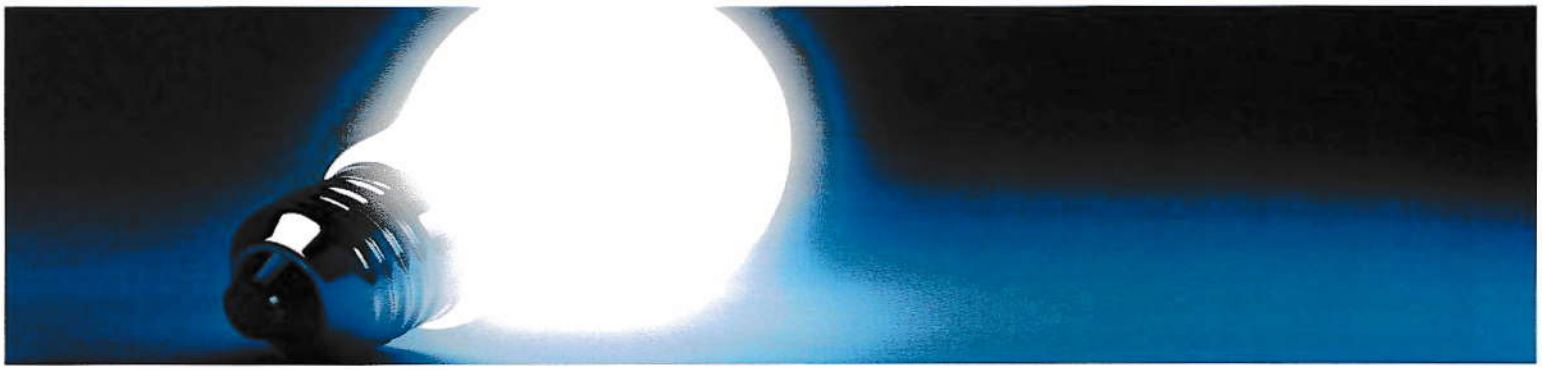

УТВЕРЖДЕН

Решением общего собрания участников
ООО «ЭНЕРГОНИКА»
от «02» марта 2023 года
(Протокол № 2 от «02» марта 2023 года)

РЕГЛАМЕНТ ПО УПРАВЛЕНИЮ ОПЕРАЦИОННЫМИ РИСКАМИ

ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ЭНЕРГОНИКА»

г. Москва
2023 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент устанавливает правила и порядок действий при управлении операционными рисками Общества с ограниченной ответственностью «ЭНЕРГОНИКА» (далее – «Общество»). Регламент разработан на основе законодательных актов Российской Федерации, а также с учетом внутренних документов Общества и сложившейся отечественной и международной практики по управлению рисками.

1.2. Действие настоящего Регламента распространяется на всех участников Общества, всех сотрудников и все структурные подразделения Общества.

1.3. Настоящий Регламент определяет следующие направления деятельности по управлению операционными рисками:

- ✓ цель, задачи и принципы управления рисками;
- ✓ основные направления и подходы к управлению рисками;
- ✓ выявление и фиксация рисков;
- ✓ методы оценки рисков;
- ✓ процесс управления и контроля рисков;
- ✓ распределение обязанностей, полномочий и ответственности между органами управления, должностными лицами, сотрудниками и структурными подразделениями.

1.4. Настоящий регламент разработан с целью достижения оптимального баланса между рисками и доходностью для Общества в целом и его клиентов, при соблюдении норм законодательства и положений Устава Общества, а также с целью выработки стимулов, адекватных уставной деятельности органов управления Общества, его структурных подразделений и отдельных сотрудников.

1.5. Под операционным риском понимается риск прямых или косвенных потерь (убытков) от неверной организации внутренних процессов Общества, действий сотрудников, сбоя операционных систем, внешних событий. Операционные убытки могут быть в виде:

- ✓ снижения стоимости активов;
- ✓ досрочного списания (выбытия) материальных активов;
- ✓ денежных выплат на основании постановлений (решений) судов, решений органов, уполномоченных в соответствии с законодательством Российской Федерации;
- ✓ денежных выплат клиентам и контрагентам, а также сотрудниками Общества в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине Общества;
- ✓ затрат на восстановление хозяйственной деятельности и устранение последствий ошибок, аварий, стихийных бедствий и других аналогичных обстоятельств;
- ✓ прочих убытков.

1.6. Основными факторами или событиями, способными усилить влияние и масштабы проявления операционного риска являются:

- ✓ изменение законодательства, требований регулирующих органов;
- ✓ расширение масштабов деятельности, увеличение объемов операций;
- ✓ усложнение финансовых инструментов и стратегий;
- ✓ освоение новых продуктов и технологий;
- ✓ усложнение систем технологической поддержки операций, внедрение новой техники.

1.7. Управление операционным риском нацелено на максимально возможное его предотвращение и основано как на применении качественных и количественных методов анализа, так и на создании адекватной системы внутреннего контроля.

1.8. Для управления операционными рисками необходимо решить следующие задачи:

- ✓ Обеспечить получение оперативных и объективных данных об объекте операционного риска;
- ✓ Произвести комплексную оценку операционного риска;
- ✓ Произвести оценку влияния операционного риска на другие типы рисков;
- ✓ Обеспечить мониторинг объектов операционного риска;
- ✓ Создать систему быстрого реагирования для принятия решения на начальной стадии реализации операционного риска.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Операционный риск – риск прямых или косвенных потерь (убытков) от неадекватных или ошибочных внутренних процессов Общества, действий сотрудников, операционных систем, внешних событий.

2.2. В зависимости от причин возникновения выделяются следующие подриски:

- ✓ **Риски бизнес-процессов** — риски потерь, связанных с несовершенством применяемых бизнес-процессов (наличием в них дефектов, которые могут привести к ресурсным потерям – средств, времени), ошибками в процессах проведения сделок расчетов по ним и их учета, отсутствием или несовершенством внутренних процедур, слабой организацией и эффективностью процессных потоков и регламентов

проведения операций и систем контроля, неадекватной реакцией на жалобы, а также потерь из-за прерывания критических бизнес-процессов;

✓ **Риски действий персонала** — риски потерь, связанных с недостаточной компетенцией (квалификацией) сотрудников при выполнении бизнес-процессов или недостатком квалифицированных сотрудников; низким уровнем исполнительской дисциплины (нарушение установленных процедур и регламентов); возможными ошибками сотрудников при выполнении производственных операций; действиями сверх предоставленных полномочий; мошенничеством, при котором информация намеренно сфальсифицирована, одним или несколькими сотрудниками с целью вывести активы компании незаконным путем и другими противоправными действиями.

✓ **Риски информационных технологий, технологические риски** — риски потерь, обусловленных несовершенством используемых технологий, т.е. соотношение цена/качество не соответствует рыночным стандартам; недостаточной емкостью систем, каналов связи, при которых пользователи могут не получить доступ к информации, либо получить его не вовремя; несоответствием возможностей систем проводимым операциям; грубостью методов обработки данных; неадекватностью используемой информации или ее потерей; недостаточной гибкостью, надежностью или устойчивостью к чрезвычайным ситуациям; возможностями персонала, не имеющего прав доступа, получить доступ к конфиденциальной информации.

✓ **Риски чрезвычайных ситуаций** – риски потерь по причинам природного и техногенного характера, а также связанные с непосредственным физическим вмешательством в деятельность Общества и его контрагентов (стихийные бедствия, пожары, ограбления, терроризм, влияние криминальной среды).

✓ **Регулятивные риски** – риски применения финансовых, административных санкций со стороны государственных и квазигосударственных органов (ФНС, Росфинмониторинг, Гострудинспекция, ФАС, Центральный Банк и других) в связи с несоответствием деятельности Общества требованиям регуляторов (часть юридических рисков).

✓ **Юридические риски** – риски возникновения убытков вследствие допускаемых правовых ошибок при осуществлении деятельности, в том числе при неадекватном мониторинге изменений действующего законодательства, отсутствия осведомленности, например, отсутствии или некорректной экспертизе полномочий контрагента при совершении сделки, несоблюдения требований нормативных правовых актов и заключенных договоров, несовершенства правовой системы (противоречивость законодательства, а также отсутствие правовых норм по регулированию отдельных вопросов).

✓ **Риски, связанные с внутренней обеспеченностью информацией** – риски потерь в связи с тем, что были приняты неверные решения или не были приняты необходимые решения из-за того, что внутренняя информация представлена некорректно, поздно или рано, или вообще не отражает суть произошедших процессов.

✓ **Риски, связанные с недостатками инфраструктуры** – риски потерь, связанных с неадекватным обеспечением производственной деятельности всеми инфраструктурными ресурсами – производственными площадями, транспортом, бесперебойным обеспечением энергопитанием, теплом, водоснабжением, и т.п., а также со сбоями в производственной деятельности вследствие нарушения поставщиком обязательств по срокам /качеству предоставляемых услуг.

Контроль операционного риска – процесс оценки результатов управления операционным риском.

Мониторинг операционного риска – процесс систематического и непрерывного сбора и анализа информации об уровне операционного риска.

Минимизация операционного риска – комплекс мероприятий по поддержанию операционного риска на уровне, не угрожающем интересам кредиторов и участников, устойчивости Общества.

Объекты риска – процессы, системы, ресурсы, активы Общества, утрата, повреждение или нарушение работы которых под действием факторов риска могут привести к финансовым убыткам, упущенной финансовой выгоде или прекращению деятельности Общества.

Операционное событие – любое неблагоприятное событие, воздействующее на объекты риска под влиянием факторов риска, следствием которого являются финансовые убытки, упущенная финансовая выгода или прекращение деятельности Общества.

Оценка операционного риска – комплекс мероприятий, направленных на выявление и анализ внутренних и внешних факторов, оказывающих воздействие на деятельность Общества и способствующих возникновению операционного риска.

Управление операционным риском – комплекс мероприятий и процедур по выявлению (идентификации), оценке (измерению), мониторингу, контролю и (или) минимизации операционного риска.

Факторы (источники) риска – это причины возникновения случайных неблагоприятных событий, приводящих к финансовым убыткам, упущенной финансовой выгоде или прекращению деятельности Общества.

2.3. Источники операционных рисков:

а) Риски мошеннических действий сотрудников внутри Общества возникают:

✓ При возможности осуществить кражу и передачу информации, представляющую коммерческую тайну;

✓ При возможности использования служебного положения при осуществлении операций в личных корыстных целях и наносящих экономический, правовой или ущерб репутации Общества.

б) Риски в сфере кадровой политики и охраны труда возникают:

✓ В результате изменения кадрового состава, что приводит к возможным ошибкам при осуществлении операции ввиду недостаточной информированности касательно осуществления бизнес-процессов;

✓ В результате повышенного уровня стресса у сотрудников, который приводит к ошибкам при выполнении операций;

✓ Недостатки корпоративной культуры, приводящие к ухудшению общей корпоративной среды и снижению эффективности труда;

✓ Другие риски, связанные с кадровым составом Общества, например, увольнение сотрудников, имеющих свои клиентские портфели.

в) Риски при взаимодействии с клиентами и контрагентами возникают:

✓ При хранении персональных данных, конфиденциальной информации о клиенте и возможности их потери;

✓ При условии недобросовестности клиентов или контрагентов, которая выражается в мошеннических действиях отказе выполнения обязательств и других действий;

✓ При ограничении возможности взаимодействия с клиентами и другими контрагентами в результате отказа их от сотрудничества с Обществом.

г) Риски информационных технологий, технологические риски возникают:

✓ В результате нарушения работы устройств, осуществляющих обработку информации, которые могут возникать как от прямого физического воздействия (бой, термическое воздействие, воздействие влагой, ущерб от наводнений, землетрясений, военных действий, терроризма, вандализма), так и от перебоя работы устройства ввиду внутренней поломки (обрыв контактов, сгорание плат);

✓ В результате сбоя работы программного обеспечения, который был вызван перебоем во внутренней архитектуре программного обеспечения, моральным истощением программного обеспечения или вредоносными программами;

✓ В результате взлома информационных систем и баз данных, которые могут привести к утечке информации, представляющей коммерческую тайну.

2.4. Убытки в результате реализации операционных рисков могут быть следующими:

✓ Снижение стоимости активов – прямое уменьшение стоимости активов Общества вследствие кражи, мошенничества, противоправной деятельности работников Общества или третьих лиц, а также рыночные и кредитные потери Общества, произошедшие в результате таких рисковых событий.

✓ Досрочное списание (выбытие) материальных активов – уничтожение или прямое уменьшение стоимости материальных ценностей и активов Общества вследствие событий случайного характера (в т.ч. халатности, неосторожности, стихийных бедствий).

✓ Денежные выплаты в судебном порядке – штрафы, неустойки и издержки Общества в результате проведения судебного урегулирования разногласий с должником / контрагентом или работником Общества.

✓ Денежные выплаты на основании решений органов, уполномоченных в соответствии с законодательством РФ – штрафы, пени или любые другие санкции в денежном выражении, наложенные на Общество органами надзора вследствие нарушения Обществом действующего законодательства.

✓ Денежные выплаты во внесудебном порядке – денежные выплаты и компенсации, осуществленные Обществом своим контрагентам, а также работникам Общества в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине Общества.

✓ Повторные затраты – затраты на восстановление хозяйственной деятельности Общества и устранение последствий ошибок, аварий, стихийных бедствий и других аналогичных обстоятельств.

3. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ

3.1. Целью управления операционными рисками как составной частью общего процесса управления рисками выступает предотвращение данного риска или максимально возможное снижение угрозы потенциальных убытков для обеспечения устойчивой и эффективной деятельности Общества, а также для соблюдения интересов его клиентов при максимальной сохранности капитала и активов.

3.2. Задачами Общества в области управления операционными рисками являются:

✓ создание, поддержание и совершенствование эффективного механизма своевременной идентификации и предотвращения возможных негативных событий, принятие адекватных мер для снижения/избежания потерь;

✓ определение приемлемого уровня конкретных видов операционных рисков с точки зрения экономической целесообразности затрат на их оценку, анализ и мониторинг;

✓ создание, поддержание и совершенствование системы внутреннего контроля над операционными рисками;

✓ принятие адекватных мер для снижения/избежания потерь.

3.3. Принципы управления операционными рисками:

✓ соответствие требованиям законодательства и стратегии Общества;

✓ соответствие виду деятельности Общества, характеру и объемам совершаемых операций (принцип пропорциональности). Работники Общества, совершающие операции, подверженные рискам, должны быть осведомлены о риске операций и должны осуществлять идентификацию, анализ и оценку рисков перед совершением операций в соответствии с Политикой об управлении рисками;

✓ принцип непрерывности и комплексности управления рисками;

✓ принцип информационной обеспеченности управления (надлежащее раскрытие информации о рисках, ее сбор, обработка, анализ и доступность информации для заинтересованных лиц). Работники Общества в соответствии с их должностными обязанностями обязаны информировать лиц, входящих в систему риск-менеджмента о рисках, возникающих в процессе выполнения их должностных обязанностей. Риск-менеджмент обязан с периодичностью не реже одного раза в год, предоставлять органам управления Общества, информацию об уровне принятых Обществом рисков и фактах нарушений, выявленных в ходе выполнения установленных процедур управления рисками.

✓ принцип предотвращения конфликтов интересов и закрепления ответственности работников Общества относительно целей и задач управления операционными рисками, а также обязанностей, возникающих в ходе реализации мероприятий по управлению ими;

✓ контроль и оценку эффективности управления;

✓ принцип документирования процедур в рамках системы управления рисками. Общество обеспечивает документальную фиксацию необходимой информации, связанной с организацией системы управления рисками также утверждение органами управления Общества регламентных документов по управлению рисками.

✓ принцип эффективности (достижения заданных результатов с использованием наименьшего объема средств) и оптимальности процессов управления рисками. Объем и сложность процедур и мер по управлению рисками должны соответствовать целям организации системы управления рисками.

✓ принцип разделения полномочий. Решения о минимизации рисков могут приниматься на различных уровнях управления Общества в зависимости от значимости рисков (размера вероятных потерь при наступлении рискового события) и вероятности их реализации. Решения о проведении операций, влекущих возникновение рисков, принимаются коллегиально группой должностных лиц, к полномочиям которых отнесено решение подобных вопросов, за исключением случаев, когда такое право предоставлено органам управления или отдельным должностным лицам.

✓ использование новейших информационных технологий;

✓ постоянное совершенствование системы управления операционными рисками.

3.4. Основные подходы к оценке и управлению операционными рисками:

✓ восходящий подход – выявляются и оцениваются источники, причины и последствия возникновения риска. Осуществляется на постоянной основе сотрудниками и руководителями подразделений Общества в соответствии с функциональными обязанностями, положениями и регламентами, другими внутренними нормативными документами;

✓ нисходящий подход – оцениваются последствия реализации риска. В целях принятия адекватных мер, направленных на совершенствование системы управления операционными рисками, руководство Общества рассматривает подготовленные отчеты о реализованных операционных рисках, фактах нарушений операционных регламентов и процедур, установленных полномочий и ограничений.

3.5. Система оценок операционного риска строится с учетом следующих характеристик:

✓ применение внутренних статистических данных по случаям убытков и величинам потерь;

✓ использование субъективных суждений экспертов о вероятности и масштабах убытков;

✓ система измерения операционного риска должна использовать соответствующие внешние данные (государственные данные или сводные данные по отраслям экономики), особенно когда есть основания считать, что Общество несет хотя и редкие, но потенциально ощутимые потери.

3. ВЫЯВЛЕНИЕ ОПЕРАЦИОННОГО РИСКА

4.1. В целях выявления операционного риска используются следующие методы:

а) Анализ внутренних условий, в которых функционирует Общество, на предмет наличия операционного риска:

✓ анализ подверженности операционному риску направлений деятельности;

- ✓ анализ отдельных операций и сделок;
- ✓ анализ внутренних нормативных документов;
- ✓ анализ внутренних процедур, включая систему отчетности и обмена информацией;
- ✓ анализ операционного риска, возникающего в сфере управления персоналом;
- ✓ другие внутренние условия.

б) Анализ внешних условий, в которых функционирует Общество, на предмет наличия операционного риска:

- ✓ анализ изменений в сфере Общества в целом (например, внедрение новых технологий или инноваций), которые могут оказать влияние на эффективность деятельности;
- ✓ анализ изменения законодательства, требований внешних надзорных органов;
- ✓ анализ внешних случаев реализации операционного риска;
- ✓ другие изменения внешних условий.

в) Анализ нововведений, производимых Обществом, на предмет наличия операционного риска:

- ✓ анализ операционного риска, связанного с внедрением новых продуктов, услуг, процедур, систем, технологий или вносимых в них изменений;
- ✓ анализ операционного риска при выходе Общества на новые рынки;
- ✓ анализ операционного риска, возникающего при использовании новых поставщиков услуг;
- ✓ анализ операционного риска, возникающего вследствие изменения структуры Общества;
- ✓ анализ операционного риска, возникающего при иных нововведениях.

г) Сбор данных о внутренних случаях реализации операционного риска:

- ✓ сбор данных о внутренних случаях реализации операционного риска лежит в основе процесса управления операционным риском, поскольку позволяет сформировать представление о видах и уровне операционного риска, которому подвержено Общество, усилить внутреннюю контрольную среду в целях снижения вероятности реализации новых случаев операционного риска, а также сформировать массив статистических данных о случаях реализации операционного риска.

4.2. Основные виды событий, которые приводят к реализации операционных рисков и требующие контроля:

- ✓ неверные (ошибочные) или умышленные негативные действия при проведении операций в специализированной программе в случаях заведения поставок (возвратов), проведения финансирования и платежей;
- ✓ несанкционированные действия по удалению какой-либо информации из специализированной программы;
- ✓ проведение операций с нарушением условий и ограничений, установленных внутренними Положениями, Регламентами и Инструкциями;
- ✓ недостаточная компетентность сотрудников клиентского обслуживания в случаях оценки юридической состоятельности документов по поставкам, передаваемым клиентами в счет уступленных денежных требований;
- ✓ недостаточная компетентность сотрудников других структурных подразделений;
- ✓ несоблюдение законодательства по ПОД/ФТ;
- ✓ внутреннее мошенничество и злоупотребление служебным положением;
- ✓ внешнее мошенничество;
- ✓ трудовые отношения и безопасность рабочих мест;
- ✓ ошибки профессиональной деятельности;
- ✓ физическое уничтожение имущества;
- ✓ приостановление процессов и ошибки систем;
- ✓ эндогенные и экзогенные нарушения в бизнес-процессах.

4.3. Перечень обстоятельств, наступление которых необходимо учитывать риск-менеджерам при управлении операционным риском:

- ✓ локальные и муниципальные чрезвычайные ситуации техногенного или природного характера (в том числе аварии, аварийные выбросы, пожары, взрывы, разрушения, затопления зданий, землетрясения, ураганы, наводнения);
- ✓ отключение электро-, водо-, теплоснабжения, систем вентиляции и кондиционирования, иных видов обеспечения повседневной деятельности;
- ✓ перебои в предоставлении услуг телефонной связи, телематических услуг связи, услуг передачи данных, услуг электронной почты, услуг доступа к информационным ресурсам в сети Интернет, других видов информационных услуг;
- ✓ акты иностранных государств, содержащие запрет или ограничивающие осуществление деятельности российских компаний;
- ✓ законы и иные нормативные акты РФ, устанавливающие запреты и ограничения;

✓ действия органов государственной власти РФ в отношении Общества, в том числе наложение ареста на счета, запрет на проведение отдельных операций, приостановление действия лицензий, проведение следственных действий и другие действия, приводящие к приостановлению нормального режима деятельности;

✓ противоправные действия в отношении Общества и его исполнительных органов, приводящие к приостановлению нормального режима его деятельности.

4.4. По каждому выявленному операционному риску риск-менеджеры в целях описания и документирования рисков составляют формализованные описания операционных рисков, которые в совокупности формируют и пополняют карту операционных рисков Общества.

5. МЕТОДЫ ОЦЕНКИ ОПЕРАЦИОННОГО РИСКА

5.1. Общество проводит оценку операционного риска в отношении отдельных бизнес-процессов и в отношении деятельности в целом. Сотрудники Комитета по управлению рисками Общества проводят оценку рисков не реже одного раза в полугодие. Помимо планового проведения оценки рисков, оценка также производится в случаях внедрения новых бизнес-процессов, технологий, продуктов и услуг.

5.2. Для оценки операционного риска могут применяться следующие методы оценки:

✓ метод, основанный на статистическом анализе распределения убытков;

✓ балльно-весовой метод (метод экспертной оценки);

✓ математические методы и модели оценки;

✓ методы теории вероятностей;

✓ методы математической статистики.

5.3. Общество осуществляет последовательный поэтапный переход от применения простых методов и подходов к оценке операционного риска к более сложным, по мере разработки более продвинутых систем и практик измерения операционного риска.

5.4. Одновременно с процессом накопления и систематизации внутренних данных о реализованных рисках, в целях развития и совершенствования процедур мониторинга уровня операционного риска Общество осуществляет последовательное формирование системы индикаторов операционных рисков с определением пороговых значений и проведением тестирования индикаторов. Применяемые индикаторы и их пороговые значения подлежат уточнению и корректировке в процессе моделирования и обратного тестирования, с учетом оценки чувствительности конкретного индикатора и анализа его эффективности.

5.5. Для целей оценки операционного риска Общество использует метод, сопоставимый с методами, рекомендованными Базельским комитетом по банковскому надзору. В соответствии с данным методом оценка операционного риска предполагает расчет величины убытков (ожидаемых и непредвиденных потерь), которые должны быть «покрыты» соответствующим размером отчисляемого на операционный риск капитала.

✓ Сумма капитала, необходимая для покрытия операционного риска (ОРК), рассчитывается по следующей формуле:

$$ОРК = (ЧД/n) * К, \text{ где}$$

- ЧД – чистые доходы (только положительные) по видам деятельности, которым присущ операционный риск, за каждый из предыдущих n лет;
- n – количество лет, в которых ЧД был положительным (берется равным 3 годам, однако может корректироваться риск-менеджерами по согласованию с руководством);
- К – бета-коэффициент (согласно современной практике, берется равным за 15%, однако может корректироваться риск-менеджерами по согласованию с руководством);

✓ Расчет риска указанным методом применяется по итогам работы Общества за год или полугодие;

✓ Расчет риска может применяться также в целях бизнес-планирования и в рамках процедур стресс-тестирования.

5.6. Оценка текущего уровня операционного риска:

✓ В целях мониторинга текущего уровня операционного риска проводится индикативная оценка на основании данных о расходах общества, связанных с реализацией операционного риска, и прибыли Общества;

✓ Текущий уровень операционного риска (ТОР) определяется по формуле:

$$ТОР = Р/П * 100\%, \text{ где:}$$

- Р – расходы, связанные с реализацией операционного риска, произведенные (понесенные) в отчетном периоде;
- П – чистая прибыль, полученная в отчетном периоде.

✓ После определения значения показателя текущего уровня операционного риска, анализируется его динамика в сравнении с предшествующим (сопоставимым) периодом, соответствующим периодом

прошлого года, а также со средним значением данного показателя за последние три года (включая текущий);

✓ Оценка текущего уровня операционного риска осуществляется на регулярной основе, по итогам работы за год, полугодие;

✓ Показатель текущего уровня операционного риска может применяться в целях прогнозирования величины потенциальных операционных убытков. При его определении применяются трендовые методы и экспертные оценки.

5.7. Экспертная оценка операционного риска:

✓ Метод экспертных оценок применяется в отношении операционных рисков, не имеющих явного стоимостного выражения, а также при отсутствии полноценных исторических или статистических данных о реализованных рисках;

✓ Экспертная оценка проводится в целях выявления подверженности процессов и операций подразделения или Общества в целом отдельным источникам и факторам операционного риска, в том числе влиянию внешней среды, а также выявления слабых мест и зон концентрации риска на отдельных направлениях бизнеса, операциях и процедурах;

✓ Процедура экспертной оценки проводится на основе комплексного анализа принимаемых операционных рисков (отдельных видов операционного риска) и оценки адекватности деятельности требованиям нормативных документов;

✓ Экспертная оценка операционных рисков (в том числе в целях стресс-тестирования отдельных направлений деятельности) осуществляется не реже одного раза в год.

5.8. В целях обеспечения учета, хранения и анализа данных о случаях реализации операционного риска Обществом ведется внутренняя база данных о случаях реализации операционного риска.

6. ПРОЦЕСС УПРАВЛЕНИЯ И КОНТРОЛЯ РИСКОВ

6.1. Основные этапы процесса управления операционными рисками:

✓ идентификация (определение причин и предпосылок, вследствие которых Обществу причинен или может быть причинен ущерб);

✓ оценка операционного риска;

✓ анализ проблемных зон процессов, выработка и принятие решения по оптимизации или изменению процессов в целях снижения уровня операционного риска;

✓ мониторинг операционного риска (выявление событий, способствующих изменению степени подверженности деятельности Общества операционному риску, а также изменению уровня операционного риска; отслеживание динамики показателей, характеризующих уровень операционного риска, с целью выявления отклонений и определения тенденций в изменении уровня операционного риска);

✓ контроль и снижение операционного риска (принятие управленческого решения в отношении выявленного операционного риска, контроль выполнения заявленных мероприятий по снижению уровня операционного риска и устранению проблемных зон в процессах).

6.2. В процессе управления операционными рисками Общество использует следующие методы:

✓ наличие постоянного контроля над корректностью выполнения операций в специализированной программе со стороны руководства подразделений клиентского обслуживания;

✓ постоянное проведение (дважды в год) аттестаций сотрудников по знанию технологического процесса и нормативных документов;

✓ максимально качественная подготовка новых сотрудников в период испытательного срока;

✓ максимально защищенная схема от несанкционированных действий в специализированной программе, позволяющая только ограниченному кругу должностных лиц проводить операции связанные с разрешением проведения финансирования, удалением зарегистрированной информации, установлением тарифов и др.;

✓ постоянное обучение и повышение квалификации сотрудников Общества в рамках знания финансово-хозяйственной деятельности предприятий, законодательства, договорных отношений и др.

✓ разработка, согласование и утверждение стратегических планов развития и отдельных направлений деятельности Общества;

✓ система разделения полномочий и иерархии подчиненности;

✓ коллегиальность принятия решений по проведению операций, подверженных риску;

✓ процедура разработки, согласования, юридической экспертизы и утверждения внутренних нормативных документов;

✓ система лимитов и ограничений;

✓ система методик и процедур проведения операций;

✓ контроль состояния технических систем;

✓ обеспечение безопасности серверов;

- ✓ реализация принципа двойного контроля при совершении операций, их отражении в бухгалтерском учете, вводе данных в учетные и операционные системы;
- ✓ система санкционирования операций, предварительного, текущего и последующего контроля;
- ✓ наличие эффективной системы внутреннего контроля;
- ✓ проведение до начала договорных отношений с клиентом его идентификации в целях ПОД/ФТ;
- ✓ регулярная ревизия адекватности действующих внутренних нормативных документов;
- ✓ обеспечение сокращения числа нештатных ситуаций и минимизация влияния сбоев в ИТ-инфраструктуре;
- ✓ обеспечение оптимальных характеристик автоматизированных систем в соответствии с требованиями бизнеса, исключение ситуаций недостатка ресурсов для решения операционных задач;
- ✓ наличие плана действий в случае возникновения аварийных и нештатных ситуаций;
- ✓ адекватная кадровая политика, определяющая систему подбора, расстановки, аттестации, повышения квалификации и мотивации персонала;
- ✓ наличие внутренних документов, определяющих функции и полномочия структурных подразделений;
- ✓ наличие должностных инструкций, определяющих полномочия, функциональные обязанности и заменяемость сотрудников;
- ✓ система администрирования (разграничения прав доступа) и контроля предоставленных прав доступа;
- ✓ система аудита действий пользователей информационных сетей;
- ✓ защита помещений, оборудования и электронных систем от взлома, несанкционированного проникновения, несанкционированных операций, хищения активов и перехвата информации;
- ✓ система мониторинга и противодействия попыткам взлома и несанкционированного проникновения в информационные сети;
- ✓ разработка типовых форм договорной документации и внутренней документации;
- ✓ разработка порядка рассмотрения, экспертизы и заключения нестандартных договоров и соглашений;
- ✓ поддержание в актуальном состоянии справочных правовых систем.

6.3. Контроль и/или минимизация операционного риска. В своей деятельности Общество использует следующие методы контроля и/или минимизации операционного риска:

- ✓ избегание (отказ от принятия) операционного риска. Избегание риска реализуется путем прекращения определенного вида деятельности (отказа от осуществления какого-то вида операций, уход с определенного рынка);
- ✓ передача риска. Решение о передачи риска зависит от вида и характера деятельности Общества, подверженной операционному риску, важности связанной с риском операции и ее финансовой значимости. Обществом могут использоваться такие механизмы, как страхование, хеджирование, аутсорсинг и др.
- ✓ минимизация риска. Спланированное действие или комплекс действий, направленных на снижение финансовых последствий и/или вероятности реализации операционного риска.

6.4. Обществом могут использоваться следующие методы минимизации риска:

- ✓ повышение квалификации персонала;
- ✓ повышение адекватности информационных систем функционалу и объемам бизнеса;
- ✓ регламентирование операций и совершенствование технологий;
- ✓ использование системы распределения полномочий;
- ✓ внедрение и повышение эффективности контрольных механизмов и процедур;
- ✓ обеспечение установленного порядка доступа к информации и материальным активам Общества;
- ✓ принятие риска. Риск принимается, если оценка уровня риска считается для Общества приемлемой и дальнейшие усилия по его минимизации не являются экономически целесообразными.

7. МОНИТОРИНГ И ОЦЕНКА ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ

7.1. Контроль над соблюдением регламента по управлению операционными рисками в Обществе осуществляет Отдел внутреннего аудита.

7.2. Мониторинг операционных рисков происходит на ежеквартальной основе.

7.3. Отчет об управлении операционными рисками Общества составляется на ежеквартальной основе Комитетом по управлению рисками Общества и представляется на Комитете по управлению рисками при Наблюдательном совете Общества.

7.4. За неисполнение (ненадлежащее исполнение) настоящего регламента работник несет ответственность в пределах, определенных законодательством РФ.

8. ПОРЯДОК УТВЕРЖДЕНИЯ ПОЛОЖЕНИЯ И ВНЕСЕНИЯ В НЕГО ИЗМЕНЕНИЙ

8.1. Настоящее Положение утверждается, дополняется и изменяется Общим собранием участников Общества.

Прошито и скреплено
9 (девять) листов

Генеральный директор
ООО «ЭНЕРГОНИКА»

_____ **Кичатова Н.С.**