Проектирование систем ПАЗ с учетом анализа опасностей и риска аварий на опасном производственном объекте

М.С. Скворцов (АО «СПИК СЗМА»)

Рассматриваются актуальные требования нормативных документов, регламентирующих создание систем противоаварийной автоматической защиты (ПАЗ). Предлагается практическая методика по реализации требований ГОСТ Р МЭК 61511 к начальным этапам проектирования систем ПАЗ с целью снижения риска аварий на опасных производственных объектах. Особое внимание уделено количественным методам оценки рисков и их распределению по слоям защиты с целью определения требований к уровню полноты безопасности контуров системы ПАЗ.

Ключевые слова: противоаварийная автоматическая защита, функциональная безопасность, проектирование, метод оценки рисков.

Одним из важнейших требований, учитываемых при создании систем ПАЗ опасных производственных объектов (ОПО), является принятие обоснованных проектных решений для обеспечения надежной и безопасной эксплуатации систем. Согласно закону о промышленной безопасности и последним редакциям федеральных норм и правил в области промышленной безопасности, обоснование выбора средств контроля, управления и ПАЗ производится по результатам анализа опасностей и риска аварий на ОПО и отражается в проектной документации. Многие из требований федеральных норм и правил (ФНиП) в области промышленной безопасности явно указывают на необходимость применения стандартов по функциональной безопасности при проектировании систем ПАЗ. Ниже приводятся данные требования с указанием номеров пунктов ФНиП «Общие правила безопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» (редакция от 02.03.2016):

- построение систем ПАЗ для объектов I и II категорий взрывоопасности на базе логических контроллеров, проверенных на соответствие требованиям функциональной безопасности (пункт 6.3.4);
- определение методов создания систем ПАЗ на основании анализа опасности и работоспособности контуров безопасности с учетом риска, возникающего при их отказе (пункт 6.3.5);
- обоснование достаточности резервирования и его типа (пункт 6.3.20);
- расчет показателей надежности систем ПАЗ для отказов типа «несрабатывание» и отказов типа «ложное срабатывание» (пункт 6.3.21).

Выполнение данных требований возможно при проведении проектирования с учетом стандарта по функциональной безопасности ГОСТ Р МЭК 61511 («Безопасность функциональная. Системы безопасности приборные для промышленных процессов»). Для применения указанных в данном стандарте подходов необходимо изменить традиционно сложившуюся практику проектирования систем ПАЗ. Необходимо использовать концепцию жизненного цикла безопасности ГОСТ Р МЭК 61511 и интегрировать ее в процесс проектирования системы ПАЗ. На рис. 1 представлены фазы жизненного цикла безопасности, которые оказывают непосредственное влияние на процесс проектирования. Рассмотрим подробно первые две фазы жизненного цикла безопасности системы ПАЗ, а именно: анализ опасностей и рисков и распределение функций безопасности по слоям защиты.

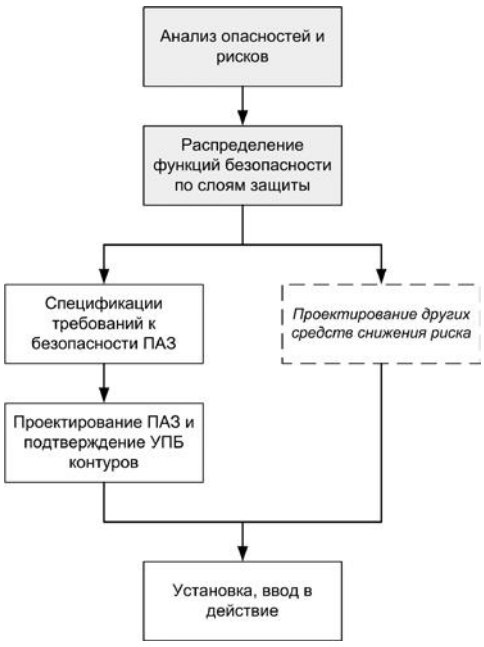

Рис. 1. Фрагмент жизненного цикла функциональной безопасности системы ПАЗ

Анализ опасностей и оценка рисков

В стандарте ГОСТ Р МЭК 61511 приводятся только общие требования к данному этапу жизненного цикла безопасности, более детально процесс анализа опасностей и оценки рисков приведен в стандартах серии «Менеджмент риска», например, в ГОСТ Р МЭК 62502-2014. «Менеджмент риска. Анализ дерева событий» и ГОСТ Р 51901.13-2005. «Менеджмент риска. Анализ дерева неисправностей». Кроме этого, для содействия соблюдению ФНиП в области промышленной безопасности Ростехнадзор разработал соответствующие методики [1, 2].

Процесс выполнения анализа риска состоит из следующих этапов:

- идентификация и сбор данных об основных опасностях;
- оценка риска с выявлением наиболее значимых факторов;
- разработка обоснованных рекомендаций по уменьшению риска.

Первым этапом при проведении анализа риска является процедура идентификации опасностей. Этот этап является важным, так как не выявленные на этом этапе опасности не будут участвовать в дальнейшем анализе. На данном этапе возможна

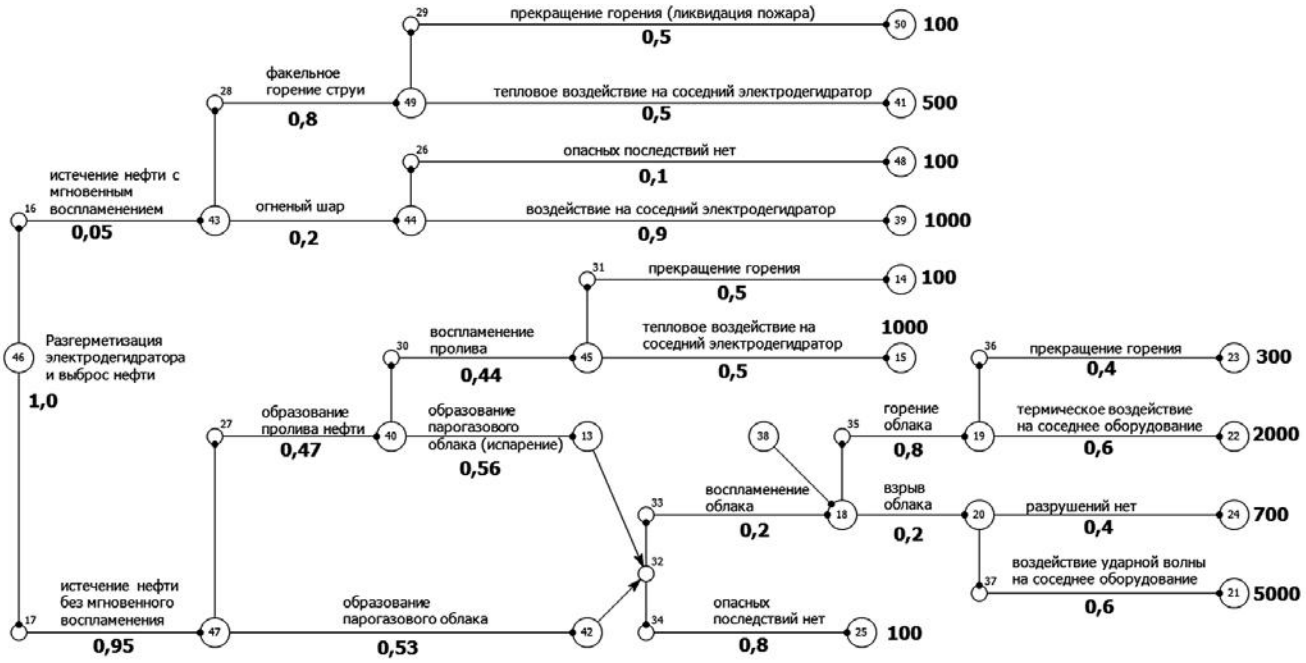

Рис. 2. Дерево событий разгерметизации электродегидратора и выброса нефти

выработка предварительных рекомендаций по уменьшению опасностей. На этапе оценки риска определяются частоты возникновения инициирующих и всех нежелательных событий, оцениваются последствия нежелательных событий, обобщаются оценки риска. На заключительном этапе разрабатываются рекомендации, в которых указываются меры по уменьшению риска или так называемые барьеры безопасности. При выборе барьеров безопасности ориентируются на достигаемое с их помощью снижение риска и величину затрат на их реализацию.

В Методике [1] (стр. 5, п. 17) в качестве приоритетных указаны методы количественной оценки риска аварий, а для оценки вероятностей инициирующих событий и возможных последствий приоритетными являются такие методы, как «анализ деревьев отказов» и «анализ деревьев событий» соответственно.

Количественный анализ риска позволяет оценить и сравнить различные опасности по единым показателям. Данный анализ наиболее эффективен:

— на стадии проектирования и размещения опасного производственного объекта;

— при обосновании и оптимизации мер безопасности;

— при оценке опасности крупных аварий на опасных производственных объектах, имеющих однотипные технические устройства (например, магистральные трубопроводы);

— при комплексной оценке опасностей аварий для людей, имущества и окружающей среды.

Проведение анализа риска даже при наличии разработанных методик без использования специализированных программных средств довольно затруднительно. К таким специализированным программным средствам относится программный комплекс (ПК) «АРБИТР» [3].

Анализ деревьев событий

Одним из способов оценки риска и анализа сценариев аварий является анализ деревьев событий. Рассмотрим пример дерева событий разгерметизации электродегидратора и выброса нефти [4]. На рис. 2 дерево событий представлено в виде схемы функциональной целостности СФЦ [5]. Рядом с каждым возможным исходом указана величина ущерба. Суммарная вероятность взаимоисключающих альтернативных вариантов развития событий равна 1. Соответствующие события попарно объединены в группы несовместных событий для учета того, что в каждый момент времени реализуется только одно событие из пары. В ПК «АРБИТР» имеется возможность объединять несколько событий в группу несовместных событий, несовместность для двух событий может быть также учтена в СФЦ при помощи инверсных выходов функциональных вершин [6].

Расчет ожидаемой величины риска проводится путем сложения произведений вероятности каждого из возможных исходов, умноженной на величину ущерба соответствующего исхода. Для случая n исходов, формула для расчета ожидаемого ущерба примет вид:

$$Wr = \sum_{i=1}^{n} p_i c_i. \qquad (1)$$

В ПК «АРБИТР» предусмотрен специальный режим расчета риска, в котором вводятся величины ущербов для каждого из возможных исходов, и автоматически происходит расчет вероятности реализации каждого исхода и вычисление ожидаемого

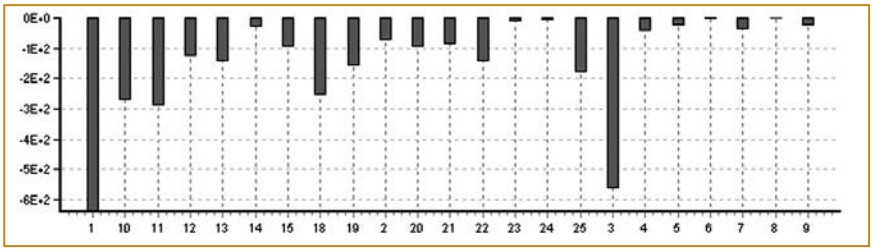

Рис. 3. Диаграмма распределения рисков по событиям дерева событий

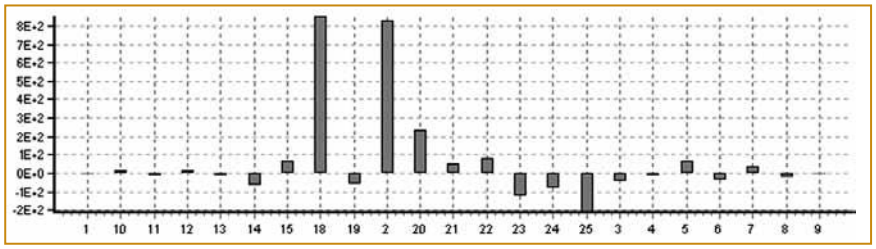

Рис. 4. Диаграмма положительных вкладов отдельных событий в величину ожидаемого риска

Таблица 1. Распределение величины риска по событиям

Номер события	Величина риска	Номер события	Величина риска
1	639,86	13	145,62
2	73,3	14	29,469
3	566,56	15	98,23
4	46	18	258,01
5	27,3	19	159,15
6	6	20	98,864
7	40	21	90,425
8	0,3	22	144,68
9	27	23	14,468
10	273,32	24	8,4396
11	293,24	25	180,85
12	127,7		

риска по формуле (1). По результатам расчета ожидаемый риск для данного дерева событий составил $Wr = 639{,}86$. Встроенные в ПК «АРБИТР» средства анализа позволяют определить распределение риска по промежуточным и конечным событиям дерева.

На рис. 3 приведена диаграмма, которая показывает количественное значение риска (ось *Y*) для каждого события (ось *X*). Из диаграммы видно, что с головным событием 1 (разгерметизация и выброс нефти) связана величина риска 639,86. Этот риск распределяется между событием 2 (истечение нефти с мгновенным воспламенением) и событием 3 (истечение нефти без мгновенного воспламенения). Риск, связанный с событием 3, равен сумме рисков, связанных с событием 10 (образование пролива нефти) и событием 11 (образование парогазового облака). При логическом объединении событий по схеме «ИЛИ» их риск суммируется, а затем распределяется по исходящим событиям. Так суммарный риск событий 11 и 13 распределяется по событиям 18 и 25. Величины рисков, связанные с событиями приведены в табл. 1. Используя эти данные можно провести анализ дерева событий и выявить наиболее опасные события и сценарии развития событий.

Дополнительно используя диаграмму положительных вкладов [5] на рис. 4, можно выделять наиболее опасные факторы, уменьшение вероятности которых приведет к максимальному снижению ожидаемого риска.

Так, например, снижение вероятности события 18 с 0,2 до 0,15 (оно вызовет увеличение вероятности события 25 с 0,8 до 0,85) уменьшит риск примерно на 8,0% до значения 588,66. Снижение вероятности события 2 с 0,05 до 1 (оно вызовет увеличение вероятности события 3 с 0,95 до 1,0) уменьшит риск примерно на 6,8% до значения 596,38.

Анализ деревьев отказов

При анализе рассмотренного ранее дерева событий предполагалось, что инициирующее событие возникает с вероятностью 1. Для точного определения вероятности вершинного события дерева событий необходимо провести анализ дерева неисправностей (отказов), приводящего к данному событию. Рассмотрим дерево отказов, которое содержит причины, приводящие к разгерметизации электродигедратора и выбросу нефти, представленное в виде СФЦ на рис. 5.

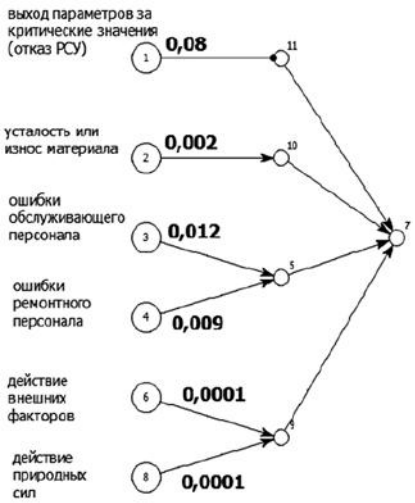

Рис. 5. Дерево отказов электродигедратора

Результат расчета дерева отказов дает вероятность 0,101202 для вершинного события. Диаграмма отрицательных вкладов на рис. 6 позволяет легко определить события, уменьшение вероятности которых окажет наибольшее влияние на общую вероятность отказа.

В данном примере отказ РСУ с последующим выходом параметров за критические значения оказывает самое сильное влияние на общую вероятность отказа. Снижение вероятности данного события с помощью слоя защиты (например, контура системы ПАЗ) будет самым эффективным решением.

Таким образом, при помощи дерева отказов происходит определение вероятности инициирующего события дерева событий.

Быстрее всего настигает та опасность, которой пренебрегают.
Публий Сир

Распределение функций безопасности по слоям защиты

При использовании количественных методов анализа риска, одним из методов распределения функций безопасности по слоям защиты является метод анализа диаграмм «галстук-бабочка». Метод основан на совместном анализе деревьев отказов и деревьев событий. Рассмотрим схему функциональной целостности, приведенную на рис. 7, которая позволяет выполнить распределение рисков по слоям защиты при помощи метода построения диаграммы «галстук-бабочка» и анализа барьеров безопасности. Барьеры безопасности — это методы и средства, предназначенные для предотвращения, контроля или смягчения нежелательных событий. Иначе говоря, барьеры безопасности (слои защиты) уменьшают риск за счет ослабления последствий нежелательных событий или за счет снижения вероятности их возникновения.

Проведем распределение риска по слоям защиты с помощью добавления на диаграмму «галстук-бабочка» трех слоев защиты (вершины 49, 50, 51, выделенные цветом). Первый слой защиты — это система ПАЗ, которая снижает вероятность возникновения инициирующего события разгерметизации и выброса нефти в результате отказа распределенной системы управления и выхода технологических параметров за критические значения. Второй слой защиты снижает вероятность воспламенения облака, образовавшегося в результате истечения нефти без мгновенного воспламенения. Третий слой защиты уменьшает результаты теплового воздействия на соседний электродигедратор. ПК «АРБИТР» позволяет оценить теоретический предел снижения риска каждого барьера в отдельности. Для этого рассчитаем величину риска с добавленными в схему слоями защиты, при этом эффективность барьеров задана равной нулю. СФЦ на рис. 7 фактически объединяет вероятность возникновения инициирующего события и его последствия. По результатам моделирования и расчета, получаем ожидаемый риск, равный 64,8.

Слои защиты, представленные в СФЦ вершинами 49, 50, 51, имеют отрицательные значения положительных вкладов (рис.8), то есть уменьшают величину риска с увеличением их эффективности (надежности или степени ослабления последствий). Отрицательные значения положительных вкладов дают теоретический предел уменьшения риска, который достижим при 100% эффективности слоя защиты (например, если бы надежность системы ПАЗ могла бы быть 1). Числовые значения теоретического предела снижения риска для слоев защиты следующие: система ПАЗ (вершина 49) — на 50 (-77,2%); барьер защиты 1 (вершина 50) — на 26,1 (-40,3%); барьер 2 (вершина 51) — 21,42 (-33.1%). Это позволяет определить очередность реализации и определить экономический эффект от реализации слоя защиты. В нашем случае, максимального снижения риска можно достичь от внедрения слоя защиты в виде системы ПАЗ.

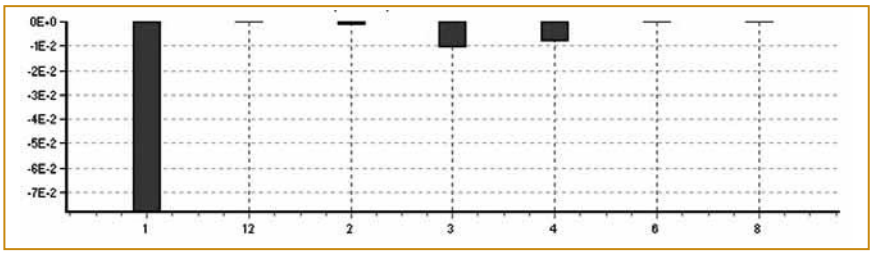

Рис. 6. Диаграмма отрицательных вкладов отдельных событий в вероятность отказа электродигедратора

Следует отметить отрицательное значение положительного вклада события 25, которое не является слоем защиты. Это связано с тем,

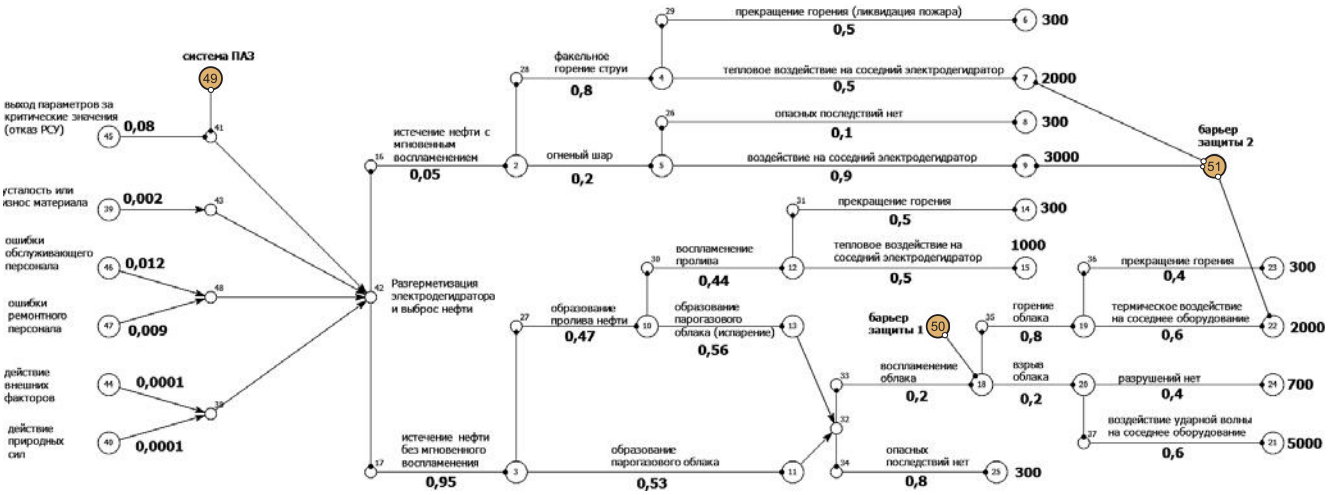

Рис. 7. Диаграмма «галстук-бабочка» с барьерами безопасности (слоями защиты)

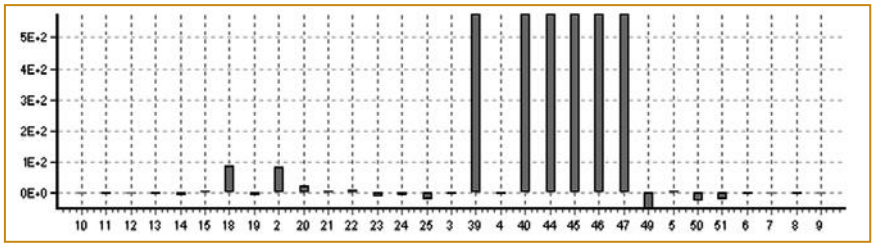

Рис. 8 Диаграмма положительных вкладов событий и слоев защиты в величину ожидаемого риска

Таблица 2. Расчет снижения риска для вариантов первого слоя защиты

Система ПАЗ		Слой защиты 1		Слой защиты 2	
Надежность	Снижение риска	Надежность	Снижение риска	Надежность	Снижение риска
SIL 1 (PFD = 0,04)	-74,1%	0,50	-20,2%	0,50	-16,6%
SIL 2 (PFD = 0,007)	-76,7%	0,75	-30,2%	0,75	-24.8%

Таблица 3. Расчет снижения риска для вариантов второго слоя защиты

Слой защиты ПАЗ		Слой защиты 1		Слой защиты 2	
Надежность	Снижение риска	Надежность	Снижение риска	Надежность	Снижение риска
–		0,50	-20,2%	0,50	-16,6%
SIL 2 (PFD = 0,007)	-9,9%	0,75	-30,2%	0,75	-24.8%

что увеличение вероятности рассеяния парогазового облака без опасных последствий (событие 25), автоматически уменьшает вероятность парного несовместного события воспламенения парогазового облака (событие 18). Так как последствия реализации события 18 несут на порядок большие риски, то, с точки зрения уменьшения риска, выгодно увеличение вероятности реализации события 25 и, как следствие, снижение вероятности реализации события 18. Таким образом, для нашего примера наиболее эффективным будет реализация слоя защиты в виде контура системы ПАЗ.

Предположим, что первый добавленный слой защиты — это контур системы ПАЗ имеет уровень полноты безопасности (УПБ) равный 1 и вероятность отказа на запрос, равную 0,04. Это позволяет снизить риск примерно на 74%, до значения 16,75. Для обоснованного выбора следующего слоя защиты необходимо использовать таблицу 3, а в качестве значения целевого остаточного риска использовать величину допустимого риска. Отметим что, для более точной оценки эффекта от применения слоя защиты необходимо учитывать его стоимость.

Заключение

В соответствии с нормативными документами в области безопасности проектирование систем ПАЗ необходимо проводить с учетом анализа опасностей и риска аварий на опасном производственном объекте. На начальных этапах жизненного цикла безопасности необходимо идентифицировать опасности и провести оценку их риска, то есть оценить вероятность их возникновения и возможные последствия. Эти мероприятия являются фундаментом для распределения рисков по слоям защиты с целью назначения уровня полноты безопасности контурам системы ПАЗ. Для количественной оценки риска рекомендуется применять методы анализа деревьев событий и деревьев отказов. Метод анализа «галстук-бабочка» (bow-tie) объединяет эти два подхода и позволяет обоснованно осуществить выбор и оценить эффективность слоев (барьеров) защиты, определить очередность их реализации. Использование аттестованных специализированных программных средств позволяет упростить проведение расчета риска и анализа эффективности слоев защиты, назначить требуемые уровни полноты безопасности контурам системы ПАЗ. После назначения требуемых уровней полноты безопасности контурам системы ПАЗ можно переходить на последующие этапы жизненного цикла безопасности — создание спецификации требований к безопасности, разработка и проектирование системы ПАЗ.

Список литературы

1. Руководство по безопасности «Методические основы по проведению анализа опасностей и оценки риска аварий на опасных производственных объектах». Серия 27. Вып. 16. М: ЗАО «Научно-технический центр исследований проблем промышленной безопасности». 2016. 56 с.
2. Руководство по безопасности «Методика оценки риска аварий на опасных производственных объектах нефтегазоперерабатывающей, нефте- и газохимический промышленности». Серия 09. Вып. 45. М: ЗАО «Научно-технический центр исследований проблем промышленной безопасности». 2016. 44 с.
3. *Можаев, А.С.* Аннотация программного средства «АРБИТР» (ПК АСМ СЗМА) // Вопросы атомной науки и техники. Серия «Физика ядерных реакторов». Раздел «Аннотации программных средств, аттестованных Ростехнадзором РФ»: науч.-техн. сб. М. : РНЦ «Курчатовский институт». 2008. Вып. 2. С. 105-116.
4. *Глухова А.В., Бич А.Н., Зубанев В.В. и др.* Анализ опасности на примере атмосферно-вакуумной комбинированной установки с электрообессоливанием (ЭЛОУ АВТ) // Актуальные вопросы промышленной безопасности и развития промышленных технологий. 2015. Вып. 1.С. 134-149.
5. *Можаев, А.С.* Технология автоматизированного структурно-логического моделирования надежности, живучести, безопасности, эффективности и риска функционирования систем // Приборы и системы, Управление, Контроль, Диагностика. 2008. №9. С. 1-14.
6. *Нозик А.А., Струков А.В., Можаева И.А.* Программная реализация методов количественного анализа риска аварий опасных производственных объектов на основе логико-вероятностного и логико-детерминированного подходов // Наука и безопасность. 2016. №1. С. 26-36.

Скворцов Михаил Сергеевич *– канд. техн. наук, ведущий инженер-программист АО «СПИК СЗМА».*
Контактный телефон: (812) 610-78-79.
E-mail: mikhail_skvortsov@szma.com