

Приложение
к решению Совета директоров
акционерного общества
«Республиканский центр
космической связи»
от 19 декабря 2023 года
протокол №15/2023

Утверждено
решением Совета директоров
акционерного общества
«Республиканский центр
космической связи»
от 19 декабря 2023 года
протокол №15/2023

Изменения и дополнения в Политику управления рисками акционерного общества «Республиканский центр космической связи»

Внести в Политику управления рисками акционерного общества «Республиканский центр космической связи», утвержденной решением Совета директоров акционерного общества «Республиканский центр космической связи» от 08 октября 2020 года №6/2020 следующие изменения и дополнения:

пункт 1.4. изложить в следующей редакции:

«1.4. Предусмотренные настоящей Политикой подходы к управлению рисками Общества следуют принципам, изложенным в международных стандартах по управлению рисками:

- ISO 31000:2018 «Менеджмент Риска. Руководство»;
- COSO ERM:2017 «Управление рисками организации. Интеграция со стратегией и эффективностью деятельности».

Общество поддерживает и предпринимает меры для следования концепции COSO Internal Control - Integrated Framework 2013, а также другим международным стандартам, концепциям и/или моделям в области управления рисками и внутреннего контроля.»;

абзац второй пункта 5.7.1. изложить в следующей редакции:

«В случае отсутствия объективных причин для актуализации Карты рисков и Регистра рисков, а также иных документов системы управления рисками данное мероприятие проводится при возникновении необходимости (появление актуальных вопросов, требующих включения в Карту рисков и Регистр рисков и/или потеря актуальности уже включенных вопросов).»;

в пункте 5.8.1. после «Плана мероприятий по управлению ключевыми рисками» дополнить словами «и внутреннего контроля»;

дополнить пунктом 5.8.3. следующего содержания:

«5.8.3. Отчетность по системе внутреннего контроля может интегрироваться в отчеты по рискам Общества»;
абзац третий пункта 6.1. исключить.

УТВЕРЖДЕНО
решением Совета директоров
акционерного общества
«Республиканский центр
космической связи»
от «15» декабря 2021 года
протокол №6/2021

**Изменения и дополнения, вносимые в
Политику управления рисками акционерного общества
«Республиканский центр космической связи»**

Внести в Политику управления рисками акционерного общества «Республиканский центр космической связи», утвержденной решением Совета директоров акционерного общества «Республиканский центр космической связи» от 08 октября 2020 года, №6/2020 следующие изменения и дополнения:

1. Пункт 1.2. изложить в следующей редакции:

«1.2. Настоящая Политика отражает видение, цели, задачи, основные принципы и методы корпоративной системы управления рисками, а также организацию управления рисками Общества, в соответствии со стратегией развития Общества, увязанную с технико-экономическим обоснованием/финансово-экономическим обоснованием проектов/ иных альтернативных документов (далее – ТЭО/ФЭО проектов/ иных альтернативных документов), определяет структуру управления рисками, основные компоненты системы управления рисками, определяет систематический и последовательный подход при осуществлении процесса управления рисками.»

2. Абзац тридцать третий пункта 2.1. раздела «Термины и определения» изложить в следующей редакции:

«ТЭО/ФЭО проектов/ иных альтернативных документов»	Технико-экономическое обоснование или финансово-экономическое обоснование/иные альтернативные документы проектов создания спутников связи и вещания, а также проектов по оказанию услуг в области спутниковой телекоммуникации, проводной и/или беспроводной телекоммуникационной связи.»
---	---

3. Пункт 2.1 дополнить следующими терминами и определениями:

«СВТ Объекты информатизации»	Средства вычислительной техники; Электронные информационные ресурсы, программное обеспечение и информационно-коммуникационная инфраструктура;
-------------------------------------	---

**Информационная
безопасность в сфере
информатизации
(информационная
безопасность)
Риск информационной
безопасности или ИТ риск
Событие
информационной
безопасности**

Состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

Любой риск, связанный с использованием информационных технологий;

Состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации.».

4.Пункты 3.4.1., 3.4.2. после слова «проектов/» дополнить словами «иных альтернативных документов».

5.Пункт 5.1.1. изложить в следующей редакции:

«5.1.1. Риск-аппетит формируется после определения стратегических целей Общества. Для определения приемлемого уровня риск-аппетита применяются субъективный и объективный подходы. Общество идентифицирует риски, которые могут помешать ему достичь поставленных целей. Общество определяет риск-аппетит – количество риска, которое является приемлемым для Общества в достижении поставленных целей. Риск-менеджер принимает меры по вынесению риск-аппетита на утверждение Совета директоров Общества».

6.Раздел 5.5. «Разработка и внедрение мероприятий по управлению рисками» дополнить пунктами 5.5.6, 5.5.7, 5.5.8, 5.5.9, 5.5.10, 5.5.11 следующего содержания:

«5.5.6. Мероприятия по управлению ИТ-рисками включают, но не ограничиваются:

– Защита от несанкционированного копирования данных пользователем;

– Защита информации, отображаемой на мониторе СВТ;

– Защита от действий вредоносных компьютерных программ и вирусов;

– Защита от хищения носителей информации;

– Контроль доступа к локальной сети Общества;

– Защита информации СВТ;

– Защита от ошибок программно-аппаратных средств;

– Защита от некомпетентного использования, настройки или неправомерного отключения средств защиты;

– Защита от частичного или полного отказа СВТ или разрушения аппаратных, программных, информационных ресурсов;

– Защита от ввода ошибочных данных.

5.5.7 Решение вопросов стратегического планирования по информационной безопасности, а также контроль нештатных ситуаций и

инцидентов в области защиты информации, осуществляет Подразделение по защите государственных секретов совместно со Структурным подразделением по информационным технологиям.

5.5.8 Работниками Структурного подразделения по информационным технологиям проводится регулярный мониторинг и аудит программно-аппаратного комплекса, обеспечивающего функционирование норм и правил настоящей политики при общем участии Подразделения по защите государственных секретов, по согласованному и утвержденному плану графику, с предоставлением отчетности.

5.5.9 Структурное подразделение по информационным технологиям выполняет мониторинг защищенности IT ресурсов, разрабатывает правила и инструкции, контролирует соблюдение требований IT безопасности всеми участниками информационного обмена.

5.5.10 Задачей каждого сотрудника Общества является соблюдение правил, инструкций, рекомендаций по обеспечению безопасной работы локальной сети, извещение руководства обо всех подозрительных ситуациях при работе с информационными ресурсами.

5.5.11 За несоблюдение порядка и правил использования информационных ресурсов к виновным могут быть применены меры, предусмотренные трудовыми договорами, заключенными между Обществом и работником, а также действующим законодательством Республики Казахстан и настоящей Политикой.».

7. Раздел 5.6. «Уменьшение и контроль рисков» дополнить пунктом 5.6.16 следующего содержания:

«5.6.16 Уменьшение и контроль IT рисков подразумевает следующие мероприятия, проводимые структурным подразделением по информационным технологиям:

- защита от вмешательства посторонних лиц в процесс функционирования локальной сети Общества;
- разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в локальной сети Общества;
- регистрация действий пользователей при использовании ресурсов локальной сети Общества в системных журналах;
- периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами информационной безопасности;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защита информации от несанкционированной модификации, искажения;
- контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносных кодов, включая компьютерные вирусы;

– защита персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;

– обеспечение аутентификации пользователей, участвующих в информационном обмене;

– своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;

– создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;

– создание условий для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.».

8.Пункты 5.7.1. и 5.7.2. после слова «Карта» дополнить словом «рисков»

9.Пункт 5.8.1. изложить в следующей редакции:

«5.8.1 Риск-менеджер ежеквартально формирует для утверждения Советом директоров Общества отчет по рискам, состоящий из отчетной информации по:

– Карте рисков Общества (утверждается ежегодно);

– Регистра рисков Общества (утверждается ежегодно);

– Риск-аппетита (утверждается ежегодно).

– Плана мероприятий по совершенствованию процесса управления рисками (утверждается ежегодно);

– Плана мероприятий по управлению ключевыми рисками (утверждается ежегодно);

– Базы данных реализовавшихся рисков (обновляется по мере реализации рисков).».

10. Дополнить разделом 5.9. «Риски информационной безопасности (IT-риски)» и изложить в следующей редакции:

«5.9. Риски информационной безопасности

5.9.1 Под IT рисками понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

– утрата сведений, составляющих коммерческую тайну Общества и иную защищаемую информацию, а также искажение (несанкционированная модификация, подделка) такой информации;

– утечка - несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.), а также утечка информации по каналам связи и за счет побочных электромагнитных излучений;

– недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;

- отсутствие планирования и контроля;
- низкая степень надежности программного обеспечения;
- недостаточная осведомленность или низкая квалификация работников Общества в области информационных технологий.

В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Общества:

- финансовые потери, связанные с утечкой или разглашением защищаемой информации;
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
- ущерб от дезорганизации деятельности Общества и потери, связанные с невозможностью выполнения им своих обязательств;
- моральные потери (ущерб репутации Общества).».

УТВЕРЖДЕНА
решением Совета директоров
акционерного общества
«Республиканский центр
космической связи»
от «8» октября 2020 г.
протокол № 6/2020

ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ
АКЦИОНЕРНОГО ОБЩЕСТВА
«РЕСПУБЛИКАНСКИЙ ЦЕНТР КОСМИЧЕСКОЙ СВЯЗИ»

1. Общие положения

1.1. Настоящая Политика по управлению рисками (далее – Политика) акционерного общества «Республиканский центр космической связи» (далее – Общество) разработана в соответствии с законодательством Республики Казахстан, с учетом принципов, определенных в Кодексе корпоративного управления акционерного общества «Республиканский центр космической связи» и другими внутренними документами Общества и внедряется на всех уровнях управления Общества.

1.2. Настоящая Политика отражает видение, цели, задачи, основные принципы и методы корпоративной системы управления рисками, а также организацию управления рисками Общества в соответствии со Стратегией развития Общества, увязанную с технико-экономическим обоснованием/финансово-экономическим обоснованием проектов (далее – ТЭО/ФЭО проектов), определяет структуру управления рисками, основные компоненты системы управления рисками, определяет систематический и последовательный подход при осуществлении процесса управления рисками.

1.3. Общество осознает важность управления рисками как ключевого компонента корпоративного управления Общества, направленного на своевременную идентификацию и принятие мер по снижению (увеличению) уровня рисков, которые могут негативно (положительно) влиять на деятельность и репутацию Общества.

1.4. Предусмотренные настоящей Политикой подходы к управлению рисками Общества следуют принципам, изложенным в международных стандартах по управлению рисками:

- ISO 31000:2018 «Менеджмент Риска. Руководство»;
- COSO ERM:2017 «Управление рисками организации. Интеграция со стратегией и эффективностью деятельности».

1.5. Настоящая Политика не ставит целью охватить все возможные сценарии, которые могут возникнуть в процессе управления рисками, предполагая, что ежедневный процесс управления должен предоставлять свободу применения различных стилей управления и творческого подхода.

1.6. Действие настоящей Политики распространяется на все виды деятельности Общества. Политика является обязательной для ознакомления и применения всеми структурными подразделениями и всеми работниками Общества. При осуществлении функциональных обязанностей и реализации поставленных задач, каждый работник Общества руководствуется настоящей Политикой.

1.7. Целью процесса управления рисками является достижение баланса между максимальным использованием возможностей в целях получения выгоды и предотвращения потерь. Данный процесс является важной составляющей управленческого процесса и неотъемлемой частью развитой системы корпоративного управления.

1.8. При осуществлении своей деятельности в рамках настоящей Политики, Общество учитывает интересы и последствия реализации рисков для Единственного акционера, и других заинтересованных сторон.

1.9. Внедрение корпоративной системы управления рисками в Обществе подразумевает установление и развитие необходимой инфраструктуры и культуры, а также охватывает применение логических и систематических методов идентификации, анализа и оценки, мониторинга, контроля и управления рисками, присущих всем направлениям деятельности, функциям или процессам Общества, в целях предотвращения потерь и максимизации выгоды.

1.10. Контроль за соблюдением настоящей Политики, поддержанием ее в актуальном состоянии осуществляет риск-менеджер.

2. Термины и определения

2.1. В настоящей Политике используются следующие термины, определения и сокращения:

Владелец риска	Структурное подразделение/корпоративный секретарь, ответственные за бизнес–процессы и риски, которые присущи этим бизнес–процессам
Идентификация рисков	Процесс определения источников риска, событий, реализация которых может негативно отразиться на способности достичь запланированные цели, исследование их причин и описание возможных последствий
Карта рисков	Описание рисков, представленное в виде графического и текстового описания ограниченного числа рисков Общества, в котором риски расположены последовательно в зависимости от их уровня (вертикальная ось – размер ущерба риска, горизонтальная ось – вероятность его возникновения)
Ключевые риски	Риски, которые попадают в красную и оранжевую зоны Карты рисков
Ключевой рисковый показатель (КРП)	Индикатор, предоставляющий ранние сигналы изменения риск–факторов и вероятной реализации рисков, в перспективе способных оказать негативное влияние на деятельность Общества. КРП позволяют обнаруживать потенциальные риски и заблаговременно принимать меры во избежание наступления негативных событий или минимизации их влияния на деятельность организации

Координатор управления рисками	Работник, ответственный за управление рисками, определенный Председателем Правления
Мероприятия по управлению риском	Действия, разработанные на основании одного из следующих методов управления: 1) Уклонение от риска; 2) Изменение риска; 3) Перенос риска; 4) Принятие риска
Мониторинг рисков	Систематическая проверка, обновление информации об уровне риска, внешних или внутренних факторах, влияющих на уровень риска, а также о статусе мероприятий по управлению риском
Оценка рисков	Определение уровня риска количественным или качественным способом
Регистр рисков	Структурированно представленная информация о рисках в табличном виде, включает: наименование рисков, описание рисков, ключевые причины и факторы наступления рисков, описание возможных последствий от реализации рисков, оценку рисков, владельцев рисков, мероприятия по управлению рисками, сроки и статус их реализации
Риск	Влияние неопределенности на цели (как положительное, так и отрицательное). Примечание 1: Влияние – это отклонение от того, что ожидается. Оно может быть положительным и/или отрицательным, и может способствовать реализации возможностей и устранению угроз, создавать или приводить к возникновению возможностей и угроз. Примечание 2: Цели могут иметь различные аспекты и категории и могут применяться на различных уровнях
Риск-аппетит	Уровень и тип риска, которые Общество желает достигнуть или сохранить (приемлемая степень риска в процессе достижения своих целей)
Риск-коммуникация	Процесс обмена информацией и мнениями о рисках между специалистами по оценке риска, лицами, принимающими управленческие решения, средствами массовой информации, заинтересованными группами и широкой общественностью
Риск-менеджер	Работник Общества, осуществляющий координацию управления рисками в Обществе
Риск-толерантность	Приемлемый уровень отклонения в отношении достижения определенной бизнес-цели
Риск-фактор	Причина, способствующая реализации риска

Управление рисками / менеджмент	Культура, методы и подходы, интегрированные во все процессы Общества; процесс, включающий в себя идентификацию, анализ, оценку рисков, разработку и реализацию мероприятий по управлению риском, а также мониторинг рисков. Примечание: Процесс управления рисками – это не обособленный процесс, который должен быть интегрирован во все бизнес-процессы Общества, в том числе в процесс принятия решений
Уровень риска	Выраженное определенным формализованным способом сочетание «Вероятности» и «Последствий» реализации риска (согласно Карте рисков)
KPI Бизнес-риск	Ключевые показатели деятельности Неблагоприятное непредвиденное изменение объема деятельности Общества, способное привести к существенным потерям прибыли
Валютный риск	Вероятность возникновения финансовых потерь от наличия открытой валютной позиции у Общества вследствие неблагоприятных изменений курсов иностранных валют при осуществлении Обществом своей деятельности
Инвестиционный риск	Вероятность возникновения непредвиденных финансовых потерь (в т.ч. обесценения активов) в ситуации неопределенности условий инвестирования
Комплаенс-риск	Риск возникновения неблагоприятного исхода (применения юридических санкций, претензий уполномоченного государственного органа, материального финансового убытка или потери репутации) вследствие несоблюдения Обществом требований законодательства Республики Казахстан, международных стандартов, применимых к деятельности Общества, а также внутренних правил и процедур
Кредитный риск	Вероятность возникновения финансовых потерь по финансовым активам Общества в результате неисполнения и/ или не полного исполнения контрагентом своих финансовых обязательств перед Обществом
Операционный риск	Вероятность возникновения финансовых и нефинансовых потерь вследствие неадекватных или ошибочных внутренних процессов, действий работников, IT-систем и внешних событий. Операционный риск включает в себя, в том числе

	риски, связанные с оплатой Обществом штрафов, пеней или взысканиями, являющимися результатами действий органов надзора, а также частных судебных исков, за исключением стратегических и репутационных рисков
Политический риск	Возможность возникновения расходов (потерь), связанных с политическими событиями
Правовой риск	Риск возникновения расходов (потерь), судебных исков вследствие нарушения Обществом требований законодательства Республики Казахстан либо несоответствия практики Общества его внутренним документам, а в отношениях с нерезидентами Республики Казахстан – законодательств других государств, а также вследствие несоблюдения Обществом договоров, соглашений
Процентный риск	Вероятность возникновения финансовых потерь от переоценки кредитных и финансовых инструментов, оцениваемых по справедливой стоимости через прочий совокупный доход и/или учитываемых через прибыль и убыток, вследствие неблагоприятного изменения кривой доходности
Репутационный риск	Риск возникновения неблагоприятного исхода вследствие негативного общественного мнения или снижения доверия к Обществу
Стратегический риск	Риск возникновения расходов (потерь), неполучения запланированных доходов в результате ошибок (недостатков), допущенных при принятии решений, определяющих стратегию деятельности и развития Общества и выражающихся в не учете или недостаточном учете возможных опасностей, которые могут угрожать деятельности Общества; неправильном или недостаточно обоснованном определении перспективных направлений деятельности, обеспечении в неполном объеме необходимых ресурсов и организационных мер, которые должны обеспечить достижение стратегических целей Общества
Фондовый риск	Вероятность возникновения финансовых потерь от отрицательной переоценки долевых ценных бумаг, входящих в портфель акций, вследствие неблагоприятных изменений в рыночных показателях фондовых индексов

Финансовый риск	Вероятность возникновения непредвиденных финансовых потерь (снижения прибыли, доходов, потери капитала и т.п.) в ситуации неопределенности условий финансовой деятельности Общества
ТЭО/ФЭО проектов	Технико-экономическое обоснование или финансово-экономическое обоснование проектов создания спутников связи и вещания, утвержденных в установленном порядке

3. Цели, задачи и принципы

3.1. Целями управления рисками являются:

- обеспечение достижения целей деятельности Общества, определенных его стратегией, путем развития и поддержания организационной структуры, процессов и ресурсов, направленных на выявление, оценку, анализ, управление и мониторинг рисков;
- принятие решений с учетом рисков и достижение баланса между максимальным использованием возможностей для достижения поставленных целей деятельности Общества и предотвращения потерь.

3.2. Задачи управления рисками:

- создание полноценной базы для принятия решений и планирования;
- обеспечение непрерывного согласованного процесса управления рисками, основанного на своевременной идентификации, оценке, анализе, мониторинге, контроле для обеспечения достижения поставленных целей;
- своевременное выявление рисков Общества;
- предотвращение реализации рисков и снижение их последствий до приемлемого уровня;
- информирование членов Правления и Совета директоров Общества по вопросам управления рисками;
- своевременная актуализация внутренних документов Общества в области управления рисками;
- мониторинг влияния рисков на финансовую устойчивость, достижение стратегических и операционных целей и на репутацию Общества;
- развитие культуры управления рисками в Обществе, в том числе, путем организации/проведения обучающих мероприятий для работников.

3.3. Управление рисками основывается на следующих принципах:

- управление рисками интегрируется во все бизнес-процессы, направления деятельности, функции и включено в зону ответственности работников Общества;
- управление рисками является неотъемлемой частью процесса принятия решений;
- информация о рисках отражается в управленческой отчетности;
- управление рисками осуществляется на систематической основе;

- система мотивации работников Общества учитывает эффективность управления рисками. Необходима измеримость результатов для дальнейшей оценки эффективности деятельности;

- деятельность в части управления рисками имеет предупредительный характер и, прежде всего, направлена на снижение вероятности реализации рисков и/или ущерба от реализации рисков, а не на устранение последствий реализации рисков;

- управление рисками – составляющая ежедневного процесса управления, где все работники должны принимать участие в выявлении и оценке рисков в целях наиболее рационального принятия решений руководством Общества;

- придерживаться баланса расходов в части реагирования на риски, если затраты сопоставимы или выше последствий риска;

- использовать точную, полную и достоверную информацию, включая данные по прошедшим периодам (при наличии);

- Общество обеспечивает накопление знаний о рисках, включая анализ реализовавшихся рисков и распространение этих знаний среди работников Общества;

- повышение компетентности по рискам осуществляется для всех работников Общества, используя внутренние и внешние ресурсы.

3.4. Связи между деятельностью и настоящей Политикой (включая, но не ограничиваясь):

3.4.1. Целеполагание:

- цели Общества должны быть увязаны с параметрами ТЭО/ФЭО проектов и определяться до идентификации потенциальных рисков, которые могут тем или иным образом влиять на их достижение;

- процесс разработки стратегических планов должен предусматривать выявление и анализ рисков, способных оказывать влияние на достижение поставленных стратегических целей.

3.4.2. Инвестиционная деятельность:

- инициаторы инвестиционных проектов совместно с риск-менеджером в процессе рассмотрения и разработки ТЭО/ФЭО инвестиционных проектов должны предусматривать выявление и анализ рисков, способных оказывать влияние на реализацию инвестиционного проекта и достижение поставленных целей инвестиционного проекта. В последующем показатели ТЭО/ФЭО должны являться основой при разработке Стратегии развития Общества;

- инициаторы процесса получения/предоставления кредита (привлечения/предоставления заемных средств) должны включать анализ рисков для финансовой устойчивости компании.

3.4.3. Процесс бюджетирования:

- утверждение Советом директоров Общества Плана мероприятий по управлению ключевыми рисками должно происходить между этапами

целеполагания и бюджетирования. Риск менеджер ежеквартально на основании данных полученных от владельцев рисков формирует План мероприятий по управлению ключевыми рисками. Владельцы рисков несут ответственность за представленные данные;

- перед утверждением Плана мероприятий по управлению ключевыми рисками, владельцам рисков необходимо предусмотреть требуемые финансовые ресурсы для реализации предлагаемого Плана мероприятий по управлению ключевыми рисками и проработать данный вопрос со структурным подразделением, ответственным за бюджетирование.

3.4.4. Операционная деятельность:

- мероприятия по управлению ключевыми рисками должны быть отражены в соответствующих операционных мероприятиях структурных подразделений Общества;

- инициаторы вопросов, выносимых на рассмотрение коллегиальных исполнительных органов и органов управления (Правление Общества, Совет директоров Общества, Единственный акционер) в свои материалы (пояснительные записки) должны включать пункты с описанием рисков, связанных как с принятием, так и не принятием выносимых решений.

3.4.5. Процесс мотивации персонала:

- обязанности участников процесса риск-менеджмента по выполнению всех необходимых процедур, должны быть закреплены в должностных инструкциях, и может проводиться мониторинг выполнения или невыполнения соответствующих обязанностей в течение отчетного периода;

- должны быть предусмотрены механизмы поощрения, призванные мотивировать руководителей и работников Общества действовать в рамках процесса риск-менеджмента должным образом, в соответствии с установленными сроками и целевыми показателями.

4. Структура управления рисками и функции участников

4.1. Структура управления рисками в Обществе:

- Единственный акционер;
- Совет директоров Общества;
- Правление Общества;
- Структурные подразделения Общества;
- Риск-менеджер;
- Служба внутреннего аудита;
- Корпоративный секретарь.

4.2. Совет директоров Общества осуществляет следующие функции в области управления рисками:

- несет ответственность перед Единственным акционером по вопросам, связанным с управлением рисками в Обществе;
- утверждает Политику управления рисками Общества;

- осуществляет надзор за эффективностью процесса управления рисками, включая полноту интеграции процесса риск-менеджмента в бизнес-процессы Общества;
- определяет краткосрочные и долгосрочные цели Общества;
- принимает решения (в соответствии с законодательством Республики Казахстан и Уставом Общества) с учетом риска;
- предоставляет рекомендации по итогам ознакомления с отчетностью о рисках, предусмотренной пунктом 5.8 настоящей Политики;
- проводит анализ заключений внешних аудиторов по улучшению внутреннего контроля и управлению рисками и результатов проверок, проведенных Службой внутреннего аудита;
- рассматривает отчеты по эффективности управления рисками;
- утверждает карту рисков (Приложение 1) и Регистр рисков (Приложение 2) Общества;
- утверждает риск-аппетит Общества;
- утверждает ключевые рискованные показатели;
- утверждает План мероприятий по управлению ключевыми рисками;
- утверждает План мероприятий по совершенствованию процесса управления рисками;
- утверждает иные документы Общества в области управления рисками.

4.3. Правление Общества:

- отвечает за организацию эффективного процесса управления рисками, позволяющего выявлять, оценивать и управлять рисками Общества;
- отвечает за организацию работ по интеграции процесса риск-менеджмента в бизнес-процессы Общества, процесс принятия решений и управленческую отчетность Общества;
- обеспечивает разработку и внедрение внутренних документов в области управления рисками, утверждение которых отнесено к компетенции Совета директоров;
- отвечает за своевременное и полное раскрытие информации о рисках и эффективности их управления перед Советом директоров;
- использует информацию о рисках, представленную в управленческой отчетности и отчетности, предусмотренной пунктом 5.8. настоящей Политики, при принятии управленческих и инвестиционных решений;
- предоставляет Совету директоров отчеты, указанные в настоящей Политике и внутренних документах Общества;
- обеспечивает соблюдение положений настоящей Политики структурными подразделениями Общества, иными работниками Общества;
- устанавливает КРІ для руководителей структурных подразделений Общества с учетом рисков.

4.4. Председатель Правления:

- определяет Координаторов управления рисками.

4.5. Владельцы рисков/корпоративный секретарь:

- обеспечивают соблюдение положений настоящей Политики в рамках своей компетенции;
- содействуют интеграции процесса риск-менеджмента в соответствующие бизнес-процессы Общества, процесс принятия решений и управленческую отчетность;
- представляют информацию о рисках в рамках своей компетенции риск-менеджеру для актуализации Карты и Регистра рисков;
- обеспечивают своевременную разработку и реализацию мероприятий по управлению рисками и мерам их снижения;
- вносят предложения по разработке Планов мероприятий по управлению ключевыми рисками и по мерам снижения рисков;
- своевременно выявляют риски, оценивают их совместно со структурным подразделением, в ведении которого финансово-хозяйственная деятельность Общества и учитывают в процессе принятия решений;
- совершенствуют бизнес-процессы с целью уменьшения уровня рисков или последствий их реализации;
- формируют отчетность с учетом рисков;
- используют информацию о рисках при формировании целей и бюджета структурного подразделения;
- содействуют процессу развития риск-коммуникаций;
- предоставляют информацию по реализованным рискам риск-менеджеру.

4.6. Риск-менеджер:

- координирует работу структурных подразделений по интеграции процесса риск-менеджмента в соответствующие бизнес-процессы Общества, процесс принятия решений и управленческую отчетность Общества;
- участвует в разработке и актуализации внутренних документов с целью интеграции в них процесса риск-менеджмента;
- формирует информацию для Совета директоров Общества о существенных отклонениях в процессах управления рисками;
- разрабатывает методические документы в области управления рисками и оказывает методологическую поддержку владельцам бизнес-процессов и работникам в процессе идентификации, документирования рисков, внедрения, мониторинга и совершенствования контрольных процедур, формирования планов мероприятий по реагированию на риски (план мероприятий по управлению ключевыми рисками) и планов мероприятий по совершенствованию системы управления рисками, отчетов по их исполнению;
- обеспечивает актуализацию настоящей Политики;
- проводит анализ рисков;
- обеспечивает проведение качественной и/или количественной оценки рисков;

- агрегирует информацию о рисках и подготавливает отчетность о рисках Общества, предусмотренную пунктом 5.8. настоящей Политики;
- осуществляет разработку, внедрение и обновление (при необходимости) методологической базы, политик, правил в области управления рисками, процедур по мониторингу рисков;
- разрабатывает и ведет систему отчетности для процедур процесса управления рисками Общества;
- обеспечивает определение риск-аппетита, уровней толерантности по рискам;
- разрабатывает и проводит мероприятия, направленные на развитие культуры управления рисками в Обществе (в том числе, посредством внутреннего и внешнего обучения);
- оказывает методологическую помощь по выявлению и оценке рисков, а также учету рисков в рамках принимаемых решений.

4.7. Служба внутреннего аудита:

- проводит аудит эффективности и надежности управления рисками и методологии по оценке рисков, при необходимости вырабатывает предложения по повышению эффективности процедур управления рисками;
- выполняет иные функции в соответствии с компетенцией.

5. Процесс управления рисками

5.1. Расчет риск-аппетита

5.1.1. Риск-аппетит формируется после определения стратегических целей Общества, увязанных с показателями ТЭО/ФЭО проектов. Для определения приемлемого уровня риск-аппетита применяются субъективный и объективный подходы. Общество идентифицирует риски, которые могут помешать ему достичь поставленных целей. Общество определяет риск-аппетит – количество риска, которое является приемлемым для Общества в достижении поставленных целей. Риск-менеджер принимает меры по вынесению риск-аппетита на утверждение Совета директоров Общества.

5.1.2. Риск-аппетит на плановый период утверждается Советом директоров Общества и имеет следующие характеристики:

- отражает Стратегию развития Общества, включая цели, бизнес-планы,
- финансовые ограничения и ожидания заинтересованных сторон;
- охватывает все ключевые направления деятельности Общества;
- учитывает желание и возможность принимать риск;
- определяет отношение Общества к риску;
- периодически пересматривается с учетом отрасли и рыночных условий;
- требует эффективного мониторинга самого риска;
- лимиты, которые ограничивают риски в повседневной деятельности;
- включает качественные, количественные показатели.

5.1.3. При обнаружении существенных изменений во внутренней или внешней среде риск-менеджер инициирует вопрос о пересмотре Риск-аппетита.

5.1.4. Риск-аппетит интегрируется в процесс принятия решений на всех уровнях Общества.

5.2. Выявление рисков

5.2.1. Выявление рисков – процесс, в рамках которого определяются внутренние или внешние события, реализация которых может повлиять на достижение Обществом поставленных целей.

5.2.2. Общество определяет методы реагирования на риски и может разрабатывать соответствующие документы при необходимости.

5.2.3. В случае обнаружения информации о возможности существования потенциального риска, ранее не включенного в Регистр рисков, владелец риска, обнаруживший потенциальный риск, своевременно направляет служебную записку и отчет риск-менеджеру для включения в Регистр рисков.

5.2.4. Риски Общества необходимо выявлять в рамках ежегодного цикла планирования и бюджетирования и актуализовать в рамках пересмотра бюджета.

5.2.5. По итогам выявления рисков риск-менеджер агрегирует информацию о выявленных рисках для последующего анализа, оценки и управления.

5.2.6. Для выявленных рисков определяются владельцы рисков.

5.2.7. Выявленные риски, указываются риск-менеджером в соответствующих разделах Регистра рисков Общества (Приложение 2).

5.3. Анализ рисков

5.3.1. Анализ рисков проводится с целью определения причин риска, его последствий и эффективности текущих контрольных мероприятий.

5.3.2. Для анализа рисков используются методы, отражённые в международном стандарте ISO 31010:2019 «Менеджмент риска. Методы оценки риска».

5.4. Оценка рисков

5.4.1. Оценка рисков проводится с целью определения уровня рисков и выделения наиболее значимых (критических) рисков, которые могут негативно влиять на деятельность Общества и достижение его стратегических целей.

5.4.2. При оценке рисков используется качественный или количественный анализы, или их комбинация, которые создают методическую базу процесса управления рисками.

5.4.3. Качественная оценка рисков является одним из основных этапов управления рисками, которая осуществляется для всех выявленных рисков.

5.4.4. Качественная оценка обнаруженных рисков проводится владельцами рисков и объединяется риск-менеджером.

5.4.5. Оценка рисков может проводиться:

– коллективно, посредством организации совещания с целью оценить риски;

– индивидуально, посредством заполнения соответствующих разделов Регистра рисков, далее направляющийся владельцам рисков риск-менеджером с указанием перечня выявленных рисков и критериев для оценки рисков.

5.4.6. Для каждого выявленного риска необходимо оценить ущерб для Общества от реализации такого риска и вероятность его реализации.

5.4.7. Ущерб от реализации риска оценивается по пятибалльной шкале:

Балл	Последствия	Потенциальный убыток от наступления ущерба
1	Незначительные	Отсутствие каких-либо последствий в случае реализации риска
2	Низкие	Последствия от реализации риска незначительные
3	Средние	Последствия от реализации риска значительные, но могут быть полностью исправлены
4	Существенные	Последствия от реализации риска очень значительные, но могут быть исправлены до определенной степени
5	Катастрофические	В случае реализации риска компания практически не сможет восстановиться от последствий, связанных с данным риском

5.4.8. Вероятность реализации риска оценивается по пятибалльной шкале:

Балл	Вероятность	Частота
1	Очень редко	Раз в 7 и более лет (или вероятность наступления до 5%)
2	Редко	Раз в 5 лет (или вероятность наступления 6-25%)
3	Время от времени	Раз в 3 года (или вероятность наступления 26-40%)
4	Часто	Раз в год (или вероятность наступления 41-80%)
5	Очень часто	Раз в полгода и чаще (или вероятность наступления 81-100%)

5.4.9. В целях накопления внутренней информации по реализовавшимся рискам в Обществе для дальнейшего использования может формироваться база данных по реализовавшимся рискам.

5.4.10. Все выявленные риски графически отображаются риск-менеджером на Карте рисков (Приложение 1), основываясь на данных о вероятности и ущербе от реализации риска, переданных владельцами рисков.

5.4.11. По результатам оценки риски Общества можно разделить на следующие уровни:

– **Критические риски** (бордовая и красная зоны) – риски, уровень которых превышает предельно допустимый уровень риска. В течение короткого периода времени необходимо предпринять меры по предотвращению реализации/снижению влияния риска на уровне Правления и Совета директоров Общества;

– **Высокие риски** (оранжевая зона) – риски, превышают допустимый уровень, но не всегда требуют немедленного принятия решения по снижению уровня риска. Решения на уровне структурных подразделений Общества. Решения по рискам из оранжевой зоны принимаются, основываясь на графике финансирования управленческих решений, и рассчитывая оптимальный период времени необходимый для устранения/снижения риска;

– **Средние и Низкие риски** (жёлтая и зелёная зоны) – находятся в зоне, приемлемой для Общества и не требуют немедленного вмешательства. Необходимо выявить границы риска и проводить мониторинг риска в случае его перехода в оранжевую зону.

5.4.12. Материалы, полученные в рамках процедуры осуществления оценки рисков, объединяются риск-менеджером и отражаются в Регистре рисков (Приложение 2).

5.4.13. По итогам процедуры идентификации и оценки рисков, Карта и Регистр рисков направляются Совету директоров Общества на рассмотрение.

5.4.14. Утвержденные Карта и Регистр рисков Общества направляются владельцам рисков для дальнейшего использования в процессах бюджетирования, целеполагания, разработки мероприятий по управлению рисками и др.

5.5. Разработка и внедрение мероприятий по управлению рисками

5.5.1. Для рисков, определенных на карте в бордовой, красной и оранжевой зонах, владельцы рисков разрабатывают мероприятия по управлению рисками, включая сроки реализации и ответственных лиц.

5.5.2. С целью получения информации о мероприятиях по управлению рисками риск-менеджер направляет владельцам рисков согласованный ранее Регистр рисков с перечнем выявленных рисков и их оценкой. Владельцы рисков заполняют соответствующие разделы Регистра, касающиеся мероприятий и сроков их реализации, и направляют Регистр рисков обратно риск-менеджеру для агрегирования и подготовки сводного Регистра рисков.

5.5.3. Мероприятия по управлению рисками должны быть разработаны на основании одного из следующих методов:

– Уклонение от риска путем принятия решения против продолжения или принятия действия, которое является источником возникновения риска;

- Снижение (сокращение) риска – сокращение вероятности наступления рискового события и объема возможных потерь путем использования предупредительных мероприятий и планирования действий на случай реализации риска;

- Перенос (перераспределение) риска – передача или разделение риска с другой стороной потерь или выгод от риска (например, путем заключения договоров страхования, хеджирования, аутсорсинга);

- Принятие риска – уровень допустим и не планируется принятие мер по устранению/снижению.

5.5.4. Уклонение или снижение риска наиболее приемлемы для управления риском. При нецелесообразности сокращения риска, владельцам риска необходимо разработать альтернативные мероприятия по переносу либо принятию риска. При этом принятие риска – наименее целесообразный способ управления риском.

5.5.5. После получения информации о мероприятиях по управлению рисками от владельцев рисков риск-менеджер агрегирует полученную информацию и обновляет соответствующие разделы Регистра рисков Общества, после чего обновленный Регистр выносится на утверждение Советом директоров Общества.

5.6. Уменьшение и контроль рисков

5.6.1. Уменьшение и контроль рисков подразумевает мероприятия, направленные на:

- предупреждение убытков – сокращение вероятности наступления определенного риска (убытка);

- контроль убытков – сокращение размера убытка в случае наступления риска;

- диверсификация – распределение риска с целью снижения его потенциального влияния.

5.6.2. Методы уменьшения и контроля рисков предполагают внедрение процедур и процессов в Обществе, направленных на уменьшение возможности наступления убытков.

5.6.3. Методы уменьшения и контроля финансовых рисков Общества включают:

- для кредитных рисков – установление лимитов на уровень принимаемого кредитного риска корпоративных контрагентов, банков второго уровня, а также установление лимитов к размеру требований в других странах;

- для рыночных рисков – контроль и расчет уровня возможных потерь, применение инструментов хеджирования и диверсификации;

- для рисков ликвидности – установление лимитов на степень долговой нагрузки Общества;

– риск возникновения убытков в результате недостатков или ошибок в ходе осуществления внутренних процессов, допущенных со стороны работников (включая риски персонала), функционирования информационных систем и технологий (технологические риски), а также вследствие внешних событий.

5.6.4. Уменьшение и контроль стратегического риска Общества осуществляется путем мониторинга исполнения утвержденных краткосрочных и долгосрочных планов и стратегий, увязанных с показателями ТЭО/ФЭО проектов по результатам которого принимаются корректирующие меры, в том числе для отражения изменений во внутренней и внешней среде.

5.6.5. Уменьшение и контроль операционных рисков в Обществе осуществляется путем проведения анализа установленных бизнес-процессов и разработки соответствующих Планов мероприятий по их усовершенствованию, внедрение системы внутренних контролей. Для операционных рисков на производстве уменьшение и контроль рисков осуществляется путем соблюдения правил охраны и безопасности труда, правил по соблюдению экологической безопасности, правил работы на производстве.

5.6.6. Методом уменьшения и контроля правовых рисков Общества является проведение мониторинга изменений законодательства. Каждое структурное подразделение самостоятельно оценивает влияние изменений на деятельность Общества и разрабатывает (актуализирует) внутренние документы Общества в рамках компетенции. Любой документ, который регулирует внутренние процедуры Общества или в соответствии с которым у Общества возникают обязательства, должен пройти обязательную правовую экспертизу в структурном подразделении, ответственном за правовое сопровождение Общества.

5.6.7. В случае, если применяемые методы по уменьшению и контролю рисков связаны с затратами и эти затраты являются существенными, проводится следующий анализ:

- насколько эти мероприятия являются необходимыми, и могут ли они быть снижены за счет удержания и/или финансирования (переноса) рисков;
- какова альтернативная стоимость затрат на мероприятия по сравнению со стоимостью удержания/переноса рисков.

5.6.8. Удержание рисков: в ходе выявления и оценки рисков рассчитывается риск-аппетит Общества.

5.6.9. Риск-аппетит Общества финансируется за счет текущих доходов Общества и/или нераспределенного дохода прошлых лет и не имеет непосредственной аллокации на незапланированные убытки (т.е. убытки вследствие наступления рисков непосредственно уменьшают прибыль Общества).

5.6.10. Распределение риск-аппетита Общества по рискам основывается на анализе влияния каждого из рисков и стоимости переноса рисков, т.е. чем дороже стоимость переноса рисков, тем более высокая вероятность удержания риска за счет собственных средств Общества.

5.6.11. Финансирование (перенос) рисков включает следующие инструменты:

- страхование (для «чистых» рисков – риски, наступление которых влечет за собой только убытки и не может приводить к получению дохода);
- хеджирование (для «спекулятивных» рисков – риски, реализация которых может привести как к убыткам, так и к доходам);
- перенос риска по контракту (перенос ответственности за риск на контрагента за дополнительное вознаграждение или соответствующее увеличение стоимости контракта);
- условная кредитная линия – доступ к банковскому финансированию на согласованных условиях при наступлении определенных событий;
- другие альтернативные методы финансирования рисков.

5.6.12. Основным отличительным признаком этих инструментов является наличие «платы» за риск, что, соответственно, требует оптимального применения этого инструмента с целью снижения расходов Общества.

5.6.13. Уход от риска/избежание риска включает в себя действия, направленные на прекращение или отказ от осуществления операций, которые потенциально приведут к негативным последствиям.

5.6.14. Выбор наиболее подходящей опции производится с учетом балансирования затрат, связанных с определенным методом, с преимуществами, которые влекут за собой его использование, и других прямых и косвенных затрат.

5.6.15. Применение соответствующих мер и методов реагирования на риски должно описываться в Плане мероприятий по управлению ключевыми рисками. Данный План должен включать в себя перечень необходимых действий и ответственных исполнителей.

5.7. Мониторинг рисков

5.7.1. В рамках мониторинга Карта и Регистр Общества (включая мероприятия по управлению рисками) актуализируются 1 раз в полгода. При этом риск-менеджер, владельцы рисков вправе внепланово инициировать процесс пересмотра рисков при наличии обоснований.

5.7.2. В рамках мониторинга рисков:

- выявляются новые риски, отсутствующие в Карте и Регистре рисков Общества;
- производится пересмотр по оценке уровня риска;
- рассматриваются вопросы в части мероприятий по управлению рисками Общества (статус, эффективность).

5.8. Отчетность о рисках

5.8.1. Риск-менеджер формирует для утверждения Советом директоров Общества отчет по рискам, состоящий из:

- Карты рисков Общества (ежегодно);
- Регистра рисков Общества (ежегодно);
- Риск-аппетита (ежегодно).
- Плана мероприятий по совершенствованию процесса управления рисками (ежегодно);
- Плана мероприятий по управлению ключевыми рисками (ежегодно);
- Базы данных реализовавшихся рисков (ежегодно).

5.8.2. При условии существенных изменений в любом из вышеуказанных документов Риск-менеджер подготавливает внеплановые отчеты о рисках для Совета директоров Общества.

6. Развитие культуры управления рисками

6.1. Для развития культуры управления рисками в Обществе риск-менеджером проводятся мероприятия по укреплению компетенций работников в области управления рисками, в том числе:

- ежегодные семинары и информационные сессии для работников, которые могут включать информацию о статусе и результатах внедрения управления рисками в Обществе, основных элементах и инструментах управления рисками, обязанностях работников;

- вновь принятым работникам Общества предоставляются информационные материалы (памятка) об управлении рисками.

Работники Общества ежегодно, а также при приеме на работу проходят обучение/вводный инструктаж для ознакомления с принятой системой управления рисками.

По результатам такого обучения проводится тестирование знаний.

7. Устойчивое развитие

7.1. Общество поддерживает применение принципов устойчивого развития в своей деятельности, что включает в себя управление взаимоотношениями с заинтересованными сторонами, оценку и управление воздействием на три основные сферы – экономическую, социальную и экологическую.

7.2. Общество проводит анализ своей деятельности и контроль рисков в разрезе трех составляющих устойчивого развития.

8. Совершенствование

8.1. Для целей совершенствования управления рисками в Обществе может разрабатываться План мероприятий по совершенствованию процесса управления рисками. Мероприятия по дальнейшему совершенствованию процесса управления рисками могут включать следующие направления:

- распределение обязанностей работников в рамках управления рисками;
- внедрение (интеграция) управления рисками в существующие бизнес-процессы;
- отражение информации о рисках в текущей управленческой отчетности;
- развитие культуры управления рисками в Обществе.

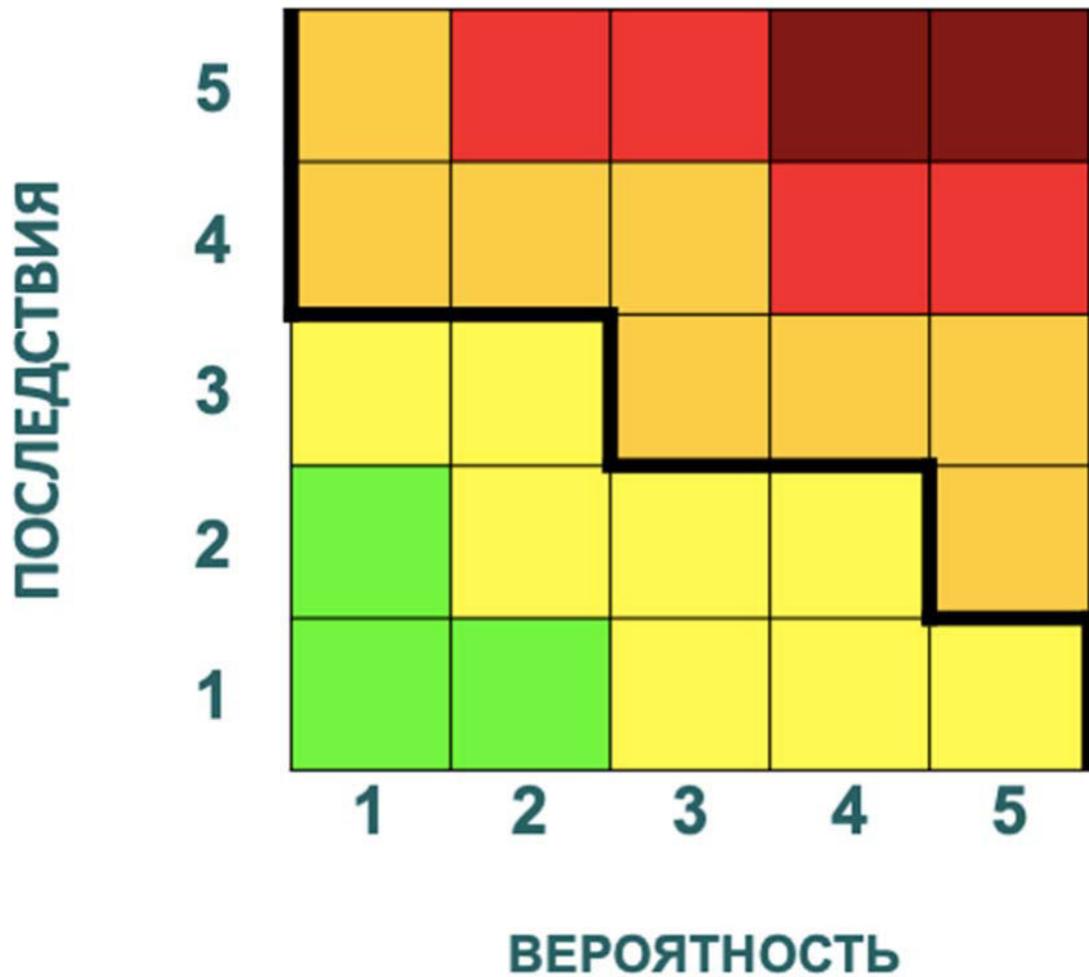
9. Заключительные положения

9.1. Правление Общества берёт на себя обязательства по обеспечению всеми необходимыми ресурсами процесса риск-менеджмента, риск-менеджер Общества несет ответственность за реализацию настоящей Политики в пределах своей компетенции, координаторы управления рисками несут ответственность за своевременное и качественное предоставление информации риск-менеджеру.

9.2. Ознакомление с настоящей Политикой обязательно для всех работников Общества.

Приложение 1
к Политике по управлению рисками
акционерного общества
«Республиканский центр
космической связи»

Карта рисков



Приложение 2
к Политике по управлению рисками
акционерного общества
«Республиканский центр
космической связи»

ФОРМА

Регистра рисков акционерного общества «Республиканский центр космической связи»

Дата подготовки: _____

Описание риска	Возможные последствия	Возможный ущерб	Вероятность наступления	Уровень риска	Владелец риска	Мероприятия	Сроки	Статус мероприятий

Таблица, содержащая структурированную информацию о рисках: наименование рисков, описание рисков и возможных последствий от реализации рисков, оценку рисков, владельцев рисков, мероприятия по управлению рисками, сроки и статус их реализации.