

УТВЕРЖДЕНО  
Решением Совета директоров  
АО «Газпром газораспределение  
Саратовская область»  
(протокол от 21.12.2020 г. №3)

**ПОЛОЖЕНИЕ**  
**о системе управления операционными рисками**  
**АО «Газпром газораспределение Саратовская область»**

## ОГЛАВЛЕНИЕ

1. Общие положения .....	3
1.1. Используемые сокращения .....	3
1.2. Термины и определения .....	3
1.3. Цель и задачи документа.....	7
1.4. Область применения .....	8
1.5. Нормативные документы .....	8
1.6. Порядок изменения документа.....	8
2. Система управления операционными рисками.....	9
2.1. Цели и задачи СУОР.....	9
2.2. Принципы организации и функционирования СУОР .....	10
2.3. Ролевая структура СУОР. Распределение полномочий.....	10
2.4. Взаимодействие в рамках СУОР .....	12
3. Процесс управления операционными рисками.....	12
3.1. Формирование внутренней контрольной среды СУОР .....	12
3.2. Постановка целей .....	13
3.3. Идентификация операционных рисков.....	14
3.4. Оценка операционных рисков .....	16
3.5. Реагирование на операционные риски.....	18
3.6. Разработка и реализация мероприятий по управлению операционными рисками .....	21
3.7. Мониторинг операционных рисков и выполнения мероприятий по управлению операционными рисками.....	22
3.8. Отчетность и обмен информацией в рамках СУОР .....	23
3.9. Оценка эффективности СУОР .....	27
3.10. Автоматизация процесса управления операционными рисками .....	27

## 1. Общие положения

В настоящем Положении о системе управления операционными рисками АО «Газпром газораспределение Саратовская область» (далее – Положение), используются сокращения, термины и определения, приведенные в пп. 1.1 и 1.2.

### 1.1. Используемые сокращения

<b>Сокращение</b>	<b>Полное название</b>
КИР	Ключевые индикаторы риска
МРГ	ООО «Газпром межрегионгаз»
Общество	АО «Газпром газораспределение Саратовская область»
Политика	Политика управления рисками и внутреннего контроля Общества
СУОР	Система управления операционными рисками
СУРиВК	Система управления рисками и внутреннего контроля

### 1.2. Термины и определения

<b>Термин</b>	<b>Определение</b>
База данных о реализации операционных рисков	Совокупность статистических данных о реализовавшихся операционных рисках и их последствиях, формируемая посредством обработки информации, полученной от владельцев рисков, с целью дальнейшего использования при принятии решений в рамках управления операционными рисками
Вред	Неблагоприятные имущественные и неимущественные последствия, которые могут возникать в результате реализации операционных рисков, включая операционные потери
Граничные значения ключевых индикаторов рисков	Значения величин показателей ключевых индикаторов риска, превышение которых с высокой вероятностью может повлечь реализацию операционных рисков
Допустимый уровень операционного риска	Уровень операционного риска, не превышающий предельно допустимый уровень операционного риска, который руководство Общества считает приемлемым и в результате реализации которого отклонение от поставленной цели не превысит установленный уровень
Ключевые индикаторы рисков (КИР)	Количественные показатели, используемые для обеспечения раннего предупреждения об изменении уровня операционного риска. Сопоставление и регулярный мониторинг КИР позволяет прогнозировать динамику уровня операционных рисков и своевременно принимать меры для его сохранения на допустимом уровне

<b>Термин</b>	<b>Определение</b>
	операционного риска. Например, текучесть кадров, количество сбоев технических устройств, время простоя технических устройств, количество аварий и инцидентов, количество выявленных нарушений законодательства Российской Федерации и локальных нормативных актов Общества
Операционные налоговые риски	Риски, связанные с исчислениями и расчетами по налогам, сборам и страховым взносам, неверным исчислением налоговой базы
Операционные риски	Риски причинения вреда Обществу, возникающие в результате ошибочных действий работников Общества, нарушений в работе систем управления, искажения бизнес-процессов или влияния внешних факторов
Операционные риски в области информационной безопасности	Риски, связанные с возможностью утраты информационных активов (информации, которая хранится, обрабатывается, передается, принимается в Обществе) в результате реализации угроз информационной безопасности
Операционные риски в области информационных технологий и автоматизации	Риски, связанные с нарушениями, возникающими в области информационных технологий и автоматизации сетей связи, которые могут привести к отсутствию необходимой информации у работников Общества в ходе принятия управленческих решений
Операционные риски в области охраны труда	Риски, связанные с возможностью причинения вреда здоровью работника Общества в результате воздействия вредных и (или) опасных факторов при исполнении им своих обязанностей по трудовому договору или в иных случаях, установленных законодательством Российской Федерации
Операционные риски в области промышленной безопасности	Риски, связанные с возникновением аварий и инцидентов на опасных производственных объектах инфраструктуры Общества, приводящие к причинению вреда жизни, здоровью людей, вреда окружающей среде, безопасности третьих лиц
Операционные риски в области пожарной безопасности	Риски, связанные с возможностью причинения вреда жизни и здоровью работников Общества, с возникновением пожара в помещениях и на объектах, принадлежащих Обществу или используемых им на других законных основаниях

<b>Термин</b>	<b>Определение</b>
Операционные риски в области технологических сетей связи	Риски, связанные с возможностью возникновения дополнительных издержек в результате перерывов в процессе эксплуатации основных производственных фондов технологических сетей связи, в работе систем и сервисов связи, а также воздействия внешних факторов, которые могут привести к снижению надежности функционирования технологических сетей связи Общества и, как следствие, к рискам нарушения производственной деятельности и управления технологическими процессами, а также рискам нарушений в работе информационных систем Общества
Операционные риски в области экономической безопасности	Риски, связанные с возможностью причинения вреда Обществу в экономической сфере в связи с реализацией угрозы экономической безопасности
Операционные риски в сфере закупочной деятельности	Риски, связанные с нарушением законодательства в сфере закупок и Положения о закупках товаров, работ, услуг Общества, Положения о закупках товаров, работ, услуг ПАО «Газпром» и Компаний Группы Газпром
Операционные риски налоговой политики	Риски, связанные с возможностью выбора неэффективных налоговых моделей и схем, риски трансфертного ценообразования, риски неправомерных действий налоговых органов
Операционные риски персонала	Риски, связанные с невозможностью организации работы по обеспечению потребностей Общества в персонале и принятием решений по управлению персоналом, а также ухудшением общей внешней ситуации на рынке труда
Операционные риски по результатам закупок	Риски, связанные с нарушением условий поставки товаров (выполнением работ, оказанием услуг), неэффективным расходованием денежных средств
Операционные риски чрезвычайных ситуаций	Риски, связанные с возникновением аварий, опасных природных явлений, катастроф, стихийных бедствий, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей среде, значительные материальные потери и нарушение условий жизнедеятельности людей

<b>Термин</b>	<b>Определение</b>
Операционные юридические риски	Риски в сфере правового сопровождения деятельности Общества, риски, связанные с невозможностью достижения положительного исхода судебного и административного правоприменения, риски в сфере правового обеспечения договорной работы, риски, возникающие в ходе участия в переговорах, риски исполнения и контроля за реализацией сделок по приобретению/отчуждению пакетов акций или долей участия в коммерческих организациях, риск ненадлежащего обеспечения единой правовой политики и координации правовой работы и др.
Остаточный уровень операционного риска	Уровень операционного риска, который остается после реализации мероприятий по управлению операционным риском
Пороговый уровень операционного риска	Уровень операционного риска, представляющий границу между существенными и несущественными операционными рисками
Потери	Последствия реализации операционного риска
Предельно допустимый уровень операционного риска	Верхняя граница допустимого уровня операционного риска
Присущий операционный риск	Риск причинения вреда Обществу, возникающий в результате ошибочных действий работников Общества, нарушений в работе систем управления, искажения бизнес-процессов или влияния внешних факторов, оценка которого производится до проведения мероприятий по управлению данным риском
Риск-профиль	Совокупность присущих операционных рисков, которым подвержены виды деятельности и бизнес-процессы Общества

<b>Термин</b>	<b>Определение</b>
Система управления операционными рисками (СУОР)	Совокупность методологии в области управления операционными рисками, видов деятельности и бизнес-процессов, работников Общества, принимающих участие в управлении операционными рисками и распределение функций между ними, согласованное исполнение которых позволяет Обществу эффективно управлять операционными рисками, в том числе проводить идентификацию, оценку, реагирование и мониторинг операционных рисков, а также обеспечивать своевременное и качественное представление отчетности и информации по управлению операционными рисками
Система управления рисками и внутреннего контроля (СУРиВК)	Совокупность взаимосвязанных организационных мер и процессов, организационной структуры, локальных нормативных актов Общества, иных документов, методик и процедур (положения, регламенты, стандарты и методические указания), норм корпоративной культуры и действий, предпринимаемых работниками Общества, направленная на обеспечение достаточных гарантий достижения целей и решения задач, а также поддержку работников Общества при принятии решений в условиях неопределенности
Уровень отсечения	Нижний порог финансовых последствий реализации операционных рисков (оцененных с применением количественных методов). Операционные риски с последствиями ниже уровня отсечения не регистрируются в реестре рисков
Эксперт	Работник Общества или приглашенный специалист, обладающий специальными знаниями по направлению деятельности Общества, формирующий суждение по рассматриваемому вопросу

Термины и определения, не предусмотренные данным разделом, подлежат применению в значении, определенном Политикой.

### **1.3. Цель и задачи документа**

Целью настоящего Положения является систематизация и обобщение методов и подходов к управлению операционными рисками в процессе деятельности Общества, а также обеспечение нормативной и методологической поддержки работников Общества.

Для достижения обозначенной цели в рамках настоящего Положения решаются следующие задачи:

- уточнение и детализация целей, задач и общих принципов организации СУОР как составной части СУРиВК;
- закрепление единой методической и терминологической базы СУОР;

- описание этапов процесса управления операционными рисками и детализация задач, решаемых работниками Общества, принимающими участие в управлении операционными рисками на каждом этапе;
- определение участников СУОР, распределение функций и ответственности между участниками СУОР, порядка их взаимодействия.

#### **1.4. Область применения**

СУОР распространяется на все уровни управления и направления деятельности Общества. Все операционные риски, присущие деятельности Общества, подлежат включению в процесс управления операционными рисками.

Действие настоящего Положения распространяется на всех участников СУОР.

Все противоречия и сомнения в содержании обязанностей участников СУОР трактуются в соответствии с настоящим Положением.

#### **1.5. Нормативные документы**

Настоящее Положение соответствует требованиям законодательных актов Российской Федерации, нормативных документов ПАО «Газпром» и МРГ, а также внутренних распорядительных и нормативных документов Общества, действующим на момент его утверждения.

В частности, Положение разработано с учетом положений и требований:

- Международных и российских стандартов в области управления рисками<sup>1</sup>;
- Политики управления рисками и внутреннего контроля ПАО «Газпром», утвержденной решением Совета директоров ПАО «Газпром»;
- Методических рекомендаций по управлению рисками с использованием качественных оценок (далее – Методические рекомендации);
- Классификатора рисков ПАО «Газпром», его дочерних обществ и организаций (далее – Классификатор рисков);
- Положения о системе управления операционными рисками Группы Газпром (далее – Положение СУОР ПАО «Газпром»);
- Политики управления рисками и внутреннего контроля ООО «Газпром межрегионгаз» и организаций, входящих в группу лиц ООО «Газпром межрегионгаз»;
- Политики управления рисками и внутреннего контроля Общества.

#### **1.6. Порядок изменения документа**

Основаниями для внесения уточнений, изменений и дополнений в настоящее Положение являются:

---

<sup>1</sup> Стандарты управления рисками ISO 31000, стандарты Федерации Европейских Ассоциаций Риск Менеджеров (FERMA) Комитета спонсорских организаций Комиссии Тредвея (COSO), Комитета директоров по рискам (CCRO), Базельского комитета по банковскому надзору, а также ГОСТы серии «Менеджмент риска».

- возникновение противоречий между настоящим Положением и законодательством Российской Федерации, нормативными актами ПАО «Газпром», МРГ или локальными нормативными актами Общества;

- изменение состава или полномочий и ответственности участников СУОР;

- выявление в рамках оценки эффективности СУОР необходимости совершенствования методологии или изменения процесса управления операционными рисками.

Контроль за соблюдением Положения, поддержанием его в актуальном состоянии, а также разрешением спорных вопросов в рамках СУОР осуществляет риск-координатор Общества.

Внесение уточнений, изменений и дополнений в настоящее Положение осуществляется в установленном порядке на основании решений Совета директоров Общества.

## **2. Система управления операционными рисками**

### **2.1. Цели и задачи СУОР**

2.1.1. СУОР как составная часть СУРиВК способствует достижению целей и решению задач СУРиВК, определенных в Политике.

2.1.2. Целями СУОР также являются:

2.1.2.1. Обеспечение допустимого уровня операционного риска.

2.1.2.2. Ограничение степени влияния потенциальных угроз, воздействия внутренних и внешних факторов на операционную деятельность и достижение целей Общества.

2.1.3. Для достижения целей СУОР определяются следующие задачи СУОР:

2.1.3.1. Определение участников СУОР и распределение их функций.

2.1.3.2. Сбор внутренних и внешних данных, а также систематизация информации о потенциально возможных операционных рисках для последующей идентификации, качественной и количественной оценки значимости уровня операционных рисков и их мониторинг с использованием КИР.

2.1.3.3. Методологическое обеспечение и поддержка процесса управления операционными рисками.

2.1.3.4. Формирование методологической базы по оценке операционных рисков.

2.1.3.5. Определение видов деятельности и бизнес-процессов, наиболее подверженных операционным рискам.

2.1.3.6. Определение способа (стратегии) реагирования на операционные риски, разработка и реализация мероприятий по управлению операционными рисками и их мониторинг на основе оценки эффективности применяемых мер.

2.1.3.7. Централизация и формализация процедур подготовки отчетности по операционным рискам.

2.1.3.8. Создание информационно-аналитической среды, в рамках которой должна быть организована база данных о реализации операционных рисков с учетом совокупного размера прямых и (или) косвенных потерь.

2.1.4. Достижение целей Общества реализуется в СУОР посредством использования эффективных технологий управления операционными рисками, обеспечивая:

2.1.4.1. Устойчивость, непрерывность и эффективность деятельности Общества.

2.1.4.2. Процесс принятия управленческих решений и планирования деятельности Общества с учетом уровня операционного риска.

2.1.4.3. Ограничение последствий от реализации операционных рисков.

2.1.4.4. Эффективность использования и распределения ресурсов Общества в рамках управления операционными рисками.

## **2.2. Принципы организации и функционирования СУОР**

2.2.1. Организация и функционирование СУОР как составной части СУРиВК осуществляется с соблюдением принципов, определенных в Политике.

2.2.2. Организация и функционирование СУОР осуществляется также с соблюдением следующих принципов:

2.2.2.1. Принцип развития культуры управления операционными рисками. Сочетание индивидуальных, общекорпоративных ценностей, установок, компетенций и поведенческих моделей, определяющих позицию Общества и отношение его работников к управлению операционными рисками и предполагающих знание работниками основных принципов и требований по управлению операционными рисками и следование им в практической деятельности, а также осведомленность работников Общества о своих функциях и обязанностях в процессе управления операционными рисками.

2.2.2.2. Принцип предупреждения. Во всех случаях, где это возможно, меры уменьшения вероятности операционных рисков должны иметь приоритет над мерами уменьшения их последствий, т.е. предпочтительно проведение предупредительных (профилактических) мероприятий, позволяющих наиболее эффективно использовать финансовые и материальные ресурсы для снижения значимости уровня операционных рисков.

## **2.3. Ролевая структура СУОР. Распределение полномочий**

В рамках СУОР в Обществе выделяют следующие роли:

- генеральный директор Общества;
- риск-координатор Общества;
- владельцы рисков Общества;
- ответственные за выполнение мероприятий по управлению операционными рисками Общества.

Основные цели и задачи генерального директора Общества, риск-координатора Общества, владельцев рисков Общества в рамках СУОР как составной части СУРиВК приведены в Политике.

Настоящее Положение уточняет следующие цели и задачи участников СУОР:

2.3.1. Для генерального директора Общества:

- обеспечение непрерывного развития, повышения эффективности СУОР и принятие управленческих решений с учетом операционных рисков;
- рассмотрение и утверждение состава и граничных значений КИР Общества;
- рассмотрение сводных предложений владельцев рисков Общества по способам (стратегиям) реагирования, мероприятиям по управлению ключевыми операционными рисками и перераспределению ресурсов в отношении управления операционными рисками.

2.3.2. Для риск-координатора Общества:

- координацию взаимодействия участников СУОР;
- методологическую поддержку процесса управления операционными рисками Общества;
- информирование генерального директора Общества о видах деятельности и бизнес-процессах Общества, наиболее подверженных операционным рискам;
- предварительное рассмотрение результатов самооценки эффективности управления операционными рисками, проведенной владельцами рисков Общества;
- организацию формирования и представления по запросу генерального директора Общества отчетности по ключевым операционным рискам и оценке эффективности процесса управления операционными рисками;
- сбор отчетности по операционным рискам и мероприятиям по управлению операционными рисками, организацию консолидации полученной информации (при необходимости) для представления генеральному директору Общества и риск-координатору МРГ;
- ведение статистики по операционным рискам.

2.3.3. Для владельца риска Общества:

- обеспечение функционирования СУОР в рамках деятельности, курируемой согласно распределению прав и обязанностей в Обществе, включая координацию деятельности ответственных за выполнение мероприятий в рамках выполнения мероприятий по управлению операционными рисками и процедур внутреннего контроля;
- идентификацию и оценку операционных рисков на основе методических документов, разработанных совместно с риск-координатором Общества;
- определение способов (стратегий) реагирования на выявленные операционные риски и разработку мероприятий по управлению выявленными рисками;
- разработку и внедрение процедур внутреннего контроля в рамках управления операционными рисками;
- обеспечение интеграции процессов управления операционными рисками и процедур внутреннего контроля в реализуемые бизнес-процессы;
- разработку и направление предложений риск-координатору Общества по совершенствованию процессов управления операционными рисками и процедур внутреннего контроля;
- обеспечение в установленном порядке ресурсами на реализацию мероприятий по управлению операционными рисками в рамках своих полномочий;
- мониторинг идентифицированных и оцененных операционных рисков;

- мониторинг статуса выполнения мероприятий по управлению операционными рисками, в том числе определение мероприятий по управлению рисками, которые не могут быть выполнены в установленные сроки, и выработку необходимых мер реагирования;

- представление на периодической основе, но не реже двух раз в год, отчетности по операционным рискам в рамках корпоративной периодической и годовой статистической отчетности риск-координатору Общества;

- представление информации по операционным рискам структурным подразделениям Общества, на цели и задачи которых оказывают влияние соответствующие риски.

2.3.4. Для ответственных за выполнение мероприятий по управлению операционными рисками:

- контроль за правильным и своевременным выполнением мероприятий по управлению операционными рисками и представление информации об их выполнении владельцам рисков Общества.

2.3.5. Работники Общества в рамках СУОР руководствуются требованиями законодательства Российской Федерации, локальных нормативных актов ПАО «Газпром», МРГ, Общества, должностными инструкциями и иными документами, своевременно информируют руководство структурных подразделений Общества о новых операционных рисках, а также проходят обучение в области управления рисками в пределах денежных средств, предусмотренных бюджетом доходов и расходов Общества.

## **2.4. Взаимодействие в рамках СУОР**

Взаимодействие внутри СУОР выстраивается по иерархическому принципу. Вышестоящей организацией по отношению к Обществу выступает МРГ.

Основные положения в части взаимодействия в рамках СУОР соответствуют положениям Политики.

## **3. Процесс управления операционными рисками**

### **3.1. Формирование внутренней контрольной среды СУОР**

Основные положения в части внутренней контрольной среды СУОР соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности формирования внутренней контрольной среды, характерные для СУОР:

3.1.1. Формирование внутренней контрольной среды СУОР обеспечивает создание единой инфраструктуры СУОР, непрерывность процесса управления операционными рисками, формирование культуры управления операционными рисками в Обществе.

3.1.2. При формировании внутренней среды осуществляются:

- разработка, развитие и поддержание в актуальном состоянии локальной нормативной и методологической базы по управлению операционными рисками;

- определение и распределение функций участников СУОР в установленном порядке;

- внедрение единой системы отчетности по управлению операционными рисками;
- внедрение мероприятий, развивающих культуру управления операционными рисками.

### **3.2. Постановка целей**

Основные положения в части постановки целей в рамках СУОР соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности постановки целей, характерные для СУОР:

3.2.1. Постановка целей в рамках СУОР предусматривает определение предельно допустимых и пороговых уровней операционных рисков, которые служат основой для ранжирования операционных рисков и установления приоритетных к управлению операционных рисков, принятия решения о способах реагирования на операционные риски, позволяют проводить мониторинг операционных рисков и оценивать эффективность мероприятий по управлению операционными рисками, а также используются для осуществления процедур внутреннего контроля.

3.2.2. Предельно допустимые и пороговые уровни операционных рисков разрабатываются владельцами рисков Общества и согласуются с владельцем риска вышестоящей организации.

3.2.3. Владельцы рисков Общества на этапе внедрения СУОР, а также по результатам последующего выявления новых операционных рисков разрабатывают предложения по определению предельно допустимых и пороговых уровней операционного риска и направляют их риск-координатору Общества.

3.2.4. Риск-координатор Общества:

- анализирует предложения владельцев рисков Общества по определению предельно допустимых и пороговых уровней операционного риска;
- формирует рекомендации по использованию предельно допустимых и пороговых уровней операционного риска и методам его установления;
- формирует и выносит на утверждение генерального директора Общества предельно допустимые и пороговые уровни операционных рисков Общества;
- обеспечивает утверждение и актуализацию полученных предложений посредством формирования соответствующих распорядительных документов Общества.

3.2.5. Для снижения трудозатрат на идентификацию и оценку несущественных операционных рисков владельцем рисков Общества может быть установлен согласованный с риск-координатором Общества уровень отсечения.

Уровень отсечения Общества должен быть согласован риск-координатором МРГ. Операционные риски с последствиями ниже уровня отсечения не регистрируются в реестре рисков.

3.2.6. В качестве дополнительной системы ограничения уровня операционных рисков владельцы рисков Общества по мере развития СУОР разрабатывают систему КИР и устанавливают граничные значения КИР. КИР

отражают уровень операционного риска, а также позволяют осуществлять оперативный контроль уровня риска в зависимости от их значений.

3.2.7. Владельцы рисков Общества определяют состав и граничные значения КИР, вносят в них изменения, согласовывают с владельцем рисков вышестоящей организации и представляют риск-координатору Общества, в свою очередь риск-координатор Общества представляет полученную информацию риск-координатору МРГ.

3.2.8. Граничные значения КИР, а также допустимые уровни риска Общества подлежат пересмотру в случае существенных изменений факторов операционного риска (в том числе при изменении внешних условий, масштабов или характера деятельности Общества, бизнес-процессов, процедур внутреннего контроля, выявлении фактов реализации ключевых операционных рисков и др.).

### **3.3. Идентификация операционных рисков**

Основные положения в части идентификации операционных рисков соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности процесса идентификации операционных рисков:

3.3.1. Операционные риски характеризуются следующими особенностями:

- операционные риски присущи всем видам деятельности и бизнес-процессам Общества;

- операционные риски могут являться источниками (факторами) реализации других групп рисков, например, финансовых, правовых, репутационных рисков и др.;

- реализация операционных рисков может приводить как к прямым, так и (или) к косвенным операционным потерям.

3.3.2. На этапе идентификации осуществляется систематическое выявление и изучение операционных рисков, которые характерны для видов деятельности и бизнес-процессов Общества.

3.3.3. Идентификация операционных рисков включает:

- описание бизнес-процессов владельца риска Общества;

- выявление потенциальных опасностей, влияющих на бизнес-процессы;

- определение шансов, создающих благоприятные возможности для достижения поставленных целей в бизнес-процессе;

- выделение в каждом бизнес-процессе уязвимых мест с учетом выявленных потенциальных опасностей;

- определение факторов операционных рисков;

- установление причинно-следственных связей между выявленными факторами операционных рисков и последствиями реализации операционных рисков.

3.3.4. Классификация операционных рисков осуществляется по классификационным признакам, распространяется на операционные риски всех видов деятельности и бизнес-процессов Общества. Классификационные

признаки, порядок классификации операционных рисков устанавливаются в Классификаторе рисков.

3.3.5. Основными областями возникновения факторов операционных рисков являются: безопасность (имущественная, информационная, пожарная, экономическая), информационные технологии и автоматизация, технологическая связь, организация закупочной деятельности, коррупция, налоги и налоговая политика, организационная среда, охрана труда, персонал, планирование, природно-климатические условия, противоправные действия третьих лиц, учет и отчетность, чрезвычайные ситуации, юридическое сопровождение деятельности, эпидемии, ситуации, приводящие к ограничениям по выходу персонала на рабочие места.

3.3.6. Ключевыми операционными рисками Общества являются риски в области управления персоналом, информационных технологий и автоматизации, риски в области информационной, экономической, пожарной и промышленной безопасности, охраны труда, чрезвычайных ситуаций, риски в сфере закупочной деятельности и другие операционные риски по видам деятельности и бизнес-процессам согласно Классификатору рисков.

3.3.7. Факторы операционных рисков по сфере возникновения могут быть внешними и (или) внутренними.

3.3.8. Внешние факторы обуславливаются окружающей средой, действиями сторонних физических и (или) юридических лиц, а также действиями федеральных органов исполнительной власти, осуществляющих нормативное правовое регулирование и функции по контролю и надзору.

К внешним факторам относятся, в частности:

- изменение законодательства Российской Федерации;
- опасные природные явления, катастрофы, стихийные бедствия;
- несвоевременная поставка или поставка некачественных товаров (работ, услуг);
- случайные или преднамеренные действия физических и (или) юридических лиц, направленные против интересов Общества;
- террористические акты;
- изменение эпидемиологической обстановки на территории Российской Федерации, приводящее к ограничениям по единовременному выходу персонала на рабочие места.

3.3.9. Внутренние факторы обуславливаются внутренней средой, действиями работников и бизнес-процессами Общества.

К внутренним факторам относятся, в частности:

- сбои в работе технических устройств и информационных систем;
- аварии и инциденты на объектах инфраструктуры Общества, кроме непосредственно вызванных внешними факторами;
- неэффективность системы внутреннего контроля;
- несовершенство организационной структуры в части распределения задач и функций, распределения (разделения) полномочий и ответственности между работниками Общества, ресурсного обеспечения;

- несоблюдение (нарушение) работниками Общества установленных требований, процедур;

- недостаточный уровень квалификации работников Общества.

3.3.10. Операционные риски могут иметь одновременно несколько источников (внешних и/или внутренних факторов). Если источником реализации операционного риска является одновременно несколько не зависящих друг от друга факторов, то в процессе идентификации следует провести декомпозицию такого риска (разделить на несколько отдельных взаимосвязанных рисков, указав информацию об их взаимном влиянии в комментариях к паспорту риска) согласно влияющим факторам. Если же источником реализации операционного риска являются одновременно несколько факторов, имеющих между собой причинно-следственную связь, то в процессе идентификации они укрупняются до одного агрегирующего фактора, в названии которого акцентируется наиболее существенная из его составляющих с учетом мнения эксперта.

3.3.11. Последствия реализации операционного риска проявляются в возникновении операционных потерь.

3.3.12. Выделяются прямые и косвенные операционные потери вследствие реализации операционных рисков.

3.3.13. Прямые операционные потери:

- снижение стоимости активов;
- досрочное списание (выбытие) материальных активов;
- денежные выплаты на основании постановлений (решений) судов, предписаний (решений) федеральных органов исполнительной власти, уполномоченных в соответствии с законодательством Российской Федерации;
- денежные выплаты контрагентам и работникам Общества в целях компенсации им во внесудебном порядке понесенных убытков;
- затраты на восстановление хозяйственной деятельности Общества и устранение последствий ошибок, аварий, инцидентов, опасных природных явлений, катастроф, стихийных бедствий;
- иные затраты, связанные с устранением причин возникновения и последствий реализации операционных рисков.

3.3.14. Косвенные операционные потери:

- потеря деловой репутации;
- упущенная выгода;
- затраты на восстановление работоспособности технических устройств и информационных систем;
- дополнительные затраты рабочего времени.

### **3.4. Оценка операционных рисков**

Основные положения в части оценки операционных рисков соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности оценки операционных рисков:

3.4.1. При качественной оценке операционного риска для целей ранжирования операционного риска по видам деятельности и бизнес-процессам Общества присваивается ранг путем учета по определенному алгоритму экспертных оценок вероятности и последствий от реализации операционного риска в соответствии с Методическими рекомендациями.

3.4.2. Результаты присвоения ранга операционному риску, относящемуся к виду деятельности и бизнес-процессу Общества, подлежат пересмотру не реже двух раз в год или по факту изменения вида деятельности, бизнес-процесса Общества, в том числе реализации мероприятий по управлению операционным риском, и включаются в состав сводной отчетности по рискам.

3.4.3. При количественной оценке операционных рисков применяются, в частности, следующие методы:

- вероятностного моделирования и статистического анализа;
- имитационного моделирования;
- сценарный анализ (стресс-тестирование);
- анализ чувствительности.

3.4.4. Количественная оценка методом вероятностного моделирования и статистического анализа предполагает определение параметров функции распределения размера потерь от реализации операционного риска с использованием теоретически обоснованных предположений о законах распределения, в том числе получаемых на основе выводов по результатам статистического анализа.

3.4.5. В рамках имитационного моделирования с использованием накопленных статистических данных о событиях реализации риска моделируется с помощью экономико-математической модели функция распределения потерь, на основании которой производится расчет специальных показателей риска (VaR, размер ожидаемых и непредвиденных потерь и др.).

3.4.6. Сценарный анализ является инструментом количественной оценки операционных рисков, основанным на анализе последствий от реализации ситуации, развивающейся по разным сценариям. Сценарии представляют собой различные варианты развития рискового события (как угрозы, реализация которых может повлечь за собой негативные последствия для Общества, или шансы, создающие благоприятные возможности для осуществления дальнейшей деятельности Общества).

3.4.7. При разработке сценариев могут использоваться внешние и внутренние источники данных, в том числе мотивированное мнение эксперта.

3.4.8. Одним из вариантов применения сценарного анализа для оценки операционного риска является стресс-тестирование, основные цели которого:

- оценка операционных потерь, связанных с реализацией редких по мнению экспертов, но возможных (обусловленных влиянием факторов операционного риска) событий со значительными последствиями (стресс-сценариев);

- разработка предложений по комплексу мероприятий по управлению операционными рисками, которые могут быть проведены при реализации стресс-сценариев.

3.4.9. Сценарии стресс-тестирования (стресс-сценарии) по операционным рискам Общества разрабатываются владельцами рисков Общества, направляются на рассмотрение риск-координатору Общества. Риск-координатор Общества в свою очередь согласовывает стресс-сценарии с риск-координатором МРГ и передает на утверждение генеральному директору Общества.

3.4.10. Стресс-тестирование может быть осуществлено также на основе применения анализа чувствительности параметров экономико-математических моделей операционной деятельности Общества или факторов операционного риска.

3.4.11. Анализ чувствительности является одним из методов проведения количественной оценки рисков, основанным на анализе изменений амплитуды параметров операционного риска в зависимости от влияния отдельных факторов. В процессе анализа чувствительности среди влияющих на операционный риск факторов выявляются ключевые, оказывающие наибольшее влияние.

Применение анализа чувствительности заключается в изменении одного из параметров экономико-математической модели для оценки его влияния на результирующий показатель такой модели.

3.4.12. Результаты количественной оценки рисков могут быть использованы, в частности:

- при установлении предельно допустимых уровней операционного риска;
- при подготовке планов по управлению операционными рисками, в том числе по обеспечению непрерывности деятельности Общества в чрезвычайных ситуациях.

### **3.5. Реагирование на операционные риски**

Основные положения в части реагирования на операционные риски соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности выбора способов реагирования на операционные риски:

3.5.1. Выбранные способы (стратегии) реагирования являются основой для разработки и внедрения мероприятий по управлению операционными рисками. Реагирование и разработка мероприятий по управлению операционными рисками осуществляются в отношении всех критических операционных рисков. Реализация мероприятий в отношении существенных операционных рисков производится с применением принципа экономической целесообразности.

3.5.2. В целях управления операционными рисками владельцы рисков Общества используют следующие способы (стратегии) реагирования:

- снижение (сокращение) операционного риска;
- перераспределение (передача) операционного риска;
- принятие операционного риска;
- уклонение (избежание) от операционного риска.

3.5.3. Снижение (сокращение) операционного риска предусматривает реализацию мероприятий, направленных на снижение вероятности реализаций

операционного риска и (или) негативных последствий (в том числе изменение характера последствий) от его реализации.

3.5.4. Снижение (сокращение) операционных рисков осуществляется в следующих случаях:

- значимость уровня операционного риска превышает предельно допустимый уровень операционного риска и существуют технически реализуемые мероприятия, позволяющие снизить значимость уровня операционного риска до допустимого уровня риска;

- проведение соответствующих мероприятий предусмотрено требованиями законодательства Российской Федерации или директивами и предписаниями федеральных органов исполнительной власти;

- затраты на мероприятия по снижению операционных рисков значительно меньше возможных потерь для Общества от реализации операционных рисков;

- эффективность применения способа (стратегии) перераспределения (передачи) операционных рисков значительно ниже, а применение других способов (стратегий) невозможно или экономически нецелесообразно.

3.5.5. Подходы к управлению и инструменты снижения отдельных классов и видов операционных рисков, определенных в Классификаторе рисков, могут быть определены в локальных нормативных актах, внутренних распорядительных и методических документах Общества.

3.5.6. Перераспределение (передача) операционных рисков – переход (передача) последствий от реализации операционных рисков полностью или частично к другому юридическому лицу на основании договора (например, договора страхования, в соответствии с которым риск передается страховой компании) либо передача юридическим лицам объектов, операций, бизнес-процессов или вида деятельности Общества, подверженных операционным рискам (аутсорсинг).

3.5.7. Перераспределение (передача) операционного риска осуществляется в случае, когда невозможно его избежать, принятие операционного риска является недопустимым, а реализация мероприятий по снижению операционных рисков не является экономически целесообразной или обоснованной.

3.5.8. Перераспределение (передача) операционных рисков сопровождается необходимостью осуществлять контроль со стороны владельцев рисков Общества за качеством оказания услуг сторонним лицом, готовым взять на себя все или часть возможных негативных последствий от реализации операционных рисков.

3.5.9. В случае принятия решения о передаче того или иного связанного с операционным риском объекта или бизнес-процесса Общества в отношении сторонних организаций осуществляется оценка рисков в сфере закупочной деятельности.

3.5.10. Владельцы рисков Общества должны оценивать операционные риски, осуществлять мониторинг и управление операционными рисками, для чего могут быть внедрены дополнительные контрольные процедуры в отношении управления указанными рисками, а именно:

- проведение правовой экспертизы документов как на этапе выбора поставщика, так и в процессе поставки товаров, выполнения работ, оказания услуг;
- установление и мониторинг стандартов качества предоставления сторонней организацией товаров, выполнения работ, оказания услуг;
- определение в договоре ответственности за нарушение договорных обязательств;
- страхование рисков ответственности контрагентов по договору.

3.5.11. Принятие операционного риска – отсутствие действий, применяемых при других способах (стратегиях) реагирования на операционный риск, самострахование, т.е. создание резервных фондов внутри Общества, предназначенных для покрытия будущих убытков от реализации рисков.

Данный способ (стратегия) реагирования на операционный риск возможен только в тех случаях, когда уровень операционного риска не превышает предельно допустимый уровень операционного риска.

Обоснованное принятие операционного риска направлено на минимизацию затрат Общества при управлении операционными рисками.

3.5.12. Принятие операционного риска осуществляется в случаях, когда реализация мероприятий по снижению данного риска не является экономически целесообразной или обоснованной, т.е. стоимость мер по снижению операционного риска, включая стоимость процедур их контроля, превышает величину возможных потерь от реализации выявленного операционного риска, либо проведение таких мероприятий невозможно в связи с внешними ограничениями (например, требования законодательства Российской Федерации).

3.5.13. При принятии операционных рисков величина возможных потерь от реализации данных рисков не должна быть критической для Общества и не должна приводить к потере экономической целесообразности реализации вида деятельности или бизнес-процесса Общества, в котором идентифицирован такой риск.

3.5.14. Применение данного способа (стратегии) реагирования на операционный риск предполагает проведение мониторинга значимости уровня данного риска и в случае превышения предельно допустимого уровня – осуществление других способов реагирования на операционный риск.

3.5.15. Уклонение (избежание) от операционного риска предполагает отказ от бизнес-процессов или вида деятельности Общества, которым присущ выявленный операционный риск, полный отказ от потенциальных источников такого риска.

3.5.16. Данный способ (стратегия) реагирования может быть выбран в тех случаях, когда:

- величина возможных потерь от реализации идентифицированных операционных рисков является, по мнению экспертов, критической для Общества и (или) приводит к потере экономической целесообразности реализации деятельности Общества, в которой идентифицированы такие риски. При этом выполнение мероприятий по снижению операционных рисков не является экономически целесообразным или обоснованным, т.е. стоимость

мероприятий по снижению такого риска, включая стоимость процедур его контроля, превышает величину возможных потерь для Общества от реализации идентифицированных операционных рисков;

- отсутствуют возможности (практически реализуемые) удержания операционного риска в пределах допустимого уровня – остаточный уровень операционного риска при реализации других возможных способов (стратегий) реагирования на такой риск превышает предельно допустимый уровень операционного риска или затраты на реализацию других способов (стратегий) превышают ожидаемый экономический эффект.

3.5.17. Применение способа (стратегии) уклонения (избежания) от операционного риска с отказом от бизнес-процессов или вида деятельности Общества, подверженного операционному риску, может осуществляться путем утверждения локальных нормативных актов Общества и вынесения решений руководством Общества.

3.5.18. При принятии решения о выборе способа (стратегии) реагирования на операционный риск необходимо учитывать воздействие данного способа (стратегии) реагирования на вероятность и существенность последствий выявленного операционного риска, соотношение затрат и эффекта от его реализации. Выбранный способ (стратегия) реагирования должен обеспечить удержание операционного риска в пределах допустимого уровня.

3.5.19. Выбор способа (стратегии) реагирования на операционный риск может осуществляться с использованием матрицы значимости/управляемости операционным риском, которая позволяет определить возможные и предпочтительные способы (стратегии) реагирования на операционный риск с точки зрения значимости его уровня и управляемости.

Значимость уровня операционного риска устанавливается при проведении оценки операционных рисков.

Управляемость операционным риском оценивается экспертными методами с применением критериев относительно сферы возникновения операционного риска, возможности воздействия Общества на факторы операционного риска и осуществления контроля за ними. Критерии определения степени управляемости отдельными группами операционных рисков и порядок выбора способа (стратегии) реагирования на них с использованием матрицы значимости/управляемости могут быть закреплены в методических документах Общества.

### **3.6. Разработка и реализация мероприятий по управлению операционными рисками**

Основные положения в части разработки и реализации мероприятий по управлению операционными рисками соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности разработки и реализации мероприятий по управлению операционными рисками:

3.6.1. На основании выбранного способа реагирования на операционные риски владельцы рисков Общества разрабатывают и выполняют мероприятия по управлению операционными рисками, определяют ответственных

за выполнение мероприятий работников Общества по управлению операционными рисками. Целью разработки мероприятий является уменьшение вероятности реализации операционного риска и (или) последствий от его реализации. Результативность мероприятий по управлению операционным риском определяется путем оценки остаточного уровня операционного риска в соответствии с Методическими рекомендациями.

3.6.2. Расходы на реализацию мероприятий по управлению операционными рисками, требующие финансирования, учитываются в бюджете доходов и расходов Общества в рамках установленного бюджетного процесса (при планировании бюджета либо посредством корректировки бюджета текущего периода).

### **3.7. Мониторинг операционных рисков и выполнения мероприятий по управлению операционными рисками**

Основные положения в части мониторинга операционных рисков и выполнения мероприятий по управлению операционными рисками соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности проведения мониторинга и выполнения мероприятий по управлению операционными рисками:

3.7.1. Мониторинг операционных рисков осуществляется владельцами рисков Общества на регулярной основе с целью оценки текущей значимости уровня операционных рисков и при необходимости принятия управленческих решений по смягчению возможных последствий реализации таких рисков, а также оценки остаточного уровня операционных рисков.

В ходе мониторинга операционных рисков владельцы рисков Общества могут выявить новые операционные риски, информация о которых должна фиксироваться и представляться в рамках корпоративной периодической и годовой статистической отчетности.

Владельцы рисков Общества осуществляют мониторинг событий реализации операционных рисков и потерь, понесенных в результате их наступления.

3.7.2. Мониторинг операционных рисков может осуществляться с помощью матрицы операционных рисков, на которой указывается местоположение операционных рисков до выполнения мероприятий по управлению такими рисками и после их реализации (остаточные риски), а также местоположение операционных рисков после пересмотра их оценок при наличии оснований для пересмотра согласно утвержденной в Обществе Политике. Это позволяет визуализировать результат управления операционными рисками, выявить количество ключевых операционных рисков, которые на момент мониторинга и актуализации матрицы операционных рисков управляются недостаточно эффективно и требуют разработки и внедрения дополнительных мероприятий по управлению такими рисками.

3.7.3. Мониторинг операционных рисков может осуществляться на основе постоянного контроля факторов операционных рисков

с применением КИР и оперативного принятия корректирующих воздействий при превышении ими порогового уровня операционного риска.

3.7.4. Методические документы по определению КИР разрабатываются владельцами рисков Общества и представляются риск-координатору Общества для дальнейшей передачи на согласование с риск-координатором МРГ.

Внедрение КИР в СУОР позволяет повысить результативность процесса предупреждения реализации операционных рисков и позволяет осуществлять контроль возможности реализации факторов таких рисков.

3.7.5. В ходе мониторинга владельцы рисков Общества определяют бизнес-процессы, наиболее подверженные операционным рискам, и составляют риск-профиль.

Риск-профиль является динамичным и представляет собой наглядное отображение операционных рисков, в наибольшей степени влияющих на бизнес-процесс, деятельность структурных подразделений Общества. Форма отображения риск-профиля может быть разной, например, в виде диаграммы или матрицы, ранжирующих операционные риски по их отдельным компонентам, параметрам.

Информация о бизнес-процессах Общества, наиболее подверженных операционным рискам, и риск-профиль предоставляются владельцами рисков Общества риск-координатору Общества, в том числе в рамках корпоративной периодической и годовой статистической отчетности, по формам, утверждаемым в установленном порядке.

3.7.6. Результаты мониторинга операционных рисков позволяют осуществлять регулярную актуализацию в рамках корпоративной периодической и годовой статистической отчетности информации об операционных рисках.

### **3.8. Отчетность и обмен информацией в рамках СУОР**

Основные положения в части отчетности и обмена информацией соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности представления отчетности и обмена информацией в рамках СУОР:

3.8.1. Отчетность об операционных рисках Общества формируется для решения следующих задач:

- обеспечение руководства Общества своевременной и систематизированной информацией о выявленных операционных рисках, их факторах, результатах оценки данных рисков и их динамике, принятых способах (стратегиях) реагирования и мероприятиях по управлению операционными рисками;

- выявление видов деятельности и бизнес-процессов Общества, наиболее подверженных операционным рискам;

- анализ совокупности операционных рисков вида деятельности, бизнес-процесса, класса/вида операционных рисков Общества для принятия решения об уровне управляемости операционных рисков в соответствии с Методическими рекомендациями.

3.8.2. Отчетность в рамках СУОР формируется по результатам идентификации и оценки операционных рисков, выбора способа (стратегии) реагирования на операционные риски и реализации мероприятий по управлению операционными рисками, мониторинга операционных рисков и выполнения мероприятий по управлению операционными рисками, оценке эффективности СУОР.

3.8.3. Требования к содержанию информации и формам представления отчетов по управлению операционными рисками (об операционных рисках, мониторинге операционных рисков и статусе мероприятий по управлению операционными рисками, оценке эффективности СУОР) определяются локальными нормативными актами и методическими документами Общества с учетом требований МРГ.

3.8.4. Оперативное информирование риск-координатора Общества осуществляется владельцами рисков Общества по вопросам наличия идентифицированных и новых операционных рисков, динамики изменения уровней операционных рисков, эффективности и статуса мероприятий по управлению ими, реализовавшихся операционных рисков и понесенных убытков, о возможных изменениях внешних и внутренних факторов возникновения операционных рисков, а также по любой другой информации, способной, по мнению владельца рисков Общества, существенно повлиять на достижение поставленных целей Общества.

3.8.5. Полугодовая и годовая отчетность по управлению операционными рисками включает (но не ограничивается) следующие формы отчетов по операционным рискам: реестр операционных рисков, паспорта операционных рисков, матрицы операционных рисков, матрицы значимости/управляемости операционных рисков, профиль операционных рисков, информацию о реализовавшихся операционных рисках, самооценке эффективности СУОР, планы развития СУОР.

3.8.6. Состав и содержание информации об отдельных классах/видах операционных рисков (информационной, пожарной безопасности, в области управления персоналом, юридические и др.), о бизнес-процессах Общества, подверженных операционным рискам, а также формах представления отчетной информации об операционных рисках могут различаться с учетом специфики операционного риска или бизнес-процесса.

Владельцы рисков Общества совместно с и риск-координатором Общества вправе разрабатывать для Общества дополнительные (по отношению к уже утвержденным МРГ) формы отчетности по операционным рискам, содержащие сведения по отдельным классам/видам операционных рисков и рискам бизнес-процессов. Такие формы отчетности должны быть направлены риск-координатору МРГ.

3.8.7. В реестр операционных рисков и паспорт операционного риска должна быть включена основная информация согласно формам отчетов, утвержденных МРГ.

3.8.8. По усмотрению владельца риска Общества в реестр или паспорт операционного риска может включаться следующая дополнительная информация:

- обстоятельства выявления операционного риска;

- описание событий, приведших к прямым и (или) косвенным операционным потерям;

- указание бизнес-процессов или направлений деятельности Общества, в рамках которых операционный риск может реализоваться или на которые может оказать влияние реализовавшийся операционный риск;

- оценка достаточности установленных контрольных процедур.

3.8.9. Дополнительные формы реестра и паспортов операционных рисков, согласованные риск-координатором Общества, должны включать основную информацию об идентифицированном операционном риске.

3.8.10. Окончательный состав информации, включаемой в реестр и паспорта операционных рисков, риск-координатор Общества определяет с учетом эффективности использования той или иной информации в сравнении с трудозатратами на ее получение и актуализацию.

3.8.11. В Обществе осуществляется сбор данных о событиях реализации операционного риска и потерях, понесенных в результате их реализации.

3.8.12. Сбор данных о реализации операционных рисков и их последствиях осуществляется для решения следующих задач:

- обеспечение руководства Общества своевременной и достоверной информацией о реализации операционных рисков и их последствиях;

- оценка уровня операционных рисков и эффективности реализуемых мероприятий по управлению (снижению) уровня операционных рисков;

- обеспечение получения страхового возмещения операционных потерь в рамках применяемых программ страхования операционных рисков;

- выявление видов деятельности и бизнес-процессов Общества, наиболее подверженных операционным рискам;

- введение дополнительных мер контроля для оперативного управления операционными рисками видов деятельности и бизнес-процессов Общества, наиболее подверженных операционным рискам;

- выявление наиболее критических факторов операционных рисков;

- сбор и систематизация данных для обеспечения количественной оценки операционных рисков.

3.8.13. Информация о реализовавшихся операционных рисках представляется владельцами рисков Общества в составе корпоративной периодической и годовой статистической отчетности и должна включать данные о событии, которое привело к реализации операционного риска, и обусловивших его факторах, о финансовых и нефинансовых последствиях реализации операционного риска, операционных потерях и возмещениях.

Включается в отчетность только информация о событиях реализации таких операционных рисков, величина последствий которых превышает установленный уровень отсеечения.

3.8.14. Специальные формы представления информации о реализовавшихся операционных рисках при необходимости утверждаются в установленном порядке Обществом с учетом требований МРГ, по соответствующим классам/видам операционных рисков и операционным рискам бизнес-

процессов Общества могут включать дополнительную информацию о событиях реализации таких рисков.

3.8.15. Накопленная статистическая информация, содержащаяся в формах отчетности по операционным рискам Общества, используется при проведении оценки операционных рисков владельцами рисков Общества и риск-координатором Общества при проведении сценарного анализа и стресс-тестирования для количественной оценки операционного риска с применением статистических методов и вероятностного моделирования.

3.8.16. Работники структурных подразделений Общества, выявившие событие реализации операционного риска, информируют о данном факте владельца риска Общества, который осуществляет необходимые действия по его регистрации и включению в отчет о реализовавшихся рисках и направляет риск-координатору Общества для дальнейшего формирования сводного отчета.

3.8.17. Сводную отчетность об уровне операционных рисков формирует риск-координатор Общества. Указанная отчетность представляется в составе сводных управленческих отчетов о рисках руководству Общества и Риск-координатору МРГ.

3.8.18. В сводную управленческую отчетность об уровне операционных рисков, представляемую по запросу руководства Общества и риск-координатору МРГ, включается (если в запросе не установлено иное) информация:

- о ключевых операционных рисках Общества;
- о событиях реализации операционных рисков, произошедших в течение отчетного периода;
- о фактах нарушения установленных ограничений допустимого уровня операционного риска;
- о способах реагирования и мероприятиях по управлению операционными рисками, в том числе о мероприятиях, направленных на минимизацию негативных последствий от реализации таких рисков;
- о результатах мониторинга уровня операционных рисков (в том числе с помощью установленных КИР, о значениях КИР, которые в отчетном периоде превышали установленные граничные значения КИР, динамике значений данных КИР).

3.8.19. Помимо сводной управленческой отчетности по операционным рискам в Обществе, по мере развития СУОР при необходимости формируется дополнительная оперативная отчетность по запросу владельца риска Общества. Оперативная отчетность обеспечивает владельцев рисков Общества информацией о состоянии и динамике уровня операционных рисков, которая используется ими для принятия оперативных управленческих решений.

3.8.20. Отчетность по операционным рискам, в том числе исходные данные при формировании отчетов по операционным рискам и другая информация, используемая в СУОР и при принятии управленческих решений в отношении операционных рисков, хранится в электронном виде на сетевых ресурсах ограниченного доступа Общества в течение 5 лет, с соблюдением требований локальных нормативных актов, устанавливающих в Обществе режим коммерческой тайны. В целях формирования статистических данных по

операционным рискам Риск-координатором Общества срок хранения информации может быть увеличен.

### **3.9. Оценка эффективности СУОР**

Основные положения в части оценки эффективности СУОР соответствуют положениям Политики.

Дополнительно настоящее Положение уточняет следующие особенности оценки эффективности СУОР:

3.9.1. Самооценка эффективности СУОР проводится владельцами рисков Общества для формирования культуры управления операционными рисками, в том числе обеспечивая:

- определение степени эффективности СУОР и достаточности мероприятий по управлению операционными рисками и контрольных процедур, направленных на предупреждение и снижение операционных рисков, возникающих в операционной деятельности;

- постоянное улучшение оперативного управления операционными рисками силами владельцев рисков Общества.

3.9.2. Внутренняя оценка эффективности СУОР осуществляется работниками Общества, принимающими участие в управлении операционными рисками на периодической основе, но не реже одного раза в пять лет.

3.9.3. Риск-координатор Общества участвует в проведении самооценки эффективности СУОР, предоставляя консультации владельцам рисков Общества по методологическим вопросам.

### **3.10. Автоматизация процесса управления операционными рисками**

3.10.1. В соответствии с Политикой все процессы управления рисками Общества по мере развития СУРиВК автоматизируются, обеспечивая минимизацию трудозатрат на управление рисками при максимальной оперативности и эффективности.

Автоматизация процесса управления операционными рисками предусматривает интеграцию с другими информационными системами Общества, в которых содержится необходимая для управления операционными рисками информация.

3.10.2. Информационно-технологическое обеспечение СУОР организуется при достижении определенного уровня развития СУОР, сформированной методологической базы, формализации описания процессов управления операционными рисками, системы требований к алгоритмам расчета, математическому моделированию, методам оценки операционных рисков, к сбору, накоплению, хранению и структурированию информации об операционных рисках, конфиденциальности и информационной безопасности, закрепленных в локальных нормативных актах Общества.

Реализация указанных требований способствует разработке и внедрению вертикально интегрированного решения, обеспечивающего поддержку процессов управления операционными рисками.

3.10.3. Автоматизация процесса управления рисками направлена на решение следующих задач:

- обеспечения достоверности, полноты и защиты централизованно обрабатываемой информации об операционных рисках;
- оперативной доступности информации об операционных рисках, их характеристиках и динамике для участников СУОР;
- установления интеграционных связей между такими показателями операционных рисков, как факторы возникновения операционных рисков, КИР, результаты оценки операционных рисков, проводимые мероприятия и т.д., для их дальнейшего системного анализа.

3.10.4. Автоматизация процесса управления рисками обеспечивает:

- интеграцию реестра и паспортов операционных рисков, базы данных о реализации операционных рисков, результатов оценки и мониторинга операционных рисков и статуса мероприятий по управлению операционными рисками;
- автоматизацию моделирования, расчета и контроля показателей операционных рисков, оперативно-календарного планирования мероприятий по управлению операционными рисками;
- формирование отчетности об уровне операционных рисков;
- минимизацию трудозатрат, связанных с обработкой информации об операционных рисках;
- повышение уровня культуры управления операционными рисками.