ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 51901.22— 2012

Менеджмент риска

РЕЕСТР РИСКА

Правила построения

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Автономной некоммерческой организацией «Научно-исследовательский центр контроля и диагностики технических систем» (АНО «НИЦ КД»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2012 г. № 1285-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Порядок разработки реестра риска организации 2
5 Разработка, утверждение, ведение и актуализация реестра риска 8
6 Обмен информацией и конфиденциальность 8
Приложение А (справочное) Классификация опасностей 9
Приложение Б (справочное) Перечень нормативной документации и федеральных законов Российской Федерации по видам опасностей 14

Введение

Реестр риска является одним из способов представления и хранения информации об опасных событиях и риске. В реестр риска обычно включают основные виды опасностей, применяемые методы оценки и снижения риска и мероприятия по предупреждению, снижению и обработке риска. При разработке реестра риска необходимо учитывать соответствующие законодательные и обязательные требования, а также иную доступную информацию о видах опасности и риске их возникновения. Однако составление реестра риска, особенно при наличии большого количества источников опасности, требует больших усилий, затрат времени, финансовых средств, а также накопления необходимого объема информации.

Необходимость разработки и ведения реестра риска организация определяет самостоятельно.

Настоящий стандарт следует применять с учетом требований основополагающих стандартов в области риска: ГОСТ Р ИСО 31000—2010 «Менеджмент риска. Принципы и руководство», ГОСТ Р ИСО/МЭК 31010—2011 «Менеджмент риска. Методы оценки риска» и ГОСТ Р 51897—2011/Руководство ИСО 73:2009 «Менеджмент риска. Термины и определения».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

РЕЕСТР РИСКА

Правила построения

Risk management. Risk register. Principles of development

Дата введения — 2013—12—01

1 Область применения

В настоящем стандарте установлены правила построения реестра риска. Общие принципы разработки и ведения реестра риска установлены в ГОСТ Р 51901.21.

Реестр риска является одним из способов представления информации о риске. Необходимость разработки и ведения реестра риска организация определяет самостоятельно.

Реестр риска может применяться как элемент системы менеджмента риска или самостоятельно. В системе менеджмента риска реестр риска не является обязательным элементом, могут быть использованы другие способы представления информации о риске.

Настоящий стандарт предназначен в первую очередь для менеджеров по риску, руководителей организаций и технических экспертов по оценке опасных событий, инцидентов и аварий, а также для ответственных за разработку политики менеджмента риска, составление реестра риска, управление и оценку риска, оценку эффективности менеджмента риска организации.

Реестр риска позволяет организациям на местном, региональном и федеральном уровнях сопоставлять данные о риске и применять апробированные методы предупреждения опасных событий и инцидентов и реагирования на них.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 51897—2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения

ГОСТ Р 51901.1—2002 Менеджмент риска. Анализ риска технологических систем

ГОСТ Р 51901.21—2012 Менеджмент риска. Реестр риска. Общие положения

ГОСТ Р 51901.23—2012 Менеджмент риска. Реестр риска. Руководство по оценке риска опасных событий для включения в реестр риска.

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 51897, а также следующие термины с соответствующими определениями.

3.1 **риск** (risk): Следствие влияния неопределенности на достижение поставленных целей[1)].

Примечание 1 — Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное).

Примечание 2 — Цели могут быть различными по содержанию (в области экономики, здоровья, экологии и т. п.) и назначению (стратегические, общеорганизационные, относящиеся к разработке проекта, конкретной продукции и процессу).

Примечание 3 — Риск часто характеризуют путем описания возможного события и его последствий или их сочетания.

Примечание 4 — Риск часто представляют в виде последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности.

Примечание 5 — Неопределенность — это состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей.

[ГОСТ Р 51897—2011/Руководство ИСО 73:2009]

3.2 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в области риска.

[ГОСТ Р 51897—2011/Руководство ИСО 73:2009]

3.3 **реестр риска** (risk register): Форма записи информации об идентифицированном риске.

Примечание — Термин «журнал риска» иногда используют вместо термина «реестр риска».

[ГОСТ Р 51897—2011/Руководство ИСО 73:2009]

3.4 **менеджер по риску** (risk manager): Специалист по идентификации, оценке, анализу, обработке, мониторингу риска, а также другим видам деятельности в области менеджмента риска организации.

4 Порядок разработки реестра риска организации

4.1 Общие положения

Основные цели разработки реестра риска, его место в системе менеджмента риска, преимущества и недостатки реестра риска, а также основные этапы разработки установлены в ГОСТ Р 51901.21.

Реестр риска должен содержать данные по идентификации опасных событий и оценке их риска, а также данные о возможных последствиях воздействия этих опасных событий на деятельность организации в стоимостном и материальном выражении. В реестр риска включают также оценку выполнения мероприятий по обработке риска. Типовая форма реестра риска приведена в таблице 1. В зависимости от особенностей организации форма и содержание реестра риска могут быть изменены или дополнены. Форма реестра риска должна быть утверждена высшим руководством организации.

Составление реестра риска начинают с определения области применения реестра риска и, в частности, с определения объектов реестра риска. Объектами реестра риска могут быть:

- организация в целом, ее структурное подразделение или его часть;
- продукция, услуга, процесс или вид деятельности;
- персонал или отдельные работники.

Общие требования к определению области применения реестра риска установлены в ГОСТ Р 51901.21.

Распределение ответственности за разработку и ведение реестра риска должно соответствовать этапам менеджмента риска, поскольку внесение информации в реестр риска и ее корректировку следует выполнять после завершения каждого этапа менеджмента риска.

При внесении в реестр риска количественных данных следует (по возможности) указывать соответствующую им неопределенность.

Основные элементы реестра риска соответствуют этапам менеджмента риска, описанным в 4.2—4.6.

[1)] В соответствии с ФЗ «О техническом регулировании» от 27.12.2002 № 184-ФЗ «риск — вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда».

Таблица 1 — Типовая форма реестра риска

Идентификация опасных событий														
Индивидуальный идентификатор опасного события														
Краткое наименование опасного события и его описание														
Этап жизненного цикла продукции (услуги), на котором может возникнуть опасное событие														
Причина опасного события														
Возможные воздействия и последствия опасных событий на деятельность организации	Объект воздействия опасного события													
	Описание воздействия опасного события													
Предупреждающие средства контроля и методы управления														
Средства контроля и методы управления по реагированию на опасное событие и восстановлению деятельности														
Анализ риска														
Уровень применяемых предупреждающих средств контроля и методов управления														
Уровень применяемых средств контроля и методов управления по реагированию на опасное событие и восстановлению деятельности														
Источники данных и предположения, используемые при оценке риска														
Метод оценки и анализа риска														
Оценка последствий (ущерба) при реализации опасного события	Дни простоя													
	Стоимость													
	Другие единицы измерения													
Вероятность опасного события														
Результат количественной оценки риска														
Уровень неопределенности оценки риска														

4 *Окончание таблицы 1*

Сравнительная оценка риска			Обработка риска														Мониторинг риска и пересмотр реестра риска			Замечания, предложения, ссылки
Критерий приемлемости риска	Результат сравнительной оценки риска (риск неприемлемый, риск приемлемый, но требует обработки (ALARP), риск приемлемый)	Ранг опасного события в порядке возрастания риска	Стратегия обработки риска (устранение, снижение, передача, принятие, оптимизация)	Значения показателей после внедрения стратегии менеджмента риска						Мероприятия по обработке риска	Срок выполнения		Ответственный за выполнение мероприятий по обработке риска			Мониторинг мероприятий по обработке риска	Результаты анализа результативности и эффективности мероприятий по обработке риска	Результаты анализа результативности и эффективности системы менеджмента риска	
				Оценка последствий		Оценка вероятности опасного события		Оценка риска			План	Факт	Под-разде-ление	Долж-ность	ФИО, под-пись				
				план	факт	план	факт	план	факт										

4.2 Идентификация опасных событий

Для идентификации опасных событий необходимо определить явления или события, которые могут воздействовать на объекты реестра риска, установленные в области применения реестра риска, и/или возможности по их улучшению. Идентификация опасных событий включает в себя:

- присвоение индивидуального идентификатора опасному событию;
- определение краткого наименования опасного события и его описание;
- установление этапа жизненного цикла продукции (услуги), на котором может возникнуть опасное событие;
- определение возможных последствий на деятельность организации и их воздействий;
- идентификация предупреждающих средств контроля и методов управления;
- идентификация средств контроля и методов управления по реагированию на опасные события и восстановлению деятельности после их реализации.

Описания опасных событий, их причин и других элементов реестра риска на этапе идентификации опасных событий должны актуализироваться по мере поступления новой информации. Первоначально достаточным является описание, понятное вовлеченному персоналу и внешним причастным сторонам.

При выявлении опасных событий, их причин следует уделять внимание исследованию взаимосвязи нескольких опасных событий при совместном появлении.

Существуют два основных требования к информации об идентификации опасных событий:

- описание опасных событий и их причин в установленной форме реестра должно быть достаточным для того, чтобы персонал, вовлеченный на стадии оценки риска, мог получить в полной мере всю необходимую информацию;
- должны быть приведены все предположения и ограничения, используемые для оценки риска.

Определение причин опасных событий обеспечивает:

- достижение точного понимания и определения проблем, требующих решения, которые напрямую не следуют из описаний опасных событий;
- разработку мер, направленных на снижение риска на стадии обработки риска;
- анализ идентифицированных опасных событий в части влияния на выполнение целей организации.

При разработке реестра риска, как правило, используют экспертные оценки, поэтому важно, чтобы к данным работам менеджеры по риску привлекали квалифицированный персонал. Рекомендуется, чтобы, начиная со стадии идентификации опасных событий и далее на стадиях оценки и обработки риска, в деятельность по разработке и ведению реестра риска были вовлечены эксперты в следующих областях:

- проектирование и разработка объектов реестра риска;
- функционирование объектов реестра риска;
- экологический менеджмент;
- финансовый менеджмент;
- оценка затрат;
- производственное планирование;
- бюджетирование/ревизионный контроль;
- операции с недвижимым имуществом;
- производственный менеджмент;
- менеджмент персонала и экспертов в области риска;
- другие области (например, юриспруденция, обеспечение безопасности, материально-техническое снабжение).

Перечисленные области деятельности для привлечения экспертов являются рекомендуемыми. В отчетах организаций по менеджменту риска должны быть указаны вовлеченные в эту деятельность эксперты и специалисты, область их знаний или экспертизы, степень квалификации, в том числе по идентификации опасных событий и возможностей по улучшению, оценке риска и обработке риска. Важно понимать, что менеджер по риску не может быть компетентным во всех областях деятельности организации и самостоятельно оценивать риск для сложных объектов. Однако одной из важных задач менеджмента риска при разработке реестра риска является назначение ответственных и организация групповой работы.

Все предположения и данные, используемые на стадии идентификации опасных событий, должны быть зафиксированы.

Для внесения в реестр опасных событий рекомендуется использовать виды опасностей, приведенные в приложении А.

4.3 Анализ риска

На основе выявленных опасных событий и их причин необходимо оценить последствие каждого опасного события и его вероятность с помощью комбинированных или количественных методов анализа и оценки риска.

Этап анализа риска включает в себя:

- определение источников данных и предположений, используемых при анализе и оценке риска;
- определение уровня применяемых средств контроля и методов управления;
- определение метода оценки и анализа риска;
- оценку последствий (ущерба) при реализации опасного события (в днях простоя, в стоимостном выражении или в других единицах измерения);
- оценку вероятности опасного события;
- определение количественной оценки риска;
- определение уровня неопределенности полученной оценки риска.

Последствия идентифицированных опасных событий следует оценивать с точки зрения установленных целей проекта или деятельности организации, при этом необходимо учитывать, что одно опасное событие может иметь несколько последствий. Существует много видов и областей воздействия опасных событий, требующих анализа и оценки риска (например, экология, безопасность строительства, бюджетирование и т. д.), поэтому все воздействия опасного события необходимо оценивать с точки зрения ущерба для деятельности организации.

Менеджеры по риску должны четко различать оценку последствий опасного события и оценку его вероятности. В противном случае существует возможность существенных ошибок при оценке риска. Менеджеры по риску должны получить четкий ответ на вопрос: «Если опасное событие произойдет, какое воздействие на деятельность организации оно окажет?».

Только после того, как будет достигнута согласованность в оценках последствий опасного события между участниками группы по менеджменту риска, менеджер по риску должен предложить оценить вероятность опасного события. Если вероятность опасного события определена, риск считают полностью определенным количественно.

Менеджер по риску должен направлять работу группы менеджмента риска на активное обсуждение до полного завершения оценки риска.

На этапе анализа риска проводят анализ дней простоя при реализации опасного события. При этом последствия каждого опасного события необходимо соотнести с количественной оценкой риска и с планом-графиком работ организации. Необходимо определить, насколько критические виды деятельности зависят от возможной продолжительности простоя. Для этого может быть использован метод моделирования Монте-Карло.

В процессе анализа и оценки риска, имеющего несколько областей воздействия, на основе описания опасного события и его причин может быть принято решение о необходимости разделить риск на несколько частей в соответствии с областями воздействия. Такое решение может быть дополнительно рассмотрено после идентификации мероприятий по обработке риска. Если мероприятия по обработке риска одинаковы как для составляющих видов риска воздействия, так и для общего риска, то риск следует исследовать как общий риск. Если мероприятия по снижению риска для различных областей воздействия различны, то рекомендуется разделить риск на несколько составляющих видов риска.

При выполнении оценки и анализа риска в реестре риска должны быть зафиксированы все использованные данные (например, условия контракта, опыт разработки аналогичных объектов, применяемые формулы, модели предположения). Полученные оценки риска должны быть также занесены в реестр риска.

Для демонстрации полноты и завершенности анализа риска должен быть составлен перечень исключенных рисков.

При выполнении анализа и оценки риска рекомендуется учитывать требования ГОСТ Р 51901.23.

4.4 Сравнительная оценка риска

Этап сравнительной оценки риска состоит в оценке приемлемости риска на основе критериев риска, ранжировании опасных событий и составлении перечня опасных событий, для которых необходимо проведение обработки риска.

Сравнительная оценка риска включает в себя:

- определение критериев приемлемости риска;
- сопоставление оценки риска с критериями приемлемости риска;
- определение приемлемости риска;

- ранжирование опасных событий в зависимости от их риска;
- принятие решения о необходимости обработки риска.

Ранжирование опасных событий проводят в соответствии с ущербом.

Результатом анализа и сравнительной оценки риска является ранжирование риска, согласованное с политикой и целями организации в области риска, и принятие решения о необходимости обработки риска.

4.5 Обработка риска

Этапы обработки риска включают в себя:

- выбор стратегии обработки риска;
- оценку последствий, вероятности опасного события и риска после применения выбранной стратегии обработки риска;
- идентификацию мероприятий по обработке риска;
- определение сроков выполнения мероприятий по обработке риска;
- определение ответственных за выполнение мероприятий;
- оценку результатов обработки риска.

Организация может применять следующие стратегии обработки риска:

- устранение риска, например, путем внесения изменений в конструкцию объекта;
- снижение риска (уменьшение последствий и/или вероятности опасного события);
- передача риска (например, передача ответственности за последствия опасного события третьей стороне);
- принятие риска;
- оптимизация риска (при наличии возможностей).

Примечание — Каждое решение о принятии риска, то есть отказ от мероприятий по снижению или устранению риска, должно быть согласовано высшим руководством.

Организация должна установить процесс обмена информацией о риске с причастными сторонами, особенно о видах риска, требования к которым установлены в соответствии с законодательными и обязательными требованиями.

Организация должна разработать план мероприятий по обработке риска. В плане должны быть установлены сроки выполнения мероприятий по обработке риска и ответственные за их выполнение. В качестве ответственных, как правило, назначают:

а) менеджеров по риску, если в качестве стратегии снижения риска выбраны устранение, снижение или оптимизация риска;

б) ответственную сторону, если в качестве стратегии снижения риска выбрана передача риска;

в) ответственного, наделенного полномочиями принятия риска, если в качестве стратегии снижения риска выбрано принятие риска.

Если принято решение об особом управлении конкретным риском, ответственность за управление этим риском должна быть установлена в реестре риска. Кроме того, в этом случае должны быть определены:

- персонал, имеющий необходимую компетентность и наделенный соответствующими полномочиями для управления установленным риском (с низкой вероятностью реализации и/или катастрофическими последствиями для деятельности организации);
- мероприятия по обработке установленных размеров риска. Реализация этих мероприятий может быть возложена на персонал, ответственный за менеджмент риска, при этом должна быть точно поставлена задача, установлен срок ее выполнения.

Лицо, несущее общую ответственность за менеджмент риска в организации, должно иметь всю необходимую информацию об особо важных видах риска и способах их менеджмента. В реестре риска соответствующие опасные события и риски могут быть выделены в отдельный раздел.

4.6 Мониторинг риска и пересмотр реестра риска

Процесс менеджмента риска должен быть непрерывным, поэтому менеджеры по риску должны проводить регулярный мониторинг всех видов риска и пересмотр записей в реестре риска, направленный на обеспечение выполнения целей организации и установленных требований к риску.

Для этого необходимо:

- проведение регулярного анализа каждого риска, направленного на оценку полноты и правильности соответствующих описаний и расчетов, их соответствия существующим угрозам, последствиям,

оценкам вероятности их появления, выбранной стратегии менеджмента риска и достаточности мер, направленных на снижение риска;

- идентификация ответственным за менеджмент риска организации ключевых видов риска и обмен информацией о них с причастными сторонами;

- актуализация мероприятий, направленных на снижение риска.

Анализ и пересмотр реестра риска выполняет уполномоченный персонал. Менеджер по риску несет ответственность за планирование и выполнение работ по анализу и пересмотру реестра риска ответственным персоналом. Менеджер по риску организации должен быть своевременно информирован об изменениях информации о ранее идентифицированных или новых рисках. Анализ и пересмотр реестра риска следует проводить не реже одного раза в год. Периодичность анализа и пересмотра реестра риска устанавливает высшее руководство организации. Анализ и пересмотр реестра риска должны включать в себя обсуждение проблем, связанных с новыми видами идентифицированного риска и исключением из реестра риска устаревшей информации.

Дополнительно в процессе мониторинга риска и пересмотра реестра риска необходимо проводить анализ результативности и эффективности мероприятий по обработке риска, а также анализ результативности и эффективности системы менеджмента риска.

5 Разработка, утверждение, ведение и актуализация реестра риска

Действия по разработке, утверждению, ведению и актуализации реестра риска и соответствующих отчетов, а также обмен содержащейся в них информации должны соответствовать требованиям процедур управления документацией и записями, а также другим требованиям, установленным в организации.

Реестр риска должен быть утвержден высшим руководством организации.

Реестр риска должен актуализироваться через запланированные интервалы времени.

Внесение изменений в реестр риска должно соответствовать процедурам управления изменениями в документации организации.

В дополнение к реестру риска менеджеры по риску должны вести:

- записи обоснований выводов и заключений, приведенных в реестре риска;

- записи обо всех предположениях, используемых при анализе всех существенных опасностей и соответствующих им рисков, представленных в реестре риска;

- контрольные журналы, идентифицирующие объект оценки риска, продолжительность, дату, участников и полученный результат оценки риска.

Ответственный менеджер по риску организации должен разработать общую форму отчета для предоставления высшему руководству организации.

В отчете по реестру риска необходимо обеспечить ответы на следующие вопросы:

- Каковы основные опасные события, их риск и способы обработки?

- Для каких ключевых видов риска меры по обработке риска не эффективны или не выполнимы?

- Какие изменения произошли за последний отчетный период?

- Что необходимо изменить в стратегиях, целях и задачах в области менеджмента риска, чтобы предотвратить возможные потери или снизить их?

- Какова причина невыполнения или неэффективности мероприятий по обработке риска?

- Какие действия должны быть предприняты для выполнения плановых мероприятий по обработке риска?

- Что должно быть предпринято для повышения эффективности менеджмента риска?

Менеджер по риску при составлении отчета должен учесть политику и цели в области менеджмента риска, данные о готовности решать возникающие проблемы в области риска, после чего предоставить отчет высшему руководству.

6 Обмен информацией и конфиденциальность

Организация должна установить обмен информацией о риске на основе данных реестра риска. Эффективный обмен информацией о риске, включенной в реестр риска, позволяет менеджерам получать данные о ключевых проблемах и изменениях, идентифицировать сферу ответственности и приоритетные меры реагирования на опасное событие.

Высшее руководство организации должно определить степень конфиденциальности реестра риска, установить порядок доступа к реестру риска и степень раскрытия содержащейся в нем информации.

Приложение А
(справочное)

Классификация опасностей

А.1 Общие положения

Опасные события могут быть отнесены к одному из следующих классов опасностей:
- природные;
- биолого-социальные;
- техногенные;
- экологические;
- профессиональные;
- информационные;
- экономические;
- террористические;
- киберопасности;
- другие виды опасности.

А.2 Природные опасности

Природная опасность — это опасность, вызванная явлениями природы, или результат природных процессов. Такие опасности по своей интенсивности, масштабу распространения и продолжительности могут нанести ущерб здоровью людей и окружающей среде, а также негативно воздействовать на деятельность организации.

Природные опасности могут быть подразделены на следующие виды:
- геологические;
- гидрологические;
- метеорологические;
- природные пожары.

Геологическая опасность — это опасность, вызванная геологическими явлениями или процессами, возникающими в земной коре под действием различных природных или геодинамических факторов или их комбинаций, оказывающими или способными оказать поражающие воздействия на людей, животных или растения, окружающую среду и деятельность организации. К геологическим опасностям относят такие опасности, как землетрясение, извержение вулкана, поток лавы, обвал горных пород, оползень и т. п.

Гидрологическая опасность — это опасность, вызванная гидрологическими явлениями или процессами, возникающими под действием различных природных или гидродинамических факторов или их комбинаций, оказывающими поражающее воздействие на людей, животных и растения, окружающую среду и деятельность организации. К гидрологическим опасностям относят такие опасности, как наводнение, половодье, паводок, затор, зажор, цунами, затопление, подтопление, сель, лавина и т. п.

Метеорологическая опасность — это опасность, вызванная природными явлениями и процессами, возникающими в атмосфере под действием различных природных факторов или их комбинаций, оказывающими или способными оказать поражающее воздействие на людей, животных и растения, окружающую среду и деятельность организации. К метеорологическим опасностям относят такие опасности, как сильный ветер, вихрь, ураган, торнадо, шторм, смерч, шквал, продолжительный дождь, гроза, ливень, град, снегопад, гололед, заморозки, сильная метель, туман, пылевая буря и т. п.

Опасность возникновения природного пожара — опасность, связанная с неконтролируемым процессом горения, стихийно возникающим и распространяющимся в природной среде. К опасностям возникновения природного пожара относят такие опасности, как опасность возникновения лесного пожара, степного пожара, ландшафтного пожара, торфяного пожара и т. п.

А.3 Биолого-социальные опасности

Биолого-социальная опасность — это опасность, последствием которой являются нарушение нормальных условий работы и жизнедеятельности персонала, существования животных и произрастания растений, возникающая угроза жизни и здоровью людей, распространения инфекционных заболеваний, потерь животных и растений и, как следствие, нарушение нормальной деятельности организации.

Источником биолого-социальных опасностей может быть распространение инфекционных заболеваний людей, сельскохозяйственных животных и растений. Состояние зараженности организма людей или животных, проявляющееся в виде инфекционного заболевания, прогрессирующего во времени и пространстве и вызывающего тяжелые последствия для здоровья и жизни людей и сельскохозяйственных животных, называют особо опасной инфекцией. Возбудителями инфекционных заболеваний являются патогенные микроорганизмы, которые эволюционно приспосабливаются к паразитированию в организме человека или животного и способны вызвать инфекционное заболевание. Источником распространения инфекции может стать организм зараженного человека или животного, в котором идут естественные процессы жизнедеятельности, в том числе размножения и выделения во внешнюю среду возбудителя инфекционной болезни.

Биолого-социальные опасности могут быть подразделены на следующие виды:

- эпидемия;
- эпизоотия;
- эпифитотия.

Эпидемия — это массовое, прогрессирующее во времени и пространстве организации и за ее пределами распространение инфекционного заболевания среди людей, значительно превышающее обычно регистрируемый уровень заболеваемости. К таким заболеваниям относят чуму, грипп, туберкулез и т. п.

Эпизоотия — это одновременное прогрессирующее во времени и пространстве организации и за ее пределами распространение инфекционных заболеваний среди одного или нескольких видов животных, значительно превышающее обычно регистрируемый уровень заболеваемости. К таким заболеваниям относят птичий грипп, бешенство, африканскую чуму свиней и другие.

Эпифитотия — это массовое, прогрессирующее во времени и пространстве инфекционное заболевание сельскохозяйственных растений и/или резкое увеличение численности вредителей растений, сопровождающееся массовой гибелью сельскохозяйственных культур и снижением их продуктивности. В виде эпифитотии проявляются, например, ржавчина и головня хлебных злаков, фитофтороз картофеля и т. п.

А.4 Техногенные опасности

Техногенная опасность — это опасность, вызванная нарушением нормальной работы технических систем, промышленных, транспортных и иных объектов. Техногенная опасность может создавать угрозу жизни и здоровью людей, оказывать поражающее действие на окружающую природную среду, вызвать разрушение зданий, сооружений, оборудования и транспортных средств, нарушение производственных и иных процессов организации.

Техногенные опасности могут быть подразделены на следующие виды:

- промышленные опасности, инциденты и/или аварии;
- пожары и взрывы;
- транспортные опасности.

Промышленная опасность — это техногенная опасность, приводящая при ее реализации к частичному или полному разрушению промышленных объектов, технических систем, промышленных установок, зданий, сооружений, оборудования и транспортных средств, нарушению производственного процесса и, как следствие, создающая угрозу жизни и здоровью людей, нанесения ущерба окружающей среде и деятельности организации. К промышленным опасностям относят опасность радиационной аварии, радиоактивного загрязнения, токсического воздействия химических веществ, выброса опасных веществ, биологического заражения, отказа оборудования, невыполнения им установленных функций или их выполнения с нарушением установленного срока, снижения производительности или простой оборудования и т. п.

Пожарная опасность — это техногенная опасность, связанная с возможностью возникновения и эскалации пожара.

Опасность взрыва — это техногенная опасность, связанная с возможностью возникновения и эскалации быстропротекающего процесса физических и химических превращений веществ, сопровождающегося освобождением значительного количества энергии в ограниченном объеме, в результате которого в окружающем пространстве образуется и распространяется ударная волна, способная привести или приводящая к возникновению техногенной опасной ситуации.

Транспортная опасность — это техногенная опасность, связанная с возможностью возникновения и эскалации опасных ситуаций, инцидентов и аварий на транспорте, которые могут повлечь за собой травмирование и гибель людей, повреждение и разрушение транспортных средств и сооружений, ущерб окружающей среде и имуществу организации. Транспортные опасности и аварии разделяют по отношению к видам транспорта, на котором они произошли, и/или по поражающим факторам опасных грузов. К транспортным опасностям относят такие опасности, как железнодорожные инциденты и аварии, дорожно-транспортные происшествия, инциденты и аварии на магистральных трубопроводах, авиационные инциденты и катастрофы, аварии на подземных сооружениях, задержка отправления и/или прибытия, полное или частичное невыполнение транспортной задачи, ухудшение качества доставляемого груза, нанесение вреда здоровью людей и т. п.

Поражающие факторы техногенных опасностей можно разделить по генезису (происхождению) и механизму воздействия.

Поражающие факторы техногенных опасностей по генезису подразделяют на факторы прямого и вторичного действия. Реализация первичных поражающих факторов техногенных опасностей непосредственно приводит к возникновению инцидента. Вторичные поражающие факторы техногенной опасности являются следствием изменений объектов организации и окружающей среды под действием поражающих факторов первичных опасностей.

Поражающие факторы техногенных опасностей по механизму действия подразделяют на факторы физического и химического действия.

К поражающим факторам физического действия относят воздушную ударную волну, волну сжатия в грунте, сейсмовзрывную волну, волну прорыва гидротехнических сооружений, их обломки или осколки, экстремальный нагрев среды, тепловое излучение, ионизирующее излучение.

К поражающим факторам химического действия относят токсическое действие опасных химических веществ.

А.5 Экологические опасности

Экологические опасности часто включают в техногенные опасности, однако при необходимости они могут быть выделены в отдельную категорию.

Экологическая опасность — опасность, последствием реализации которой является негативное воздействие (случайного или детерминированного характера) на элементы окружающей среды, приводящее к заболеванию и/или гибели человека; ухудшению состояния окружающей человека среды, обусловленному нанесением материального или социального ущерба и/или ухудшением качества природной среды.

По видам опасных воздействующих факторов экологические опасности подразделяются на:

- абиотические;
- биотические;
- антропогенные.

Абиотические факторы связаны с воздействием на человека, животных, растения, неживую природу, включая климатические (метеорологические) факторы (температуру окружающей среды, влажность воздуха, атмосферное давление, скорость и силу ветра и др.), физические свойства почвы и воды; геофизические (орографические) факторы, определяющие освещенность, влажность воздуха, силу ветра, солнечную радиацию, космическое излучение, геомагнетизм, особенности ландшафта или рельефа и химические компоненты воды, воздуха, почвы, кислотность, примеси и др.

Биотические факторы связаны с совокупным воздействием одних организмов на другие. Среди биотических факторов различают фитогенные (воздействие растений), зоогенные (воздействие животных), микробиогенные (воздействие микроорганизмов). К биотическим факторам относят также особенности питания тех или иных организмов и вытекающие из этого формы взаимодействия видов и особей между собой (хищничество, конкуренция, паразитизм и др.). По уровню организации к биотическим факторам относят наличие сообщества, популяции или отдельных организмов.

Антропогенные факторы, связанные с деятельностью человека, которые либо косвенно воздействуют на живые организмы, изменяя естественную (природную) среду и, как следствие, условия обитания, либо непосредственно влияют на отдельные виды животных и растений. Антропогенные факторы подразделяют на хозяйственные, связанные с непосредственным удовлетворением потребностей жизнеобеспечения человека, и техногенные, связанные с применением машин и оборудования для достижения определенных целей. Антропогенные факторы также относят к биотическим, так как своим происхождением они обязаны биологическому существу — человеку. Однако эти факторы выделяют в особую группу по причине их многообразия и специфичности.

Факторы техногенной опасности загрязнений подразделяют в зависимости от типов воздействий на:

- физические (механические, тепловые, шум, вибрация, полевые загрязнения различной природы, в т. ч. электромагнитные, световые, радиоактивные);
- химические (аэрозоли, химические вещества, тяжелые металлы, пестициды, пластмассы);
- биологические (биогенные, микробиологические и генетические);
- биотические (психофизиологические, нервно-психологические и другие воздействия, негативно влияющие на людей, приводящие к перегрузкам, ошибкам в работе, конфликтам).

А.6 Профессиональные опасности

Профессиональные опасности часто включают в техногенные опасности, однако при необходимости они могут быть выделены в отдельную категорию.

Профессиональная опасность — это опасность, создающая угрозу жизни и здоровью персонала организации.

Профессиональные опасности должны быть определены организацией в соответствии с законодательными и обязательными требованиями РФ в области охраны труда. Для них должна быть разработана и внедрена соответствующая техника безопасности.

Кроме того, при разработке перечня профессиональных опасностей могут быть использованы в качестве справочной информации разработанные Международной организацией труда международные информационные листки опасностей по профессиям, которые содержат сведения об опасностях, риске и мерах по их предотвращению для конкретных профессий. Информационные листки содержат описание опасностей в стандартизованной форме, которым работник может подвергаться при нормальных условиях работы, что позволяет предусмотреть меры предотвращения несчастных случаев на производстве и профессиональных заболеваний. Международные информационные листки опасностей по профессиям предназначены для описания всего диапазона опасностей, которым может подвергаться работник конкретной профессии.

А.7 Экономические опасности

Экономическая опасность — это опасность, последствием реализации которой является нарушение нормальной экономической и финансовой деятельности, бизнеса и устойчивого развития организации.

Экономическая опасность для субъекта хозяйственной деятельности имеет разнообразные формы проявления, которые можно отнести к одной из следующих групп:

- организационные опасности — это опасности, связанные с ошибками менеджмента организации, ее сотрудников, проблемами системы внутреннего контроля, плохо разработанными правилами выполнения работ, т. е. опасности, связанные с внутренней организацией работы организации;

- рыночные опасности — это опасности, связанные с нестабильностью экономической конъюнктуры. К рыночным опасностям относят риск финансовых потерь, вызванных изменениями цены товара, риск снижения спроса на продукцию, трансляционный валютный риск, риск потери ликвидности и пр.;

- кредитные опасности — это опасность того, что контрагент не выполнит своих обязательств в полной мере в установленный срок. Кредитные опасности существуют как у банков (риск невозврата кредита), так и у предприятий, имеющих дебиторскую задолженность, и у организаций, работающих на рынке ценных бумаг;

- юридические опасности — это опасности потерь, связанных с тем, что законодательные требования и нормы не были учтены или изменились в период сделки; опасность несоответствия законодательству других стран; опасность некорректно составленной документации, в результате чего контрагент может не выполнять условия договора и пр.

Существуют и другие виды экономических опасностей, такие как опасности, возникающие при взаимодействии с поставщиками, потребителями, конкурентами, инвесторами, органами власти, персоналом, а также инновационные, маркетинговые, инвестиционные опасности и т. п.

А.8 Информационные опасности

Информационная опасность — это опасность, последствием реализации которой являются нарушения конфиденциальности, целостности, доступности и защищенности информации и поддерживающей их инфраструктуры вследствие случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений с организацией.

Примечание — Поддерживающая инфраструктура — системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал. Неприемлемый ущерб — ущерб, которым нельзя пренебречь.

Информационные опасности подразделяют на три вида нарушения состояния информации:

- конфиденциальность (свойство информационных ресурсов, в том числе информации, связанное с недоступностью и/или возможностью их раскрытия для неуполномоченных лиц);
- целостность (неизменность информации в процессе ее передачи или хранения);
- доступность (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц).

В соответствии с этим объектами информационных опасностей являются:

- аппаратное обеспечение;
- программное обеспечение;
- средства связи (коммуникации);
- персонал, работающий с информацией.

Информационные опасности подразделяют на опасности:

- физического уровня;
- опасности для персонала;
- опасности для организации.

А.9 Террористические опасности

Террористическая опасность — опасность, последствием реализации которой являются действия, устрашающие население и создающие опасность гибели людей, причинения значительного имущественного ущерба либо иных тяжких последствий, совершаемые в целях воздействия на органы власти или международные организации. К таким опасностям относятся террористические действия в местах массового скопления людей, атаки на инфраструктуру, транспортные системы и др.

А.10 Киберопасности

Киберопасности обычно включают либо в информационные опасности, либо в террористические опасности, однако при необходимости они могут быть выделены в отдельную категорию.

Киберопасности связаны с промышленным и государственным шпионажем, киберпреступностью и иными формами несанкционированного доступа к ИТ[1)] системам организации.

Опасности и угрозы кибератак на ИТ и системы связи организации могут значительно отличаться в различных сферах деятельности. Потенциальное воздействие кибератак связано с возможностью экспортировать, изменять или удалять информацию или заставлять устройства выходить из строя. Кибератаки обычно направлены на получение важной информации из ИТ устройств в организациях различной формы собственности незаконным путем.

А.11 Другие виды опасностей

Кроме вышеперечисленных видов опасностей могут существовать другие виды опасностей, которые трудно отнести к одной из этих групп. Например социальные, политические и иные опасности.

К социальным источникам опасностей отнесены опасности, вызванные низким духовным и культурным уровнем людей. Это такие явления, как бродяжничество, проституция, пьянство, алкоголизм, преступность и т. д. Пер-

---

[1)] ИТ — информационные технологии.

воисточниками этих опасностей являются неудовлетворительное материальное положение, плохие условия проживания, революции, конфликтные ситуации на межнациональной, этнической, расовой или религиозной почве.

Источниками политических опасностей являются конфликты на межнациональном и межгосударственном уровнях, религиозное противостояние, политический терроризм, идеологические, межпартийные, межконфессиональные и вооруженные конфликты, войны.

Организации могут выделить опасности в отдельные группы опасностей в соответствии со спецификой деятельности.

А.12 Комбинированные опасности

В современной деятельности организации многие опасности носят комбинированный характер. Это такие опасности, как природно-техногенные (смог, кислотные дожди, пылевые бури, уменьшение плодородия почв, возникновения пустынь и другие явления, вызванные человеческой деятельностью), природно-социальные (наркомания, эпидемии инфекционных заболеваний, венерических заболеваний, СПИДа и др.), социально-техногенные (профессиональная заболеваемость, профессиональный травматизм, психические заболевания, вызванные производственной деятельностью, массовые психические заболевания, вызванные воздействием на сознание и подсознание средств массовой информации и специальных технических средств, токсикомания) и т. п.

При составлении реестра риска организация должна учитывать различные виды опасностей и их всевозможные комбинации. Это необходимо для обеспечения качества данных, содержащихся в реестре риска, объективной оценки совокупного риска и разработки мероприятий по его снижению в организации.

Справочный перечень законов, технических регламентов и национальных стандартов по видам опасностей приведен в приложении Б.

А.13 Обеспечение безопасности

Обеспечение безопасности от воздействия природных опасностей связано с принятием и соблюдением законодательных требований и правовых норм, выполнением экологических норм и требований, а также комплексом организационных мероприятий на основе прогнозируемых данных, инженерно-технических, защитных и специальных мероприятий, направленных на обеспечение защиты от воздействия поражающих факторов природных опасностей людей, окружающей среды и деятельности организации.

Обеспечение биологической безопасности связано с соблюдением законодательных требований и правовых норм, выполнением санитарно-гигиенических и санитарно-эпидемиологических правил, технологических и организационно-технических требований, а также проведением соответствующего комплекса правовых, санитарно-гигиенических, санитарно-эпидемиологических, организационных и технических мероприятий, направленных на предотвращение, ослабление и ликвидацию опасности заражения людей, сельскохозяйственных животных и растений инфекционными заболеваниями.

Обеспечение промышленной безопасности связано с принятием и соблюдением законодательных требований и правовых норм, а также проведением комплекса организационных, технологических и инженерно-технических мероприятий, направленных на предотвращение техногенных опасностей в организации.

Обеспечение экологической безопасности связано с принятием и соблюдением законодательных требований и правовых норм, а также проведением комплекса организационных, технологических и инженерно-технических мероприятий, направленных на предотвращение экологических опасностей в организации.

Обеспечение профессиональной безопасности связано с принятием и соблюдением законодательных требований и правовых норм в области охраны и безопасности труда, соблюдением санитарных и гигиенических норм, а также проведением комплекса организационных, технологических и инженерно-технических мероприятий, направленных на предотвращение профессиональных опасностей в организации.

Экономическая безопасность, или финансовая безопасность, — это состояние какого-либо хозяйствующего субъекта, характеризующееся наличием стабильного дохода и ресурсов, которые позволяют поддержать нормальное функционирование и устойчивое развитие организации.

Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности:

- законодательная, нормативно-правовая и научная база;
- структура и задачи органов (подразделений), обеспечивающих безопасность ИТ;
- организационно-технические меры и меры особого режима (политика информационной безопасности);
- программно-технические способы и средства обеспечения информационной безопасности.

Разработку мероприятий по противодействию угрозам террористического характера и обеспечению безопасности объекта в целом выполняют в два этапа. Сначала разрабатывают модели угроз, модели поведения потенциальных нарушителей; оценку риска выполняют с использованием математических моделей объектов и на основе этих оценок разрабатывают специальные требования к разработке мероприятий по обеспечению антитеррористической защищенности объекта. На втором этапе проводят проектирование технических средств безопасности в соответствии с действующими нормами и требованиями. Проводят повторную оценку риска с учетом спроектированных технических средств обеспечения безопасности и организационных мероприятий.

Состав технических средств и систем антитеррористической защиты определяют индивидуально для каждого объекта на основании анализа угроз, возможных последствий их реализации и категории объекта. В общем случае все подсистемы должны быть интегрированы в единый комплекс технических средств обеспечения безопасности объекта.

Приложение Б
(справочное)

Перечень нормативной документации и федеральных законов Российской Федерации по видам опасностей

Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов»

Федеральный закон от 21.07.1997 № 117-ФЗ «О безопасности гидротехнических сооружений»

Федеральный закон от 23.11.1995 № 174-ФЗ «Об экологической экспертизе»

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»

Федеральный закон от 09.01.1996 № 3-ФЗ «О радиационной безопасности населения»

Федеральный закон от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения»

Федеральный закон от 10.01.2002 № 7-ФЗ «Об охране окружающей среды»

Федеральный закон от 24.06.1998 № 89-ФЗ «Об отходах производства и потребления»

Федеральный закон от 04.05.1999 № 96-ФЗ «Об охране атмосферного воздуха»

Технический регламент «О требованиях к автомобильному и авиационному бензину, дизельному и судовому топливу, топливу для реактивных двигателей и топочному мазуту». Постановление Правительства Российской Федерации от 27.02.2008 № 118

ГОСТ 21964—76 Внешние воздействующие факторы. Номенклатура и характеристики

ГОСТ 12.0.003—74 Система стандартов безопасности труда. Опасные и вредные производственные факторы. Классификация

ГОСТ 30630.0.0—99 Методы испытаний на стойкость к внешним воздействующим факторам машин, приборов и других технических изделий. Общие требования

ГОСТ 30333—2007 Паспорт безопасности химической продукции. Общие требования

ГОСТ Р 22.0.04—95 Безопасность в чрезвычайных ситуациях. Биолого-социальные чрезвычайные ситуации. Термины и определения

ГОСТ Р 14.03—2005 Экологический менеджмент. Воздействующие факторы. Классификация

ГОСТ Р 53691—2009 Ресурсосбережение. Обращение с отходами. Паспорт отхода I—IV класса опасности. Основные требования

ГОСТ Р 17.0.0.06—2000 Охрана природы. Экологический паспорт природопользователя. Основные положения. Типовые формы

ГОСТ Р МЭК 60068-2-1—2009 Испытания на воздействие внешних факторов. Часть 2-1. Испытания. Испытание А: Холод

ГОСТ Р МЭК 60068-2-2—2009 Испытания на воздействие внешних факторов. Часть 2-2. Испытания. Испытание В: Сухое тепло

ГОСТ Р МЭК 60068-2-10—2009 Испытания на воздействие внешних факторов. Часть 2-10. Испытания. Испытание J и руководство: Грибостойкость

ГОСТ Р МЭК 60068-2-30—2009 Испытания на воздействие внешних факторов. Часть 2-30. Испытания. Испытание Db: Влажное тепло, циклическое (12 ч +12-часовой цикл)

ГОСТ Р МЭК 60068-2-78—2009 Испытания на воздействие внешних факторов. Часть 2-78. Испытания. Испытание Cab: Влажное тепло, постоянный режим

ГОСТ Р 22.0.06—95 Безопасность в чрезвычайных ситуациях. Источники природных чрезвычайных ситуаций. Поражающие факторы. Номенклатура параметров поражающих воздействий

ГОСТ Р 22.2.03—97 Безопасность в чрезвычайных ситуациях. Паспорт безопасности административно-территориальных единиц. Общие положения

ГОСТ 22.0.07—97 Безопасность в чрезвычайных ситуациях. Источники техногенных чрезвычайных ситуаций. Классификация и номенклатура поражающих факторов и их параметров

ГОСТ Р 22.0.03—95 Безопасность в чрезвычайных ситуациях. Природные чрезвычайные ситуации. Термины и определения

Global Risks 2010 A Global Risk Network Report. World Economic Forum. January, 2010

ГОСТ Р 51275—2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 53109—2008 Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности

Технический регламент о требованиях пожарной безопасности. Федеральный закон Российской Федерации № 123-ФЗ от 22.07.2008

ГОСТ Р 52551—2006 Системы охраны и безопасности. Термины и определения

ГОСТ Р 52860—2007 Технические средства физической защиты. Общие технические требования

ГОСТ 30772—2001 Ресурсосбережение. Обращение с отходами. Термины и определения

ГОСТ Р 1.0—2012 Стандартизация в Российской Федерации. Основные положения

ГОСТ Р 1.5—2012 Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения

ГОСТ Р 14.07—2005 Экологический менеджмент. Руководство по включению аспектов безопасности окружающей среды в технические регламенты

ГОСТ Р 14.08—2005 Экологический менеджмент. Порядок установления аспектов окружающей среды в стандартах на продукцию (ИСО/МЭК 64)

ГОСТ Р 14.11—2005 Экологический менеджмент. Общие требования к органам, проводящим оценку и сертификацию/регистрацию систем экологического менеджмента (ИСО/МЭК 66)

ГОСТ Р 14.12—2006 Экологический менеджмент. Интегрирование экологических аспектов в проектирование и разработку продукции

ГОСТ Р 14.13—2007 Экологический менеджмент. Оценка интегрального воздействия объектов хозяйственной деятельности на окружающую среду в процессе производственного экологического контроля

ГОСТ Р 52104—2003 Ресурсосбережение. Термины и определения

ГОСТ Р ИСО 14001—2007 Системы экологического менеджмента. Требования и руководство по применению

ГОСТ ИСО 9000—2011 Системы менеджмента качества. Основные положения и словарь

УДК 658:562.014:006.354 ОКС 07.030 Т59

Ключевые слова: риск, менеджмент риска, анализ риска, оценка риска, реестр риска, реестр опасностей, опасное событие, идентификация опасных событий, сравнительная оценка риска, обработка риска, последствие опасного события, вероятность последствия

Редактор *С.Д. Золотова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 26.03.2014. Подписано в печать 10.04.2014. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,05. Тираж 108 экз. Зак. 697.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru