ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации Банка России об организации профессиональными участниками рынка ценных бумаг системы управления операционным риском

29.11.2024 № 20-МР

Глава 1. **Общие положения**

1.1. Настоящие Методические рекомендации Банка России предназначены для использования некредитными финансовыми организациями, осуществляющими деятельность профессионального участника рынка ценных бумаг, за исключением центрального депозитария и инвестиционных советников, являющихся индивидуальными предпринимателями (далее – Организации), в целях повышения эффективности функционирования системы управления операционным риском. Понятие «операционный риск» применяется в настоящих Методических рекомендациях Банка России в значении, установленном в абзаце третьем подпункта 2.2.1 пункта 2.2 Указания Банка России № 4501-У[1] (далее – Указание № 4501-У).

1.2. Организациям в целях управления операционным риском в рамках мероприятий, реализуемых в соответствии с главой 2 Указания № 4501-У, рекомендуется:

1.2.1. Осуществлять в соответствии с порядком, установленным во внутренних документах Организации, в том числе регламентирующих

[1] Указание Банка России от 21.08.2017 № 4501-У «О требованиях к организации профессиональным участником рынка ценных бумаг системы управления рисками, связанными с осуществлением профессиональной деятельности на рынке ценных бумаг и с осуществлением операций с собственным имуществом, в зависимости от вида деятельности и характера совершаемых операций».

организацию системы управления операционным риском (далее – внутренние документы Организации), выявление случаев реализации операционного риска, повлекших нарушение и (или) приостановление (полное или частичное) процессов Организации, осуществляемых в рамках лицензируемой деятельности (далее – событие операционного риска), и их фиксацию в реестре событий операционного риска (далее – база событий).

1.2.2. Определить источник операционного риска:

несовершенство или ошибки во внутренних процессах Организации, в том числе недостатки процессов управления в Организации, несоответствие указанных процессов характеру и масштабу осуществляемой деятельности;

действия (бездействие) сотрудников Организации;

сбои и (или) ошибки в функционировании программно-технических средств, представляющих собой взаимосвязанную совокупность технических и программных средств, сбои и (или) ошибки в функционировании которых либо неработоспособность которых влечет за собой нарушение процессов Организации, осуществляемых в рамках лицензируемой деятельности Организации (далее – программно-технические средства);

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

1.2.3. При оценке операционного риска исходить из оценки вероятности наступления и характера последствий реализации операционного риска, в том числе нефинансового характера, с учетом исторических данных, а также результатов самооценки[2] и при необходимости анализа потенциальных источников операционного риска и возможных потерь от его реализации (моделирование угроз).

1.2.4. Проводить оценку наличия операционных рисков, связанных с внедрением в эксплуатацию и (или) обновлением программно-технических средств Организации.

---

[2] В терминологии подпункта 2.2.3 пункта 2.2 Указания № 4501-У.

1.2.5. При установлении в соответствии с подпунктом 2.3.4 пункта 2.3 Указания № 4501-У предельного размера (допустимого уровня) операционного риска исходить в том числе из стратегии развития бизнеса Организации, характера и масштаба ее деятельности.

1.2.6. Осуществлять регулярный (не реже одного раза в год) пересмотр предельного размера (допустимого уровня) операционного риска.

1.2.7. Определить во внутренних документах Организации:

1.2.7.1. Перечень внутренних процессов, осуществляемых в рамках лицензируемой деятельности, с указанием структурных подразделений – участников данных процессов и допустимого времени восстановления в случае нарушения и (или) приостановления указанных процессов.

1.2.7.2. Значение показателя операционного риска, при достижении которого информация доводится до сведения исполнительного органа Организации и применяются меры реагирования, установленные во внутренних документах Организации (далее – контрольное значение операционного риска).

1.2.7.3. Виды событий в зависимости от степени их влияния на деятельность Организации:

события, повлекшие последствия, указанные в абзацах третьем – шестом пункта 1.2 Указания № 4501-У, а также события операционного риска, соответствующие критериям, установленным Организацией (значимые события операционного риска);

события, не относящиеся к значимым событиям операционного риска, соответствующие критериям, установленным Организацией (существенные события операционного риска);

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

1.2.7.4. Перечень сведений, включаемых в отчеты об управлении рисками, формируемые в соответствии с абзацем десятым пункта 3.1 Указания № 4501-У (далее – отчеты об управлении рисками), включая сведения, указанные

в подпункте 1.2.9 пункта 1.2 настоящих Методических рекомендаций Банка России.

1.2.7.5. Порядок ведения базы событий, включая требования к содержанию информации, вносимой в базу событий с учетом положений главы 2 настоящих Методических рекомендаций Банка России.

1.2.7.6. Порядок ведения реестра операционных рисков[3], включая требования к содержанию информации, вносимой в реестр операционных рисков с учетом положений главы 3 настоящих Методических рекомендаций Банка России.

1.2.7.7. Порядок проведения самооценки и оформления отчета по итогам ее проведения на основании разработанной Организацией методологии с учетом положений главы 4 настоящих Методических рекомендаций Банка России.

1.2.8. Осуществлять регулярный (не реже одного раза в год) пересмотр контрольного значения операционного риска и его актуализацию при необходимости.

1.2.9. Не реже одного раза в квартал (далее – отчетный период) отражать в отчетах об управлении рисками следующие сведения:

перечень операционных рисков, выявленных за отчетный период;

перечень выявленных событий операционного риска с указанием источников операционного риска за отчетный период;

описание обстоятельств наступления каждого события операционного риска;

оценку соблюдения Организацией установленного предельного размера (допустимого уровня) операционного риска;

оценку риска до проведения мероприятий по управлению операционным риском (присущего риска) и риска по результатам проведения мероприятий по управлению операционным риском (остаточного риска) за отчетный период;

методы управления операционным риском, в том числе отказ от риска, его снижение, передача (страхование), принятие или увеличение;

---

[3] В терминологии подпункта 2.2.2 пункта 2.2 Указания № 4501-У.

описание мер по управлению операционным риском, принятых (планируемых к принятию) в связи с наступлением событий операционного риска в отчетном периоде;

рекомендации должностного лица, ответственного за управление операционным риском, по управлению операционным риском (при наличии);

результаты выполнения ранее выданных должностным лицом, ответственным за управление операционным риском, рекомендаций по управлению операционным риском (при наличии);

результаты исполнения за отчетный период плана мероприятий, содержащего перечень мероприятий по снижению или исключению операционных рисков[4];

результаты проведенной самооценки (в случае ее проведения в отчетном периоде);

информацию об актуализации реестра операционных рисков, в том числе содержащую сведения об измененных данных реестра (в случае внесения изменений в отчетном периоде).

1.2.10. Обеспечить регулярное (не реже 1 раза в год) предоставление отчетов об управлении рисками на рассмотрение совета директоров (наблюдательного совета), а при его отсутствии – высшему органу управления Организации.

1.2.11. Организовать контроль за исполнением решений, принятых в соответствии с рекомендациями должностного лица, ответственного за управление операционным риском.

1.2.12. Организовать обучение сотрудников Организации по вопросам управления операционным риском.

1.2.13. Определить разграничение ответственности и полномочий между структурными подразделениями (сотрудниками) Организации в рамках управления операционным риском.

---

[4] В терминологии абзаца второго подпункта 2.4.3 пункта 2.4 Указания 4501-У в отношении операционных рисков.

1.3. В целях управления риском реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности Организации (риском информационной безопасности), как одним из видов операционного риска, рекомендуется:

Организациям, указанным в подпункте 1.4.3 пункта 1.4 Положения № 757-П[5], – определить состав и обеспечить применение организационных и технических мер, направленных на реализацию стандартного уровня защиты, определенного пунктом 6.7 ГОСТ Р 57580.3-2022[6];

Организациям, указанным в подпункте 1.4.4 пункта 1.4 Положения № 757-П, – определить состав и обеспечить применение организационных и технических мер, направленных на реализацию минимального уровня защиты, определенного пунктом 6.7 ГОСТ Р 57580.3-2022.

Глава 2. **Рекомендации по ведению базы событий**

2.1. Ведение учета событий операционного риска рекомендуется осуществлять путем фиксации не позднее трех рабочих дней со дня выявления события операционного риска в базе событий следующих сведений:

уникальный порядковый идентификационный номер события операционного риска;

фамилия, имя, отчество (при наличии), должность сотрудника, внесшего запись о событии операционного риска;

дата внесения записи о событии операционного риска в базу событий;

дата наступления события операционного риска;

---

[5] Положение Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

[6] Национальный стандарт Российской Федерации ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 22.12.2022 № 1548-ст (М., ФГБУ «РСТ», 2023).

дата выявления структурным подразделением (сотрудником / должностным лицом) события операционного риска;

структурное подразделение, в котором наступило событие операционного риска (при наличии);

структурное подразделение (сотрудник), выявившее (выявивший) событие операционного риска;

источник операционного риска;

описание обстоятельств наступления каждого события операционного риска;

вид события операционного риска в зависимости от степени его влияния на деятельность Организации: значимые, существенные, иные события операционного риска;

взаимосвязь с другими видами риска, выявляемыми Организацией (при наличии такой связи);

внутренний процесс, при реализации которого возникло событие операционного риска, в том числе указание на 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 (планируемые и (или) реализованные);

мероприятия, направленные на снижение вероятности наступления в будущем и степени негативных последствий событий операционного риска, аналогичных выявленным;

планируемая дата завершения мероприятий по устранению последствий события операционного риска;

фактическая дата завершения мероприятий по устранению последствий события операционного риска;

убытки вследствие наступления события операционного риска, отраженные (подлежащие отражению) в бухгалтерском учете Организации (при наличии).

Глава 3. **Рекомендации по ведению реестра операционных рисков**

3.1. Организациям рекомендуется отражать в реестре операционных рисков следующие сведения:

выявленный операционный риск;

внутренний процесс, при реализации которого возникает либо может возникнуть выявленный операционный риск;

источник операционного риска;

оценка операционного риска;

указание на владельца операционного риска;

дата внесения информации об операционном риске в реестр операционных рисков;

методы управления операционным риском, в том числе отказ от риска, его снижение, передача (страхование), принятие или увеличение;

описание мероприятий по управлению операционным риском (при наличии).

3.2. Актуализацию реестра операционных рисков рекомендуется проводить по мере выявления операционных рисков, с учетом информации о результатах самооценки, а также в случае изменения сведений, содержащихся в реестре операционных рисков, в том числе указанных в пункте 3.1 настоящих Методических рекомендаций Банка России.

Глава 4. **Рекомендации по проведению самооценки**

4.1. Проведение самооценки и оформление отчета по итогам ее проведения рекомендуется осуществлять с учетом следующего:

самооценка проводится в виде анкетирования сотрудников структурных подразделений Организации с целью выявления операционного риска в

соответствии с методологией, установленной во внутренних документах Организации;

Организация определяет направления проводимой самооценки с учетом риск-ориентированного подхода в отношении внутренних процессов, осуществляемых в рамках лицензируемой деятельности, включая функционирование программно-технических средств;

в формируемый отчет по итогам проведенной самооценки рекомендуется включить сведения о наличии/отсутствии выявленных в структурном подразделении операционных рисков; возможных причинах их возникновения; предложенных мерах по управлению операционными рисками; влиянии выявленных операционных рисков на деятельность Организации; возможных потерях при реализации операционных рисков (при возможности проведения оценки указанных потерь).

Глава 5. **Заключительные положения**

5.1. Настоящие Методические рекомендации Банка России подлежат опубликованию в «Вестнике Банка России» и размещению на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Заместитель
Председателя Банка России Ф.Г. Габуния