**УТВЕРЖДЕНО**

решением Совета директоров

АО «Полипласт»

Протокол № 16-01/2023 от 16.01.2023

**Регламент по управлению операционными рисками**

**АО «Полипласт»**

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

* 1. Настоящий Регламент устанавливает правила и порядок действий при управлении операционными рисками АО «Полипласт» (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.
	2. Действие настоящего Регламента распространяется на всех участников группы компаний Общества, всех сотрудников и все структурные подразделения Общества.
	3. Настоящий Регламент определяет следующие направления деятельности по управлению операционными рисками:
1. цель, задачи и принципы управления операционными рисками;
2. основные направления и подходы к управлению операционными рисками;
3. выявление и фиксация операционных рисков;
4. методы оценки операционных рисков;
5. процесс управления и контроля операционных рисков;
6. распределение обязанностей, полномочий и ответственности между органами управления, должностными лицами, сотрудниками и структурными подразделениями.
	1. 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.
	2. 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:
7. снижения стоимости активов;
8. досрочного списания (выбытия) материальных активов;
9. денежных выплат на основании постановлений (решений) судов, решений органов, уполномоченных в соответствии с законодательством Российской Федерации;
10. денежных выплат клиентам и контрагентам, а также сотрудниками Общества в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине Общества;
11. затрат на восстановление хозяйственной деятельности и устранение последствий ошибок, аварий, стихийных бедствий и других аналогичных обстоятельств;
12. прочих убытков.
	1. Основными факторами или событиями, способными усилить влияние и масштабы проявления операционного риска являются:
13. изменение законодательства, требований регулирующих органов;
14. расширение масштабов деятельности, увеличение объемов операций;
15. усложнение финансовых инструментов и стратегий;
16. освоение новых продуктов и технологий;
17. усложнение систем технологической поддержки операций, внедрение новой техники.
	1. 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.
	2. Для управления операционными рисками необходимо решить следующие задачи:
18. Обеспечить получение оперативных и объективных данных об объекте операционного риска;
19. Произвести комплексную оценку операционного риска;
20. Произвести оценку влияния операционного риска на другие типы рисков;
21. Обеспечить мониторинг объектов операционного риска;
22. Создать систему быстрого реагирования для принятия решения на начальной стадии реализации операционного риска.
	1. Органы управления Общества (в частности, Совет Директоров и Генеральный директор Общества) получают информацию о состоянии операционного риска регулярно, а при необходимости – незамедлительно.
	2. Основанием для пересмотра Регламента могут являться:
23. изменение подходов Общества к управлению операционным риском;
24. введение новых нормативных требований, касающихся управления операционным риском;
25. реализация Обществом новых продуктов, новых видов деятельности, выход на новые рынки;
26. другие внешние и внутренние факторы, оказывающие влияние на показатели деятельности Общества.
27. **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**
	1. **Операционный риск** – риск прямых или косвенных потерь (убытков) от неадекватных или ошибочных внутренних процессов Общества, действий сотрудников, операционных систем, внешних событий.
	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 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.
	1. **Контроль операционного риска** - процесс оценки результатов управления операционным риском.
	2. **Мониторинг операционного риска** - процесс систематического и непрерывного сбора и анализа информации об уровне операционного риска.
	3. **Минимизация операционного риска** - комплекс мероприятий по поддержанию операционного риска на уровне, не угрожающем интересам кредиторов и участников, устойчивости Общества.
	4. **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.
	5. **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.
	6. **Оценка операционного риска** - комплекс мероприятий, направленных на выявление и анализ внутренних и внешних факторов, оказывающих воздействие на деятельность Общества и способствующих возникновению операционного риска.
	7. **Управление операционным риском** - комплекс мероприятий и процедур по выявлению (идентификации), оценке (измерению), мониторингу, контролю и (или) минимизации операционного риска.
	8. **Факторы (источники) риска** — это причины возникновения случайных неблагоприятных событий, приводящих к финансовым убыткам, упущенной финансовой выгоде или прекращению деятельности Общества.
	9. Источники операционных рисков:
		1. Риски мошеннических действий сотрудников внутри Общества возникают:
1. При возможности осуществить кражу и передачу информации, представляющую коммерческую тайну;
2. При возможности использования служебного положения при осуществлении операций в личных корыстных целях и наносящих экономический, правовой или ущерб репутации Общества.
	* 1. Риски в сфере кадровой политики и охраны труда возникают:
3. В результате изменения кадрового состава, что приводит к возможным ошибкам при осуществлении операции ввиду недостаточной информированности касательно осуществления бизнес-процессов;
4. В результате повышенного уровня стресса у сотрудников, который приводит к ошибкам при выполнении операций;
5. Недостатки корпоративной культуры, приводящие к ухудшению общей корпоративной среды и снижению эффективности труда;
6. Другие риски, связанные с кадровым составом Общества, например, увольнение сотрудников, имеющих свои клиентские портфели.
	* 1. Риски при взаимодействии с клиентами и контрагентами возникают:
7. При хранении персональных данных, конфиденциальной информации о клиенте и возможности их потери;
8. При условии недобросовестности клиентов или контрагентов, которая выражается в мошеннических действиях отказе выполнения обязательств и других действий;
9. При ограничении возможности взаимодействия с клиентами и другими контрагентами в результате отказа их от сотрудничества с Обществом.
	* 1. Риски информационных технологий, технологические риски возникают:
10. 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);
11. В результате сбоя работы программного обеспечения, который был вызван перебоем во внутренней архитектуре программного обеспечения, моральным истощением программного обеспечения или вредоносными программами;
12. В результате взлома информационных систем и баз данных, которые могут привести к утечке информации, представляющей коммерческую тайну.
	1. Убытки в результате реализации операционных рисков могут быть следующими:
13. 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.
14. 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).
15. Денежные выплаты в судебном порядке – штрафы, неустойки и издержки Общества в результате проведения судебного урегулирования разногласий с должником / контрагентом или работником Общества.
16. 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.
17. 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.
18. Повторные затраты – затраты на восстановление хозяйственной деятельности Общества и устранение последствий ошибок, аварий, стихийных бедствий и других аналогичных обстоятельств.
19. **ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ**
	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.
	2. Задачами Общества в области управления операционными рисками являются:
20. создание, поддержание и совершенствование эффективного механизма своевременной идентификации и предотвращения возможных негативных событий, принятие адекватных мер для снижения/избежания потерь;
21. определение приемлемого уровня конкретных видов операционных рисков с точки зрения экономической целесообразности затрат на их оценку, анализ и мониторинг;
22. создание, поддержание и совершенствование системы внутреннего контроля над операционными рисками;
23. принятие адекватных мер для снижения/избежания потерь.
	1. Принципы управления операционными рисками:
24. соответствие требованиям законодательства и стратегии Общества;
25. 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;
26. принцип непрерывности и комплексности управления рисками;
27. 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.
28. 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;
29. контроль и оценку эффективности управления;
30. 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.
31. 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.
32. 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, к полномочиям которых отнесено решение подобных вопросов, за исключением случаев, когда такое право предоставлено органам управления или отдельным должностным лицам.
33. использование новейших информационных технологий;
34. постоянное совершенствование системы управления операционными рисками.
	1. Основные подходы к оценке и управлению операционными рисками:
35. 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;
36. 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.
	1. Система оценок операционного риска строится с учетом следующих характеристик:
37. применение внутренних статистических данных по случаям убытков и величинам потерь;
38. использование субъективных суждений экспертов о вероятности и масштабах убытков;
39. 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.
40. **ВЫЯВЛЕНИЕ ОПЕРАЦИОННОГО РИСКА**
	1. В целях выявления операционного риска используются следующие методы:
		1. Анализ внутренних условий, в которых функционирует Общество, на предмет наличия операционного риска:
41. анализ подверженности операционному риску направлений деятельности;
42. анализ отдельных операций и сделок;
43. анализ внутренних нормативных документов;
44. анализ внутренних процедур, включая систему отчетности и обмена информацией;
45. анализ операционного риска, возникающего в сфере управления персоналом;
46. другие внутренние условия.
	* 1. Анализ внешних условий, в которых функционирует Общество, на предмет наличия операционного риска:
47. анализ изменений в сфере Общества в целом (например, внедрение новых технологий или инноваций), которые могут оказать влияние на эффективность деятельности;
48. анализ изменения законодательства, требований внешних надзорных органов;
49. анализ внешних случаев реализации операционного риска;
50. другие изменения внешних условий.
	* 1. Анализ нововведений, производимых Обществом, на предмет наличия операционного риска:
51. анализ операционного риска, связанного с внедрением новых продуктов, услуг, процедур, систем, технологий или вносимых в них изменений;
52. анализ операционного риска при выходе Общества на новые рынки;
53. анализ операционного риска, возникающего при использовании новых поставщиков услуг;
54. анализ операционного риска, возникающего вследствие изменения структуры Общества;
55. анализ операционного риска, возникающего при иных нововведениях.
	* 1. Сбор данных о внутренних случаях реализации операционного риска:
56. 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.
	1. Основные виды событий, которые приводят к реализации операционных рисков и требующие контроля:
57. неверные (ошибочные) или умышленные негативные действия при проведении операций в специализированной программе в случаях заведения поставок (возвратов), проведения финансирования и платежей;
58. несанкционированные действия по удалению какой-либо информации из специализированной программы;
59. проведение операций с нарушением условий и ограничений, установленных внутренними Положениями, Регламентами и Инструкциями;
60. недостаточная компетентность сотрудников клиентского обслуживания в случаях оценки юридической состоятельности документов по поставкам, передаваемым клиентами в счет уступленных денежных требований;
61. недостаточная компетентность сотрудников других структурных подразделений;
62. несоблюдение законодательства по ПОД/ФТ;
63. внутреннее мошенничество и злоупотребление служебным положением;
64. внешнее мошенничество;
65. трудовые отношения и безопасность рабочих мест;
66. ошибки профессиональной деятельности;
67. физическое уничтожение имущества;
68. приостановление процессов и ошибки систем;
69. эндогенные и экзогенные нарушения в бизнес-процессах.
	1. Перечень обстоятельств, наступление которых необходимо учитывать менеджеру по рискам при контроле операционных рисков:
70. локальные и муниципальные чрезвычайные ситуации техногенного или природного характера (в том числе аварии, аварийные выбросы, пожары, взрывы, разрушения, затопления зданий, землетрясения, ураганы, наводнения);
71. отключение электро-, водо-, теплоснабжения, систем вентиляции и кондиционирования, иных видов обеспечения повседневной деятельности;
72. 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;
73. акты иностранных государств, содержащие запрет или ограничивающие осуществление деятельности российских компаний;
74. законы и иные нормативные акты РФ, устанавливающие запреты и ограничения;
75. 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;
76. противоправные действия в отношении Общества и его исполнительных органов, приводящие к приостановлению нормального режима его деятельности.
	1. По каждому выявленному операционному риску менеджеры по рискам в целях описания и документирования рисков составляют формализованные описания операционных рисков, которые в совокупности формируют и пополняют карту операционных рисков Общества.
77. **МЕТОДЫ ОЦЕНКИ ОПЕРАЦИОННОГО РИСКА**
	1. Общество проводит оценку операционного риска в отношении отдельных бизнес-процессов и в отношении деятельности в целом. Сотрудники Комитета по управлению рисками 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.
	2. Для оценки операционного риска могут применяться следующие методы оценки:
78. метод, основанный на статистическом анализе распределения убытков;
79. балльно-весовой метод (метод экспертной оценки);
80. математические методы и модели оценки;
81. методы теории вероятностей;
82. методы математической статистики.
	1. 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.
	2. 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.
	3. Для целей оценки операционного риска Общество использует экспертный метод.
		1. 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;
		2. Процедура экспертной оценки проводится на основе комплексного анализа принимаемых операционных рисков (отдельных видов операционного риска) и оценки адекватности деятельности требованиям нормативных документов;
		3. Экспертная оценка операционных рисков (в том числе в целях стресс-тестирования отдельных направлений деятельности) осуществляется не реже одного раза в год.
	4. В целях обеспечения учета, хранения и анализа данных о случаях реализации операционного риска Обществом ведется внутренняя база данных о случаях реализации операционного риска. Во внутреннюю базу данных о случаях реализации операционного риска включаются сведения о рисках, повлекших убытки в любом размере.
83. **ПРОЦЕСС УПРАВЛЕНИЯ И КОНТРОЛЯ РИСКОВ**
	1. Основные этапы процесса управления операционными рисками:
84. идентификация (определение причин и предпосылок, вследствие которых Обществу причинен или может быть причинен ущерб);
85. оценка операционного риска;
86. анализ проблемных зон процессов, выработка и принятие решения по оптимизации или изменению процессов в целях снижения уровня операционного риска;
87. 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);
88. 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).
	1. В процессе управления операционными рисками Общество использует следующие методы:
89. наличие постоянного контроля над корректностью выполнения операций в специализированной программе со стороны руководства подразделений клиентского обслуживания;
90. постоянное проведение (один раз в год) аттестаций сотрудников по знанию технологического процесса и нормативных документов;
91. максимально качественная подготовка новых сотрудников в период испытательного срока;
92. 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.;
93. постоянное обучение и повышение квалификации сотрудников Компании в рамках знания финансово-хозяйственной деятельности предприятий, законодательства, договорных отношений и др.
94. разработка, согласование и утверждение стратегических планов развития и отдельных направлений деятельности Общества;
95. система разделения полномочий и иерархии подчиненности;
96. коллегиальность принятия решений по проведению операций, подверженных риску;
97. процедура разработки, согласования, юридической экспертизы и утверждения внутренних нормативных документов;
98. система лимитов и ограничений;
99. система методик и процедур проведения операций;
100. контроль состояния технических систем;
101. обеспечение безопасности серверов;
102. реализация принципа двойного контроля при совершении операций, их отражении в бухгалтерском учете, вводе данных в учетные и операционные системы;
103. система санкционирования операций, предварительного, текущего и последующего контроля;
104. наличие эффективной системы внутреннего контроля;
105. проведение до начала договорных отношений с клиентом его идентификации в целях ПОД/ФТ;
106. регулярная ревизия адекватности действующих внутренних нормативных документов;
107. обеспечение сокращения числа нештатных ситуаций и минимизация влияния сбоев в ИТ-инфраструктуре;
108. обеспечение оптимальных характеристик автоматизированных систем в соответствии с требованиями бизнеса, исключение ситуаций недостатка ресурсов для решения операционных задач;
109. наличие плана действий в случае возникновения аварийных и нештатных ситуаций;
110. адекватная кадровая политика, определяющая систему подбора, расстановки, аттестации, повышения квалификации и мотивации персонала;
111. наличие внутренних документов, определяющих функции и полномочия структурных подразделений;
112. наличие должностных инструкций, определяющих полномочия, функциональные обязанности и заменяемость сотрудников;
113. система администрирования (разграничения прав доступа) и контроля предоставленных прав доступа;
114. система аудита действий пользователей информационных сетей;
115. защита помещений, оборудования и электронных систем от взлома, несанкционированного проникновения, несанкционированных операций, хищения активов и перехвата информации;
116. система мониторинга и противодействия попыткам взлома и несанкционированного проникновения в информационные сети;
117. разработка типовых форм договорной документации и внутренней документации;
118. разработка порядка рассмотрения, экспертизы и заключения нестандартных договоров и соглашений;
119. поддержание в актуальном состоянии справочных правовых систем.
	1. Контроль и/или минимизация операционного риска
		1. В своей деятельности Общество использует следующие методы контроля и/или минимизации операционного риска:
120. 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);
121. 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.
122. минимизация риска. Спланированное действие или комплекс действий, направленных на снижение финансовых последствий и/или вероятности реализации операционного риска. 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. Решение о принятии риска принимается в соответствии с действующей в Обществе системой полномочий.
123. **МОНИТОРИНГ И ОЦЕНКА ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ.**
	1. Контроль над соблюдением регламента по управлению операционными рисками в Компании осуществляет Комитет по управлению рисками и Менеджер по рискам.
	2. Мониторинг операционных рисков происходит ежегодно.
	3. Отчет об операционных рисках Общества составляется Менеджером по рискам для Комитета по управлению рисками, также и представляется Генеральному директору и Совету Директоров.