Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

«___»_____2023 г. №_____-П

г. Москва

П О Л О Ж Е Н И Е

О требованиях к управлению операционным риском и порядку проведения операционного аудита организаторов торговли, клиринговых организаций, центральных контрагентов, центрального депозитария и репозитариев

Настоящее Положение на основании частей 1 и 4 статьи 15, пункта 12 части 1 статьи 25 Федерального закона от 21 ноября 2011 года № 325-ФЗ «Об организованных торгах»[1], части 24 статьи 5, части 2 статьи 6^1, части 5 и 5^1 статьи 22, пунктов 10, 11 и 12 части 1 статьи 25 Федерального закона от 7 февраля 2011 года № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте»[2], пунктов 1 и 3 статьи 32, Федерального закона от 7 декабря 2011 года № 414-ФЗ «О центральном депозитарии»[3] и пункта 5 статьи 15^7 Федерального закона от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг»[4] устанавливает требования к управлению операционным риском и порядку проведения операционного аудита организаторов торговли, клиринговых организаций, центральных контрагентов, центрального депозитария и репозитариев.

---

[1] Собрание законодательства Российской Федерации, 2011, № 48, ст. 6726; 2013, № 30, ст. 4084.
[2] Собрание законодательства Российской Федерации, 2011, № 7, ст. 904; 2013, № 30, ст. 4084; 2015, № 27, ст. 4001; 2016, № 1, ст. 23.
[3] Собрание законодательства Российской Федерации, 2011, № 50, ст. 7356; 2013, № 30, ст. 4084; 2019, № 52, ст. 7802.
[4] Собрание законодательства Российской Федерации, 1996, № 17, ст. 1918; 2016, № 1, ст. 50.

Глава 1. Общие положения

1.1. Организатор торговли, клиринговая организация, центральный контрагент, центральный депозитарий и репозитарий (далее при совместном упоминании – финансовая организация) в рамках управления рисками должны осуществлять управление риском нарушения лицензируемой деятельности финансовой организации (деятельности, осуществляемой в соответствии с присвоенным статусом) (далее – лицензируемая деятельность), деятельности ее контрагентов и (или) ее клиентов, в результате несовершенства или ошибочных внутренних процессов финансовой организации, действий или бездействия персонала и иных лиц, сбоев и (или) ошибок в функционировании программно-технических и информационных систем, а также в результате внешнего воздействия (далее – операционный риск) в соответствии с настоящим Положением.

1.2. Финансовая организация в целях управления операционным риском должна на непрерывной основе осуществлять выявление инцидентов, потенциально угрожающих финансовой организации нарушением осуществления лицензируемой деятельности в результате реализации операционного риска (далее – инцидент операционного риска).

1.3. Финансовая организация в целях управления операционным риском должна на непрерывной основе осуществлять выявление событий, оказывающих негативное воздействие на осуществление лицензируемой деятельности и (или) способное вследствие указанного воздействия оказать негативное влияние на осуществление деятельности финансовой организации, деятельности ее контрагентов и (или) ее клиентов, в связи с реализацией операционного риска (далее – событие операционного риска).

1.4. Финансовая организация должна осуществлять фиксацию всех инцидентов операционного риска в базе данных инцидентов (далее – База инцидентов) и всех событий операционного риска в базе данных событий операционного риска (далее – База событий) в соответствии с главой 3 настоящего Положения.

1.5. Финансовая организация в целях управления операционным риском должна определить во внутренних документах, закрепляющих меры, направленные на снижение рисков (далее – внутренние документы), перечень процессов, отрицательное (негативное) воздействие событий операционного риска на которые и (или) приостановление которых вследствие реализации событий операционного риска влечёт или может повлечь нарушение осуществления лицензируемой деятельности финансовой организации, деятельности ее контрагентов и (или) ее клиентов (далее – критически важный процесс), включая критически важные процессы, указанные в приложении 1 к настоящему Положению. При определении критически важных процессов финансовая организация должна указать структурные подразделения – участники критически важных процессов. Финансовая организация должна проводить регулярный (не реже одного раза в год) анализ необходимости пересмотра перечня критически важных процессов.

1.6. Финансовая организация в рамках управления операционным риском должна осуществлять регулярную (не реже одного раза в два года) оценку основных процессов создания и эксплуатации программно-технических средств и информационных систем, сбои и (или) ошибки в функционировании которых способны повлечь за собой приостановление критически важных процессов финансовой организации и (или) оказать иное неблагоприятное воздействие на критически важные процессы финансовой организации (далее – программно-технические средства), а также оценку функционирования критически важных процессов финансовой организации, с привлечением независимых консультантов (экспертов) (далее – операционный аудит), в соответствии с главой 4 настоящего Положения.

1.7. Финансовая организация в рамках управления операционным риском должна обеспечить регулярное (не реже одного раза в год) проведение структурными подразделениями финансовой организации самостоятельной оценки осуществляемой ими деятельности, в том числе в части составляющих процессов, с целью выявления операционного риска (далее - самооценка) в

соответствии с требованиями, установленными подпунктом 2.1.8 пункта 2.1 настоящего Положения.

Глава 2. Процедуры управления операционным риском

2.1. Финансовая организация в рамках управления операционным риском должна обеспечить реализацию следующих процедур (мер).

2.1.1. Определение перечня программно-технических средств .

2.1.2. Осуществление идентификации угроз, которые могут привести к неработоспособности программно-технических средств, а также постоянного мониторинга текущего состояния программно-технических средств финансовой организации на предмет необходимости их обновления.

2.1.3. Проведение испытательных работ (тестирования) программно-технических средств финансовой организации при их введении в эксплуатацию или обновлении с учетом возможного изменения объемов проводимых операций и устранение недостатков, выявленных в работе программно-технических средств, по итогам испытательных работ (тестирования).

2.1.4. Осуществление мероприятий по замене или улучшению (обновлению) программно-технических средств, в том числе в случае выхода их из строя и (или) выявления их несоответствия характеру и объему совершаемых финансовой организацией операций.

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

2.1.6. Определение перечня мер по защите информации и их реализация.

2.1.7. Обучение работников по вопросам выявления, оценки и управления операционным риском.

2.1.8. Проведение структурными подразделениями финансовой организации самооценки и оформление отчета по итогам проведения самооценки, содержащего информацию о выявленном операционном риске, с учетом следующих требований:

самооценка проводится финансовой организацией по установленной во внутренних документах методике (далее – методика самооценки) в виде анкетирования сотрудников структурных подразделений финансовой организации и (или) при помощи иных методов, в случае принятия финансовой организацией решения о применении иных методов проведения самооценки;

финансовая организация в порядке, установленном методикой самооценки, определяет направления проводимой самооценки, включающие в себя в том числе оценку: критически важных процессов финансовой организации; существенности операционного риска; эффективности форм (способов) управления операционным риском; уровня возможных потерь при реализации операционного риска;

подготовка отчета по итогам проведенной самооценки осуществляется должностным лицом (отдельным структурным подразделением), ответственным за управление рисками финансовой организации, на основании информации, полученной от структурных подразделений по итогам проведенной самооценки, в порядке и форме, установленными методикой самооценки.

2.1.9. Определение показателей операционного риска финансовой организации, характеризующих эффективность управления операционным риском финансовой организации, в том числе бесперебойность ее деятельности, и позволяющих отслеживать изменения определенных финансовой организацией параметров в целях принятия мер по поддержанию операционного риска на определенном (допустимом) уровне, и осуществление контроля соблюдения финансовой организацией показателей операционного риска. Определение значения показателя, при достижении которого проводится его ежедневный мониторинг и реализация мер, направленных на устранение превышения фактического значения показателя над его определенным (допустимым) значением (далее – сигнальное значение), а также значение показателя, при нарушении которого информация доводится

до исполнительного органа финансовой организации и применяются меры реагирования, установленные во внутренних документах финансовой организации (далее – контрольное значение). Финансовая организация должна обеспечить проведение регулярного (не реже одного раза в три месяца) анализа показателей операционного риска, включая сигнальное и контрольное значение уровня операционного риска, и при необходимости актуализировать их.

2.1.10. Определение и реализация мер по выявлению операционного риска, обусловленного взаимодействием финансовой организации с ее контрагентами и (или) клиентами, в том числе с иными организациями финансового рынка и (или) поставщиками услуг, а также мер, направленных на снижение или устранение возможного негативного влияния операционного риска при осуществлении лицензируемой деятельности финансовой организации.

2.1.11. Определение и реализация мер по выявлению операционного риска, обусловленного передачей отдельных функций, связанных с осуществлением лицензируемой деятельности финансовой организации, третьему лицу, в случае такой передачи, а также мер, направленных на снижение или устранение возможного негативного влияния операционного риска при осуществлении лицензируемой деятельности финансовой организации.

2.1.12. Определение и реализация мер по защите персонала финансовой организации от воздействия последствий событий операционного риска.

2.2. Финансовая организация в рамках управления операционным риском должна разработать систему процедур (мер), направленных на обеспечение условий для бесперебойного функционирования программно-технических средств, а также для восстановления осуществляемой лицензируемой деятельности финансовой организации в случае реализации событий операционного риска, включающую в себя следующие мероприятия.

2.2.1. Определение перечня критически важных процессов, с указанием допустимого времени их восстановления в случае приостановления или прерывания в соответствии с приложением 1 к настоящему Положению.

2.2.2. Обеспечение контроля за бесперебойным функционированием программно-технических средств.

2.2.3. Распределение ответственности и полномочий между структурными подразделениями финансовой организации в случае реализации события операционного риска.

2.2.4. Определение перечня потенциальных чрезвычайных ситуаций.

2.2.5. Фиксация чрезвычайных ситуаций в Базе событий и проведение анализа обстоятельств возникновения чрезвычайных ситуаций.

2.2.6. Разработка и утверждение документа (документов), определяющего (определяющих) меры, принимаемые в чрезвычайных ситуациях и направленные на обеспечение непрерывности осуществления лицензируемой деятельности финансовой организации (далее - План ОНД), в соответствии с требованиями приложения 2 к настоящему Положению.

2.2.7. Проверка (тестирование) и оценка Плана ОНД в целях определения достаточности содержащихся в нем мер для обеспечения непрерывности осуществления лицензируемой деятельности финансовой организации, исходя из характера осуществляемой финансовой организацией деятельности и объема совершаемых операций, в случае выявления недостаточности указанных мер для обеспечения непрерывности осуществления лицензируемой деятельности финансовой организации - осуществление пересмотра Плана ОНД.

2.2.8. Организация функционирования резервного комплекса, функционально дублирующего основной комплекс программно-технических средств финансовой организации (далее – резервный комплекс), удовлетворяющего следующим требованиям:

расположение резервного комплекса в отдельном здании (вне основного комплекса программно-технических средств);

территориальное удаление резервного комплекса от основного комплекса программно-технических средств на расстояние, обеспечивающее возможность работников финансовой организации возобновить работу в резервном комплексе в течение двух часов с момента возникновения чрезвычайной ситуации;

проведение мероприятий по поддержанию постоянного функционирования резервного комплекса и возможности переключения на него в случае невозможности осуществления критически важных процессов финансовой организации с использованием основного комплекса программно-технических средств.

В случае принятия финансовой организацией соответствующего решения, резервный комплекс располагается на нескольких объектах, соответствующих требованиям, предъявляемым настоящим Положением к резервному комплексу.

2.2.9. Осуществление ежедневного резервного копирования информации, связанной с осуществлением лицензируемой деятельности финансовой организации, в случае изменений по сравнению с предыдущим резервным копированием.

2.2.10. Проверка наличия и техническое обслуживание независимых генераторов электричества в основном и резервном комплексе программно-технических средств финансовой организации, обеспечивающих осуществление ее критически важных процессов.

2.2.11. Создание и поддержание технического оснащения резервного комплекса на уровне, обеспечивающем восстановление критически важных процессов финансовой организации, осуществляемых с использованием программно-технических средств, и возможность их переноса из основного комплекса программно-технических средств финансовой организации в резервный комплекс в порядке и в сроки, установленные финансовой организацией.

2.2.12. Мероприятия, обеспечивающие возможность оказания услуг, необходимых для функционирования программно-технических средств основного и резервного комплекса как минимум двумя независимыми поставщиками телекоммуникационных услуг.

2.2.13. Поддержание резервного комплекса на уровне, обеспечивающем возможность функционирования всех критически важных процессов в течение не менее одного месяца с момента возникновения чрезвычайной ситуации.

2.3. Порядок реализации процедур (мер), указанных в пунктах 2.1 и 2.2 настоящего Положения, должен быть определен финансовой организацией во внутренних документах.

2.4. Должностное лицо (отдельное структурное подразделение), ответственное за управление рисками финансовой организации, должно составлять и представлять на рассмотрение исполнительного органа финансовой организации отчет об операционном риске финансовой организации, включая отчет по итогам проведенной самооценки, с приложением предлагаемого плана мероприятий в отношении существенных событий операционного риска, направленных на управление операционным риском, а также с приложением отчета по итогам реализации плана мероприятий за предыдущий отчетный период. Указанный отчет должен включаться в состав отчета, подготавливаемого должностным лицом (отдельным структурным подразделением), ответственным за управление рисками финансовой организации, о рисках финансовой организации.

Глава 3. Порядок ведения базы данных инцидентов и базы данных событий операционного риска

3.1. Финансовая организация должна установить во внутренних документах порядок ведения Базы инцидентов и Базы событий, включая требования к структуре и содержанию информации, срокам внесения информации в Базу инцидентов и в Базу событий, а также критерии

инцидентов операционного риска и событий операционного риска с учетом положений настоящей главы.

3.2. При включении событий операционного риска в Базу событий должна указываться степень их влияния на процессы финансовой организации:

существенные события операционного риска – события, влекущие за собой приостановление или прерывание осуществления критически важных процессов финансовой организации, включая чрезвычайные ситуации, а также иные события операционного риска, соответствующие критериям существенности события операционного риска, установленным соответствующим решением финансовой организации;

значимые события операционного риска – события, не относящиеся к существенным событиям операционного риска, но, оказывающие прямое негативное влияние на осуществление лицензируемой деятельности финансовой организации, в том числе на осуществление критически важных процессов, а также события, оказывающие негативное влияние на осуществление деятельности контрагентов и (или) клиентов финансовой организации;

иные события операционного риска – события, не являющиеся существенными или значимыми событиями операционного риска.

3.3. Ведение Базы инцидентов и Базы событий должно осуществляться финансовой организацией по следующим источникам (факторам) операционного риска:

3.3.1. Недостатки процессов, в том числе недостатки внутренних процессов управления в финансовой организации, несоответствие указанных процессов объему и характеру осуществляемой лицензируемой деятельности.

3.3.2 Недостатки, связанные с действиями персонала финансовой организации (непреднамеренные ошибки, умышленные действия или бездействие).

3.3.3. Отказы и (или) нарушения функционирования применяемых финансовой организацией программно-технических средств, иных систем, оборудования и (или) несоответствие их функциональных возможностей и характеристик потребностям финансовой организации.

3.3.4. Воздействие внешних причин, включая действия третьих лиц, в том числе действия суда и исполнительных органов государственной власти, Банка России, других организаций, а также иные воздействия внешнего характера.

3.4. По решению финансовой организации в рамках каждого из источников (факторов) могут быть выделены дополнительные уровни классификации операционного риска.

3.5. Содержание Базы инцидентов и Базы событий должно устанавливаться финансовой организацией в соответствии с приложением 3 к настоящему Положению.

3.6. По решению финансовой организации осуществляется ведение единой базы, включающей в себя Базу инцидентов и Базу событий, и отвечающей требованиям настоящей главы.

3.7. Финансовая организация должна ежемесячно представлять выписку из Базы событий в Банк России в соответствии с порядком взаимодействия Банка России с некредитными финансовыми организациями, определенным на основании частей первой и восьмой статьи 76^9 Федерального закона «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2015, № 29, ст. 4357; 2021, № 27, ст. 5187) (далее – Порядок взаимодействия с Банком России) не позднее десяти рабочих дней после окончания календарного месяца.

Глава 4. Порядок проведения операционного аудита

4.1. Финансовая организация должна осуществлять проведение операционного аудита с учетом положений настоящей главы и в соответствии с порядком проведения операционного аудита, установленного во внутренних

документах финансовой организации, и содержащим, в том числе, порядок определения привлекаемого независимого юридического лица для оказания консультационных услуг оценки предмета операционного аудита (далее - консультант).

4.2. Финансовая организация должна самостоятельно определять актуальные национальные и (или) международные стандарты, оценка соответствия которым будет проводиться в ходе операционного аудита, а также разрабатывать план проведения операционного аудита.

4.3. План проведения операционного аудита должен утверждаться советом директоров (наблюдательным советом) финансовой организации и должен включать в себя указание на национальные и (или) международные стандарты, оценка соответствия которым проводится в рамках операционного аудита, а также предмет проводимого аудита, в том числе:

оценка основных процессов создания и эксплуатации программно-технических средств;

оценка достаточности и эффективности применяемых мер (система контролей) в сфере функционирования критически важных процессов финансовой организации.

По решению финансовой организации определяются дополнительные направления проведения операционного аудита.

Финансовая организация направляет в Банк России (структурное подразделение, осуществляющее надзор за лицензируемой деятельностью финансовой организации) план проведения операционного аудита в Порядке взаимодействия с Банком России не позднее двадцати рабочих дней до дня утверждения плана проведения операционного аудита.

4.4. В целях проведения операционного аудита финансовая организация должна привлечь одного или нескольких консультантов.

4.5. По результатам операционного аудита должностным лицом (отдельным структурным подразделением), ответственным за управление

рисками финансовой организации, подготавливается отчет, который должен содержать:

информацию о консультанте, привлеченном в целях проведения операционного аудита (полное фирменное и сокращенное (при наличии) наименование на русском языке; идентификационный номер налогоплательщика (при наличии); основной государственный регистрационный номер (для российского юридического лица); номер, присвоенный юридическому лицу в торговом реестре или ином учетном регистре государства, в котором зарегистрировано юридическое лицо (при наличии), и дата государственной регистрации юридического лица или присвоения ему номера (для иностранного юридического лица); адрес в пределах места нахождения; номер телефона);

информацию о критически важных процессах финансовой организации в отношении которых проводилась оценка;

информацию об иных процессах, обеспечивающих осуществление лицензируемой деятельности финансовой организации, в отношении которых проводилась оценка управления операционным риском, включая показатели уровня развития каждого из процессов, в отношении которых проводился аудит;

информацию об оценке управления операционным риском в рамках процессов финансовой организации с указанием национальных и международных стандартов, оценка соответствия которым проводилась в ходе операционного аудита, а также информацию о методиках, использованных для оценки указанных процессов финансовой организации;

итоги (результаты) операционного аудита, выявленные недостатки, рекомендации по их устранению;

оценку эффективности мер, принятых в целях реализации рекомендаций и устранения недостатков, установленных по итогам ранее проведенного операционного аудита;

динамику изменения показателей уровней развития процессов финансовой организации по сравнению с аналогичными показателями, установленными по итогам предыдущего операционного аудита.

4.6. Отчет, указанный в пункте 4.5 настоящего Положения, должен направляться финансовой организацией на рассмотрение совета директоров (наблюдательного совета) финансовой организации в целях его утверждения.

4.7. В срок не позднее 5 рабочих дней со дня подписания протокола заседания совета директоров (наблюдательного совета) финансовой организации, на котором был утвержден отчет, указанный в пункте 4.5 настоящего Положения, финансовая организация в Порядке взаимодействия с Банком России должна представлять копию отчета в Банк России (структурное подразделение, осуществляющее надзор за лицензируемой деятельностью финансовой организации).

Глава 5. Заключительные положения

5.1. Положения пункта 1.6, подпунктов 2.1.3, 2.1.9 – 2.1.11 пункта 2.1, подпунктов 2.2.8, 2.2.10 – 2.2.13 пункта 2.2 и главы 4 настоящего Положения не распространяются на организаторов торговли, осуществляющих деятельность на основании лицензии торговой системы, и оказывающих услуги исключительно по проведению организованных торгов товарами, совокупный годовой объем торгов на которых во всех торговых секциях на последний рабочий день каждого квартала не превышает 50 миллиардов рублей (далее – товарная торговая система).

5.2. В течение года со дня получения лицензии торговой системы, положения пунктов 1.2 – 1.4, 1.7, подпунктов 2.1.4, 2.1.7, 2.1.8 пункта 2.1, подпунктов 2.2.6, 2.2.7, 2.2.9 пункта 2.2, пункта 2.5 и главы 3 настоящего Положения не распространяются на Товарные торговые системы, получившие лицензию торговой системы в течение года со дня вступления в силу настоящего Положения.

5.3. Положения подпункта 2.2.6 пункта 2.2 настоящего Положения не распространяются на центрального контрагента.

5.4. Положения пункта 1.6, подпункта 2.2.6 пункта 2.2 и глава 4 настоящего Положения не распространяются на центральный депозитарий.

5.5. Со дня вступления в силу настоящего Положения признать утратившим силу Положение Банка России от 11.11.2016 № 556-П «О порядке проведения центральным контрагентом операционного аудита»[5].

5.6. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от __ _____ 20__ года № ПСД-__) вступает в силу с 01 апреля 2024 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

[5] Зарегистрировано в Минюсте России 02.12.2016 N 44532

Приложение 1
к Положению Банка России
от __ ____ ____ года № ___-П
«О требованиях к управлению операционным риском и порядку проведения операционного аудита организаторов торговли, клиринговых организаций, центральных контрагентов, центрального депозитария и репозитариев»

Допустимое время восстановления критически важных процессов финансовой организации

Финансовая организация в случае приостановления или прерывания осуществления критически важных процессов, указанных в настоящем приложении, должна обеспечить их восстановление в следующие сроки:

N п/п	Критически важный процесс финансовой организации (в зависимости от вида осуществляемой деятельности)	допустимое время восстановления критически важного процесса в случае его приостановления или прерывания (в часах)
1. Финансовая организация, осуществляющая деятельность центрального депозитария		
1.1	Внесение учетных записей в учетные регистры	2
1.2	Осуществление расчетным депозитарием расчетов по результатам сделок, совершенных на организованных торгах (в случае осуществления таких расчетов)	24
1.3	Выплата депоненту доходов в денежной форме по ценным бумагам, учет прав на которые осуществляет депозитарий, и иных причитающихся	4

	владельцам указанных ценных бумаг денежных выплат	
1.4	Осуществление центральным депозитарием сверки учитываемых центральным депозитарием прав на ценные бумаги с регистратором по счету номинального держателя центрального депозитария	4
2. Финансовая организация, осуществляющая клиринговую деятельность и деятельность центрального контрагента		
2.1	Определение подлежащих исполнению обязательств	2
2.2	Совершение действий, направленных на исполнение подлежащих исполнению обязательств	2
2.3	Направление поручения на возврат имущества, являющегося клиринговым обеспечением	2
3. Финансовая организация, осуществляющая деятельность организатора торговли		
3.1	Заключение договора между участниками торгов	2
3.2	Ведение реестра участников торгов и их клиентов, реестра заявок, реестра заключенных на организованных торгах договоров, реестра внебиржевых договоров	2
3.3	Раскрытие и предоставление информации организатором торговли	2

4. Финансовая организация, осуществляющая репозитарную деятельность		
4.1	Учет заключенных не на организованных торгах договоров репо, договоров, являющихся производными финансовыми инструментами, а также иных договоров	2
4.2	Учет регистратором финансовых транзакций информации о совершении финансовых сделок и об операциях по ним с использованием финансовой платформы	6
4.3	Передача (предоставление) реестра, ведение которого осуществляет репозитарий, в Банк России или в другой репозитарий	24

Приложение 2
к Положению Банка России
от __ ____ ____ года № ___-П
«О требованиях к управлению операционным
риском и порядку проведения операционного аудита
организаторов торговли, клиринговых организаций,
центральных контрагентов, центрального
депозитария и репозитариев»

Требования к содержанию плана обеспечения непрерывности деятельности финансовой организации

План ОНД финансовой организации должен содержать:

меры, направленные на предупреждение возможного нарушения непрерывности осуществления финансовой организацией лицензируемой деятельности в условиях режима повседневного функционирования, восстановление способности финансовой организацией оказывать услуги в полном объеме в случае возникновения чрезвычайных ситуаций (далее - ЧС), обеспечение оказания финансовой организацией услуг в условиях ЧС;

порядок доступа работников финансовой организации к сведениям, составляющим План ОНД;

сведения о должностных лицах, ответственных за разработку (в том числе внесение изменений), анализ, пересмотр и реализацию (активацию и применение) Плана ОНД, а также о лицах, исполняющих соответствующие обязанности в случае их отсутствия, с указанием их должностей, фамилий, имен и отчеств (при наличии), телефонов и электронной почты;

перечень возможных ЧС, определяемый исходя из оценки вероятности их наступления, а также вероятности и характера возможных убытков и иных неблагоприятных последствий от ЧС (далее - перечень возможных ЧС), включая ресурсы, необходимые для восстановления способности финансовой организации оказывать услуги в полном объеме;

перечень критически важных процессов, а также услуг, нарушение непрерывности оказания которых приведет к неблагоприятным последствиям для финансовой организации;

порядок принятия решения о начале реализации Плана ОНД;

порядок принятия решения о переводе деятельности финансовой организации в режим ЧС (включая порядок определения момента возникновения ЧС);

перечень событий, информация о наступлении которых подлежит направлению в Банк России;

порядок информирования финансовой организацией Банка России о наступлении в деятельности финансовой организации событий, предусмотренных Планом ОНД, и принятии финансовой организацией решения о начале реализации Плана ОНД;

мероприятия, необходимые для восстановления критически важных процессов в сроки, указанные в приложении 1 к настоящему Положению;

информацию о месте сбора работников финансовой организации в случае возникновения ЧС;

адрес резервного комплекса финансовой организации;

порядок осуществления процессов, необходимых для оказания финансовой организацией услуг в условиях возникновения ЧС, включая очередность и сроки их выполнения;

порядок взаимодействия между органами управления, структурными подразделениями и работниками финансовой организации в условиях возникновения ЧС;

информацию о контактах экстренных оперативных служб (номера телефонов) и лиц, привлеченных к выполнению мер по восстановлению способности финансовой организации оказывать услуги в полном объеме (номера телефонов, адреса электронной почты);

порядок и способ экстренного оповещения органов управления, структурных подразделений и работников финансовой организации о переводе финансовой организации в режим ЧС;

инструкции для структурных подразделений и работников финансовой организации с описанием действий, необходимых для поддержания и восстановления способности финансовой организации оказывать услуги в полном объеме, порядок информирования совета директоров (наблюдательного совета), клиентов и контрагентов финансовой организации, а также Банка России о возникновении ЧС и срок такого информирования, не превышающий 1 часа с момента возникновения ЧС;

порядок завершения работы в режиме ЧС и возврата в режим повседневного функционирования финансовой организации;

программу (программы) тестирования Плана ОНД с учетом перечня возможных ЧС, предусматривающую (предусматривающие) в том числе инструкции для структурных подразделений и работников финансовой организации с описанием действий, необходимых для проведения тестирования Плана ОНД, утверждаемую (утверждаемые) исполнительным органом финансовой организации (далее - программа (программы) тестирования Плана ОНД);

порядок тестирования Плана ОНД, проводимого в форме учений, не реже 1 раза в шесть месяцев;

порядок разработки и утверждения финансовой организацией программы тестирования Плана ОНД;

порядок подготовки и срок представления совету директоров (наблюдательному совету) финансовой организации для рассмотрения отчетов о результатах тестирования Плана ОНД, содержащих описание примененных в рамках тестирования Плана ОНД сценариев, выявленных недостатков Плана ОНД, а также предложения по их устранению и совершенствованию Плана ОНД;

порядок подготовки отчета о непрерывности деятельности финансовой организации, в том числе включающего порядок и сроки его представления совету директоров (наблюдательному совету) финансовой организации, но не реже 1 раза в квартал.

Приложение 3
к Положению Банка России
от __ ____ ____ года № ___-П
«О требованиях к управлению операционным
риском и порядку проведения операционного аудита
организаторов торговли, клиринговых организаций,
центральных контрагентов, центрального
депозитария и репозитариев»

Требования к содержанию базы данных инцидентов и базы данных событий операционного риска

1. База инцидентов финансовой организации должна содержать следующую информацию:

фамилия, имя, отчество, должность ответственного сотрудника, внесшего запись об инциденте операционного риска;

уникальный порядковый идентификационный номер инцидента операционного риска;

уникальный порядковый идентификационный номер связанного события операционного риска, в случае, если такая связь установлена;

дату, когда инцидент операционного риска был зарегистрирован в Базе инцидентов (дата регистрации);

время регистрации инцидента операционного риска в Базе инцидентов (время регистрации);

дату (и время в случае, если характер инцидента операционного риска это предусматривает), когда финансовой организации стало известно об инциденте операционного риска (дата выявления);

дату, когда произошел (начался) инцидент операционного риска (дата реализации);

источник инцидента операционного риска (в соответствии с пунктами 3.3 и 3.4 настоящего Положения);

описание инцидента операционного риска;

статус рассмотрения инцидента операционного риска.

2. База событий финансовой организации должна содержать следующую информацию:

фамилия, имя, отчество, должность ответственного сотрудника, внесшего запись о событии операционного риска;

уникальный порядковый идентификационный номер события операционного риска;

уникальный порядковый идентификационный номер связанного инцидента операционного риска, в случае, если такая связь установлена;

дату, когда событие операционного риска было зарегистрировано в Базе событий (дата регистрации);

время регистрации события операционного риска в Базе событий (время регистрации);

дату, когда произошло (началось) событие операционного риска (дата реализации);

дату (и время в случае, если характер события операционного риска это предусматривает), когда финансовой организации стало известно о событии операционного риска (дата выявления);

структурное подразделение, в котором произошло событие операционного риска;

структурное подразделение, выявившее событие операционного риска;

источник (фактор) события операционного риска (в соответствии с пунктами 3.3 и 3.4 настоящего Положения);

описание события операционного риска;

оценка события операционного риска в зависимости от степени его влияния на процессы финансовой организации;

связь с другими видами риска (правовым, стратегическим, риском потери деловой репутации и другими) при наличии такой связи;

уникальный порядковый идентификационный номер связанного события операционного риска в случае, если такая связь установлена;

направление деятельности;

процесс согласно перечню критически важных процессов, определенному во внутренних документах финансовой организации;

элемент программно-технических средств (в случае, если программно-технические средства подверглись воздействию последствий события операционного риска или послужили причиной возникновения события операционного риска);

меры, направленные на устранение последствий события операционного риска;

меры, направленные на недопущение повторной реализации события операционного риска.

потери вследствие реализации события операционного риска (при наличии).