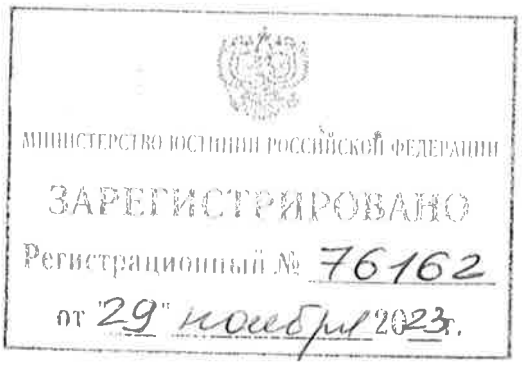
ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«02» октября 2023 г. № 827-П

г. Москва



О требованиях к управлению рисками клиринговых организаций, центральных контрагентов, центрального депозитария и репозитариев в части управления операционным риском

Настоящее Положение на основании пунктов 11 и 12 части 1 статьи 25 Федерального закона от 7 февраля 2011 года № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте», пункта 1 статьи 32 Федерального закона от 7 декабря 2011 года № 414-ФЗ «О центральном депозитарии» и пункта 5 статьи 15^7 Федерального закона от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг» устанавливает требования к управлению рисками клиринговой организации в части управления

операционным риском, требования к управлению рисками центрального контрагента в части управления операционным риском, требования к деятельности центрального депозитария в части управления операционным риском, связанным с осуществлением деятельности центрального депозитария, и требования к системе управления рисками, связанными с осуществлением репозитарной деятельности, в части управления операционным риском.

1. Клиринговая организация, центральный контрагент, центральный депозитарий и репозитарий (далее при совместном упоминании – финансовая организация) должны осуществлять управление рисками в части риска нарушения деятельности финансовой организации в результате несовершенства внутренних бизнес-процессов финансовой организации и (или) действий или бездействия работников финансовой организации, ошибок в функционировании программно-технических средств финансовой организации, а также в результате внешних событий и (или) действий или бездействия третьих лиц (далее – операционный риск).

2. Финансовая организация должна на непрерывной основе осуществлять выявление событий реализации операционного риска (далее – события операционного риска).

3. Финансовая организация должна определить перечень процессов, нарушение которых вследствие воздействия событий операционного риска влечет нарушение деятельности финансовой организации, в том числе технологических процессов, требующих обеспечения информационного взаимодействия, обработки и хранения информации с помощью программно-технических средств финансовой организации (далее соответственно – критически важные процессы, перечень критически важных процессов), а также не реже одного раза в год проводить анализ необходимости пересмотра перечня критически важных процессов.

4. Финансовая организация должна распределить полномочия в рамках управления операционным риском между советом директоров (наблюдательным советом), коллегиальным исполнительным органом финансовой организации (в случае его отсутствия – единоличным исполнительным органом финансовой организации), а также между структурными подразделениями финансовой организации.

5. Финансовая организация в рамках управления операционным риском должна:

5.1. Определить перечень программно-технических средств, ошибки в функционировании которых влекут за собой нарушение критически важных процессов (далее – критически важные программно-технические средства), и не реже одного раза в год проводить анализ необходимости пересмотра перечня критически важных программно-технических средств.

5.2. Идентифицировать угрозы, которые могут привести к ошибкам в функционировании критически важных программно-технических средств, а также осуществлять постоянный мониторинг состояния критически важных программно-технических средств на предмет необходимости их обновления.

5.3. Проводить испытательные работы в отношении критически важных программно-технических средств при их введении в эксплуатацию, в том числе при их обновлении, с учетом возможного изменения объемов проводимых операций, подготавливать отчет по итогам проведенных испытательных работ и устранять недостатки, выявленные в работе критически важных программно-технических средств, по итогам проведенных испытательных работ.

5.4. Осуществлять замену критически важных программно-технических средств в случае выхода их из строя и (или) выявления их несоответствия характеру и объему совершаемых финансовой организацией операций.

5.5. Устанавливать, разделять и осуществлять контроль прав доступа работников финансовой организации к критически важным программно-техническим средствам.

5.6. Проводить не реже одного раза в год в установленном финансовой организацией порядке оценку осуществляемой деятельности в целях выявления операционного риска, при которой должны осуществляться:

выявление и оценка структурными подразделениями финансовой организации операционного риска, возникающего в деятельности структурного подразделения финансовой организации и (или) в деятельности финансовой организации, путем определения вероятности реализации и негативного влияния от реализации операционного риска (далее – самооценка), а также подготовка отчета по итогам проведенной самооценки;

моделирование сценариев реализации операционного риска, включающее в себя оценку источников возникновения события операционного риска и его негативного влияния на деятельность финансовой организации вследствие реализации указанных сценариев (далее – моделирование), а также подготовка отчета по итогам проведенного моделирования.

5.7. Выявлять операционный риск, возникающий в связи с совмещением деятельности финансовой организации с иной деятельностью и (или) передачей отдельных функций финансовой организации третьему лицу.

5.8. Предотвращать случаи дублирования полномочий структурных подразделений финансовой организации.

5.9. Обеспечивать защиту от угроз безопасности информации.

6. Финансовая организация в рамках управления операционным риском в целях обеспечения условий для бесперебойного функционирования

критически важных программно-технических средств, а также восстановления деятельности финансовой организации в случае реализации события операционного риска должна:

6.1. Определить допустимое (по решению финансовой организации) время восстановления критически важных процессов в случае их приостановления.

6.2. Обеспечить контроль за функционированием критически важных программно-технических средств.

6.3. Распределить полномочия между структурными подразделениями финансовой организации в случае реализации события операционного риска.

6.4. Организовать функционирование резервного комплекса, функционально дублирующего основной комплекс критически важных программно-технических средств (далее соответственно – основной комплекс, резервный комплекс), удовлетворяющего следующим требованиям:

расположение резервного комплекса на территориальном удалении от основного комплекса, обеспечивающем (по решению финансовой организации) защиту резервного комплекса от событий операционного риска, источником которых являются внешние события, оказывающие воздействие на основной комплекс;

расположение резервного комплекса на территориальном удалении от основного комплекса, обеспечивающем (по решению финансовой организации) возможность работников финансовой организации возобновить критически важные процессы в резервном комплексе в течение времени, определенного в соответствии с подпунктом 6.1 настоящего пункта;

проведение мероприятий по поддержанию резервного комплекса в состоянии, обеспечивающем возможность возобновления критически важных процессов с использованием резервного комплекса в течение двух часов с

момента невозможности осуществления критически важных процессов с использованием основного комплекса.

По решению финансовой организации резервный комплекс может располагаться на нескольких объектах, каждый из которых должен соответствовать требованиям, предъявляемым настоящим подпунктом к резервному комплексу.

6.5. Обеспечить наличие и техническое обслуживание резервных источников питания в целях автономного осуществления критически важных процессов посредством основного и резервного комплексов.

6.6. Обеспечить обслуживание критически важных программно-технических средств основного и резервного комплексов не менее чем двумя поставщиками телекоммуникационных услуг.

6.7. Обеспечить возможность функционирования всех критически важных процессов в резервном комплексе в течение не менее одного месяца со дня невозможности осуществления критически важных процессов с использованием основного комплекса.

7. Финансовая организация при выявлении события операционного риска должна осуществлять его регистрацию в базе событий операционного риска (далее – база событий) с указанием следующей информации:

7.1. Вид события операционного риска:

событие, влекущее за собой приостановление осуществления критически важных процессов, а также иные события операционного риска, соответствующие критериям существенности события операционного риска, установленным решением финансовой организации (далее – существенные события операционного риска);

событие, не относящееся к существенным событиям операционного риска, но оказывающее негативное влияние на осуществление критически важных процессов, а также иные события операционного риска,

соответствующие критериям значимости события операционного риска, установленным решением финансовой организации (далее – значимые события операционного риска);

событие, не являющееся существенным событием операционного риска или значимым событием операционного риска.

7.2. Источник возникновения события операционного риска:

несовершенство внутренних бизнес-процессов финансовой организации;

действия (бездействие) работников финансовой организации;

ошибки в функционировании программно-технических средств финансовой организации;

внешние события и (или) действия или бездействие третьих лиц.

7.3. Указание на то, что событие операционного риска является событием операционного риска, связанным с нарушением операционной надежности, регистрируемым в соответствии с пунктом 1.14 Положения Банка России от 15 ноября 2021 года № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76[1] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)»[1] (при наличии).

7.4. Указание на то, что событие операционного риска является инцидентом защиты информации, регистрируемым в соответствии с пунктом 1.14 Положения Банка России от 20 апреля 2021 года № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при

[1] Зарегистрировано Минюстом России 28 марта 2022 года, регистрационный № 67961.

осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»[1] (при наличии).

7.5. Фамилия, имя, отчество (при наличии), должность работника финансовой организации, внесшего запись о событии операционного риска в базу событий.

7.6. Уникальный идентификационный номер события операционного риска.

7.7. Дата регистрации события операционного риска в базе событий (дата регистрации).

7.8. Время регистрации события операционного риска в базе событий (время регистрации) (при наличии).

7.9. Дата, когда произошло (началось) событие операционного риска (дата реализации).

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

7.11. Структурное подразделение финансовой организации, в котором произошло событие операционного риска (при наличии).

7.12. Структурное подразделение финансовой организации, выявившее событие операционного риска (при наличии).

7.13. Описание события операционного риска.

7.14. Связь события операционного риска с другими видами рисков финансовой организации (при наличии).

7.15. Уникальный идентификационный номер события операционного риска, связанного с выявленным событием операционного риска (в случае если данная связь установлена).

---

[1] Зарегистрировано Минюстом России 15 июня 2021 года, регистрационный № 63880.

7.16. Влияние события операционного риска на критически важные процессы (в случае если выявленное событие операционного риска влияет на критически важные процессы).

7.17. Указание на программно-технические средства, которые подверглись негативному воздействию события операционного риска или послужили причиной возникновения события операционного риска (в случае если программно-технические средства подверглись указанному негативному воздействию события операционного риска или послужили причиной возникновения события операционного риска).

7.18. Меры, направленные на устранение последствий реализации события операционного риска, которые были приняты в связи с выявлением события операционного риска.

7.19. Меры, направленные на недопущение повторной реализации события операционного риска, которые были приняты в связи с выявлением события операционного риска.

7.20. Убытки вследствие реализации события операционного риска, отраженные в бухгалтерском учете на счетах по учету расходов в соответствии с планом счетов бухгалтерского учета для некредитных финансовых организаций, утвержденным в соответствии с пунктом 14 статьи 4 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», и приравненных к ним счетах по учету дебиторской задолженности (при наличии).

8. Финансовая организация должна определить контрольные показатели операционного риска, позволяющие отслеживать их изменения (далее – контрольные показатели операционного риска), а также количественные показатели, направленные на измерение и контроль операционного риска в определенный момент времени (далее – ключевые индикаторы операционного риска).

Финансовая организация должна определять и утверждать:

значения контрольных показателей операционного риска и ключевых индикаторов операционного риска на плановый годовой период в разрезе процессов в рамках деятельности финансовой организации, при достижении которых проводится реализация мер, направленных на устранение превышения фактического значения показателя над данным значением (далее – сигнальные значения);

значения контрольных показателей операционного риска и ключевых индикаторов операционного риска на плановый годовой период в разрезе процессов в рамках деятельности финансовой организации, при достижении которых информация доводится до совета директоров (наблюдательного совета) финансовой организации, коллегиального исполнительного органа финансовой организации (в случае его отсутствия – до единоличного исполнительного органа финансовой организации) (далее – контрольные значения).

Финансовая организация не реже одного раза в три месяца должна проводить анализ контрольных показателей операционного риска и ключевых индикаторов операционного риска и актуализировать их.

Финансовая организация должна определить орган управления финансовой организации, который утверждает сигнальные значения и контрольные значения.

9. Положения подпунктов 5.3–5.5 пункта 5, а также подпунктов 6.2– 6.7 пункта 6 настоящего Положения не распространяются на центральных контрагентов.

10. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол

заседания Совета директоров Банка России от 27 сентября 2023 года № ПСД-39) вступает в силу с 1 октября 2024 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина