведения торгов);
- территориальное удаление резервного офиса от основного комплекса средств проведения торгов на расстояние, обеспечивающее возможность работников Биржи продолжить работу в резервном офисе в течение одного часа 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 Биржи в основном комплексе средств проведения торгов.

- Работники уведомляются в рамках обязательных тестирований, о способах транспортировки в резервный офис и о порядке действий при нахождении на территории резервного офисе.

7.23. Создание резервных копий информации, содержащейся в реестрах, ведение которых Биржа должна осуществлять в соответствии с требованиями части 14 статьи 5, части 2 статьи 11, части 5 статьи 18 Закона Об организованных торгах, в порядке, объемах и в сроки, определенные Биржей (но не реже одного раза в день), и хранение указанных копий в течение пяти лет со дня их создания.

- Организация резервного копирования информации:
  - Администраторы определяют способ, объем и периодичность проведения резервного копирования, выбирают тип носителя, на который будет выполняться резервное копирование, и определяют использование криптографических средств для защиты резервных копий информации, исходя из критичности информации, особенностей использования информации и требований бизнеса, а также с учетом требований ГОСТ Р 57580.1-2017. Данные параметры определяются отдельно для каждой Информационной системы (далее – ИС). Критичность информации ИС определяется её владельцем.
  - Для резервного копирования используются технические средства, удовлетворяющие параметрам выполнения резервного копирования (способ, объем, периодичность, скорость).

- Хранение резервных копий информации:
  - Администраторы совместно с ДОРИБиНБ и владельцами ИС определяют время хранения резервных копий для каждой ИС, но не менее пяти лет. При определении времени хранения учитывается уровень критичности информации для бизнес-процессов Биржи, а также требования законодательства Российской Федерации в т. ч. нормативно-правовых актов государственных органов, осуществляющих регулирование, контроль и надзор в сфере финансового рынка;

- Резервные копии (внешние носители) хранятся в отличном от основного носителя информации помещении для минимизации вероятности их одновременного повреждения;
- Доступ в помещения, в которых хранятся резервные копии, ограничен;
- Условия хранения физических носителей соответствуют требованиям их производителей;
- По истечении срока хранения, информация на внешних носителях удаляется в соответствии с требованиями Процедуры учета, хранения и уничтожения конфиденциальной информации, а носитель – возвращается в эксплуатацию;
- По истечении срока эксплуатации внешнего носителя, информация на нем удаляется, а носитель физически уничтожается в соответствии с требованиями процедуры учета, хранения и уничтожения конфиденциальной информации.

- Тестирование резервных копий информации и процедуры восстановления:

  - Резервные копии подвергаются регулярному тестированию на предмет отсутствия сбоев, чтобы гарантировать восстановление информации в случае возникновения такой необходимости;
  - В рамках тестирования резервных копий выполняются следующие проверки:
    a) верификация целостности резервных копий, осуществляемая техническими средствами резервного копирования;
    b) выборочная проверка возможности восстановления информации из резервных копий (для данных, не относящихся к торговым системам);
    c) регулярное восстановление информации из резервных копий (для данных, относящихся к торговым системам).
  - Настройки резервного копирования включают в себя последующую верификацию целостности;
  - В отношении данных, не относящихся к торговым системам, выборочная проверка возможности восстановления осуществляется таким образом, чтобы в течение года в неё попадало не менее 5% от общего количества резервных копий сроком хранения от года и выше. Выборочная проверка

возможности восстановления информации включает также все случаи восстановления данных по запросам пользователей. Резервная копия считается работоспособной, если с неё в течение года производилось хотя бы одно восстановление;

- В отношении данных, относящихся к торговой системе ASTS, осуществляются следующие действия:
  a) для оперативных данных осуществляется ежедневное резервное копирование баз данных средствами используемой СУБД с верификацией возможности чтения (восстановления) и корректности создания архивных копий. Восстановление баз данных из архивных копий выполняется в соответствии с действующим регламентом проведения технологических операций реорганизации баз данных после массового обновления данных (удаление, модификация), но не реже 1 раза в месяц;
  b) для архивных данных осуществляется контроль формирования архивов на момент их создания путем восстановления из них базы данных. В последующем, после помещения архивных данных на внешний носитель, указанные носители проверяются возможность чтения (восстановления) не менее 1 раза в год.
- В отношении данных, относящихся к торговой системе SPECTRA, осуществляются следующие действия:
  a) дублирование (зеркалирование) критичных данных с верификацией целостности средствами используемой СУБД;
  b) ежедневное резервное копирование данных с последующим восстановлением на резервной площадке средствами используемой СУБД;
  c) ежемесячное резервное копирование архивных данных с ежемесячным восстановлением.
- Во всех случаях восстановления данных с резервных копий осуществляется верификация их целостности техническими средствами резервного копирования, в том числе проверка целостности, записанной на носитель, информации при построении его каталога;

- В случае обнаружения нарушения корректности резервной копии Администратором осуществляется определение и устранение причин нарушения.

- Восстановление информации из резервных копий:

  - Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы или ее компонент, выполняется на основании заявки, оформленной через службу технической поддержки;
  - Процесс восстановления информации выполняется в следующем порядке:
    a) работник, которому необходимо восстановить потерянную информацию, направляет заявку с обязательным указанием причин необходимости восстановления в службу технической поддержки;
    b) работник, запросивший восстановление информации, к которой он ранее не имел доступ, должен его согласовать в соответствии с правилами управления доступом к информационным системам и процедурами изменения прав доступа к информационным системам;
    c) администратор при получении заявки на восстановление выполняет процедуру восстановления информации в соответствии с информацией, указанной в заявке, и уведомляет Заявителя через службу технической поддержки об успешной процедуре восстановления.

Порядок контроля за созданием резервных копий информации, содержащейся в реестрах, ведение которых Биржа осуществляет в соответствии с требованием законодательства (но не реже одного раза в день) включает следующие мероприятия:

- ДОРИБиНБ проводит контроль успешности выполнения резервного копирования в следующем порядке:

  - работник ДОРИБиНБ, осуществляющий проверку, определяет перечень ИС подлежащих проверке, производит восстановление копий из резервного носителя и проверяет функционирование программно-технических систем;

- далее указанным работником у Администраторов запрашиваются результаты выполнения процедур резервного копирования выбранных ИС за определенный период времени, который выбирается работником ДОРИБиНБ случайным образом;
- по результатам контроля процедур резервного копирования работник ДОРИБиНБ, проводивший проверку, составляет отчет о контроле процедур резервного копирования;
- Не реже раза в год проводится восстановление и проверка работоспособности процедуры резервного копирования.

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

- В зданиях ЦОД, в отдельных помещениях установлены дизельные генераторные установки (далее - ДГУ). В соответствии с требованиями заводов изготовителей проводятся еженедельные, двухмесячные и годовые обслуживания;
- При проведении еженедельных обслуживаний производится запуск всех ДГУ без подключения нагрузки, проверка технических параметров по стандартной программе;
- При проведении двухмесячных обслуживаний производится запуск всех ДГУ без подключения нагрузки, проверка технических параметров по расширенной программе с использованием технических средств силами вендора;
- При ежегодном техническом обслуживании производится запуск всех ДГУ с подключением испытательной нагрузки (внешнего нагрузочного устройства). Выполняется замена расходных материалов (масло, фильтра, антифриз и т.д.), проверяются технические параметры по дополнительной программе с использованием технических средств силами вендора ДГУ.

7.25. Создание и поддержание технического оснащения резервного офиса на уровне, обеспечивающем восстановление критически важных процессов Биржи и возможность начала работы по переносу критически важных процессов Биржи, осуществляемых с использованием средств проведения торгов, из основного комплекса средств проведения торгов в резервный офис в порядке и в сроки, установленные Биржей.

- В рамках ежегодного тестирования работники проводят тестирование оборудования в резервном офисе;
- В случае обнаружений отклонений, выявленные проблемы доводятся до работника, ответственного за обеспечение непрерывности бизнеса;
- На основании проведенного анализа проблем разрабатываются планы действий по решению выявленных проблем.

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

Биржа осуществляет мероприятия, обеспечивающие возможность оказания услуг, необходимых для функционирования основного комплекса средств проведения торгов и резервного офиса, независимыми поставщиками телекоммуникационных услуг. Порядок обеспечения возможности оказания услуг, необходимых для функционирования основного комплекса средств проведения торгов и резервного офиса включает:

- Регулярный мониторинг рынка поставщиков телекоммуникационных услуг;
- Оценка качества действующих поставщиков телекоммуникационных услуг;
- Внедрение механизма аккредитации поставщиков для доступа к средствам проведения торгов операторами связи;
- Поддержание наличия нескольких действующих договоров с поставщиками телекоммуникационных услуг (минимум с двумя) для резервного офиса и резервного ЦОД.

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

- Резервные рабочие места тестируются согласно утвержденному графику тестирования программы ОНБ, но не реже чем один раз в течение последних 12 месяцев;
- По результатам тестирования формируется отчет и рассылается всем заинтересованным сторонам;
- Резервные места тестируют работники подразделений, за которыми данные места закреплены в плане рассадки резервного офиса.

Под тестированием понимается оценка на соответствие требованиям подразделений к оборудованию резервных мест, инфраструктуре офиса, подготовленности к восстановлению критичных процессов подразделений в определенные заранее временные рамки и т.д.

Также для поддержания резервного офиса на уровне, обеспечивающем возможность функционирования всех критически важных процессов Биржи, и поддержание таких процессов в течение не менее одного месяца с момента возникновения чрезвычайной ситуации удовлетворяются следующие требования к резервному офису:

- резервный офис на территории Российской Федерации находится в достаточной территориальной отдаленности от основного офиса с учетом возможности работников Биржи продолжить работу в резервном офисе в течение одного часа с момента возникновения чрезвычайных ситуаций;
- обеспечивается наличие работоспособных независимых генераторов электричества необходимой мощности в основном и резервном офисах;
- используются не менее двух поставщиков телекоммуникационных услуг для основного и резервного офисов;
- обеспечивается возможность начала функционирования резервного офиса Биржи в кратчайшие сроки после возникновения чрезвычайных ситуаций, в

том числе возобновления в нем критически важных процессов в плановое (целевое) время восстановления;

- обеспечивается возможность незамедлительного с момента возникновения чрезвычайных ситуаций начала работы по переносу критически важных процессов, осуществляемых с использованием программно-технических средств Биржи, из основного офиса в резервный офис;
- поддерживается техническое состояние, технологическое и методологическое сопровождение резервного офиса на уровне, достаточном для обеспечения возможности функционирования всех критически важных процессов Биржи и обеспечения возможности поддержания этих процессов в течение одного месяца с момента возникновения чрезвычайной ситуации;
- обеспечивается резервное копирование информации и баз данных, обслуживающих критически важные процессы, на резервные носители информации для возобновления указанных процессов в случае утраты или повреждения информации или баз данных вследствие возникновения чрезвычайных ситуаций, и хранение указанных копий в течение пяти лет со дня их создания.

7.28. Биржа в рамках управления риском потери деловой репутации Биржи организует сбор и анализ отзывов о деятельности Биржи в средствах массовой информации, в том числе с использованием специализированных автоматизированных информационных систем.

Подразделением, осуществляющим сбор и оценку информации о фактах РПДР, является Департамент по маркетингу, PR и клиентскому сервису. Департамент по маркетингу, PR и клиентскому сервису совместно с ДОРИБиНБ осуществляет:

- Построение связей с внешними источниками распространения массовой информации (печатные издания, радио, Интернет и т.д.), в том числе периодических печатных изданий, радио, телевидение, иных форм периодического распространения массовой информации, включая Интернет, а также информацию, полученную от структурных подразделений Биржи, с целью сбора и анализа отзывов о Бирже, включая информацию, полученную в рамках ведения претензионной работы.

- Полученные сведения о фактах РПДР проверяются на достоверность и значимость. Оценка полученных сведений проводится экспертно Департаментом по коммуникациям, исходя из того, насколько ущерб репутации Биржи усложнит достижение целей, которые ставит перед собой Биржа в своей деятельности. Проверка на достоверность предполагает подтверждение сведений перекрестной информацией из другого источника;
- За получением подтверждающей, а также уточняющей информации подразделение, ответственное за сбор и анализ информации о фактах РПДР, имеет право обращаться к структурным подразделениям Биржи, запрашивая, в том числе информацию о выявленных нарушениях и предписаниях со стороны регулирующих органов, претензиях со стороны клиентов, претензиях со стороны регулирующих, правоохранительных органов, иное;
- В процессе оценки РПДР может анализироваться влияние деловой репутации на финансовое состояние, влияние деловой репутации компаний Группы на деловую репутацию Биржи, превентивных и контрольных мероприятий (благотворительной и общественной деятельности, рекламно-информационной политики) на деловую репутацию Биржи.

При оценке уровня РПДР могут учитываться:

- изменение финансового состояния Биржи (например, изменение структуры активов, их обесценение в целом или в части отдельных групп, изменение структуры собственных средств (капитала);
- возрастание (сокращение) количества жалоб и претензий, в том числе относительно качества обслуживания клиентов и контрагентов, соблюдения обычаев делового оборота;
- динамика доли активов, размещенных в результате сделок с аффилированными лицами, дочерними организациями, в общем объеме активов;
- выявление в рамках системы внутреннего контроля случаев несоблюдения требований нормативных документов, в том числе по легализации (отмыванию) доходов, полученных преступных путем, а также признаков

возможного вовлечения Биржи, компаний Группы работников, клиентов Биржи в легализацию (отмывание) доходов;

- выявление фактов хищения, подлогов, мошенничества Биржей, использования работниками Биржи конфиденциальной информации, полученной от клиентов и контрагентов, в личных целях;
- отказ постоянных или крупных клиентов и контрагентов от сотрудничества с Биржей.

Оценка и мониторинг риска потери деловой репутации осуществляется на постоянной основе, в том числе путем:

- регулярного изучения показателей деятельности Биржи;
- мониторинга количества жалоб и претензий к Бирже, в том числе относительно качества обслуживания клиентов и контрагентов, соблюдения обычаев делового оборота;
- мониторинга позитивных и негативных отзывов и сообщений в СМИ об акционерах и аффилированных лицах.

Мероприятия по минимизации возможности возникновения фактов РПДР включают в себя:

- мониторинг деловой репутации акционеров, аффилированных лиц, менеджмента Группы;
- контроль достоверности бухгалтерской отчетности и иной публикуемой информации, представляемой акционерам, клиентам и контрагентам, органам регулирования и надзора и другим заинтересованным лицам, в том числе в рекламных целях;
- наличие системы информационного обеспечения, не допускающей использования информации лицами, имеющими доступ к такой информации, в личных интересах и предоставляющей органам управления и работникам информацию о негативных и позитивных отзывах и сообщениях о Бирже из средств массовой информации (периодические печатные издания, радио, телевидение, иные формы периодического распространения массовой информации, включая Интернет), иных источников; своевременное

рассмотрение, анализ полноты, достоверности и объективности указанной информации; своевременное реагирование на имеющуюся информацию;

- применение дисциплинарных мер к работникам, виновным в повышении уровня риска потери деловой репутации Биржи, совершившим дисциплинарный проступок.

Также, в целях минимизации возможности возникновения фактов РПДР осуществляются мероприятия по минимизации вероятности возникновения фактов РПДР, соответствующие мероприятия по минимизации операционного риска, которые осуществляются в рамках системы управления рисками в соответствии с внутренними документами Биржи.

7.29. Биржа в рамках управления стратегическим риском Биржи обеспечивает выполнение следующих мероприятий в целях выявления потенциальных источников возникновения рисков:

7.29.1. Разработка проектов изменений в порядок осуществления деятельности по проведению организованных торгов или связанной с проведением организованных торгов деятельности, предоставления дополнительных услуг, допуска к организованным торгам новых финансовых инструментов, иностранной валюты, товара, а также иных организационных и (или) технологических изменений (далее - проекты изменений).

Порядок разработки проектов изменений включает:

- Для проектных инициатив инициатор подготавливает документ об инициативе, дополнительно согласовав его с руководителем функционального подразделения (заказчиком), и передает его в ПО;
- ПО осуществляет централизованный сбор и регистрацию всех инициатив, направленных на изменение и создание новых процессов в рамках проведения организованных торгов и других инициатив.

Целью единой регистрации является унификация процесса сбора и оценки инициатив для дальнейшего оптимального распределения ограниченных ресурсов Биржи между проектами и задачами с учетом стратегии Биржи.

Вопросы контроля и управления изменениями в ИТ-инфраструктуре, обеспечивающей деятельность Биржи, рассматриваются на Комитете по согласованию технологических изменений ПТК.

7.29.2. Анализ целесообразности внедрения проектов изменений.

- В рамках анализа целесообразности внедрения проектов и инициатив формируется реестр инициатив, который консолидируется ответственным структурным подразделением – ПО и выносится на рассмотрение уполномоченного органа – КПП, созданного в качестве совещательного органа при Правлении Биржи;
- ДОРИБиНБ совместно с УФР и ДВКиК проводит оценку рисков, связанных с реализацией проекта, а также оценку рисков, снижаемых вследствие реализации проекта по каждой инициативе, и формирует заключение о рисках;
- Блок финансов совместно с менеджерами проектов рассчитывает ряд финансовых показателей по каждой инициативе (NPV, TCO и т. д.);
- Заключение о рисках и список финансовых показателей выносятся на рассмотрение КПП;
- КПП рекомендует Правлению, а Правление принимает решение о реализации проектов, изменений, осуществляет приоритезацию реализации инициатив.

Решение принимается на основе баланса целесообразности инвестиций и экономической выгоды и целесообразности снижения выявленных рисков, и совершенствования деятельности Биржи.

7.30. Анализ эффективности реализованных Биржей проектов изменений по итогам их введения в деятельность, осуществляемую Биржей.

Для оценки успешности проекта проводится пост-проектный (пост-инвестиционный) мониторинг. Пост-проектный мониторинг не включен в жизненный цикл проекта и может проводиться уже после завершения всех работ по проекту, включая его завершение.

7.31. Мероприятия по планированию развития деятельности Биржи, в том числе посредством разработки стратегии развития Биржи на срок, соответствующий характеру осуществляемой деятельности Биржи и объему совершаемых операций.

Биржа осуществляет следующие мероприятия по планированию развития деятельности Биржи:

- разработка стратегии развития Биржи на 5 лет;
- разработка дорожной карты реализации стратегии;
- расчет ресурсов, необходимых для реализации дорожной карты стратегии;
- утверждение стратегии Наблюдательным советом Биржи;
- Наблюдательным светом Биржи может быть принято решение о внесении изменений в стратегию развития Биржи.

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

Порядок оценки стратегии развития Биржи на предмет определения возможности и целесообразности ее реализации:

- Выявление рисков достижения стратегических целей;
- Выявление рисков целеполагания стратегии Биржи;
- Проведение оценки рисков достижения целей;
- Проведение оценки рисков целеполагания стратегии Биржи;
- Вынесение указанных рисков на рассмотрение Наблюдательного совета, для определения целесообразности пересмотра Стратегии;
- Мониторинг выявленных рисков в течение срока реализации Стратегии.

Оценка стратегии развития Биржей предполагает:

- оценку выработанных стратегических вариантов для определения их пригодности;
- сравнения результатов оценки стратегии;
- внесение изменений в стратегию развития Биржи в случае необходимости.

Основные критерии оценки:

- последовательность осуществления стратегии;
- согласованность с требованиями среды;
- осуществимость;
- приемлемость для групп влияния;
- преимущества по отношению к конкурентам.

Оценка стратегии развития является заключительным этапом стратегического планирования и продолжается на всех этапах реализации стратегии, включая оценку выработанных конкретных стратегических вариантов для определения их пригодности, осуществимости, приемлемости и последовательности для Биржи.

7.33. Разработка и утверждение документа, определяющего меры, принимаемые Организатором торговли в случаях необходимости поддержания и восстановления финансовой устойчивости Организатора торгов и направленные на обеспечение непрерывности предоставления критически значимых услуг (далее - План восстановления финансовой устойчивости, ПВФУ).

Организатором торгов разработан и утвержден План восстановления финансовой устойчивости, основной целью которого является заблаговременная разработка порядка действий и мероприятий по поддержанию и восстановлению финансовой устойчивости Организатора торгов для обеспечения непрерывности предоставления Организатором торгов критически значимых услуг в случае существенного ухудшения его финансового положения, а также мероприятий по предупреждению и предотвращению доступными Организатору торгов инструментами и методами ухудшения своего финансового положения.

ПВФУ позволяет оценить способность Организатора торгов противостоять стрессовым событиям, способным оказать негативное влияние на ее финансовую устойчивость и возможность предоставления критически значимых услуг, за счет возможностей, не связанных с привлечением государственных средств, а также средств Банка России.

ПВФУ базируется на рассмотрении вариантов (сценариев) потери финансовой устойчивости Организатора торгов и содержит условия, при наступлении

которых реализуются мероприятия по предупреждению ухудшения финансового положения Организатора торгов и восстановлению финансовой устойчивости, а также описание процесса принятия решений о начале реализации данных мероприятий.

ПВФУ предусматривает мероприятия, принимаемые для восполнения капитала и поддержания ликвидности в случае развития событий по одному или нескольким неблагоприятным для Биржи сценариям, в том числе связанным с ухудшением финансового положения ее дочерних компаний имеющей для нее стратегическое значение. По каждому сценарию определяются механизмы его реализации, в том числе соответствующие сценарию индикаторы, меры раннего реагирования и меры восстановления.

8 Порядок обеспечения контроля за выполнением процессов и мероприятий по выявлению, анализу, мониторингу риска, и обмену информацией между подразделениями и органами управления Биржи, а также порядок осуществления процессов и мероприятий, осуществляемых Биржей в рамках управления отдельными видами рисков Биржи

Контроль за процессом выявления и анализа рисков Биржи осуществляется путем:

- Проведения регулярных тестирований средств проведения торгов, помогающих выявить потенциальные риски, связанные с отклонением от нормальной штатной работы ТКС;
- Инвентаризации программно-технических средств, которая проходит цикл один раз в три года с целью осуществления контроля за мероприятиями по замене или улучшению (обновлению) программно-технических средств Биржи в случае выявления их несоответствия характеру и объему совершаемых Биржей операций;
- Независимого контроля основных процессов создания и эксплуатации автоматизированных систем, входящих в состав средств проведения торгов, включая контроль обеспечения информационной безопасности, на соответствие требованиям документов, разрабатываемых в рамках законодательства Российской Федерации о техническом регулировании с

учетом положений международных стандартов (операционный аудит), не реже одного раза в два года с привлечением независимых консультантов;

- Независимого сертификационного аудита на соответствие процесса проведения испытательных работ (тестирования) средств проведения торгов, а также порядка устранения недостатков, выявленных в результате их проведения, стандарту ISO 22301 на ежегодной основе;
- Проведения периодических аудитов СВА;
- Проведения периодических проверок отдельных процессов работниками ДОРИБиНБ, СВК и ДВКиК.
- Проведения контрольных процедур работниками иных структурных подразделений;
- Анализа, оценки и разработки последующих мер реагирования на результат контрольных процедур, документирования результатов, ведения отчетности работниками ДОРИБиНБ или иными подразделениями, управляющими отдельными видами рисков;
- Принятия управленческих решений уполномоченными органами управления Биржи по итогам рассмотрения отчетности по рискам. На разных этапах управления рисками эти функции осуществляются Директором ДОРИБиНБ, Начальником УФР, Правлением;
- Биржей проводятся периодические проверки адекватности системы управления рисками СВА, независимыми аудиторскими компаниями и надзорными органами.

Этап контроля процесса управления рисками обеспечивает полноценное информирование органов управления Биржи, а также является основой для принятия управленческих решений.

Порядок обеспечения контроля как этапа процесса управления риском содержит в себе следующие мероприятия:

- Разработка и внедрение автоматизированных контрольных процедур;
- Составление планов для неавтоматизированных контрольных процедур: определение объектов контроля (процессов, мероприятий, деятельности

структурных подразделений), контрольных процедур (в рамках самооценки, проверка/аудит, запроса и т. п.) и сроков их проведения;

- Выполнение контрольных процедур в отчетном периоде;
- По окончании отчетного периода сбор информации и данных, агрегирование их по типам рисков, анализ, оценка и составление отчетности;
- Предоставление отчетности органам управления Биржи для принятия управленческих решений;
- Проведение дополнительных контрольных процедур в отношении выполненных мероприятий на предмет анализа их достаточности;
- Периодический пересмотр и совершенствование контрольных процедур в рамках оценки результативности и эффективности системы управления рисками.

9 Порядок внесения рисков Биржи и результатов их оценки в реестр рисков Биржи, порядок осуществления оценки реестра рисков Биржи на предмет его актуальности, а в случае выявления в реестре рисков Биржи неактуальных сведений - на предмет пересмотра реестра рисков Биржи

Каждый работник Биржи обязан сообщить о риске в ДОРИБиНБ в момент обнаружения.

По факту получения сообщения о риске работник ДОРИБиНБ осуществляет анализ и оценку риска с учетом вероятности его реализации, величины возможного убытка, влияния на процессы, системы и другие виды риска, оценки адекватности применяемых контрольных процедур, возможной стратегии реагирования на риск, проводит оценку на предмет возможного нарушения ограничений уровня риска и при необходимости эскалирует информацию органам управления Биржи. При необходимости работник ДОРИБиНБ может привлекать работников структурных подразделений, ответственных за управление отдельными видами риска.

По факту проведенного анализа информация о нефинансовых рисках вносится в БДР работником ДОРИБиНБ.

По факту появления и учета информации о риске в БДР работник ДОРИБиНБ отслеживает исполнение контрольных мероприятий по минимизации риска лицом,

ответственным за выполнение мероприятий в установленный срок, если принято решение о снижении риска.

По факту выполнения мероприятий по минимизации риска проводится анализ, закрывают ли риск проведенные мероприятия или снижают. Во втором случае данный риск подлежит ежегодной инвентаризации. В отдельных случаях внедряется КИР для мониторинга сниженного/принятого уровня риска.

Если в рамках ежегодной инвентаризации рисков БДР работник ДОРИБиНБ получает подтверждение о том, что риск закрыт/утратил актуальность, проставляет соответствующий статус в БДР, что позволяет исключить закрытый/неактуальный риск из последующего цикла ежегодной инвентаризации.

Работником ДОРИБиНБ осуществляется регулярная оценка БДР на предмет ее актуальности, а в случае выявления неактуальных сведений - пересмотр реестра рисков Биржи с периодичностью не реже одного раза в год.

Для выявления и идентификации риска используются следующие процессы и процедуры:

- сбор сведений о рисках (как внутренних, так и внешних), способных нанести Бирже ущерб, и о факторах их возникновения (в том числе способом самооценки), сбор сведений о событиях риска и факторах их возникновения;
- рассмотрение возможности/вероятности возникновения рисков в деятельности Биржи, причинении ущерба (в размере - ожидаемом, наихудшем, наиболее частом и т. д.);
- диагностика бизнес-процессов на выявление точек (узлов) возникновения рисков, анализ пересечений в полномочиях и ответственности подразделений и работников Биржи;
- анализ результатов внутреннего и внешнего аудита контролей/процедур/систем;
- анализ новых продуктов, процессов и систем (анализ всех нововведений, проводимых Биржей: изменения структуры и процедур, внедрение новых услуг и технологий, освоение новых направлений деятельности и т. п.);

- применение сценарного анализа для идентификации угроз, которые по оценке Биржи могут привести к неработоспособности средств проведения торгов и/или иной причине прекращения деятельности по организации торгов;
- использование результатов стресс-тестирования программно-технических средств для осуществления деятельности по организации торговли с периодичностью, определенной внутренними документами Биржи, но не реже одного раза в шесть месяцев.

Для каждого из видов рисков, входящих в систему управления рисками Биржи, возможен набор методов выявления рисков, присущий только данному виду рисков.

10 Порядок ведения базы данных о событиях операционного риска

Ведение базы данных о событиях операционного риска (в том числе реализация событий риска информационной безопасности таких, как компьютерные атаки и факты (индикаторы) компрометации объектов информатизации) (БДСОР) осуществляется на регулярной основе по мере выявления событий операционного риска в следующем порядке:

- Сбор данных о событиях осуществляется ответственными работниками ДОРИБиНБ. Каждый работник Биржи обязан при выявлении события сообщить о нем в порядке, описанном в настоящем разделе;
- В случае возникновения события:
    a) Работник Биржи, располагающий информацией о событии, извещает об этом непосредственного руководителя и ответственного работника ДОРИБиНБ не позднее дня его выявления;
    b) В случае отсутствия полной информацией о событии (событие не является завершенным и необходимо отслеживание предоставленной информации), работником направляется вся доступная в настоящее время информация в ДОРИБиНБ;
    c) Ответственный работник ДОРИБиНБ проводит первичный анализ информации о событии в рамках доступных ему полномочий и, в случае если событие является событием операционного риска, осуществляет следующие действия:

- анализирует сообщение о событии операционного риска на предмет дублирования информации (в БДСОР);
- классифицирует событие операционного риска в соответствии с классификационным справочником БДСОР;
- регистрирует событие операционного риска с присвоением ему уникального номера.

d) В течение рабочего дня регистрации события операционного риска Риск-менеджером уточняется у Владельца риска оценка влияния, осуществляется анализ и оценка события операционного риска, осуществляется в целях определения существенности его влияния на деятельность Биржи и последующего принятия решения о мерах по минимизации вероятности повторного возникновения события операционного риска;

e) На регулярной основе Риск-менеджер самостоятельно или совместно с ответственным работником (владельцем риска, в котором произошло событие операционного риска) проводит анализ возможных исходов событий БДСОР и БДР, т. е. тех негативных последствий, к которым потенциально могли бы привести события, но не привели.

Результаты такого анализа используются для определения сценариев стресс-тестирования, при сценарном и what if анализе, при формировании матрицы рисков в части возможных причин и вероятных исходов, при построении карты и матрицы рисков и прогнозировании.

Риск-менеджер осуществляет контроль и несет ответственность за полноту и актуальность информации о событии операционного риска в БДСОР.

ДОРИБиНБ ежедневно осуществляет контроль полноты и актуальности данных о расходах (убытках), понесенных Биржей вследствие реализации событий операционного риска.

11 Порядок и периодичность (не реже одного раза в год) проведения идентификации угроз, которые по оценке Биржи могут привести к неработоспособности средств проведения торгов

Биржей проводится идентификация угроз, которые по оценке Биржи могут привести к неработоспособности средств проведения торгов, а также постоянный мониторинг текущего состояния средств проведения торгов, в том числе на предмет необходимости их обновления с периодичностью не реже одного раза в год.

Порядок проведения идентификации угроз, которые по оценке Биржи могут привести к неработоспособности средств проведения торгов включает следующие мероприятия:

- Определение источников, факторов, воздействие которых способно привести к приостановке средств проведения торгов и их анализ;
- Классификация угроз с последующей оценкой степени вероятности их реализации;
- Проведение нагрузочных тестирований программно-технических комплексов, тестов на вторжение;
- Постоянный мониторинг текущего состояния средств проведения торгов, в том числе на предмет необходимости их обновления;
- Осуществление не реже одного раза в год идентификации угроз информационной безопасности, которые могут привести к неработоспособности средств проведения торгов;
- Определение перечня требующих защиты от противоправных действий программно-технических средств Биржи, сбои и (или) ошибки в функционировании которых способны повлечь за собой приостановление или прекращение оказания услуг по проведению организованных торгов в полном или неполном объеме и (или) оказать иное неблагоприятное воздействие на деятельность Биржи.
- Определение перечня и реализация мер по защите информации, осуществляемых в рамках соответствия требованиям законодательства.

Данные мероприятия осуществляются в рамках внедренной и поддерживаемой Биржей области деятельности по управлению непрерывностью бизнеса, которая

функционирует в соответствии с требованиями законодательства, а также в соответствии с рекомендациями международных стандартов.

Для идентификации угроз непрерывности осуществляются мероприятия по управлению рисками непрерывности в следующем порядке и с установленной периодичностью:

- Идентификация угроз непрерывности бизнеса требует рассмотрения деятельности Биржи как единого взаимосвязанного комплекса разноплановой деятельности отдельных структурных подразделений. В специализации отдельных структурных подразделений выделяются критичные к непрерывности процедуры и функционал, нарушение штатной работы которых неминуемо ведет к прерыванию и сбоям в функционировании других подразделений вплоть до приостановки их деятельности;
- Оценка рисков непрерывности бизнеса проводится следующим этапом по завершению анализа воздействия на бизнес. При этом если анализ воздействия на бизнес позволяет проанализировать влияние сбоев в процессах подразделений на бизнес Биржи, то оценка рисков показывает, каким угрозам подвержена Биржа в целом в текущий период и как реализация этих угроз может привести к сбоям в критичных процессах. Процесс оценки рисков непрерывности включает в себя:
  - определение областей, рабочих процессов и функционала, в рамках которых Биржа может быть подвержена рискам непрерывности бизнеса;
  - выделение угроз непрерывности, реализация которых может привести к нарушению штатного функционирования критичных подпроцессов и процедур, определенных на этапе анализа воздействия на бизнес;
  - анализ степени влияния угроз на Биржи в случае их реализации, в том числе на работников Биржи, инфраструктуру Биржи, информационные активы Биржи;
  - оценку вероятности реализации угрозы непрерывности;
  - анализ существующих контрольных процедур.
- В процессе оценки рисков непрерывности оценивается вероятность реализации угрозы, степень возможного влияния на Биржи и существующие

организационно-технические мероприятия, и контрольные процедуры, направленные на снижение рисков;

- Оценка рисков непрерывности проводится на регулярной основе как в рамках ежегодного анализа деятельности по управлению непрерывностью со стороны руководства, так и в случае существенных изменений внутренних и внешних факторов, влияющих на непрерывность.

Порядок мониторинга текущего состояния средств проведения торгов, в том числе на предмет необходимости их обновления включает следующие мероприятия:

- Мониторинг Торгово-клиринговой системы (далее – ТКС) в целом и отдельных ее элементов, включая параметры подключения клиентов. Процесс восстановления системы мониторинга ТКС идентичен процессу восстановления самой системы;
- Прохождение сертификации любых ВПТС в соответствии с Регламентом сертификации ВПТС и Требованиями, предъявляемыми Биржейк сопряжению ВПТС с ПТК ТЦ;
- В случае идентификации угроз, которые могут привести к неработоспособности средств проведения торгов Дежурный работник по соответствующей системе анализирует и эскалирует проблему в соответствующее подразделение. Для более специфичных классов проблем разработаны инструкции, в которых прописаны действия работников по реагированию на такие проблемы. Инструкции подлежат постоянному обновлению по результатам текущей эксплуатации, анализа разноплановых ситуаций и т. д.;
- В случае выявления инцидента информация также направляется ДОРИБиНБ и анализируется.

К угрозам, которые по оценке Биржи могут привести к неработоспособности средств проведения торгов, относятся:

- выход из строя технических средств, сбои в работе информационных систем (в том числе в результате технического сбоя), используемых для обслуживания критически важных процессов;
- нарушение коммунальной инфраструктуры (затопление помещений Биржи, например, вследствие прорыва труб и т. п.);

- перебои в электроснабжении (в том числе в связи с отказом поставщиков электроэнергии от исполнения своих обязательств), которые не могут быть нейтрализованы имеющимися в распоряжении Биржи техническими средствами;
- нарушение работы каналов связи (в том числе в связи с техническим сбоем, отказом поставщика канала связи выполнять свои обязательства).

Иные обстоятельства, которые по оценке Биржи могут привести к приостановлению или прекращению осуществления критически важных процессов:

- получение Биржей сообщения от клирингового центра о возникновении чрезвычайной ситуации, которая может привести к нарушению обслуживания участников торгов;
- попытка третьих лиц и/или внутреннего нарушителя получить несанкционированный доступ к защищаемой информации, либо умышленное создание условий, осложняющих штатное функционирование программно-технических средств Биржи (сетевые атаки);
- принятие или любые изменения законодательных или иных нормативных правовых актов государственных органов Российской Федерации или нормативных актов Банка России, а также получение инструкций, указаний, заявлений, писем, телеграмм, иные действия данных органов, которые временно или на неопределенный срок сделали, делают или могут сделать невозможным или значительно затруднить дальнейшее осуществление деятельности, а также оказания иных значимых услуг в том виде и порядке, в которых данные операции проводились до принятия указанных актов.

12 Порядок ведения базы данных о расходах (убытках), понесенных Биржей вследствие реализации событий операционного риска Биржи

Ведение базы данных о расходах (убытках), понесенных Биржей вследствие реализации событий операционного риска (в том числе реализация событий риска информационной безопасности таких, как компьютерные атаки и факты (индикаторы) компрометации объектов информатизации), осуществляется в рамках ведения единой БДСОР на регулярной основе по мере выявления информации. Помимо общей

детальной информации по каждому событию операционного риска, в БДСОР содержится следующая информация:

- размер расходов (убытков), понесенных вследствие реализации события операционного риска;
- вид убытка (прямые, косвенные, почти потери «near miss»);
- статус убытка (резерв, списание);
- источник риска;
- вид (направление) деятельности;
- возмещение убытка;
- дата реализации события операционного риска Биржи, повлекшего за собой возникновение расходов (убытков) Биржи;
- анализ обстоятельств возникновения (выявления) события операционного риска Биржи, приведшего к расходам (убыткам) и возможности покрытия расходов (убытков).

Таким образом, ведение единой БДСОР не только удовлетворяет требованию ведения базы данных о расходах (убытках), понесенных Биржей вследствие реализации событий операционного риска, но и содержит всю существенную информацию о событиях операционного риска, позволяющую осуществлять устранение последствий событий операционного риска и планировать действия и долгосрочные мероприятия по управлению данным риском наиболее эффективным способом.

Срок хранения информации о событиях операционного риска и о расходах (убытках), понесенных Биржей вследствие реализации событий операционного риска Биржи, составляет не менее 10 лет.

13 Права и обязанности органов управления Биржи, руководителей и работников структурных подразделений Биржи, в том числе должностного лица (руководителя отдельного структурного подразделения), ответственного за организацию системы управления рисками, а также должностного лица, ответственного за управление операционным риском (при наличии), в рамках организации системы управления рисками

Управление рисками осуществляется на всех уровнях Биржи и подразумевает вовлечение всех органов управления и работников, роли и функции которых

разграничены и в то же время дополняют друг друга. Обязанности и ответственность за принятие и реализацию (выполнение) решений в области управления рисками между участниками системы управления рискам распределены таким образом, что исключено дублирование функций, но при этом обеспечены согласованность и эффективность реализуемых мер по управлению рисками.

Система управления рисками Биржи определяет полномочия и функции структурного подразделения, ответственного за организацию системы управления рисками Биржи, и органов управления Биржи в области организации и руководства системой управления рисками.

- ДОРИБиНБ – отвечает за систему управления рисками Биржи, в том числе за управления операционным риском, включая риск информационной безопасности и непрерывности деятельности, стратегическим риском, риском потери деловой репутации, модельным риском.

  ДОРИБиНБ в рамках управления отдельными видами рисков привлекает:
- УФР – в части финансовых рисков, в том числе, связанных с осуществлением операций с собственным имуществом;
- СВК – в части управления регуляторным риском в соответствии с утвержденными документами;
- ДВКиК – в части управления комплаенс риском;
- ЮД – в части управления правовым риском;
- Департамент по коммуникациям – в части управления риском потери деловой репутации;
- Департамент стратегии – в части управления стратегическим риском;
- ПО – в части управления риском проекта.

- Группу по налогообложению Блока финансов – в части управления налоговым риском

Директор ДОРИБиНБ и руководители отдельных структурных подразделений, указанные в настоящем пункте Правил, могут входить в состав создаваемых комитетов и комиссий, не являющихся структурными подразделениями Биржи.

Для Директора ДОРИБиНБ ПАО Московская Биржа является основным местом работы.

Директор ДОРИБиНБ, работники структурных подразделений, указанные в настоящем пункте Правил, вправе требовать у работников и должностных лиц Биржи предоставления информации (документов), в том числе письменных объяснений, по вопросам, возникающим в ходе выполнения им (ими) своих обязанностей.

В компетенцию Директора ДОРИБиНБ входит, в том числе:

- разработка программ обучения (консультаций) работников Биржи по вопросам выявления, идентификации и оценки рисков, а также их контроля;
- разработка методологии и инструментов управления рисками;
- оценка рисков Биржи с учетом вероятности его наступления и влияния на деятельность по проведению организованных торгов;
- разработка рекомендаций органам управления, должностным лицам, в том числе руководителям структурных подразделений Биржи, о мерах, которые необходимо предпринять для устранения того или иного риска Биржи;
- осуществление контроля выполнения мер, направленных на устранение рисков Биржи;
- предоставление информации о рисках Биржи коллегиальному исполнительному органу и Единоличному исполнительному органу Биржи;
- принятие иных мер, направленных на организацию системы управления рисками, предусмотренных внутренними документами Биржи.

В компетенцию Наблюдательного совета входит в том числе решение вопросов, связанных с организацией системы управления рисками, а именно:

- определение принципов и подходов к организации системы управления рисками;
- утверждение внутренних документов, определяющих политику Биржи в области организации управления рисками;
- утверждение документов, определяющих правила организации системы управления рисками Биржи;
- утверждение методики определения предельного уровня рисков (допустимого уровня рисков) Биржи, а также совокупного предельного уровня рисков Биржи;

- утверждение документа, определяющего меры, принимаемые в чрезвычайных ситуациях и направленные на обеспечение непрерывности осуществления деятельности по проведению организованных торгов;
- утверждение контрольных показателей риск-аппетита;
- утверждение критериев оценки эффективности СУР;
- рассмотрение и анализ результатов оценки эффективности СУР;
- принятие решений по результатам проведенного анализа и оценки.

В целях организации выполнения решений Наблюдательного совета в соответствии с утвержденными им внутренними документами в области управления рисками, Председатель Правления и Правление осуществляют:

- распределение полномочий и ответственности по управлению рисками между руководителями подразделений Биржи 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;
- принятие решений по осуществлению мероприятий в отношении управления рисками;
- утверждение лимитов кредитного и рыночного рисков (лимитной ведомости);
- утверждение отчетности по рискам.

Комиссией по управлению рисками Наблюдательного совета осуществляется предварительное рассмотрение до утверждения Наблюдательным советом следующих документов:

- документов, определяющих принципы управления рисками;
- критерии оценки эффективности системы управления рисками Биржи;
- документов, устанавливающих ключевые показатели рисков, включая показатели риск-аппетита, уровня толерантности к риску;
- отчётных документов по результатам деятельности системы управления рисками.

Обязанность всех работников Биржи сообщать обо всех известных им рисках и событиях рисков, а также предоставлять информацию по запросу ДОРИБиНБ.

Обязанность руководителей структурных подразделений, осуществляющих функции управления рисками, – проводить анализ событий и рисков, обеспечивать функционирование системы и реагирование в случае превышения пороговых значений контрольных показателей риск-аппетита.

Права руководителей структурных подразделений, осуществляющих функции управления рисками, – получать исчерпывающую информацию о рисках от работников структурных подразделений.

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

Ввиду существенной функциональной взаимозависимости, имеющей место в деятельности компаний Группы «Московская Биржа», руководители подразделений, курирующие вопросы управления рисками компаний Группы «Московская Биржа», на постоянной основе обмениваются информацией о событиях и выявленных рисках, а также о применяемых методах их снижения.

При Правлении могут создаваться коллегиальные консультативно-совещательные органы (далее - Комитеты), в состав которых могут входить представители риск-менеджмента компаний Группы «Московская Биржа».

Комитеты создаются для решения, в том числе, следующих задач:

- реализации согласованного подхода к вопросам управления рисками, возникающими в деятельности компаний Группы;
- обеспечения планирования взаимодействия подразделений компаний Группы «Московская Биржа» при внедрении процедур выявления, оценки, анализа рисков;
- анализа событий и фактов, которые могут создать угрозу интересам клиентов или оказать влияние на финансовую устойчивость, репутацию компаний Группы «Московская Биржа», определения их причин и выработки рекомендаций по их устранению.

14 Порядок назначения отдельного должностного лица, ответственного за реализацию мероприятий, осуществляемых Биржей в рамках управления отдельными видами рисков, и порядок его взаимодействия с должностным лицом (отдельным структурным подразделением), ответственным за организацию системы управления рисками, в случае принятия Биржей решения о назначении указанного лица

Назначение отдельного структурного подразделения, ответственного за реализацию системы управления рисками, определено Приказом Председателя Правления и утверждением Положения о ДОРИБиНБ Приказом Председателя Правления.

Квалификационные требования Директора ДОРИБиНБ проверяются на предмет соответствия законодательству. Должность Директора ДОРИБиНБ согласуется с Банком России.

Работники, ответственные за управление отдельными видами рисков, назначаются Приказом Председателя Правления.

Работники, которые должны предоставлять информацию об операционных рисках и событиях операционных рисков, назначены Приказом Председателя Правления. Ими являются все работники Биржи.

Работники, ответственные за реализацию отдельных мероприятий по минимизации рисков, осуществляют мероприятия в силу своих должностных обязанностей.

15 Порядок и периодичность обмена информацией о рисках Биржи между подразделениями Биржи, между подразделениями Биржи и органами управления Биржи, в том числе порядок доведения плана мероприятий и информации о его реализации, а также информации об ограничениях рисков и нарушениях установленных ограничений до сведения органов управления Биржи

Порядок и периодичность обмена информацией о рисках Биржи между подразделениями Биржи включает следующие мероприятия:

- Периодичность обмена информацией о рисках между структурными подразделениями: осуществляется на ежедневной основе в рабочем режиме;
- ДОРИБиНБ информирует об идентифицируемом риске подразделения, на которые оказывает влияние риск, и подразделения, участвующие в реализации мероприятий по минимизации риска в момент обнаружения;
- В случае идентификации угроз, риска высокого уровня влияния или события высокого уровня влияния, информация эскалируется органам управления в день обнаружения. В иных случаях информация направляется в рамках регулярной отчетности;
- В отношении анализа событий риска, оценки уровня риска и статусов выполнения мероприятий по минимизации риска проводятся встречи в рамках рабочих групп с обязательным участием ДОРИБиНБ с периодичностью не реже одного раза в месяц в следующем порядке:
  - Проводится анализ и обсуждение произошедших за отчетных месяц событий операционного риска;
  - Анализ статуса выполнения мероприятий по событиям, идентифицированным в предыдущих периодах.
- Информация о рисках подлежит ежегодному циклу инвентаризации в рамках самооценки рисков;
- Отчет о результатах проведенного нагрузочного тестирования предоставляется ДОРИБиНБ ответственным структурным подразделениям Блока информационных технологий в срок не позднее 10 дней с даты формирования отчета;
- В ходе работ по идентификации, оценке, мониторингу, контролю рисков ДОРИБиНБ, информирует работников Биржи 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.

Порядок обмена информацией о рисках Биржи между подразделениями Биржи и органами управления Биржи осуществляется путем предоставления регулярных и внеплановых (оперативных) отчётов о рисках.

Порядок и периодичность обмена информацией о плане мероприятий по минимизации рисков следующий:

- В рамках регулярной отчетности информация о мероприятиях по минимизации рисков предоставляется органам управления Биржи.
- Между компаниями Группы организован обмен информацией, позволяющий обеспечить прозрачность процессов и процедур отдельных компаний, а также их эффективное взаимодействие в рамках как текущей, так и проектной деятельности.

16 Порядок и периодичность (не реже одного раза в три месяца) составления и представления на рассмотрение органов управления Биржи отчетов и информации о результатах осуществления Биржей в рамках организации системы управления рисками процессов и мероприятий, по управлению отдельными видами рисков

Органам управления Биржи Директором ДОРИБиНБ и Начальником УФР предоставляется полная и своевременная информация, в том числе отчётность по нефинансовым и финансовым рискам соответственно, в соответствии со сроками и порядком, определённым в данном разделе Правил.

Отчетность подразделяется на регулярную и внеочередную (оперативную).

Регулярная отчётность включает в себя следующие отчеты:

- Отчётность по финансовым и нефинансовым рискам входит в состав отчётности по рискам Группы, предоставляемая ДОРИБиНБ Правлению и Комиссии по управлению рисками Наблюдательного Совета на ежеквартальной основе;
- Отчетность о показателях риск-аппетита, предоставляемая Директором ДОРИБиНБ Правлению не реже одного раза в месяц.

Порядок подготовки отчетности по рискам описывается в том числе в Политике по управлению финансовыми рисками.

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

Информация о выявленном событии риска с высокими убытками, существенном изменении уровня риска, проведении дополнительных специальных программ оценки риска предоставляется Директором ДОРИБиНБ Правлению и Председателю Правления Биржи не позднее десяти дней с даты выявления соответствующего нарушения.

Предоставление отчетности другим пользователям осуществляется по решению органов управления Биржи, за исключением случаев, когда такое предоставление отчетности осуществляется на основании федеральных законов и принятых в соответствии с ними нормативных правовых актов федерального органа исполнительной власти в области финансовых рынков.

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.

17 Содержание отчетов и информации о результатах осуществления Биржей процессов и мероприятий в рамках организации системы управления и в рамках управления отдельными видами рисков, представляемых на рассмотрение органов управления Биржи

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

Регулярная отчетность по нефинансовым рискам включает в себя:

- оценку рисков по основным направлениям деятельности Биржи, ее обоснование, включая сведения о нарушениях Биржей требований Закона об организованных торгах, принятых в соответствии с ним нормативных правовых актов Банка России, Устава Биржи и внутренних документов, связанных с деятельностью по организации торговли;
- меры, принятые для устранения выявленных нарушений и снижения рисков;
- сведения о выполнении рекомендаций;
- информацию о существенных событиях нефинансовых рисков;
- информацию о показателях мониторинга риск-аппетита, выявленных нарушениях ограничений (если применимо);
- иные сведения, предусмотренные внутренними документами Биржи.

Содержание регулярной отчетности по финансовым рискам раскрыто в Политике по управлению финансовыми рисками.

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

Отчетность, которая формируется по результатам проведения нагрузочного тестирования, содержит:

- информацию о том, в рамках какого релиза было проведено внутреннее нагрузочное тестирование;
- информацию о средних и максимальных показателях, достигнутых при разных пороговых значениях транзакций в секунду;
- заключение о корректности функциональности системы.

Протокол проведения нагрузочного тестирования формируется примерно за 3-4 дня до даты релиза, перед каждым релизом Торгово-клиринговой системы (далее – ТКС). Отчетность предоставляется работникам тестирования, работникам Релизного планирования и складывается в перечень документов по релизу.

Отчетность, которая формируется по результатам проведения тестирования аварийного восстановления, содержит хронологию проделанного анализа, а также замечания, которые были выявлены в ходе тестирования.

Отчетность формируется при получении результатов тестирования, которое проводится не реже, чем раз в год, и обязательно раскрывается для внутренних участников тестирования.

Отчетность, которая формируется по результатам проведения теста на проникновение (пентеста), содержит:

- отчет о проделанном анализе защищенности информационной системы;
- перечень слабостей, уязвимостей, анализ рисков;
- рекомендации по устранению и снижению рисков.

Отчётность формируется в процессе выполнения тестирования (предварительные версии), после завершения проведения пентеста и при формировании финальных версии.

Потребителями данной отчётности являются: владельцы проверяемой информационной системой, бизнес-владельцы, технические владельцы и ДОРИБиНБ.

18 Порядок управления рисками, связанными с оказанием поставщиками внешних услуг в течение всего периода их оказания, в случае заключения Биржей договоров на оказание внешних услуг с поставщиками услуг

В рамках управления операционными рисками выделяют процесс управления рисками, связанными с оказанием поставщиками услуг внешних услуг в течение всего периода их оказания. Заключение Биржей договоров на оказание внешних услуг с поставщиками услуг сопряжено со следующими рисками:

- не оказание услуги должным образом;
- не предоставление документов, подтверждающих факт выполнения договора;
- нарушение иных условий договора поставщиком, включая нарушение соглашения о конфиденциальности, предоставление недостоверных сведений.

Порядок управления рисками, связанными с оказанием поставщиками услуг внешних услуг:

- В целях управления рисками, связанными с оказанием поставщиками услуг, проводится оценка поставщиков, включая проверку достоверности сведений, предоставленных контрагентом, анализ и оценка его финансовой состоятельности, надежности и деловой репутации;
- Проводится оценка возможности использования резервных поставщиков;
- По результатам проведенной проверки делается заключение о возможности заключения договора с представленным контрагентом;
- В случае заключения Биржей договора на оказание услуг, связанных с осуществлением деятельности по проведению организованных торгов / обмена ЦФА (далее - внешние услуги), с третьим лицом (далее - поставщик услуг), система управления рисками обеспечивает предоставление Бирже информации и документов, сформированных поставщиком услуг в связи с оказанием внешних услуг, а также управление рисками, связанными с оказанием поставщиком внешних услуг в течение всего периода их оказания.

19 Порядок и периодичность (не реже одного раза в год) проведения самооценки, порядок документального оформления результатов самооценки

Самооценка риска представляет собой инструмент управления риском, который служит для выявления (идентификации) рисков, их анализа и оценки, а также оценки контролей и определения способов реагирования на риски. Решение о реагировании на операционный риск, включая риск информационной безопасности и риск, связанный с непрерывностью деятельности, принимается и утверждается директором ДОРИБиНБ, а в отдельных случаях может приниматься уполномоченными коллегиальными органами.

Целью Самооценки является выявление и оценка подразделениями Биржи нефинансовых рисков, присущих их деятельности. Самооценка представляет собой совместную работу Риск-менеджера и руководителей/работников различных структурных подразделений Биржи.

В ходе Самооценки проводится получение экспертной информации о видах и размере присущего риска, существующих контрольных процедурах для его предотвращения, их эффективности. В ходе Самооценки происходит выявление и оценка рисков и контролей на основе экспертного суждения руководителей/работников структурных подразделений в рамках выполняемых ими функций и задач.

Сведения, полученные в ходе Самооценки, используются в оценке операционного риска, как элемент проактивного подхода к управлению рисками, в том числе, в сценарном анализе, стресс-тестировании, прогнозировании возможных негативных исходов от реализации риска, what if анализе, построении карты рисков, определении показателей мониторинга риск-аппетита, оценке эффективности и совершенствовании контрольных процедур и т.д., и могут быть включены в регулярную отчетность по управлению риском.

Самооценка позволяет решать ряд важных для формирования эффективного управления рисками задач:

- выявление рисков до их реализации;
- повышение понимания проблематики управления рисками работниками непрофильных подразделений;
- выявление отсутствующих или чрезмерных контрольных процедур, областей контроля, несоразмерного бизнес-процессам структурного подразделений.

Самооценка проводится на регулярной основе, периодичность - не реже одного раза в год, а также может проводиться в случае запуска новых продуктов, изменения бизнес-процесса, необходимости актуализации Карты рисков. В рамках Самооценки также осуществляется пересмотр рисков, содержащихся в БДР.

При проведении самооценки могут использоваться информация из внешней и внутренней БДСОР, а также результаты предыдущей самооценки.

Перечень основных функциональных ролей участников самооценки операционных рисков:

- Эксперт;
- Риск-менеджер;

- Бизнес-владелец риска;
- Владелец риска;
- Ответственный за план.

Основные функции участников процесса самооценки операционных рисков.

Эксперт участвует в:

- анкетировании (интервьюировании) в рамках проводимых самооценок;
- экспертном определении тяжести потерь от реализации возможных рисковых сценариев (самооценка).

В роли эксперта может выступать любой работник, в том числе Бизнес-владелец риска и Владелец риска. Также выделяют риск-экспертов – руководителей отдельных структурных подразделений, ответственных за управление отдельными видами рисков (финансовыми, правовыми, налоговыми и т.д.). Роль риск-экспертов важна при оценке влияния видов рисков друг на друга и процессы в целом.

Риск-менеджер определяет:

- уровень проведения Самооценки (топ-менеджмент, линейный менеджмент, отдельные направления деятельности, подразделения или отдельные бизнес-процессы);
- сроки проведения Самооценки;
    f) перечень источников информации для формирования итогового заключения по Самооценке. Наиболее важным источником информации для выявления и оценки рисков является профессиональное суждение работников. Могут также использоваться выявленные события операционного риска, результаты тестирования контролей, данные анализа ключевых индикаторов риска, результаты внутреннего и внешнего аудита, стресс-тестирования операционного риска, информация о рисках, сопутствующих запуску новых проектов (риски продукта), информация, идентифицируемая в рамках ведения претензионной работы и иная.

Бизнес-владелец риска участвует в:

- принятии решения о реагировании на риски, информирование о решении Риск-менеджера;
- осуществлении мониторинга уровня риска при необходимости, информирование о результатах мониторинга Риск-менеджера;
- оценке эффективности существующих контролей по недопущению реализации риска и разработке предложений по их совершенствованию в случае необходимости;
- обеспечении реализации и соблюдения сроков реализации мероприятий по минимизации и контролю риска или определение лица, ответственного за выполнение мероприятий.

Решение о необходимости эскалации вопроса о реагировании на риск на более высокий управленческий уровень принимается Бизнес-владельцем риска экспертно либо на основании соответствующих внутренних документов при их наличии.

В случае решения о принятии риска Бизнес-владельцем риска разрабатывается план мониторинга данного риска (по итогам мониторинга может быть повторно принято решение о реагировании).

В случае решения о передаче риска Бизнес-владелец риска инициирует процедуры по разработке механизмов передачи риска.

В случае решения об избегании/удержании риска Бизнес-владелец риска разрабатывает план мониторинга риска, оценки эффективности контрольных мер или снижения бизнес-активности в этом направлении.

В случае решения о минимизации риска Бизнес-владелец риска инициирует подготовку поручения Владельцу риска о разработке планов внедрения контрольных процедур (мероприятий по минимизации риска).

Владелец риска участвует в:

- разработке и реализации плана мер по минимизации риска;
- информировании Бизнес-владельца риска или непосредственно Риск-менеджера о статусе выполнения мероприятий по недопущению реализации риска и/или совершенствованию существующих контролей.

План мер по минимизации риска согласуется с Риск-менеджером, Бизнес-владельцем риска, утверждается в установленном внутренними документами порядке и передается Риск-менеджеру, который осуществляет регулярный контроль за соблюдением планов внедрения контрольных процедур (оперативные отчеты передаются в адрес Бизнес-владельца риска, Владельца риска).

Риск-менеджер является координатором процедуры проведения Самооценки, обеспечивает методологическое сопровождение и консультирует участников процесса Самооценки.

Самооценка проводится в формате интервью и (или) анкетирования структурных подразделений с целью выявления рисков и оформления отчета по итогам проведения Самооценки, содержащего информацию о выявленных рисках.

Риск-менеджер информирует руководителей структурных подразделений о сроках проведения Самооценки по электронной почте.

Риск-менеджер согласовывает расписание встреч с работниками структурных подразделений либо проводит Самооценку в заочном формате (анкетирования).

В процессе Самооценки работник совместно с Риск-менеджером определяют следующие аспекты:

- какие риски существуют в структурном подразделении, процессах или в целом у Биржи, или какие события операционного риска могут происходить;
- факторы и источники риска, причины его возникновения;
- значимость каждого риска (тяжесть последствий);
- вероятность/возможность реализации риска;
- воздействие на другие виды риска (комплаенс, регуляторный стратегический риски и риски потери деловой репутации, правовой, риск проекта);
- оценка потенциальных последствий риска с точки зрения оценки финансового влияния на финансовую устойчивость Биржи посредством оценки события (событий) риска, наступление которого (которых), в том числе с учетом вероятности его (их) наступления и степени влияния, повлечет за собой возникновение у Биржи расходов (убытков);

- оценка потенциальных последствий риска с точки зрения влияния на непрерывность деятельности, т. е. возникновения последствий, влекущих за собой приостановление или прекращение оказания услуг по проведению организованных торгов в полном или неполном объеме.

В процессе анализа для каждого риска Риск-менеджером определяется присущий уровень риска (до внедрения контролей), остаточный уровень риска (с учетом контролей) и целевой уровень риска (желаемый уровень).

Для каждого риска определяется Владелец риска.

В случае, если целевой уровень риска ниже, чем остаточный, то прописываются планы мероприятий по минимизации риска, определяются ответственные за их исполнение, а также сроки по их минимизации. Контроль за исполнением плана мероприятий по минимизации осуществляет Риск-менеджер. В процессе Самооценки проводится сопоставление результатов оценки выявленных рисков с установленными критериями существенности последствий, к которым может привести реализация соответствующих рисков, в целях признания Биржей таких рисков значимыми, а также с установленным значением предельного уровня рисков (допустимого уровня рисков).

В процессе Самооценки проводится оценка эффективности контрольных процедур.

Участники Самооценки оценивают каждый риск и заполняют анкету по форме.

Результаты Самооценки собираются и систематизируются Риск-менеджером: выявляется наличие одного и того же риска, влияющего на разные структурные подразделения, также проводится сопоставление результатов Самооценки с размером совокупного предельного уровня рисков и т.п.

После сбора информации в рамках Самооценки, Риск-менеджер анализирует выявленные в ходе Самооценки риски, исходя из существующих контрольных процедур и остаточного уровня риска. Риск-менеджер формирует перечень выявленных в ходе Самооценки рисков, корректирующие мероприятия по которым необходимо проводить в первую очередь, и выносит их на рассмотрение Бизнес-владельца для принятия решения о реагировании на риск.

В отношении рисков возможны следующие варианты решений о реагировании:

- принятие риска;
- избегание/исключение риска (в частности, соответствующая деятельность приостанавливается);
- передача риска;
- снижение риска.

В большинстве случаев принимается решение о снижении риска с учетом корректирующих мероприятий, которые разрабатываются ответственными подразделениями совместно с Риск-менеджером. Разработка мер по снижению риска включает в себя следующую информацию:

- ФИО работников, ответственных за мероприятия;
- срок выполнения мероприятий;
- отметки об отнесении мероприятия к проекту или стратегической инициативе, номеру изменения или релизу, если применимо.
- Дальнейшая работа с риском проходит в соответствии с процедурами, описанными во внутренних документах по управлению операционным риском. Решение о реагировании на риск принимается Бизнес-владельцем с учётом оценки расходов на внедрение новых контролей и/или изменение процессов и оценки, получаемой в результате этих действий выгоды.

После проведения встреч Риск-менеджер составляет Карты рисков, согласует их с руководителями структурных подразделений по электронной почте. Карта рисков формируется исходя из шаблона для проведения Самооценки и определяется Риск-менеджером.

Если Самооценка проводится в заочном формате (анкетирования), уже составленные в ходе предыдущей Самооценки Карты рисков обновляются и согласуются с руководителями подразделений по электронной почте.

Риски, выявленные в ходе Самооценки, а также риски, выявленные «внепланово», т.е. по результатам произошедших инцидентов, изменений в бизнес-процессах, законодательстве, в процессе реализации проектов или инициатив, в результате

сценарного анализа и стресс-тестирования, внешних и внутренних проверок, а также результаты оценки информации о рисках заносятся в реестр рисков, который хранится в БДР.

Порядок документального оформления результатов самооценки, следующий:

- Ответственный работник ДОРИБиНБ заносит риски, идентифицированные в рамках Самооценки в матрицу рисков Самооценки.
- Ответственный работник ДОРИБиНБ подготавливает отчет о результатах Самооценки, содержащий сводный реестр рисков, карту рисков и сводную аналитическую информацию об исполнении мероприятий по рискам, идентифицированным в рамках предыдущей Самооценки.
- Отчеты или выдержки из них могут представляться органам управления Биржи по запросу.

20 Порядок и периодичность (не реже одного раза в шесть месяцев) проведения испытательных работ (тестирования) средств проведения торгов в соответствии с пунктом 1 приложения 1 к Положению о деятельности по проведению организованных торгов, а также порядок устранения недостатков, выявленных в результате их проведения

Для выявления (идентификации), анализа и оценки операционных рисков используется также стресс-тестирование программно-технических средств, используемых для осуществления деятельности по организации торговли, с периодичностью, определенной внутренними документами Биржи, но не реже одного раза в шесть месяцев.

Тестирование средств проведения организованных торгов осуществляются путем имитации технических условий, в которых проводятся реальные организованные торги, а при необходимости - путем проведения пробной эксплуатации.

При проведении стресс-тестирования обязательными сценариями тестирования являются:

- увеличения пиковой нагрузки тестируемых компонент не менее чем на 50% от максимальных величин за последние шесть месяцев;

- увеличение средней нагрузки не менее чем на 30% от усреднённых показателей нагрузки за последние шесть месяцев;
- увеличение объема обрабатываемых данных не менее чем на 30% от усреднённых дневных показателей за последние шесть месяцев.

Порядок проведения нагрузочного тестирования:

- Выбор полигона для проведения нагрузочного тестирования;
- Определение параметров проведения нагрузочного тестирования исходя из исторических значений пиковой нагрузки за предыдущие 52 недели;
- Согласование даты проведения нагрузочного тестирования с участниками торгов;
- Создание нагрузки на системы Биржи с превышением нагрузки от среднего значения.

Периодичность проведения нагрузочного тестирования - не реже одного раза в год с участниками торгов и при каждом релизе ТКС без их участия.

В рамках управления операционным риском Биржа обеспечивает осуществление следующих мероприятий:

- Устранение недостатков в работе средств проведения торгов, выявленных в результате проведения испытательных работ (тестирования) средств проведения торгов;

- Если в процессе проведения испытательных работ (тестирования) средств проведения торгов были обнаружены недостатки уровня critical, включая уязвимости защиты информации в средствах проведения торгов (их релизов), то такие средства (их релизы) не вводятся в эксплуатацию до устранения выявленных уязвимостей или замены ПО и/или оборудования.

Биржей предусмотрено несколько уровней контроля за обеспечением надежности ПО и оборудования, начиная от структурных подразделений, деятельность которых целиком предназначена для тестирования нового или доработанного функционала, модернизируемого оборудования, взаимодействия различных составных частей единого комплекса средств по обеспечению торгов до деятельности коллегиального

Комитета по изменениям, без санкции которого невозможно какое-либо изменение конфигурации торгово-клиринговых и обеспечивающих систем.

Порядок проведения теста на проникновение:

- Периодичность проведения теста на проникновение - не реже одного раза в год;
- Этапы проведения теста на проникновение:
  - Составление технического задания на работы;
  - Составление модели угроз для исследуемой информационной системы и исследуемого ПО;
  - Проведение анализа исходного кода программного обеспечения;
  - Проведение комплексного анализа защищенности информационных систем. Методики, применяемые для выполнения указанных работ, должны соответствовать, не ограничиваясь, методикам OSSTMM, NIST, PTES, OWASP;
  - Моделирование действий злоумышленника, направленных на достижение целей нарушения информационной безопасности (связанные с нарушением конфиденциальности и целостности информации, нарушением доступности сервиса, с нарушением принципа неотказуемости, с нарушением бизнес-логики) через эксплуатацию слабостей и уязвимостей информационных систем;
  - Проведение проверки устранения ранее выявленных уязвимостей в информационных системах Биржи;
  - Оценка рисков информационной безопасности;
  - Выработка рекомендаций для снижения выявленных рисков информационной безопасности.

Порядок проведения тестирования аварийного восстановления:

- Периодичность проведения тестирования - не реже одного раза в год;
- ДСТиВС готовит план тестирования, который подлежит обязательному согласованию с внутренними участниками тестирования, а также внешними участниками торгов;

- ДСТиВС совместно ДОРИБиНБ организует и проводит тестирование в соответствии с согласованным планом тестирования;
- По результатам тестирования ДОРИБиНБ составляет отчет, который подлежит обязательному согласованию с внутренними участниками тестирования;
- Для выявленных в ходе тестирования недочетов составляется план действий, который включает конкретные мероприятия, срок их выполнения и ответственных за их выполнение работников.

21 Порядок оценки 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

В рамках процесса управления рисками не реже одного раза в год проводится оценка эффективности управления рисками посредством анализа результативности своей деятельности, анализа качества, скорости и адекватности выполнения мероприятий по выявлению нарушений ограничений рисков, их устранению и (или) осуществлению иных мероприятий в рамках снижения рисков или их исключения.

Порядок оценки эффективности системы управления рисками:

- Установление в начале оцениваемого периода целевых показателей эффективности системы управления рисками для последующего проведения оценки;
- Проведение оценки эффективности, которая 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, а также проведение оценки качества и срока устранения нарушений целевых показателей, если таковые были, оценка даётся в качественных и количественных показателях;
- Оценка соответствия текущих значений показателей эффективности системы управления рисками показателям, установленным в начале отчетного периода;

- Если установленные показатели были достигнуты, то система управления рисками признается эффективной;
- Оценка эффективности включается в регулярную отчетность по рискам за квартал, в котором была проведена соответствующая оценка эффективности, на Правление и на Комиссию по рискам Наблюдательного совета.

Кроме того, в систему ключевых показателей эффективности включены метрики выполнения мероприятий по воздействию на риск и их эффективности, а для более объективного анализа также учитывается наличие ресурсов, выделенных на выполнение данных мероприятий.

Биржа регулярно проводит оценку эффективности управления рисками посредством анализа результативности своей деятельности по выявлению нарушений ограничений рисков, их устранению и (или) осуществлению иных мероприятий в рамках снижения этих рисков или их исключения. Система управления рисками, внедренная и поддерживаемая Биржей, должна оцениваться на предмет эффективности и результативности не реже одного раза в год.

Оценка эффективности системы управления рисками также осуществляется СВА как подразделением, структурно независящим от подразделений риск-менеджмента (в частности, ДОРИБиНБ), не реже одного раза в год.

Анализ эффективности системы управления рисками осуществляется на основе анализа результативности деятельности по выявлению нарушений ограничений рисков, их устранению и (или) осуществлению иных мероприятий в рамках снижения этих рисков или их исключения.

Для анализа результативности деятельности по управлению рисками в рамках действующей системы управления рисками могут быть выбраны различные действующие методы оценки с установленными критериями оценки результативности. Выбор методов оценки и установление пороговых значений для проведения оценки в определенном временном периоде функционирования системы управления рисками утверждается органом управления Биржи. Сбор данных и анализ результативности, их представление для отчета производят работники ДОРИБиНБ.

Под эффективностью системы управления рисками Биржи подразумевается способность системы решать следующие задачи и достигать следующие цели:

- Отсутствие существенных потерь, влияющих на достаточность капитала и выполнение стратегических целей;
- Отсутствие фактов нарушения риск-аппетита;
- Соблюдение лимитов и ограничений, установленных в рамках системы управления рисками;
- Своевременность выполнения рекомендаций СВА и внешних аудиторов в области системы управления рисками;
- Своевременность и успешность проведения испытательных работ (тестирования) средств проведения торгов;
- Успешное проведение тестирования планов ОНИВД.
- Оценка полноты и точности информации, отраженной в БДСОР, а также корректности ее ведения;
- Оценка корректности определения вида и величины потерь от реализации событий риска (в частности, операционного риска);
- Оценка корректности проведенных оценок величины потерь от реализации риска (в частности, операционного риска);
- Оценка полноты и качества мероприятий, направленных на снижение риска (в частности, операционного риска).

22 Порядок принятия Биржей мер по предотвращению и урегулированию конфликта интересов, возникающего у Биржи в связи с совмещением им своей деятельности с иными видами деятельности

Для целей предотвращения конфликта интересов устанавливается система управления конфликтами интересов, действующая на основе следующих принципов:

- обеспечение организационной и (или) функциональной независимости работников Биржи, в том числе руководителей подразделений, созданных для осуществления деятельности Оператора финансовой платформы и деятельности Организатора торговли / Оператора обмена ЦФА, если отсутствие указанной организационной и (или) функциональной

независимости приводит или может привести к возникновению или реализации конфликта интересов;

- ограничение обмена и (или) контроль за обменом информацией между работниками Биржи и иными лицами, если указанный обмен информацией приводит или может привести к возникновению или реализации конфликта интересов;
- обеспечение отсутствия в системах оплаты труда работников Биржи, а также вознаграждения лиц, действующих за счет Биржи, условий, которые приводят или могут привести к возникновению конфликта интересов;
- обеспечение контроля за действиями работников Биржи, а также лиц, действующих за счет Биржи, если они приводят или могут привести к возникновению или реализации конфликта интересов;
- предоставление потребителю финансовых услуг и клиенту информации об имеющихся у него рисках, вызванных конфликтом интересов;
- ограничение в осуществлении (непосредственно или опосредованно) сделки за свой счет, в которых используется служебная информация клиента, ставшая известной работникам Биржи и способная оказать негативное влияние на интересы и права потребителей финансовых услуг, а также передавать указанную информацию третьим лицам;
- информирование потребителей финансовых услуг и клиентов о совмещении различных видов деятельности, а также о существовании, в связи с этим риска возникновения конфликта интересов, в том числе, путем размещения информации на сайте Биржи в сети Интернет;
- внедрение практики двойного контроля (соблюдение принципа четырех глаз);
- выявление потенциальных рисков возникновения конфликта интересов при приеме на работу работников, в чьей деятельности может возникать конфликт интересов, а также установление соответствующих требованиям к личным, профессиональным качествам кандидатов и их репутации;
- обязательное раскрытие сведений о реальном или потенциальном конфликте интересов;
- индивидуальное рассмотрение каждого конфликта интересов, оценка рисков и принятие мер, направленных на разрешение такого конфликта интересов;

- конфиденциальность процесса раскрытия сведений о конфликте интересов и процесса урегулирования;
- соблюдение баланса интересов Биржи и его работников при урегулировании конфликта интересов.

В целях управления данным видом риска проводятся регулярные процедуры 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.

23 Порядок разработки и утверждения плана непрерывности бизнеса

План непрерывности бизнеса (далее – План) разрабатывается ДОРИБиНБ совместно с руководителями соответствующих структурных подразделений. План утверждается решением Наблюдательного совета. План подлежит пересмотру не реже, чем один раз в год, а также в случае существенных изменений в инфраструктуре Биржи (появление новых офисов, смена перемещения более 20% кадрового состава и т. д.).

Плана подлежит тестированию не реже, чем один раз в год. План подлежит активации при обнаружении существенных инцидентов, представляющих потенциальную угрозу для деятельности Биржи. По итогам анализа инцидента определяется уровень опасности, в зависимости от которого:

- может быть принято решение об устранении инцидента в рабочем порядке;
- активированы планы технологического восстановления систем Биржи;
- активированы планы ОНиВД;
- объявлен режим ЧС.

При оценке уровня опасности используются следующие определения:

- Потеря объекта (офиса или ЦОД) - безвозвратная гибель (пожар, разрушение и т. п.), приводящая к необходимости обустройства нового объекта;
- Недоступность объекта/ офиса - временная невозможность доступа работников (в связи с действиями силовых структур, чрезвычайными ситуациями и т. п.), либо полное отсутствие коммуникаций (по основным и резервным каналам), либо сбой инженерных систем (в т. ч. гарантированного

электроснабжения), приводящий к невозможности эксплуатации объекта. Офис – любой из ключевых офисов Биржи;

- Потеря ИТ сервисов - недоступность ключевых ИТ систем. Пример: недоступность основных и вспомогательных торговых и клиринговых систем Группы;
- Потеря персонала - массовая недоступность ключевых работников. Примеры: эпидемии, недоступность общественного транспорта в округе расположения офиса и т. д.

24 Порядок и периодичность оценки плана непрерывности бизнеса в целях определения достаточности содержащихся в нем мер для обеспечения непрерывности осуществления деятельности по организации торгов, а также порядок пересмотра плана непрерывности бизнеса в случае выявления недостаточности содержащихся в нем мер для обеспечения непрерывности осуществления деятельности по организации торгов

Оценка Плана непрерывности бизнеса содержит в себе следующие мероприятия:

- ежегодный пересмотр Плана непрерывности бизнеса на предмет актуальности, в т. ч. случае существенных изменений в инфраструктуре Биржи (появление новых офисов, смена/перемещение более 20% кадрового состава и т. п.);
- внесение изменений и комментариев, полученных в рамках анализа воздействия на бизнес от структурных подразделений Биржи;
- согласование новой редакции Плана непрерывности бизнеса со всеми вовлеченными подразделениями и утверждение уполномоченным коллегиальным органом.

25 Порядок выявления чрезвычайных ситуаций и проведения анализа обстоятельств их возникновения

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.

В рамках управления рисками непрерывности деятельности Биржи определяются порядок, способы и сроки осуществления комплекса мероприятий по предотвращению

или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования Биржи (подразделений), вызванного непредвиденными обстоятельствами (возникновением ЧС или иным событием, наступление которого возможно, но трудно предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению Биржей принятых на себя обязательств), составляется План непрерывности бизнеса, описываются процессы функционирования и определяются приоритеты деятельности Биржи от момента объявления ЧС до момента перехода к нормальному функционированию и впоследствии отмены действия режима ЧС, рассматривается наихудший из возможных сценариев (недоступность основного офиса; недоступность основного центра обработки данных; недоступность основного офиса и недоступность основного центра обработки данных).

Биржа обеспечивает осуществление следующих мероприятий:

- Выявление чрезвычайных ситуаций и проведение анализа обстоятельств возникновения чрезвычайных ситуаций. Данный процесс регламентируется внутренними документами по операционным рискам и непрерывности бизнеса;
- Поддержание резервного офиса на уровне, обеспечивающем возможность функционирования всех критически важных процессов Биржи, и поддержание таких процессов в течение не менее одного месяца с момента возникновения чрезвычайной ситуации.

Выявление чрезвычайных ситуаций и анализ обстоятельств их возникновения являются существенной частью при организации системы управления рисками Биржи.

26 Порядок ведения Биржей перечня потенциальных чрезвычайных ситуаций

Порядок ведения перечня потенциальных ЧС включает в себя следующие действия:

- определение областей, в рамках которых Биржа может быть подвержен рискам непрерывности бизнеса;
- выделение перечня потенциальных ЧС, реализация которых может привести к нарушению хода критичных процессов, определенных на этапе анализа воздействия на бизнес;

- анализ степени влияния потенциальных ЧС на Биржи в случае их реализации, в т. ч. на:
  - работников Биржи;
  - средства проведения торгов Биржи;
  - инфраструктуру Биржи;
  - оценку вероятности реализации угрозы;
  - анализ существующих контрольных процедур;
  - определение возможных мер по минимизации рисков.

27 Порядок распределения ответственности и полномочий между структурными подразделениями Биржи и их работниками в случае реализации существенных событий операционного риска

Порядок распределения ответственности и полномочий между структурными подразделениями Биржи и их работниками в случае реализации НС содержит в себе следующее:

- При возникновении существенного события операционного риска (далее – нештатная ситуация или НС) собирается Рабочая группа, состоящая из работников компаний Группы «Московская Биржа» и осуществляющая первичную оценку события, которая принимает решение о действиях в конкретной ситуации и (или) о созыве Рабочей группы в расширенном составе, в состав которой входят члены Правления ПАО Московская Биржа, а также координирует действия компаний Группы «Московская Биржа» по регулированию НС. В случае появления необходимости внештатного изменения установленных лимитов Биржа действует в соответствии с Регламентом действий подразделений ПАО Московская Биржа, НКО НКЦ (АО), НКО АО НРД, АО НТБ в нештатных ситуациях при проведении торгов и клиринга;
- Любой работник, обнаруживший НС или признаки возникновения НС, обязан сообщить об этом работнику, включённому в Рабочую группу;
- Член Рабочей группы, получивший информацию об НС, обязан немедленно приступить к выяснению характера возможной причины и последствий НС;

- Проводится анализ возникшей НС и определение мер, необходимых для принятия решения по урегулированию НС, в том числе по приостановлению торгов, закрытию торгов, изменению времени проведения торгов, клиринга и/или расчетов в соответствии с правилами торгов и/или клиринга, а также определение мер по информированию участников, регулирующих органов, контрагентов о последствиях НС;
- Осуществляется мониторинг хода выполнения мероприятий по урегулированию последствий НС;
- Пресс-служба Биржи осуществляет регулярное уведомление (на официальном сайте ПАО Московская Биржа в сети Интернет и/или средствах массовой информации) участников торгов/участников клиринга о возникшей НС и мерах, предпринимаемых компаниями Группы «Московская Биржа» для устранения последствий НС. После 18:00 уведомление может осуществляться работниками Операционного департамента (на официальном сайте ПАО Московская биржа в сети Интернет);
- При возникновении НС, которая привела к приостановке торгов, член Рабочей группы незамедлительно информирует ДОДа. ДОД незамедлительно организовывает и, не позднее 15 минут после обнаружения НС, обеспечивает раскрытие информации о НС на официальном сайте ПАО Московская Биржа в сети интернет;
- ДОД координирует деятельность работников Биржи в целях:
  - направления по системе оперативного информирования сообщения о НС участникам торгов, руководству, Банку России, вендорам;
  - информирования Банка России;
  - сбора Рабочей группы в расширенном составе.

- При возникновении НС, которая не привела к приостановке торгов, член Рабочей группы оповещает весь состав участников Рабочей группы о сборе конференции.

- Член рабочей группы, получивший информацию о НС, докладывает:
  - о времени получения информации о НС;
  - о работнике, сообщившем о НС;
  - о характере причин и последствий НС.

Члены Рабочей группы вырабатывают коллегиальное решение о действиях в НС:

- При принятии решения о приостановке торгов, такая приостановка осуществляется не позднее, чем через пятнадцать минут с момента выявления технического сбоя;
- При принятии решения о сборе Рабочей группы в расширенном составе ДОД организует работу в соответствии со следующим порядком:
  - Общую координацию по организации и работе Рабочей группы в расширенном составе осуществляет ДОД;
  - Для организации работы Рабочей группы в расширенном составе ДОД инициирует информирование его членов и обеспечивает организацию конференции в целях проведения совещания.

После устранения причин НС и/или восстановления штатного функционирования ПТК ДОД обеспечивает:

- Не позднее чем за 15 минут до времени возобновления торгов, раскрытие на официальном сайте ПАО Московская Биржа в сети интернет информации о времени доступности торговой системы для снятия заявок, времени возобновления и регламенте проведения торгов. Раскрытие информации на официальном сайте ПАО Московская Биржа в сети Интернет осуществляется работниками ОД;
- Направление по СОИ сообщения участникам торгов, руководству компаний Группы «Московская Биржа», а также Банку России и вендорам о времени возобновления и регламенте проведения торгов. Направление сообщений по СОИ осуществляется работниками ОД;
- Направление сообщения о времени возобновления и регламенте проведения торгов в Банк России. Направление сообщения в Банк России осуществляют работники СВК;
- Информирование представителя Банка России о времени возобновления и регламенте торгов;
- Информирование организаций, заключивших с ПАО Московская Биржа договоры о взаимодействии при проведении кредитных и депозитных

операций, о времени возобновления проведения операций по размещению средств на депозиты в банках;

- В случае необходимости переноса иных регламентных операций, которые могут затронуть участников торгов соответствующая компания Группы «Московская Биржа» размещает необходимое уведомление о переносе регламентных операций на своем официальном сайте в сети Интернет, за исключением тех случаев, когда подобное уведомление нельзя реализовать по причине технического сбоя;
- Взаимодействие со СМИ и их информирование;
- По факту произошедшего существенного события операционного риска ДОРИБиНБ организует работу по формированию плана мероприятий по урегулированию события и снижению негативных последствий от его реализации совместно с ответственными подразделениями, а также организует разработку плана мероприятий по предотвращению повторения события в будущем с указанием сроков и ответственных за реализацию мероприятий;
- ДОРИБиНБ контролирует соблюдение сроков и факт реализации планов мероприятий, упомянутых в предыдущем пункте, также может разработать КИР для целей мониторинга уровня риска, связанного с произошедшим существенным событием операционного риска;
- Если существенное событие операционного риска привело к нарушению установленных пороговых значений риск-аппетита, проводится эскалация информации и предоставление отчетности Правлению, Комиссии по рискам Наблюдательного совета и Наблюдательному Совету.

28 Порядок проведения оценки Правил управления рисками

Биржа проводит оценку Правил управления рисками по мере необходимости (но не реже одного раза в год) на предмет их актуальности и эффективности и в случае выявления в них неактуальных сведений и (или) мер, по оценке Биржи не обеспечивающих эффективность функционирования системы управления рисками, осуществляет пересмотр настоящих Правил.