

**УТВЕРЖДЕНЫ**

Решением Наблюдательного Совета  
Акционерного общества  
«Национальная товарная биржа»  
08 июня 2021 г., Протокол № 17

**ПРАВИЛА УПРАВЛЕНИЯ РИСКАМИ,  
СВЯЗАННЫМИ С ОСУЩЕСТВЛЕНИЕМ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАТОРА  
ТОРГОВЛИ**

**Москва, 2021 г.**

## Содержание

1	Термины и определения, используемые в настоящих Правилах .....	5
2	Общие положения, определяющие цели управления рисками.....	14
3	Критерии существенности последствий, к которым может привести реализация рисков Организатора торговли, в целях признания Организатором торговли таких рисков (за исключением операционного риска Организатора торговли) значимыми, а также порядок сопоставления результатов оценки выявленных рисков Организатора торговли с указанными критериями.....	16
4	Методика определения предельного размера рисков (допустимого уровня рисков) Организатора торговли, а также совокупного предельного размера рисков Организатора торговли .....	17
5	Порядок выявления нарушений ограничений рисков .....	18
6	Порядок осуществления мероприятий по устранению выявленных нарушений ограничений рисков и (или) иных мероприятий в отношении рисков Организатора торговли в рамках снижения таких рисков Организатора торговли или их исключения 19	19
7	Порядок осуществления процессов и мероприятий по выявлению, анализу, мониторингу риска, и обмену информацией между подразделениями и органами управления Организатора торговли, а также порядок осуществления процессов и мероприятий, осуществляемых Организатором торговли в рамках управления отдельными видами рисков Организатора торговли.....	20
8	Порядок обеспечения контроля за выполнением процессов и мероприятий по выявлению, анализу, мониторингу риска, и обмену информацией между подразделениями и органами управления Организатора торгов, а также порядок осуществления процессов и мероприятий, осуществляемых Организатором торговли в рамках управления отдельными видами рисков Организатора торговли .....	54
9	Порядок внесения рисков Организатора торговли и результатов их оценки в реестр рисков Организатора торговли, порядок осуществления оценки реестра рисков Организатора торговли на предмет его актуальности, а в случае выявления в реестре рисков Организатора торговли неактуальных сведений - на предмет пересмотра реестра рисков Организатора торговли.....	56
10	Порядок ведения базы данных о событиях операционного риска .....	57
11	Порядок и периодичность (не реже одного раза в год) проведения идентификации угроз, которые по оценке Организатора торговли могут привести к неработоспособности средств проведения торгов .....	59
12	Порядок ведения базы данных о расходах (убытках), понесенных Организатором торговли вследствие реализации событий операционного риска Организатора торговли.....	62
13	Права и обязанности органов управления Организатора торговли, руководителей и работников структурных подразделений Организатора торговли, 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.....	63
14 Порядок назначения отдельного должностного лица, ответственного за реализацию мероприятий, осуществляемых Организатором торговли 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 Организатором торговли решения о назначении указанного лица .....	66
15 Порядок и периодичность обмена информацией о рисках Организатора торговли между подразделениями Организатора торговли, между подразделениями Организатора торговли и органами управления Организатора торговли, 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 Организатора торговли .....	67
16 Порядок и периодичность (не реже одного раза в три месяца) составления и представления на рассмотрение органов управления Организатора торговли отчетов и информации о результатах осуществления Организатором торговли в рамках организации системы управления рисками процессов и мероприятий, по управлению отдельными видами рисков .....	68
17 Содержание отчетов и информации о результатах осуществления Организатором торговли процессов и мероприятий в рамках организации системы управления и в рамках управления отдельными видами рисков, представляемых на рассмотрение органов управления Организатора торговли .....	70
18 Порядок управления рисками, связанными с оказанием поставщиками внешних услуг в течение всего периода их оказания, в случае заключения Организатором торговли договоров на оказание внешних услуг с поставщиками услуг .....	70
19 Порядок и периодичность (не реже одного раза в год) проведения самооценки, порядок документального оформления результатов самооценки .....	71
20 Порядок и периодичность (не реже одного раза в шесть месяцев) проведения испытательных работ (тестирования) средств проведения торгов, а также порядок устранения недостатков, выявленных в результате их проведения.....	77
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 .....	80
22 Порядок принятия Организатором торговли мер по предотвращению и урегулированию конфликта интересов, возникающего у Организатора торговли в связи с совмещением им своей деятельности с иными видами деятельности .....	82
23 Порядок разработки и утверждения плана непрерывности бизнеса .....	84
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 .....	85
25 Порядок выявления чрезвычайных ситуаций и проведения анализа обстоятельств их возникновения .....	85
26 Порядок ведения Организатором торговли перечня потенциальных чрезвычайных ситуаций.....	86
27 Порядок распределения ответственности и полномочий между структурными подразделениями Организатора торговли/компаний Группы и их работниками в случае реализации существенных событий операционного риска .....	87
28 Порядок проведения оценки Правил управления рисками .....	90

## **1 Термины и определения, используемые в настоящих Правилах**

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

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

**Бизнес-владелец риска** – единоличный или коллегиальный орган Организатора торговли или руководитель структурного подразделения Организатора торговли, 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 Организатора торговли. 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/АО НТБ/Организатор торговли** – Акционерное общество «Национальная товарная биржа», АО НТБ, Организатор торговли

**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.

**Владелец плана** - руководитель структурного подразделения, ответственный за координацию мероприятий по минимизации негативных последствий СОР или возможных негативных последствий риска.

**Внешняя база данных о событиях операционных рисков (внешняя БДСОР)** – электронное хранилище информации о внешних событиях операционного риска, которые произошли вне Организатора торговли.

**ВПТС** – внешние программно-технические средства проведения торгов.

**Группа/Группа «Московская Биржа»**– Группа «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 Организатора торговли, а также действий его акционеров и аффилированных лиц.

**Заключение о рисках** – профессиональное суждение работников подразделений риск-менеджмента и СВК 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 Организатора торговли.

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

**Комплаенс риск** – риск возникновения у Организатора торговли 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 из (но не единственной) составляющих комплаенс-рисков.

**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 Организатора торговли влияет или может повлиять на добросовестное и эффективное исполнение ими должностных обязанностей и может привести к неблагоприятным последствиям для Организатора торговли, ее 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, при которой деятельность продолжает осуществляться в измененном виде, в частности, за счет внедрения новых или оптимизации существующих контрольных процедур.

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

**Нештатная ситуация (НС)** – обстоятельства, вызывающие и/или создающие предпосылки к возникновению сбоев (отказов) при эксплуатации подсистем программно-технического комплекса Организатора торговли 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 АО НТБ и другими компаниями Группы «Московская Биржа», Банком России, АО «Объединенная зерновая компания», Государственной корпорацией "Банк развития и внешнеэкономической деятельности (Внешэкономбанк)", Государственным учреждением - Пенсионный фонд Российской Федерации и Федеральным казначейством;

- 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 Организатора торговли для соответствующего рынка;

- могут привести к приостановке деятельности АО НТБ;

- вызвали или могут вызвать аномальные ситуации на соответствующих рынках;

- могут привести к существенному изменению условий исполнения сделок, заключаемых на организованных торгах, либо существенным образом повлиять на права и обязанности сторон по соответствующим сделкам, либо каким-либо образом препятствовать их исполнению и/или нормальному ходу торгов, включая, но не ограничиваясь:

- i. принятие государственным органом Российской Федерации или уполномоченным органом иностранного государства (союза государств), Банком России и центральными банками иностранных государств (союза государств), а также организациями, наделенными функциями центральных банков, какого-либо нормативно-правового или иного акта, вводящего любые торгово – экономические санкции, ограничительные меры, или запрет на операции с иностранной валютой или иные меры, делающие невозможным осуществление расчетов в иностранной валюте;
- ii. возникновение факторов, которые в значительной степени влияют либо могут повлиять на формирование цены финансового инструмента, в том числе, цены базового актива (аналогичного срочного контракта, торгуемого на иностранной бирже);
- iii. прекращение / приостановление опубликования значений расчетных цен срочных контрактов, торгуемых на иностранных биржах, либо возникновение

обстоятельств, препятствующих получению расчетных цен срочных контрактов, торгуемых на иностранных биржах, либо делающих использование соответствующих расчетных цен незаконным.

- связаны с получением от государственных органов Российской Федерации, Банка России писем, предписаний, постановлений, иных документов предписывающего характера:

- i. оказывающих влияние на допуск участника(ов) торгов к участию в торгах и (или) допуск участника(ов) клиринга к клиринговому обслуживанию;
- ii. влекущих необходимость изменения порядка проведения организованных торгов и клиринга и (или) условий осуществления отдельных операций, в том числе с отдельными Активами/в отдельных режимах;
- iii. иным образом влияющих на стандартное функционирование АО НТБ, в том числе на нормальный ход организованных торгов/клиринга.

**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 Организатора торговли, используемых для предоставления финансовых услуг.

**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) Организатора торговли в результате сбоев и (или) ошибок программно-технических средств Организатора торговли, включая программно-технические средства и информационно-коммуникационные средства связи, с помощью которых обеспечивается проведение организованных торгов, и (или) во внутренних бизнес-процессах Организатора торговли, ошибок работников и (или) в результате внешних событий, оказывающих негативное воздействие на деятельность Организатора торговли.

**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 Организатора торговли, 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 (План ОНиВД)** - внутренний документ Организатора торговли, определяющий цели, задачи, порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования Организатора торговли (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 Организатором торговли принятых на себя обязательств).

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

**Предельный уровень риска (риск-аппетит)** – это максимальный уровень риска, который Организатора торговли готов 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 Организатора торговли. 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, представляющих ценность для компаний Группы «Московская Биржа», а также для третьих лиц.

**ПТК** - Программно-технический комплекс Организатора торговли.

**Регуляторный риск** – риск возникновения у Организатора торговли расходов (убытков) и (или) иных неблагоприятных последствий в результате несоответствия деятельности, осуществляемой им на основании лицензии Организатора торговли или лицензии торговой системы, требованиям законодательства Российской Федерации, регулирующего деятельность Организатора торговли, правилам организованных торгов, учредительным и иным документам Организатора торговли, и (или) в результате применения мер в отношении Организатора торговли со стороны Банка России.

**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 Организатор торговли 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.

**Риск-события** – в терминах Правил события нефинансовых рисков, т.е. события операционного, репутационного, стратегического и регуляторного (комплаенс), правового, проектного риска, риска информационной безопасности.

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

- возникновение потерь Организатора торговли, его клиентов, контрагентов;
- нарушение непрерывного предоставления Организатора торговли финансовых и (или) информационных услуг в условиях реализации информационных угроз;
- невыполнение обязательств по обеспечению защиты интересов клиентов Организатора торговли 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) Организатора торговли или иные негативные последствия в

результате негативного восприятия Организатора торговли со стороны контрагентов Организатора торговли, участников торгов и их клиентов, акционеров Организатора торговли, Банка России и иных лиц, которые могут негативно повлиять на способность Организатора торговли поддерживать существующие и (или) устанавливать новые деловые отношения и поддерживать на постоянной основе доступ к источникам финансирования (далее - РПДР).

**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.

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

**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 Организатору торговли убытков (возникновения расходов).

**Совокупный предельный уровень рисков** – максимальная величина потенциальных убытков, которые Организатор торговли может понести в случае реализации рисков, предусмотренных его риск-аппетитом.

**СОИ** - Система оперативного информирования.

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

**Стресс-тестирование нефинансовых рисков** – это моделирование различных негативных сценариев реализации нефинансовых рисков, влекущих финансовые и нефинансовые последствия для Организатора торговли. 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, используемые Организатором торговли.

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

**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 Организатора торговли;
- неработоспособность (недоступность) основных каналов связи, в том числе корпоративной сети Организатора торговли, информационно-телекоммуникационной сети Интернет, других каналов связи с взаимодействующими организациями, необходимых для выполнения критичных процессов Организатора торговли;
- отсутствие физической возможности нахождения работников Организатора торговли 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 Организатора торговли.

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

**Чрезвычайная ситуация (ЧС)** - это совокупность внешних воздействий, способных нарушить режим нормального функционирования Организатора торговли и его способность выполнять принятые на себя обязательства, вследствие чего Организатор торговли может понести убытки. При этом, под внешним 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 Организатора торговли.

**Эксперт** – работник подразделения, принимающего участие в самооценке, владелец процессов, подверженных самооценке.

**Дежурный операционный директор** – работник ПАО Московская Биржа, осуществляющий организацию и координацию работы в кризисных условиях, обладающий компетенциями и наделенный полномочиями.

**Комитет по продуктам и проектам при Правлении ПАО Московская Биржа (КПП)** – консультативно-совещательный орган при Правлении ПАО Московская Биржа, 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 КПП;
- Обеспечение взаимодействия между компаниями Группы «Московская Биржа» при принятии решений по проектам и продуктам за счет включения в состав КПП представителей компаний Группы.

**Управление развития и сопровождения торгов** – структурное подразделение АО НТБ.

**СВА** – Служба внутреннего аудита. Структурное подразделение АО НТБ.

**СВК** – Служба внутреннего контроля. Структурное подразделение АО НТБ.

**СУР** – Система управления рисками.

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

**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.

**TRP (Technology Recovery Plan)** - План технологического восстановления систем Организатора торговли.

Термины, специально не определенные в Правилах, используются в значениях, определенных во внутренних документах Организатора торговли, 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 (далее - Правила), являются основополагающим документом, определяющим основные принципы организации системы управления рисками в Акционерном обществе «Национальная товарная биржа» (далее – Биржа, Организатор торговли, АО НТБ), связанными с организацией торгов, а также с осуществлением операций с собственным имуществом (далее при совместном упоминании - риски Организатора торговли), и формируют регулятивную основу для построения эффективно работающей системы управления рисками, соответствующей масштабам деятельности Организатора торговли.

2.2. Правила разработаны на основании требований:

- Федерального закона от 21.11.2011 г. №325-ФЗ «Об организованных торгах» (далее – Закон об организованных торгах);
- Положения Банка России от 17 октября 2014 г. №437-П «О деятельности по проведению организованных торгов»;
- 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 Организатора торговли являются:

- ограничение принимаемых рисков по всем направлениям деятельности в соответствии с собственными стратегическими задачами и целями;
- обеспечение достаточности собственных средств на покрытие принимаемых рисков;
- обеспечение надежного функционирования бизнес-процессов Организатора торговли.

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 Организатора торговли в процессе выявления рисков;
- качественная и количественная оценка (измерение) рисков;
- установление порядка предоставления отчетности по вопросам управления рисками органам управления Организатора торговли;

- 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. Организатором торговли сформировано отдельное структурное подразделение, ответственное за организацию системы управления рисками – Служба по управлению рисками, руководство которым осуществляет руководитель Службы по управлению рисками.

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

3.1 Организатор торговли 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 Организатора торговли;
- Финансовый убыток, превышающий предельное, установленное на текущий год значение для соответствующего вида риска;
- Нарушение работоспособности ключевых систем Организатора торговли;
- Нарушение сроков реализации ключевых проектов на срок 12 и более месяцев;
- Существенное увеличение стоимости реализации ключевых проектов;



- Существенное снижение доходности реализуемых проектов;
- Существенное снижение доходности по ключевым продуктам Организатора торговли;
- Существенные утечки информации, успешные атаки на ключевые системы Организатора торговли;
- Иные последствия, способные оказать существенное негативное влияние на деятельности Организатора торговли.

3.2. Для сопоставления результатов оценки выявленных рисков Организатора торговли с указанными критериями Организатор торговли придерживается следующего порядка действий:

- 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.

3.3. 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) Организатора торговли, а также совокупного предельного размера рисков Организатора торговли**

4.1. В целях определения предельного уровня риска, а также совокупного предельного размера рисков Организатор торговли использует следующие подходы:

- оценка размера реализации риска производится на основе 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;

- проведение сценарного анализа осуществляется по наиболее вероятным сценариям реализации риска и установление показателей на уровне полученных значений;
- проведение оценки влияния потенциальных убытков на финансовые результаты Организатора торговли и установление предельных показателей устанавливается исходя из размера потенциального убытка, при котором отсутствует влияние на реализацию стратегических инициатив Организатора торговли;
- проведение стресс-тестирований риска проводится для установления предельных ожидаемых убытков от реализации риска.

4.2. 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 Организатора торговли.

4.3. Детальнее методика определения предельного размера рисков (допустимого уровня рисков) Организатора торговли, а также совокупного предельного размера рисков Организатора торговли регламентирует Методика определения контрольных показателей риск-аппетита.

4.4. Предельные показатели риска устанавливаются Наблюдательным Советом Организатора торговли на каждый календарный год.

## **5 Порядок выявления нарушений ограничений рисков**

5.1. 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 Службой по управлению рисками.

5.2. 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;
- если достигаются сигнальные значения показателей, то об этом информируются члены Правления АО НТБ;

- если достигаются (преодолеваются) пороговые значения показателей риск-аппетита, то об этом информируется Наблюдательный Совет АО НТБ.

5.3. По результатам мониторинга риск-аппетита формируется отчет, представляемый руководителем Службы по управлению рисками на рассмотрение Правления 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).

5.4. 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 Организатором торговли.

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

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

- определяют причину нарушения ограничения риска или определяют факторы, которые могут способствовать реализации выявленного риска;
- определяют возможные последствия, которые могут возникнуть вследствие реализации такого риска;
- определяют работников Организатора торговли, ответственных за область возникновения факторов риска и за область последствий реализации риска;
- разрабатывают с работниками, указанными выше, набор мероприятий, направленных на устранение факторов риска, либо мероприятий, направленных на снижение тяжести последствий реализации риска, либо мероприятий, направленных на исключение риска;
- согласовывают с руководителями структурных подразделений Организатора торговли ответственных и сроки реализации указанных мероприятий;
- осуществляют регулярный контроль за сроками и фактом выполнения назначенных мероприятий;
- при необходимости формируют отчетность по статусу выполнения мероприятий для коллегиальных органов управления Организатора торговли.

## **7 Порядок осуществления процессов и мероприятий по выявлению, анализу, мониторингу риска, и обмену информацией между подразделениями и органами управления Организатора торговли, а также порядок осуществления процессов и мероприятий, осуществляемых Организатором торговли в рамках управления отдельными видами рисков Организатора торговли**

### 7.1. Выявление рисков Организатора торговли.

Порядок выявления рисков:

- каждый работник Организатора торговли обязан информировать Службу по управлению рисками о рисках в момент их обнаружения;
- Служба по управлению рисками осуществляет сбор сведений о рисках (как внутренних, так и внешних), способных нанести Организатору торговли ущерб, их факторах, о возможности/вероятности возникновения рисков в деятельности Организатора торговли и о размере ущерба (ожидаемом, наихудшем, наиболее частом и т.д.);
- Служба по управлению рисками может привлекать СВК и иные структурные подразделения для определения видов риска, на которые оказано влияние, проведения оценки рисков и разработки мероприятий по реагированию на риски;
- Служба по управлению рисками осуществляет самооценку операционного риска. Самооценка проводится в формате интервью или анкетирования ответственных подразделений на регулярной основе, но не реже одного раза в год;
- Служба по управлению рисками осуществляет диагностику бизнес-процессов, анализ пересечений в полномочиях и ответственности подразделений и работников Организатора торговли;
- под руководством Службы по управлению рисками различными структурными подразделениями проводится анализ результатов внутреннего и внешнего аудитов контролей/процедур/систем;
- Службой по управлению рисками, СВК проводится анализ новых продуктов, процессов и систем (анализ всех нововведений, проводимых Организатором торговли: изменения структуры и процедур, внедрение новых услуг и технологий, освоение новых направлений деятельности и т.п.).

### 7.2. Анализ и оценка рисков Организатора торговли.

#### 7.2.1. Для анализа и оценки рисков используются следующие методы:

- сценарный анализ. В рамках сценарного анализа проводится идентификация угроз, которые по оценке Организатора торговли 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 Организатора торговли на ее финансовую устойчивость посредством оценки событий риска, наступление которых, в том числе с учетом вероятности их наступления и степени влияния, повлечет за собой возникновение убытков;
- для выявления (идентификации), анализа и оценки операционных рисков используется также стресс-тестирование программно-технических средств, используемых для осуществления деятельности по Организации торгов, с периодичностью, определенной внутренними документами Организатора торговли, но не реже одного раза в 6 месяцев.

#### 7.2.2. Порядок анализа и оценки рисков:

- выявление факторов и источников риска, определение видов риска;
- анализ сведений о риске (как внутренних, так и внешних), способных нанести Организатору торговли ущерб, о возможности/вероятности возникновения риска в деятельности Организатора торговли, 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 Организатора торговли 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 рискзащищенность Организатора торговли, на которую он оказывает воздействие по полному списку финансовых и нефинансовых рисков;
  - оценку нефинансовых рисков и стоимостную оценку рисков будущего продукта;

- оценку влияния рисков будущего продукта на текущую деятельность Организатора торговли;
- 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 Организатора торговли или их исключение.

7.3.1. Порядок мониторинга рисков Организатора торговли включает:

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

7.3.2. Организатор торговли в рамках мониторинга, контроля и снижения рисков или их исключения выполняет следующие мероприятия:

- определяет уровень рисков Организатора торговли, в том числе на предмет соответствия установленным Организатором торговли ограничениям рисков;
- разрабатывает и осуществляет мероприятия по устранению выявленных нарушений ограничений рисков и мероприятия по снижению рисков или их исключению. Организатор торговли 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 Организатора торговли:
  - мероприятия в отношении рисков проекта и продукта доводятся до сведения Правления АО НТБ;
  - мероприятия по снижению рисков, связанных с нарушением ограничений по показателям риск-аппетита, доводятся до Правления АО НТБ;
  - мероприятия в рамках существенных событий риска доводятся до единоличного исполнительного органа, Правления АО НТБ.

7.3.3. Для осуществления мониторинга рисков Организатора торговли внедрены ключевые индикаторы риска - показатели деятельности Организатора торговли (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 Организатора торговли 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 Организатора торговли, содержащих 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.

7.3.4. Контроль рисков координируется Службой по управлению рисками и осуществляется подразделениями, ответственными за управление отдельными видами рисков, путем реализации следующих мер:

- Служба по управлению рисками на постоянной основе контролирует своевременность выполнения мероприятий по минимизации операционного риска ответственными лицами при мониторинге рисков, включенных в БДР;

- Подразделение, ответственное за управление финансовыми рисками, на постоянной основе осуществляет контроль казначейских лимитов и иных показателей уровня финансовых рисков;
- Служба по управлению рисками на ежегодной основе актуализирует БДР и контролирует реализацию мероприятий в рамках самооценки рисков;
- СВК проводит регулярные тематические проверки, в том числе для проверки лиц по спискам комплаенс, обеспечивает наличие политик и процедур, проводит обязательное обучения;
- Управление развития и сопровождения торгов выполняет предварительные согласования и проверки при принятии на обслуживание клиентов, заключении соглашений с контрагентами, допуске к торгам участников, запуске новых продуктов/услуг, организует автоматизированные контроли,
- Независимый контроль за реализацией всех мероприятий по управлению рисками осуществляется СВА с периодичностью не реже, чем раз в три года, и внешними аудиторами.

#### 7.3.5. Снижение рисков осуществляется путем реализации мероприятий:

- страхование деятельности;
- автоматизация контрольных процедур и процессов;
- реализация контроля полномочий в рамках управления рисками, в т.ч. риском информационной безопасности;
- совершенствование торгово-клиринговых и вспомогательных систем Биржи, переход к более совершенным технологиям осуществления деятельности;
- регламентация и оптимизация внутренних процессов;
- обучение работников, применение мотивационных программ.

#### 7.3.6. Исключение рисков Организатора торговли заключается в отказе от совершения определенного вида деятельности и/или проекта, создающего риск.

Организатор торговли 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 Организатора торговли и (или) руководители структурных подразделений в рамках своих полномочий.

#### 7.3.7. Мероприятия по финансовым рискам в рамках данных направлений деятельности отражены в Политике по финансовым рискам.



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

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

7.4.2. Для анализа событий риска, оценки уровня риска и статусов выполнения мероприятий по минимизации риска проводятся регулярные совещания в рамках рабочих групп с обязательным участием специалистов в следующем порядке:

- работник Службы по управлению рисками назначает встречи с периодичностью не реже одного раза в месяц работникам и руководителям структурных подразделений, задействованных в процессе реализации мероприятий по минимизации риска;
- на совещаниях рабочих групп проводится анализ и обсуждение произошедших за отчетный месяц событий операционного риска;
- осуществляется анализ статуса выполнения мероприятий по событиям, идентифицированным в предыдущих периодах.

7.4.3. Сроки и форма обмена информацией о рисках Организатора торговли между подразделениями Организатора торговли следующие, если иное не определено во внутренних документах Организатора торговли:

- сроки информирования работников и предоставление отчётности структурным подразделениям Организатора торговли о рисках определяются руководителем Службы по управлению рисками на основе его профессионального суждения, формируемого с учётом оценки риска, потребностей Организатора торговли, величины того или иного риска и принципа существенности;
- сроки и форма предоставления информации работниками Организатора торговли, определяется в соответствующих запросах руководителя Службы по управлению рисками.

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

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

7.6. Определение перечня требующих защиты от противоправных действий программно-технических средств Организатора торговли, сбоя 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 Организатора торговли. Порядок определения перечня включает следующие мероприятия:

7.6.1. Создается перечень программно-технических средств Организатора торговли составляется с учетом критичности систем и времени, необходимого для восстановления в случае сбоя и/или ошибки.

7.6.2. Все программно-технические средства Организатора торговли подразделяются на несколько групп в зависимости от уровня требований к надежности их функционирования. 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.).

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 в рамках процесса управления обеспечения непрерывности деятельности, а именно:
  - Целевое время восстановления;
  - Допустимый диапазон потери данных.

7.6.3. Отнесение системы обработки данных (входящей в ее состав задачи) к группе надежности осуществляется по методике, основанной на анализе бизнес-процессов, и утверждается решением Комитета по ИТ-Архитектуре ПАО Московская Биржа. Системе

(входящей в ее состав задачи), по тем или иным причинам не отнесенной к группе надежности, по умолчанию присваивается группа С.

7.6.4. Для каждой из групп надежности устанавливаются коэффициенты доступности. Для обеспечения высокой доступности функциональных систем Организатора торговли 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 Организатора торговли.

7.7. Определение перечня и реализация мер по защите информации.

7.7.1. Деятельности Организатора торговли свойственен операционный риск, связанный с нарушением безопасности информации. Понизить риск нарушения информационной безопасности можно лишь до определенного остаточного уровня. Для управления операционным риском, связанным с безопасностью информации, Организатор торговли обеспечивает:

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

Вышеперечисленный перечень мер применяется Организатором торговли также для обеспечения конфиденциальности и защиты информации о рисках Организатора торговли, а также информации, предоставляемой Организатором торговли 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 всех 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 Организатора торговли требованиям Национального стандарта Российской Федерации «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

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

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

7.7.3. Перечень мер по защите информации также включает следующие технологические и организационные мероприятия:

- повышение вовлеченности и осведомленности работников Организатора торговли в вопросах выявления нарушений требований по защите информации и противодействия реализации информационных угроз;
- обеспечение защиты информации при управлении доступом и регистрацией пользователей информационных систем, а именно:
  - 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 защиты информации на всех этапах жизненного цикла автоматизированных информационных систем;
- обеспечение защиты информации средствами антивирусной защиты, которые признаны соответствующими самым современным требованиям в области антивирусной защиты информации;
- обеспечение защиты информации при использовании ресурсов информационно-телекоммуникационной сети «Интернет», обеспечение защиты вычислительных сетей в целом;
- контроль целостности и защищенности информационной инфраструктуры самыми современными методами;
- 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) при удаленной работе пользователей;
- обеспечение защиты информации при назначении и распределении ролей в системе управления информационной безопасностью;
- регламентация и документирование деятельности по обеспечению защиты информации, включая политику управления информационной безопасностью и политики/процедуры для всех аспектов системы информационной безопасности;
- обнаружение инцидентов информационной безопасности, в том числе инцидентов в отношении критичной архитектуры, и своевременное реагирование на них;
- мониторинг и анализ обеспечения защиты информации, проведение анализа причин и последствий реализации угроз и возникновения инцидентов;
- своевременное совершенствование средств обеспечения защиты информации, использование информации об актуальных сценариях реализации информационных угроз;
- обеспечение долгосрочного планирования при выборе и последующем сопровождении информационных и компьютерных систем, модернизация спецификаций требований к ним, выбора поставщиков и контроля за проектами создания систем и технологий обработки и передачи данных;
- организацию взаимодействия Организатора торговли и причастных сторон, в том числе клиентов Организатора торговли при обмене информацией об актуальных сценариях реализации информационных угроз;

- организацию взаимодействия между подразделениями Организатора торговли, а также между Организатором торговли и Банком России, причастными сторонами в рамках реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации в случае реализации угроз и возникновения инцидентов;- обеспечение процедур бесперебойного функционирования программно-технических средств Организатора торговли, используемых для осуществления деятельности по организации торгов, и процедур восстановления функционирования бизнес- и технологических процессов и объектов информатизации в случае реализации угроз и возникновения инцидентов, в том числе:

- наличие полностью резервированной архитектуры вычислительного комплекса, не содержащей нерезервированных точек отказа и обладающей устойчивостью к неоднократным аппаратным отказам любого типа компонентов, способной обеспечить функционирование основных информационных систем, используемых Организатором торговли;
- наличие резервных каналов связи;
- наличие поддерживаемого в актуальном состоянии плана действий при возникновении необходимости использования резервных мощностей и компонентов вычислительных систем и регулярного тестирования 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 и документированных процедур восстановления;

- наличие резервных универсальных рабочих мест;
- наличие в помещениях центров обработки данных автоматической системы пожаротушения;
- наличие круглосуточного мониторинга состояния вычислительных и телекоммуникационных ресурсов, помещений центров обработки данных Организатора торговли;
- перераспределение функций, полномочий и обязанностей подразделений и работников в случае реализации угроз и возникновения инцидентов;
- меры по поддержанию адекватного информационного обеспечения, оценку готовности к чрезвычайной ситуации внешних поставщиков информационных услуг.

7.7.4. Организатор торговли разработал и поддерживает политику управления информационной безопасностью. Эта мера способствует управлению рисками информационной безопасности, а именно обеспечивает:

- установление структуры и организации системы управления рисками информационной безопасности, а также распределение функций, ролей и ответственности в рамках управления рисками информационной безопасности;
- определение принципов управления рисками информационной безопасности;
- декларирует участие Наблюдательного Совета АО НТБ и исполнительных органов Организатора торговли в решении вопросов управления рисками информационной безопасности.

7.7.5. Применяемые Организатором торговли меры по оценке рисков информационной безопасности обеспечивают:

- идентификацию критичной архитектуры;
- идентификацию рисков информационной безопасности;
- выявление и моделирование информационных угроз;
- оценку присущего и остаточного уровня рисков информационной безопасности.

7.7.6. Применяемые Организатором торговли меры по разработке мероприятий, направленных на уменьшение негативного влияния присущих рисков информационной безопасности, обеспечивают:

- выбор и применение способа реагирования на риски информационной безопасности;
- разработку мероприятий, направленных на снижение степеней вероятности реализации рисков информационной безопасности;

- разработку мероприятий, направленных на ограничение степени тяжести последствий при реализации рисков информационной безопасности.

7.7.7. Применяемые Организатором торговли меры по защите от реализации рисков информационной безопасности обеспечивают:

- защиту информации Организатора торговли;
- операционную надежность;
- управление риском нарушения информационной безопасности при взаимодействии с поставщиками услуг;
- управление риском внутреннего нарушителя;
- управление риском информационной безопасности в финансовой экосистеме.

7.7.8. Применяемые Организатором торговли меры по планированию ресурсного (кадрового и финансового) обеспечения осуществляются:

- организацию ресурсного (кадрового и финансового) обеспечения процессов системы управления рисками информационной безопасности;
- организацию ресурсного (кадрового и финансового) обеспечения функционирования Службы по управлению рисками.

7.7.9. В случае возникновения в информационной инфраструктуре Организатора торговли 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, Организатор торговли предусматривает осуществление работниками Организатора торговли действий, направленных на выполнение своих служебных обязанностей в условиях отсутствия применения отдельных мер защиты информации, а также должный контроль указанных действий.

7.7.10. Меры защиты информации, входящие в систему управления информационной безопасностью, распространяются и на обеспечение защиты:

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

7.7.11. 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 Организатором торговли.

7.7.12. Организатором торговли определены, выполняются, регистрируются и контролируются правила и процедуры мониторинга доступа к информации, анализа и хранения данных о действиях и операциях работников, позволяющие выявлять неправомерные или подозрительные операции и направленные на реализацию мер, предусмотренных процессом «Обеспечение защиты информации при управлении доступом» ГОСТ Р 57580.1-2017.

7.7.13. Организатором торговли 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.

7.7.14. 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 Организатора торговли к программно-техническим средствам Организатора торговли и порядок его осуществления.

7.8.1. Мониторинг прав доступа пользователей к Информационной системе (далее - ИС) проводится регулярно, но не реже одного раза в 12 месяцев;

7.8.2. Внеплановый мониторинг прав доступа к ИС Организатора торговли может проводиться в случае возникновения инцидента ИБ и иных обстоятельств, требующих пересмотра предоставленных прав доступа, по инициативе работника Службы по управлению рисками;

7.8.3. Мониторинг прав доступа пользователей к ИС осуществляется в следующем порядке:

- работник Службы по управлению рисками 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 Службы по управлению рисками 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 Службы по управлению рисками запрашивает у администраторов системы регистрации заявок на предоставление прав доступа заявки, имеющиеся в данной системе, на предоставление прав доступа пользователям из указанной выборки;
- работник Службы по управлению рисками проверяет предоставленные данные с целью выявления наличия прав доступа, не подтвержденных соответствующими заявками;
- в случае выявления нарушений работник Службы по управлению рисками 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 Службы по управлению рисками, проводивший мониторинг, документирует его результаты.

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

7.9.1. Порядок определения перечня мер, направленных на обеспечение предоставления Организатору торговли участниками торгов и их клиентами, а также иными контрагентами Организатора торговли информации о событиях операционного риска участников торгов и их клиентов, связанных с их участием в организованных торгах:

- Организатор торговли организует горячую линию для участников торгов и принимает обращения в техническую поддержку в случае технических сбоев, возникающих на стороне участников торгов;
- Организатор торговли оказывает поддержку по восстановлению работы средств проведения торгов в случае проблем на стороне участников торгов;
- работник Организатора торговли эскалирует ситуацию в случае, если проблемы представляются признаком технического сбоя на стороне Организатора торговли;
- Организатор торговли инициирует последующее обсуждение, подтверждение мер, направленных на недопущение повторения технических проблем на Комитете по согласованию технологических изменений ПТК ПАО Московская Биржа.

7.9.2. Перечень мер, направленных на обеспечение предоставления Организатору торговли участниками торгов и их клиентами, а также иными контрагентами Организатора торговли 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 Организатора торговли, 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 пользователей ТКС резко меняется (падает), работник подразделения, ответственного за мониторинг торгов, следует специальным инструкциям для различного класса проблем (в т.ч. нештатных ситуаций). Инструкции подлежат постоянному обновлению по результатам текущей эксплуатации, анализа разноплановых ситуаций и т.д;

- мониторинг количества соединений и поведения участника торгов на наличие большого количества ошибочных транзакций:

- если зафиксирована нештатная ситуация, которая заключается в том, что поведение участников торгов отклоняется от нормального, то информация передается ответственным работником руководству и в Управление развития и сопровождения торгов, которое связывается с клиентом для разъяснения проблемы. Организатор торговли имеет право инициировать процедуру отключения от торгов данного клиента в соответствии с Правилами допуска к участию в организованных торгах, 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;

- прохождение сертификации любой ВПТС;

- 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 ТКС 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 Организатора торговли.

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

Устранение недостатков производится в следующем порядке:

- 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 системе Jira с присвоением им тикета. Тикет назначается на тот или иной релиз (версию ПО), 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, minor, major 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 вводится в эксплуатацию до момента их устранения. В этом 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. Обо всех критических недостатках докладывается на Комитете по релизному планированию при Правлении Публичного акционерного общества «Московская Биржа ММВБ-РТС»;

- статус хода тестирования ПО рассматривается на каждом Комитете по релизному планированию при Правлении Публичного акционерного общества «Московская Биржа ММВБ-РТС» на еженедельной основе;

- также при выявлении недостатков в ВПТС и/или средствах мониторинга о данных инцидентах извещается Служба по управлению рисками и информация по ним входит в состав отчетности в качестве события операционного риска, статус по которым отслеживается на ежемесячной основе.

7.13. Ведение базы данных о событиях операционного риска Организатора торговли.

7.13.1. Ведение базы данных о событиях операционного риска (БДСОР) производится по следующим видам событий операционного риска Организатора торговли:

- события, влекущие за собой приостановление или прекращение осуществления процессов Организатора торговли, приостановление или прекращение которых вызывает нарушение порядка осуществления Организатором торговли 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 Организатора торговли), в том числе чрезвычайные ситуации (далее - существенные события операционного риска);
- события операционного риска, не относящиеся к существенным событиям операционного риска, но по оценке Организатора торговли оказывающие негативное влияние на порядок и условия осуществления критически важных процессов Организатора торговли, 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).

7.13.2. Помимо этого в БДСОР содержатся события, не являющиеся событиями операционного риска, подпадающими под определения существенных, значимых событий или событий низкого уровня влияния, не оказывающих влияния на деятельность Организатора торговли, но потенциально способных привести к реализации событий операционного риска.

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

Обучение производится в следующем порядке:

- все новые работники Организатора торговли перед тем, как приступить к работе, проходят обучение по вопросам выявления, оценки и снижения операционного риска в обязательном порядке;
- сотрудники Службы по управлению рисками проводят углублённое обучение работников Организатора торговли по вопросам управления операционным риском, адаптированное для конкретных фокус-групп (в зависимости от функций подразделения);
- обязательным для отдельных работников Организатора торговли является прохождение электронных курсов, которые являются общедоступными на корпоративном портале;
- Служба по управлению рисками осуществляет мониторинг статистики прохождения обучения периодичностью не реже одного раза в месяц.

7.15. Осуществление мероприятий по замене или улучшению (обновлению) программно-технических средств Организатора торговли в случае выявления их несоответствия характеру и объёму совершаемых Организатором торговли операций.

7.15.1. Для выявления необходимости замены и/или улучшения (обновления) программно-технических средств Организатора торговли подразделения, ответственные за эксплуатацию и модернизацию ПО и оборудования, на ежегодной основе проводят нагрузочные тестирования. По результатам тестирований, в случае выявления несоответствия характеру и объёму совершаемых Организатором торговли операций, реализуется набор мер, заключающихся в оценке необходимости обновления ПО и реализации мероприятий по его обновлению.

7.15.2. Порядок осуществления мероприятий по замене или улучшению (обновлению) программно-технических средств Организатора торговли в случае выявления их несоответствия характеру и объёму совершаемых Организатором торговли операций включает:

- регулярный мониторинг работоспособности программно-технических средств Организатора торговли;
- ежегодное нагрузочное тестирование программно-технических средств Организатора торговли;
- реализация мер по обновлению программно-технических средств Организатора торговли. При обнаружении несоответствия характеру и объёму совершаемых Организатором торговли операций осуществляется доработка или закупка программно-технических средств.

7.16. Организатор торговли в рамках управления операционным риском разработал систему мер, направленных на обеспечение условий для бесперебойного функционирования программно-технических средств Организатора торговли, а также

для восстановления осуществляемой Организатором торговли деятельности в случае реализации событий операционного риска Организатора торговли, включающую в себя следующие мероприятия:

- определение перечня критически важных процессов Организатора торговли, а также процессов участников торгов и (или) контрагентов Организатора торговли, приостановление или прекращение которых влечет за собой нарушение порядка осуществления Организатором торговли 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;
- составление Планов обеспечения непрерывности и восстановления деятельности (План ОНиВД). В Плане ОНиВД каждое подразделение указывает перечень критически важных процессов, возникающих при взаимодействии с другими подразделениями, с контрагентами, включая процессы взаимодействия с участниками торгов. Подобное взаимодействие оценивается в рамках анализа воздействия на бизнес;
- определение плана мероприятий по реагированию на НС, возникающих в критически важных процессах Организатора торговли, а также процессах участников торгов и (или) контрагентов Организатора торговли;
- периодическое тестирование адекватности и достаточности мероприятий по реагированию на НС.

Определение перечня критически важных процессов Организатора торговли соответствует следующим положениям:

- перечень критически важных процессов Организатора торговли определяется сотрудниками Службы по управлению рисками совместно с руководителями структурных подразделений;
- перечень критически важных процессов Организатора торговли описывается в Планах ОНиВД структурных подразделений непосредственно структурными подразделениями совместно с сотрудниками Службы по управлению рисками;
- сотрудники Службы по управлению рисками совместно с руководителями структурных подразделений регулярно проводит анализ текущего воздействия внешней среды на бизнес;
- перечень критически важных процессов обновляется не реже, чем раз в год.

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

Порядок выявления ЧС и анализа обстоятельств возникновения ЧС:

- постоянный мониторинг средств проведения торгов и штатного функционирования всех процессов Организатора торговли с целью своевременного выявления аномалий и отклонения от нормальной работы процессов Организатора торговли;
- оперативное информирование любым работником всех заинтересованных лиц подразделений Организатора торговли в случае выявления аномалий и отклонения от нормальной работы процессов Организатора торговли;
- 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.

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;
- 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 Организатором торговли возможных расходов (убытков) Организатора торговли, участников торгов и их клиентов, а также иных его контрагентов вследствие нарушения непрерывности осуществления деятельности Организатора торговли, вероятности и времени возможного возникновения такого нарушения, а также характера и объема совершаемых Организатором торговли операций.



7.19.1. Идентификация угроз, которые могут привести к неработоспособности средств проведения торгов, осуществляется в рамках управления непрерывностью деятельности с периодичностью не реже одного раза в год.

7.19.2. Перечень потенциальных угроз может быть пересмотрен внеочередным порядком, в связи с меняющейся международной обстановкой (санкции), внутривнутриполитическими проблемами, экономическими, техногенными и эпидемиологическими ситуациями и их влияния на финансовую устойчивость Организатора торговли. 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 Организатором торговли в чрезвычайных ситуациях и направленные на обеспечение непрерывности осуществления деятельности по организации торгов (далее - План непрерывности бизнеса).

7.20.1. Организатором торговли разработан и утверждён План непрерывности бизнеса, определяющий меры, принимаемые Организатором торговли в чрезвычайной ситуации (ЧС) для обеспечения непрерывности осуществления деятельности по организации торгов.

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

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

7.20.4. Целью Плана непрерывности бизнеса является обеспечение реагирования на существенные инциденты, он включает в себя оценку возможных последствий инцидента на деятельность Организатора торговли, принятие решений об активации планов реагирования структурных подразделений, поддержание способности Организатора торговли выполнять принятые на себя обязательства перед клиентами, предупреждение и предотвращение возможного нарушения режима повседневного функционирования Организатора торговли, обеспечение способности Организатора

торговли осуществлять расчетные и клиринговые операции, в соответствии с принятыми на себя обязательствами, сохранение уровня управления Организатора торговли, позволяющего обеспечить условия для принятия обоснованных и оптимальных управленческих решений, их своевременную и полную реализацию.

7.20.5. 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 Организатора торговли, 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 Организатором торговли 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 Организатором торговли деятельности и объема совершаемых операций, в случае выявления недостаточности указанных мер для обеспечения непрерывности осуществления деятельности по организации торгов.

7.21.1. Для оценки Плана непрерывности бизнеса Организатор торговли обеспечивает осуществление следующих мероприятий:

- для 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.

7.21.2. 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 Организатора торговли 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).

Резервный офис Организатора торговли организуется при условии соответствия 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 Организатора торговли 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 Организатора торговли в основном комплексе средств проведения торгов.

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

7.23. Создание резервных копий информации, содержащейся в реестрах Организатора торговли.

7.23.1. Создание резервных копий информации, содержащейся в реестрах, ведение которых Организатор торговли должен 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 Организатором торговли (но не реже одного раза в день), и хранение указанных копий в течение пяти лет со дня их создания.

7.23.2. Организация резервного копирования информации отвечает следующим требованиям:

- администраторы ПО и систем 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).

7.23.3. Хранение резервных копий информации отвечает следующим требованиям:

- администраторы ПО и систем, совместно с сотрудниками Службы по управлению рисками и владельцами ИС, определяют время хранения резервных копий для каждой ИС (не менее пяти лет). При определении времени хранения учитывается уровень критичности информации для бизнес-процессов Организатора торговли, 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 хранения 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.

7.23.4. Тестирование резервных копий информации и процедуры восстановления отвечает следующим требованиям:

- 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:

- верификация целостности резервных копий, осуществляемая техническими средствами резервного копирования;

- выборочная проверка возможности восстановления информации из резервных копий (для данных, не относящихся к торговым системам);

- 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;

- 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 ПО или системы осуществляется определение и устранение причин нарушения.

7.23.5. Восстановление информации из резервных копий отвечает следующим требованиям:

- 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:

- работник, которому необходимо восстановить потерянную информацию, направляет заявку с обязательным указанием причин необходимости восстановления в службу технической поддержки;

- 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;

- 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.

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

- уполномоченный работник подразделения Организатора торговли, 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 проверяющим случайным образом;
- по результатам контроля процедур резервного копирования работник, 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 Организатора торговли.

Организатором торговли в зданиях центров обработки данных, в отдельных помещениях установлены дизельные генераторные установки (далее - ДГУ) для обеспечения функционирования критически важных процессов Организатора торговли, в том числе в условиях их восстановления при нарушении непрерывности бизнеса. В соответствии с требованиями заводов изготовителей проводятся их 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 Организатора

торговли и возможность начала работы по переносу критически важных процессов Организатора торговли, осуществляемых с использованием средств проведения торгов, из основного комплекса средств проведения торгов в резервный офис в порядке и в сроки, установленные Организатором торговли.

Для поддержания технического оснащения резервного офиса на необходимом уровне проводятся следующие мероприятия:

- 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.

Организатор торговли 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;
- оценку 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 центра обработки данных.

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

7.27.1. Для поддержания резервного офиса на необходимом уровне проводятся следующие мероприятия по тестированию:

- резервные рабочие места тестируются согласно утвержденному графику тестирования, 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.

7.27.2. Также для поддержания резервного офиса на уровне, обеспечивающем возможность функционирования всех критически важных процессов Организатора торговли, 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 Организатора торговли 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 Организатора торговли 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 Организатора торговли, 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 Организатора



торговли 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. Организатор торговли в рамках управления риском потери деловой репутации (РДПР) Организатора торговли организует сбор и анализ отзывов о деятельности Организатора торговли в средствах массовой информации, в том числе с использованием специализированных автоматизированных информационных систем.

7.28.1. Подразделением, осуществляющим сбор и оценку информации о фактах РДПР, является Служба по управлению рисками. Служба по управлению рисками, совместно с иными подразделениями, 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 Организатора торговли, с целью сбора и анализа отзывов об Организаторе торговли, включая информацию, полученную в рамках ведения претензионной работы;

- полученные сведения о фактах РДПР проверяются на достоверность и значимость. Оценка полученных сведений проводится экспертно, исходя из того, насколько ущерб репутации Организатора торговли усложнит достижение целей, которые ставит перед собой Организатор торговли 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 РДПР, имеет право обращаться к структурным подразделениям Организатора торговли, 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 РДПР может анализироваться влияние деловой репутации на финансовое состояние, влияние деловой репутации компаний Группы на деловую репутацию Организатора торговли, превентивных и контрольных мероприятий (благотворительной и общественной деятельности, рекламно-информационной политики) на деловую репутацию Организатора торговли.

7.28.2. При оценке уровня РПДР могут учитываться:

- изменение финансового состояния Организатора торговли (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 преступным путем, а также признаков возможного вовлечения Организатора торговли, работников компаний Группы, клиентов Организатора торговли в легализацию (отмывание) доходов;
- выявление фактов хищения, подлогов, мошенничества Организатором торговли, использования работниками Организатора торговли конфиденциальной информации, полученной от клиентов и контрагентов, в личных целях;
- отказ постоянных или крупных клиентов и контрагентов от сотрудничества с Организатором торговли.

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

- регулярного изучения показателей деятельности Организатора торговли;
- мониторинга количества жалоб и претензий к Организатору торговли, 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.

7.28.4. Мероприятия по минимизации возможности возникновения фактов РПДР включают в себя:

- мониторинг деловой репутации акционеров, аффилированных лиц, менеджмента компаний 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 об Организаторе торговли 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 Организатора торговли, 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 Организатора торговли.

7.29. Организатор торговли в рамках управления стратегическим риском Организатора торговли обеспечивает проведение должностным лицом, ответственным за организацию системы управления рисками, следующих мероприятий по оценке изменений для выявления потенциальных источников возникновения рисков:

7.29.1. Оценка разработки 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, товара, а также иных организационных и (или) технологических изменений (далее - проекты изменений).

Порядок разработки проектов изменений включает:

- Для проектных инициатив инициатор, являющийся сотрудником компании Группы, подготавливает документ об инициативе, дополнительно согласовав его с руководителем функционального подразделения (заказчиком), и передает его в структурное подразделение, ответственное за ведение проектной деятельности в соответствующей компании Группы;

- структурное подразделение (или сотрудник), ответственное за ведение проектной деятельности в компании Группы, 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 Организатора торговли между проектами и задачами с учетом стратегии Организатора торговли.

Вопросы контроля и управления изменениями в ИТ-инфраструктуре, обеспечивающей деятельность Организатора торговли, рассматриваются на Комитете по согласованию технологических изменений ПТК ПАО Московская Биржа.

#### 7.29.2. Анализ целесообразности внедрения проектов изменений.

- в рамках анализа целесообразности внедрения проектов и инициатив формируется реестр инициатив, который консолидируется ответственным структурным подразделением (сотрудником) компании Группы и выносится на рассмотрение Комитета по продуктам и проектам при Правлении ПАО Московская Биржа (далее - КПП), являющегося уполномоченным органом рассматривать и принимать соответствующие решения по общегрупповым проектам;

- Служба по управлению рисками, совместно с сотрудником, ответственным за управление финансовыми рисками, проводит оценку рисков, связанных с реализацией проекта, а также оценку рисков, снижаемых вследствие реализации проекта по тем инициативам, которые затрагивают бизнес Организатора торговли, и формирует заключение о рисках по этим проектам;

- сотрудники, ответственные за управление финансами, совместно с менеджерами проектов рассчитывают ряд финансовых показателей по каждой инициативе (NPV, TCO и т.д.);

- заключение о рисках и список финансовых показателей выносятся в установленном внутренними документами порядке на рассмотрение КПП;

- КПП рекомендует Правлению, а Правление принимает решение о реализации проектов, изменений, осуществляет приоритизацию реализации инициатив.

Решение принимается на основе баланса целесообразности инвестиций, экономической выгоды и целесообразности снижения выявленных рисков, а также совершенствования деятельности Организатора торговли.

#### 7.30. Анализ эффективности реализованных Организатором торговли проектов изменений по итогам их введения в деятельность, осуществляемую Организатором торговли.

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 Организатора торговли, в том числе посредством разработки стратегии развития Организатора торговли на срок, соответствующий характеру осуществляемой деятельности Организатора торговли и объему совершаемых операций.

Организатор торговли осуществляет следующие мероприятия по планированию развития деятельности Организатора торговли:

- разработка стратегии развития Организатора торговли на 5 лет;
- разработка дорожной карты реализации стратегии;
- расчет ресурсов, необходимых для реализации дорожной карты стратегии;
- утверждение стратегии Наблюдательным Советом Организатора торговли.

Наблюдательным советом Организатора торговли может быть принято решение о внесении изменений в стратегию развития Организатора торговли.

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

7.32.1. Порядок оценки стратегии развития Организатора торговли на предмет определения возможности и целесообразности ее реализации:

- выявление рисков достижения стратегических целей;
- выявление рисков целеполагания стратегии Организатора торгов;
- проведение оценки рисков достижения целей;
- проведение оценки рисков целеполагания стратегии Организатора торгов;
- вынесение указанных рисков на рассмотрение Наблюдательного Совета, для определения целесообразности пересмотра Стратегии;
- мониторинг выявленных рисков в течение срока реализации Стратегии.

7.32.2. Оценка стратегии развития Организатором торговли предполагает:

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

7.32.3 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 Организатора торговли.

## **8 Порядок обеспечения контроля за выполнением процессов и мероприятий по выявлению, анализу, мониторингу риска, и обмену информацией между подразделениями и органами управления Организатора торгов, а также порядок осуществления процессов и мероприятий, осуществляемых Организатором торговли в рамках управления отдельными видами рисков Организатора торговли**

8.1. Контроль за процессами управления рисками, включающими выявление, анализ, мониторинг рисков и обмен информацией, а также за порядком осуществления процессов и мероприятий по управлению отдельными видами рисков Организатора торгов 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 Организатора торговли в случае выявления их несоответствия характеру и объему совершаемых Организатором торговли 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 аудита на соответствие процесса проведения испытательных работ (тестирования) средств проведения торгов, а также порядка устранения недостатков, выявленных в результате их проведения, на ежегодной основе;
- проведения периодических аудитов СВА;
- проведения периодических проверок отдельных процессов работниками Службы по управлению рисками и СВК.
- проведения контрольных процедур работниками иных структурных подразделений;
- анализа, оценки и разработки последующих мер реагирования на результат контрольных процедур, документирования результатов, ведения отчетности работниками Службы по управлению рисками или иными подразделениями, управляющими отдельными видами рисков;
- принятия управленческих решений уполномоченными органами управления Организатора торговли по итогам рассмотрения отчетности по рискам. На разных этапах управления рисками эти функции осуществляются руководителем Службы по управлению рисками, Правлением;
- проведения периодических проверок адекватности системы управления рисками СВА, независимыми аудиторскими компаниями и надзорными органами.

Контроль процесса управления рисками обеспечивает полноценное информирование органов управления Организатора торговли, а также является основой для принятия управленческих решений.

8.2. 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, проверки/аудита, 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 Организатора торговли 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 Организатора торговли и результатов их оценки в реестр рисков Организатора торговли, порядок осуществления оценки реестра рисков Организатора торговли на предмет его актуальности, а в случае выявления в реестре рисков Организатора торговли неактуальных сведений - на предмет пересмотра реестра рисков Организатора торговли**

9.1. Порядок внесения рисков и результатов их оценки в реестр рисков:

- каждый работник Организатора торговли обязан сообщить о риске в Службу по управлению рисками в момент обнаружения;

- по факту получения сообщения о риске работник Службы по управлению рисками 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 правления Организатора торговли. При необходимости работник Службы может привлекать работников структурных подразделений, ответственных за управление отдельными видами риска;

- по факту проведенного анализа информация о нефинансовых рисках вносится в БДР работником Службы по управлению рисками;

- по факту появления и учета информации о риске в БДР работник Службы по управлению рисками 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 Службы 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 Службы осуществляется регулярная оценка БДР на предмет ее актуальности, а в случае выявления неактуальных сведений - пересмотр реестра рисков Организатора торговли с периодичностью не реже одного раза в год.

9.2. Для выявления и идентификации риска используются следующие процессы и процедуры:

- сбор сведений о рисках (как внутренних, так и внешних), способных нанести Организатору торговли 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 Организатора торговли, 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 Организатора торговли;

- анализ результатов внутреннего и внешнего аудита контролей/процедур/систем;

- анализ новых продуктов, процессов и систем (анализ всех нововведений, проводимых Организатором торговли: 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 Организатора торговли 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 Организатора торговли, но не реже одного раза в шесть месяцев.

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

## **10 Порядок ведения базы данных о событиях операционного риска**

10.1. 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 Службы по управлению рисками. Каждый работник Организатора торговли обязан при выявлении события сообщить о нем в порядке, описанном в настоящем разделе;

- в случае возникновения события:

- работник Организатора торговли, располагающий информацией о событии, извещает об этом непосредственного руководителя и ответственного работника Службы не позднее дня его выявления;

- 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 Службу;

- ответственный работник Службы 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 и определения Риск-менеджера.

- 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 Организатора торговли и последующего принятия решения о мерах по минимизации вероятности повторного возникновения события операционного риска;

- на регулярной основе Риск-менеджер самостоятельно или совместно с ответственным работником (владельцем подразделения, 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.

10.2. Результаты анализа события 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.

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

10.4. Служба по управлению рисками ежедневно осуществляет контроль полноты и актуальности данных о расходах (убытках), понесенных Организатором торговли вследствие реализации событий операционного риска.

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

11.1. Организатором торговли проводится идентификация угроз, которые по оценке Организатора торговли 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.

11.2. Порядок проведения идентификации угроз, которые по оценке Организатора торговли 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 Организатора торговли, 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 Организатора торговли.

11.3. Определение перечня и реализация мер по защите информации, осуществляемых в рамках соответствия требованиям законодательства.

Данные мероприятия осуществляются в рамках внедренной и поддерживаемой Организатором торговли области деятельности по управлению непрерывностью бизнеса, которая функционирует в соответствии с требованиями законодательства, а также в соответствии с рекомендациями международных стандартов.

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

- Идентификация угроз непрерывности бизнеса требует рассмотрения деятельности Организатора торговли 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, т.е. проводится анализ воздействия на бизнес;

- 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 Организатора торговли, то оценка рисков показывает, каким угрозам подвержен Организатор торговли 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 Организатор торговли может быть подвержен 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 Организатора торговли в случае их реализации, в том числе на работников Организатора торговли, инфраструктуру Организатора торговли, информационные активы Организатора торговли;

- оценку вероятности реализации угрозы непрерывности;

- анализ существующих контрольных процедур.

- в процессе оценки рисков непрерывности оценивается вероятность реализации угрозы, степень возможного влияния на Организатора торговли 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.

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

- мониторинг Торгово-клиринговой системы 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 требованиями, предъявляемыми Организатором торговли к сопряжению ВПТС с ПТК;

- в случае идентификации угроз, которые могут привести к неработоспособности средств проведения торгов работник, ответственный за мониторинг систем, анализирует и передает информацию о проблеме в соответствующее подразделение. Для разных классов проблем разработаны инструкции, в которых прописаны действия работников по реагированию на проблемы. Инструкции подлежат постоянному обновлению по результатам текущей эксплуатации, анализа разноплановых ситуаций и т.д.;

- в случае выявления инцидента информация о нем направляется в Службу по управлению рисками и анализируется.

11.6. К угрозам, которые по оценке Организатора торговли могут привести к неработоспособности средств проведения торгов, относятся:

- выход из строя технических средств, сбой в работе информационных систем (в том числе в результате технического сбоя), используемых для обслуживания критически важных процессов;

- нарушение коммунальной инфраструктуры (затопление помещений Организатора торговли, 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 Организатора торговли 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 Организатора торговли могут привести к приостановлению или прекращению осуществления критически важных процессов:

- получение Организатором торговли 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 Организатора торговли (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 Организатором торговли вследствие реализации событий операционного риска Организатора торговли**

12.1. Ведение базы данных о расходах (убытках), понесенных Организатором торговли 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, в том числе в разрезе комплекса деятельностей; - возмещение убытка;
- дата реализации события операционного риска Организатора торговли, повлекшего за собой возникновение расходов (убытков) Организатора торговли;

- анализ обстоятельств возникновения (выявления) события операционного риска Организатора торговли, приведшего к расходам (убыткам) и возможности покрытия расходов (убытков).

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

12.2. Таким образом, ведение единой БДСОР не только удовлетворяет требованию ведения базы данных о расходах (убытках), понесенных Организатором торговли 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.

**13 Права и обязанности органов управления Организатора торговли, руководителей и работников структурных подразделений Организатора торговли, 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**

13.1. Управление рисками осуществляется на всех уровнях Организатора торговли 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.

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

Служба по управлению рисками АО НТБ отвечает за систему управления рисками Организатора торговли, в том числе за управления операционным риском, включая риск информационной безопасности и непрерывности деятельности, стратегическим риском, риском потери деловой репутации, иными видами риска.

Служба по управлению рисками АО НТБ в рамках управления отдельными видами рисков привлекает:

Руководителя направления по управлению финансовыми рисками – в части финансовых рисков, в том числе, связанных с осуществлением операций с собственным имуществом;

СВК – в части управления регуляторным риском и комплаенс-риском в соответствии с утвержденными документами;

Работников структурных подразделений компаний Группы – в части управления отдельными видами рисков в соответствии с договорными обязательствами.

13.3. Руководитель Службы по управлению рисками и руководители отдельных структурных подразделений компаний Группы, указанные в настоящем пункте Правил, могут входить в состав создаваемых компаниями Группы комитетов и комиссий.

Для руководителя Службы по управлению рисками АО НТБ является основным местом работы.

Руководитель Службы по управлению рисками, работники структурных подразделений, указанные в настоящему пункте Правил, вправе требовать у работников и должностных лиц Организатора торговли предоставления информации (документов), в том числе письменных объяснений, по вопросам, возникающим в ходе выполнения им (ими) своих обязанностей.

13.4. В компетенцию руководителя Службы по управлению рисками входит, в том числе:

- разработка программ обучения (консультаций) работников Организатора торговли по вопросам выявления, идентификации и оценки рисков, а также их контроля;
- разработка методологии и инструментов управления рисками;
- оценка рисков Организатора торговли 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 Организатора торговли, о мерах, которые необходимо предпринять для устранения того или иного риска Организатора торговли;
- осуществление контроля выполнения мер, направленных на устранение рисков Организатора торговли;
- предоставление информации о рисках Организатора торговли коллегиальному исполнительному органу и единоличному исполнительному органу Организатора торговли;



- принятие иных мер, направленных на организацию системы управления рисками, предусмотренных внутренними документами Организатора торговли.

13.5. В компетенцию Наблюдательного Совета входит решение вопросов, связанных с организацией системы управления рисками, а именно:

- определение принципов и подходов к организации системы управления рисками;
- утверждение внутренних документов, определяющих политику Организатора торговли в области организации управления рисками;
- утверждение документов, определяющих правила организации системы управления рисками Организатора торговли;
- утверждение методики определения предельного уровня рисков (допустимого уровня рисков) Организатора торговли, а также совокупного предельного уровня рисков Организатора торговли;
- утверждение документа, определяющего меры, принимаемые в чрезвычайных ситуациях и направленные на обеспечение непрерывности осуществления деятельности по проведению организованных торгов;
- утверждение пороговых показателей риск-аппетита;
- утверждение критериев оценки эффективности СУР;
- рассмотрение и анализ результатов оценки эффективности СУР;
- принятие решений по результатам проведенного анализа и оценки.

13.6. Для выполнения решений Наблюдательного Совета в соответствии с утвержденными им внутренними документами в области управления рисками Директор АО НТБ и Правление осуществляют:

- распределение полномочий и ответственности по управлению рисками между руководителями подразделений Организатора торговли в целях соблюдения основных принципов по управлению рисками;
- создание и поддержание эффективной системы управления рисками;
- обеспечение организации процесса управления рисками, включая образование рабочих органов;
- принятие решений по осуществлению мероприятий в отношении управления рисками;
- утверждение лимитов кредитного и рыночного рисков (лимитной ведомости);
- утверждение отчетности по рискам.

13.7. Обязанность всех работников Организатора торговли сообщать обо всех известных им рисках и событиях рисков, а также предоставлять информацию по запросу Службы по управлению рисками.

Обязанности руководителей структурных подразделений, осуществляющих функции управления рисками, – проводить анализ событий и рисков, обеспечивать функционирование системы и реагировать 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 Организатора торговли, в том числе Положениями о подразделениях.

13.8. 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.

В компаниях Группы могут создаваться коллегиальные консультативно-совещательные органы (далее - Комитеты), в состав которых могут входить представители риск-менеджмента компаний Группы «Московская Биржа» (по согласованию с ними), включая представителей АО НТБ.

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 Организатором торговли 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 Организатором торговли решения о назначении указанного лица**

14.1. Создание отдельное структурное подразделение, ответственного за реализацию системы управления рисками действует в соответствии с Положением о Службе по управлению рисками, утвержденным Приказом Директора АО НТБ.

14.2. Руководитель Службы по управлению рисками проверяется на предмет соответствия квалификационным требованиям, установленным действующим законодательством Российской Федерации. Должность руководителя Службы по управлению рисками согласуется с Банком России. Руководитель Службы по управлению рисками назначается на должность Директором АО НТБ.

14.3. Работники, ответственные за управление отдельными видами рисков, назначаются Приказом Директора АО НТБ.

14.4. Работники, которые должны предоставлять информацию об операционных рисках и событиях операционных рисков, назначены Приказом Директора АО НТБ. Ими являются все работники Организатора торговли.

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

## **15 Порядок и периодичность обмена информацией о рисках Организатора торговли между подразделениями Организатора торговли, между подразделениями Организатора торговли и органами управления Организатора торговли, 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 Организатора торговли**

15.1. Порядок и периодичность обмена информацией о рисках Организатора торговли между подразделениями Организатора торговли включает следующие мероприятия:

- Служба по управлению рисками 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;

- обмен информацией о рисках между структурными подразделениями осуществляется на ежедневной основе в рабочем режиме.

15.2. В отношении анализа событий риска, оценки уровня риска и статусов выполнения мероприятий по минимизации риска проводятся встречи в рамках рабочих групп с обязательным участием сотрудников Службы по управлению рисками с периодичностью не реже одного раза в месяц в следующем порядке:

- проводится анализ и обсуждение произошедших за отчетных месяц событий операционного риска;

- проводится 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 Службе по управлению рисками ответственным структурным подразделением в срок не позднее 10 дней с даты формирования отчета;

- в ходе работ по идентификации, оценке, мониторингу, контролю рисков Служба по управлению рисками информирует работников Организатора торговли 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.

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

Порядок и периодичность обмена информацией о плане мероприятий по минимизации рисков - в рамках регулярной отчетности информация о мероприятиях по минимизации рисков предоставляется органам управления Организатора торговли.

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 Организатора торговли отчетов и информации о результатах осуществления Организатором торговли в рамках организации системы**

## **управления рисками процессов и мероприятий, по управлению отдельными видами рисков**

16.1. Органам управления Организатора торговли руководителем Службы по управлению рисками и руководителем направления по управлению финансовыми рисками 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.

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

Регулярная отчётность включает в себя следующие отчеты:

- Отчётность по нефинансовым рискам, предоставляемая руководителем Службы по управлению рисками Директору АО НТБ не реже одного раза в квартал в срок не позднее 30 дней с даты окончания квартала и Правлению не реже одного раза в квартал;
- Отчетность о показателях риск-аппетита, предоставляемая руководителем Службы по управлению рисками Правлению не реже одного раза в месяц;
- Отчётность по финансовым рискам Организатора торговли, предоставляемая руководителем направления по управлению финансовыми рисками Правлению на ежемесячной основе.

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.

16.3. Информация о выявленном событии риска с высокими убытками, существенном изменении уровня риска, проведении дополнительных специальных программ оценки риска предоставляется руководителем Службы по управлению рисками Директору АО НТБ и Правлению Организатора торговли не позднее десяти дней с даты выявления соответствующего нарушения.

16.4. Предоставление отчетности другим пользователям осуществляется по решению органов управления Организатора торговли, 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 Организатором торговли процессов и мероприятий в рамках организации системы управления и в рамках управления отдельными видами рисков, представляемых на рассмотрение органов управления Организатора торговли**

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

17.2. Регулярная отчетность по нефинансовым рискам включает в себя:

- оценку рисков по основным направлениям деятельности Организатора торговли, ее обоснование, включая сведения о нарушениях Организатором торговли требований Закона об организованных торгах, принятых в соответствии с ним нормативных правовых актов Банка России, Устава Организатора торговли 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 Организатора торговли.

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

17.4. Внеочередная (оперативная) отчетность формируется в виде Отчета руководителя Службы по управлению рисками в случае выявления событий риска с высокими убытками, существенного изменения уровня риска, проведения дополнительных специальных программ оценки риска.

## **18 Порядок управления рисками, связанными с оказанием поставщиками внешних услуг в течение всего периода их оказания, в случае заключения**

## **Организатором торговли договоров на оказание внешних услуг с поставщиками услуг**

18.1. В рамках управления операционными рисками выделяют процесс управления рисками, связанными с оказанием поставщиками услуг внешних услуг в течение всего периода их оказания. Заключение Организатором торговли 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.

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

- для 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 Организатором торговли договора на оказание услуг, связанных с осуществлением деятельности по проведению организованных торгов (далее - внешние услуги), с третьим лицом (далее - поставщик услуг), система управления рисками обеспечивает предоставление Организатору торговли 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**

19.1. 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

руководителем Службы по управлению рисками, а в случаях, предусмотренных Уставом Организатора торговли, может приниматься уполномоченными органами управления.

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

19.3. 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, определение контролей на основе экспертного суждения руководителей/работников структурных подразделений в рамках выполняемых ими функций и задач.

19.4. 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.

19.5. 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.

19.6. 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.

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

19.8. 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.

#### 19.8.1. Эксперт участвует в:

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

#### 19.8.2. Риск-менеджер определяет:

- уровень проведения самооценки (топ-менеджмент, линейный менеджмент, отдельные направления деятельности, подразделения или отдельные бизнес-процессы);
- сроки проведения самооценки;
- 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, полученная в рамках ведения претензионной работы и иное.

#### 19.8.3. 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).

19.8.4. 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.

19.9. 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).

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

19.11. 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.

19.12. 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).

19.13. В процессе самооценки работник совместно с Риск-менеджером определяют следующие аспекты:

- какие риски существуют в структурном подразделении, процессах или в целом у Организатора торговли, 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 Организатора торговли 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 Организатора торговли 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.

19.14. 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 Организатором торговли таких рисков значимыми, а также с установленным значением предельного уровня рисков (допустимого уровня рисков).

В процессе самооценки проводится оценка эффективности контрольных процедур.

19.15. 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.

19.16. 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.

19.17. 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.

19.18. 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.

19.19. 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.

19.20. Порядок документального оформления результатов самооценки следующий:

- ответственный работник Службы по управлению рисками заносит риски, идентифицированные в рамках самооценки в БДР;
- ответственный работник Службы по управлению рисками готовит отчет о результатах самооценки, содержащий сводный реестр рисков, сводную аналитическую информацию об исполнении мероприятий по рискам, идентифицированным в рамках предыдущей самооценки.

Отчеты или выдержки из них могут представляться органам управления Организатора торговли по запросу.

## **20 Порядок и периодичность (не реже одного раза в шесть месяцев) проведения испытательных работ (тестирования) средств проведения торгов, а также порядок устранения недостатков, выявленных в результате их проведения**

20.1. 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 Организатора торговли, 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.

20.2. 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.

### 20.3. Нагрузочное тестирование.

#### 20.3.1. 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 Организатора торговли 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.

#### 20.3.2. 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 систем. Отчетность предоставляется работникам тестирования, работникам, ответственным за релизное планирование и складывается в место хранения документов по релизу.

### 20.4. Проведения теста на проникновение.

#### 20.4.1. 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 методикам OSSTMM, NIST, PTES, OWASP, но не ограничиваться ими;
- Моделирование действий злоумышленника, направленных на достижение целей нарушения информационной безопасности (связанные с нарушением конфиденциальности и целостности информации, нарушением доступности сервиса, с нарушением принципа безотказности, с нарушением бизнес-логики) через эксплуатацию слабостей и уязвимостей информационных систем;
- Проведение проверки устранения ранее выявленных уязвимостей в информационных системах Организатора торговли;
- Оценка рисков информационной безопасности;
- Выработка рекомендаций для снижения выявленных рисков информационной безопасности.

20.4.2. 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.

20.5. Тестирование аварийного восстановления (DR тестирование).

20.5.1. Порядок проведения DR тестирования:

- Периодичность проведения DR тестирования - не реже одного раза в год;
- Подготовка плана тестирования техническими специалистами. План подлежит обязательному согласованию с внутренними участниками тестирования, а также внешними участниками торгов;
- Технические подразделения совместно со Службой по управлению рисками организуют и проводят тестирование в соответствии с согласованным планом тестирования;
- По результатам тестирования составляется 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.

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

Потребителями данной отчётности являются: владельцы проверяемой информационной системой, бизнес-владельцы, технические владельцы и Служба по управлению рисками.

20.6. В рамках управления операционным риском Организатор торговли 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.

20.7. Организатором торговли 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 Комитета по согласованию технологических изменений ПТК ПАО Московская Биржа, без рассмотрения которого невозможно какое-либо изменение конфигурации торгово-клиринговых и обеспечивающих систем.

## **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**

21.1. В рамках процесса управления рисками не реже одного раза в год проводится оценка эффективности управления рисками посредством анализа результативности 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.



## 21.2. 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 руководителя Службы по управлению рисками 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, и выносится на рассмотрение Правления и Наблюдательного Совета.

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

21.4. Организатор торговли 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 Организатором торговли, должна оцениваться на предмет эффективности и результативности 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.

Утверждение критериев оценки эффективности системы управления рисками осуществляется Наблюдательным Советом АО НТБ не реже одного раза в год.

В процессе оценки эффективности системы управления рисками также принимает участие СВА как подразделение внутреннего аудита, структурно не зависящее от подразделений риск-менеджмента (в частности, Службы управления рисками),

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 Организатора торговли. Сбор данных и анализ результативности, их представление для отчета по оценке эффективности производят работники Службы по управлению рисками.

Под эффективностью системы управления рисками Организатора торговли 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 полноты и качества мероприятий, направленных на снижение риска (в частности, операционного риска).

## **22 Порядок принятия Организатором торговли мер по предотвращению и урегулированию конфликта интересов, возникающего у Организатора торговли в связи с совмещением им своей деятельности с иными видами деятельности**

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

- обеспечение организационной и (или) функциональной независимости работников Организатора торговли, в том числе руководителей подразделений, созданных для осуществления деятельности Организатора торговли, 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 Организатора торговли и иными лицами, если указанный обмен информацией приводит или может привести к возникновению или реализации конфликта интересов;
- обеспечение отсутствия в системах оплаты труда работников Организатора торговли, а также вознаграждения лиц, действующих за счет Организатора торговли, условий, которые приводят или могут привести к возникновению конфликта интересов;
- обеспечение контроля за действиями работников Организатора торговли, а также лиц, действующих за счет Организатора торговли, 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 Организатора торговли и способная оказать негативное влияние на интересы и права потребителей финансовых услуг, а также запрет 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 Организатора торговли 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 Организатора торговли и его работников при урегулировании конфликта интересов.

22.2. В целях управления данным видом риска проводятся регулярные процедуры оценки не реже одного раза в год, выявленные риски подлежат обработке в соответствии с настоящими Правилами.

## **23 Порядок разработки и утверждения плана непрерывности бизнеса**

23.1. План непрерывности бизнеса (далее – План) разрабатывается Службой по управлению рисками 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 Организатора торговли (появление новых офисов, смена/перемещение более 20% кадрового состава и т. д.).

23.2. План подлежит тестированию не реже, чем один раз в год. План подлежит активации при обнаружении существенных инцидентов, представляющих потенциальную угрозу для деятельности Организатора торговли. 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 Организатора торговли;
- активированы планы ОНВД;
- объявлен режим ЧС.

23.3. При оценке уровня опасности используются следующие условия:

- 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;
- 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 Организатора торговли (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 Организатора торговли;
- 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**

25.1. 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.

25.2. В рамках управления рисками непрерывности деятельности Организатора торговли определяются:

- порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования Организатора торговли (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 Организатором торгов принятых на себя обязательств),
- составляется План непрерывности бизнеса, в котором описываются процессы функционирования и определяются приоритеты деятельности Организатора торговли 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).

25.3. Организатор торговли 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 Организатора торговли, 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 Организатора торговли.

## **26 Порядок ведения Организатором торговли перечня потенциальных чрезвычайных ситуаций**

Порядок ведения перечня потенциальных ЧС включает в себя следующие действия:

- определение областей, в рамках которых Организатор торговли может быть подвержен рискам непрерывности бизнеса;
- выделение перечня потенциальных ЧС, реализация которых может привести к нарушению хода критических процессов, определенных на этапе анализа воздействия на бизнес;
- анализ степени влияния потенциальных ЧС на Организатора торговли в случае их реализации, в т.ч. на:
  - работников Организатора торговли;
  - средства проведения торгов Организатора торговли;
  - инфраструктуру Организатора торговли;
- оценку вероятности реализации угрозы;
- анализ существующих контрольных процедур;
- определение возможных мер по минимизации рисков.

## **27 Порядок распределения ответственности и полномочий между структурными подразделениями Организатора торговли/компаний Группы и их работниками в случае реализации существенных событий операционного риска**

27.1. Порядок распределения ответственности и полномочий между структурными подразделениями Организатора торговли/компаний Группы и их работниками в случае реализации нештатной ситуации (НС) содержит в себе следующее:

- При возникновении НС собирается Малый Кризисный Центр – рабочий орган, состоящий из работников компаний Группы «Московская Биржа» (в т.ч. АО НТБ) и осуществляющий первичную оценку НС. Малый Кризисный Центр дает рекомендации о действиях в конкретной НС и (или) принимает решение о созыве Большого Кризисного Центра. Большой Кризисный Центр принимает решения по вопросам, связанным с возникновением нештатных ситуаций при проведении торгов в ПАО Московская Биржа, а также вырабатывает рекомендации уполномоченным органам компаний Группы «Московская Биржа» по вопросам урегулирования нештатных ситуаций при проведении торгов и клиринга.;
- Любой работник, обнаруживший НС или признаки возникновения НС, обязан не позднее 5 минут сообщить об этом работнику, включённому в Малый Кризисный Центр;
- Член Малого Кризисного Центра, получивший информацию об НС, обязан немедленно приступить к выяснению характера возможной причины и последствий НС и в зависимости от необходимости или отсутствия необходимости приостанавливать торги, обязан осуществлять действия, указанные во внутреннем документе АО НТБ, предусматривающего действия подразделений компаний Группы в нештатных ситуациях при проведении торгов и клиринга.
- 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;
- Уполномоченный сотрудник Организатора торговли осуществляет уведомление (на официальном сайте АО НТБ 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 (если это требуется).

27.2. При возникновении НС, которая привела к приостановке торгов и клиринга,

Дежурный операционный директор незамедлительно организывает и не позднее 15 минут после обнаружения НС обеспечивает раскрытие информации о НС на официальном сайте АО НТБ в сети интернет.

Дежурный операционный директор координирует деятельность работников Организатора торговли и компаний Группы в соответствии с внутренним документом Организатора торговли/компаний Группы, предусматривающего действия подразделений в нештатных ситуациях при проведении торгов и клиринга.

27.3. При возникновении НС, которая не привела к приостановке торгов, член Малого Кризисного Центра рассылает сообщения остальным членам МКЦ в целях организации телефонной конференции для принятия решения в порядке, установленном во внутреннем документе, Организатора торговли/компаний Группы, предусматривающего действия подразделений в нештатных ситуациях при проведении торгов и клиринга.

После организации телефонной конференции член Малого Кризисного Центра, получивший информацию о НС, докладывает:

- о времени получения информации о НС;
- о работнике, сообщившем о НС;
- о характере причин и последствий НС.

Члены Малого Кризисного Центра коллегиально вырабатывают рекомендации 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 Большого Кризисного Центра дежурный операционный директор организует работу Большого Кризисного Центра в соответствии со следующим порядком:

- Общую координацию по организации и работе Большого Кризисного Центра осуществляет дежурный операционный директор;

- Для организации работы Большого Кризисного Центра дежурный операционный директор инициирует информирование его членов и обеспечивает организацию конференции в целях проведения совещания.
- 27.4. После устранения причин НС и/или восстановления штатного функционирования ПТК дежурный операционный директор выполняет действия, указанные во внутреннем документе Организатора



торговли/компаний Группы, предусматривающего действия подразделений в нештатных ситуациях при проведении торгов и клиринга.

- Не позднее чем за 15 минут до времени возобновления торгов раскрытие на официальном сайте АО НТБ в сети интернет информации о времени доступности торговой системы для осуществления отдельных операций, времени возобновления и регламенте проведения торгов. Раскрытие информации на официальном сайте АО НТБ в сети Интернет осуществляется уполномоченными работниками;

- 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 уполномоченными работниками;

- Информирование иных организаций, заключивших с АО НТБ договоры о взаимодействии при проведении торговых операций, о времени возобновления проведения торговых и иных операций. Информирование осуществляется уполномоченными работниками;

- 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.

27.5. По факту произошедшего существенного события операционного риска Служба по управлению рисками 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.

Служба по управлению рисками 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;

27.6. Если существенное событие операционного риска привело к нарушению установленных пороговых значений риск-аппетита, проводится эскалация информации и предоставление отчетности Правлению и Наблюдательному Совету.

## **28 Порядок проведения оценки Правил управления рисками**

Организатор торговли проводит оценку Правил управления рисками по мере необходимости (но не реже одного раза в год) на предмет их актуальности и эффективности.

В случае выявления в них неактуальных сведений и(или) мер, не обеспечивающих эффективность функционирования системы управления рисками по оценке Организатора торговли, осуществляется пересмотр настоящих Правил.