

УДК 629.039.58

## **АЛГОРИТМ СНИЖЕНИЯ РИСКА И СИСТЕМЫ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ**

*Гоголь Я.В., студент*

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана  
кафедра «Экология и промышленная безопасность»*

*Сладкова К.Д., студент*

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана  
кафедра «Экология и промышленная безопасность»*

*Научный руководитель: Переездчиков И.В., д.т.н., профессор кафедры «Экология и промышленная безопасность» МГТУ им. Н.Э. Баумана*

*[E9@mx.bmstu.ru](mailto:E9@mx.bmstu.ru)*

### **Идеализированная модель объекта и алгоритм анализа опасностей**

Практически все технические объекты можно рассматривать на базе идеализированной модели системы «человек – среда – машина». СЧМС в общем случае представляет собой совокупность иерархически зависимых систем, содержащих персонал, технику, среду, объединенных между собой вещественными и информационными связями сообразно действующей иерархии целей, в целях функционирования всей системы как единого целого. СЧМС часто рассматривают как систему, состоящую из операторов и техники, взаимодействующих по определенной программе, и производственной среды, определяющей условия работы [1]. Главным звеном СЧМС, независимо от степени её автоматизации, является человек, который ставит цели, планирует и контролирует процесс её функционирования. Таким образом, подсистему (компонент) «человек» целесообразно наделять функциями *системы управления*.

Подсистема «человек» понимается и трактуется как система управления подсистемой «машина», и в частности как система управления опасностями.

Подсистема «машина» в общем случае включает в себя техническую систему (механическую) и персонал (операторов).

Что касается подсистемы «среда», то, вообще говоря, её элементами могут быть внешняя среда, производственная среда, рабочие среды и социальная среда, влияющие на состояние СЧМС. За границей СЧМС начинается внешняя среда.

Для анализа опасностей СЧМС, который выполняется на базе четкой логики и теории вероятности, можно предложить алгоритм, представленный на рисунке 1.

Основной процесс анализа опасностей и аварийных ситуаций осуществляется на стадии проектирования системы [2]. Именно на этой стадии необходимо прогнозировать уровни опасностей, а также сделать заключение о том будет ли этот прогноз оставаться в заданных пределах.

### **Понятие функциональной безопасности**

Определим функциональную безопасность как часть общей безопасности системы или элемента (оборудования), которая требует, чтобы система или элемент работали заданным образом в ответ на получаемые ими воздействия. Последние могут включать в себя ошибки операторов, отказы оборудования или воздействия со стороны окружающей среды. Целью безопасности является защита людей от причинения им вреда. Функциональная безопасность достигает этой цели, используя системы, снижающие вероятность чепе<sup>1</sup> и уменьшающие неблагоприятные последствия.

Функциональная безопасность, внедренная в машину, обычно означает существование систем, которые осуществляют мониторинг безопасности, а при необходимости отключают рабочие операции машин для обеспечения безопасности. Иначе говоря, компонент «машина» имеет встроенную систему функциональной безопасности (СФБ), которая выполняет требуемые функции безопасности, т.е. защиты, диагностируя опасные состояния и переводя, при необходимости, процесс в безопасное состояние с помощью нужного действия. СФБ применяются в процессах и машинах для обеспечения последних функциями, гарантирующими безопасность, например такими функциями, как безопасный останов, аварийное отключение, обнаружение возгорания, продувка ресиверов для освобождения от горючих газов и т.д.

---

<sup>1</sup> Чепе - нежелательное, незапланированное событие, нарушающее обычный ход вещей и происходящее на практике в относительно короткий отрезок времени.

<http://sntbul.bmstu.ru/issue/634797.html>

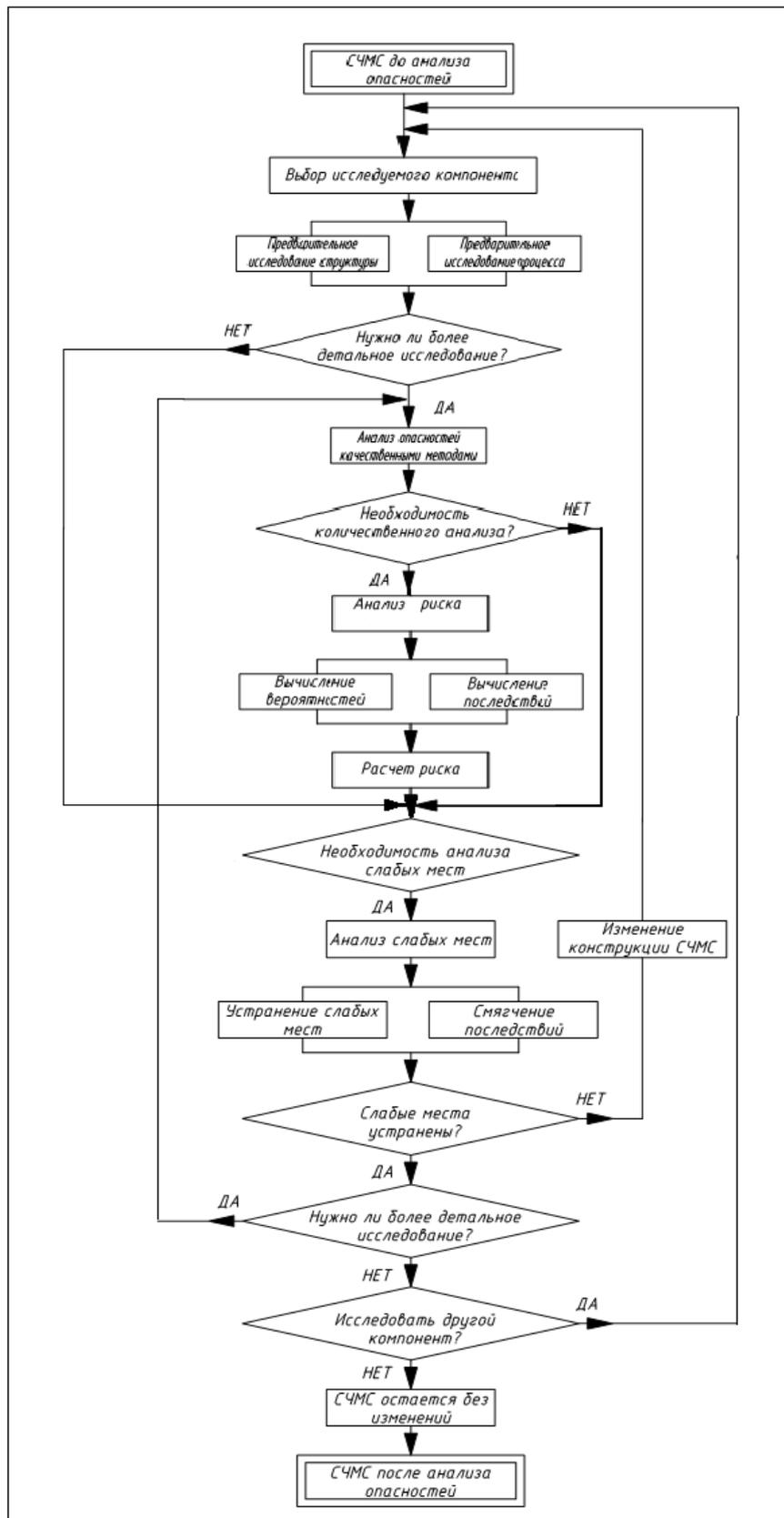


Рис. 1. Алгоритм анализа опасностей СЧМС

Для достижения функциональной безопасности необходимы следующие шаги: оценка риска; идентификация требуемых функций безопасности, снижающих риск; практическая реализация этих функций и обеспечения их надежного выполнения [3].

В соответствии с международными стандартами функциональная безопасность достигается как минимум следующими шагами:

1. Идентификацией опасностей и требуемых функций безопасности. Для этого обычно используются качественные методы анализа опасностей;

2. Оценкой величины снижения риска, на которую будет рассчитана функция безопасности. Это означает определение встроенного уровня снижения риска (ВУСР), при этом ВУСР относится ко всей встроенной функции безопасности (ВФБ), т.е. ко всем элементам СФБ;

3. Гарантированным обеспечением работоспособности ВФБ в соответствии с заданным конструкторским замыслом даже в условиях появления на входе сигналов об отказах или ошибках операторов;

4. Верификацией того, что система отвечает установленному ВУСР путем определения средней наработки между отказами и вероятности отказобезопасности (ВОБ) наряду с проведением необходимых испытаний. ВОБ есть вероятность того, что система безопасно откажет, при этом опасные (или критические) состояния определяются при применении к системе анализа видов и последствий отказов (АВиПО) или анализа видов, последствий и критичности отказов (АВиПКО) [4];

5. Проведением экспертиз состояния ФСБ, чтобы убедиться в том, что техника обслуживания системы в течение всего жизненного срока осуществляется планомерно и в полном объеме.

ВУСР есть статистическая величина, характеризующая надежность ФСБ во время запроса на выполнение функции безопасности. ВУСР коррелирует с вероятностью отказа при запросе, которая эквивалентна вероятности неготовности системы во время процесса запроса.

### **Этапы оценки риска и методология его снижения**

Опасность машин можно определить в результате выполнении следующих этапов (рисунок 4):

этап 1. Наложение граничных условий в виде определения:

- требований к машине на всех стадиях жизненного цикла;
- предназначения выполняемых операций и видимых неисправностей;
- ограничений на управление машиной, обусловленные, например, полом, возрастом, доминирующей рукой, физическими возможностями (зрением, слухом, размерами, силой);
- необходимого уровня тренировки, опыта работы, компетенции;
- последствий возможности воздействия на людей опасных и вредных факторов.

этап 2. Анализ опасностей. Анализ опасностей означает идентификацию всех опасных состояний и всех цепе, связанных с машиной, при этом используют качественные методы анализа: контрольный листы, АВиПО, АВиПКО, НАЗОР, метод «что если» и другие [4].

этап 3. Определяются составляющие риска: вероятности чепе и размер последствий;

этап 4. В результате оценивания риска определяют необходимость его снижения и те меры, которые следует при этом использовать.

Процесс организации функциональной безопасности в основных чертах представлен на рисунке 2.

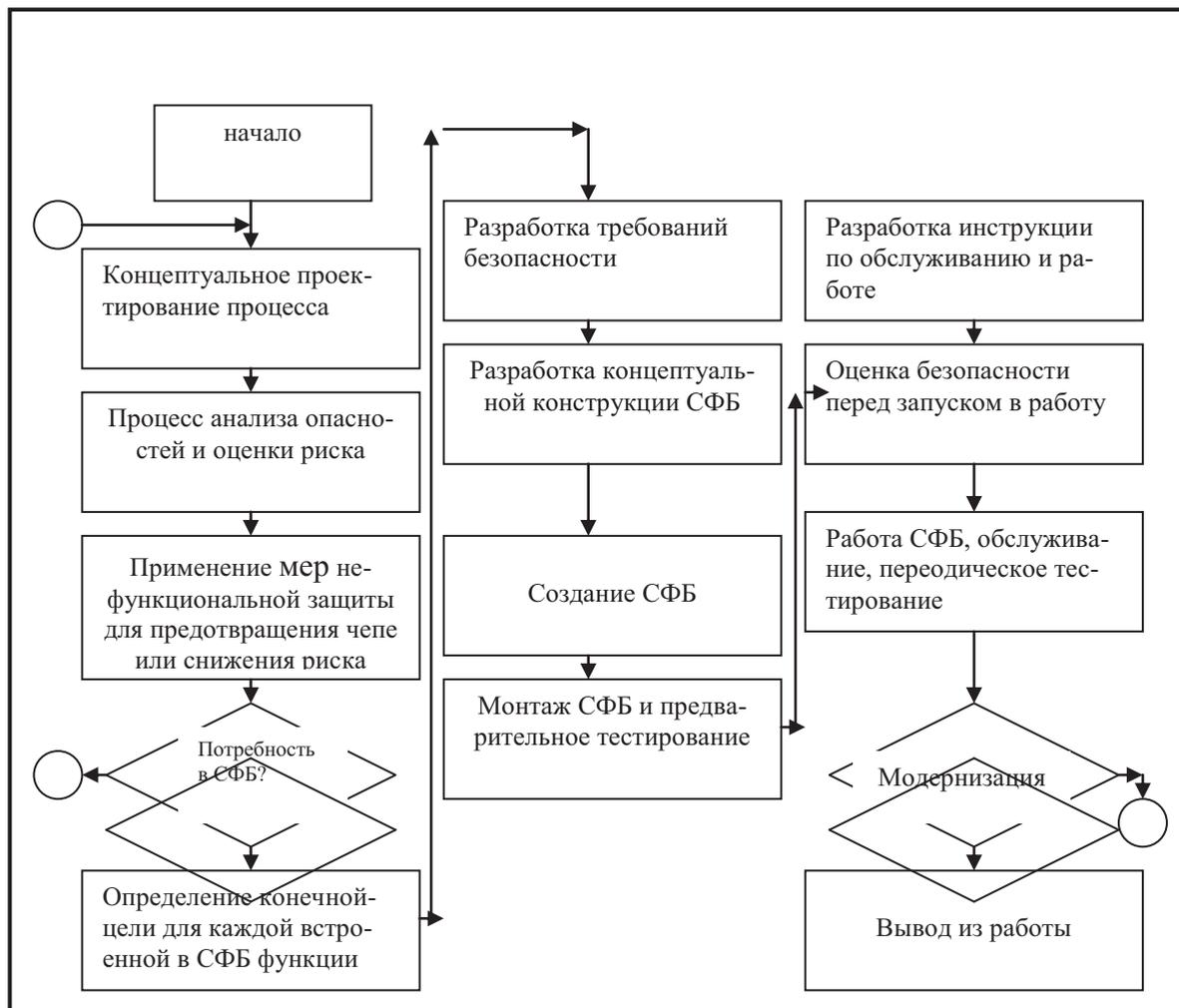


Рис. 2. Процесс организации функциональной безопасности

Величину потенциального риска, генерируемого машиной, оценивают в соответствии со стандартом, после чего принимаются меры по его снижению (рисунок 3). Снижение риска достигается за счет непосредственно конструкционных решений и при использовании защитных устройств. Сначала, внедряются конструкционные решения, для чего устанавливается категория безопасности исходя из частоты и тяжести потенциального несчастного случая, т.е. конструкционные меры безопасности выбирают руководствуясь двумя факторами: степенью

тяжести несчастного случая (легкое или сильное повреждение) и частотой рассматриваемого чепе (изменяется от значения «никогда» до оценки «постоянно, всегда» [3].

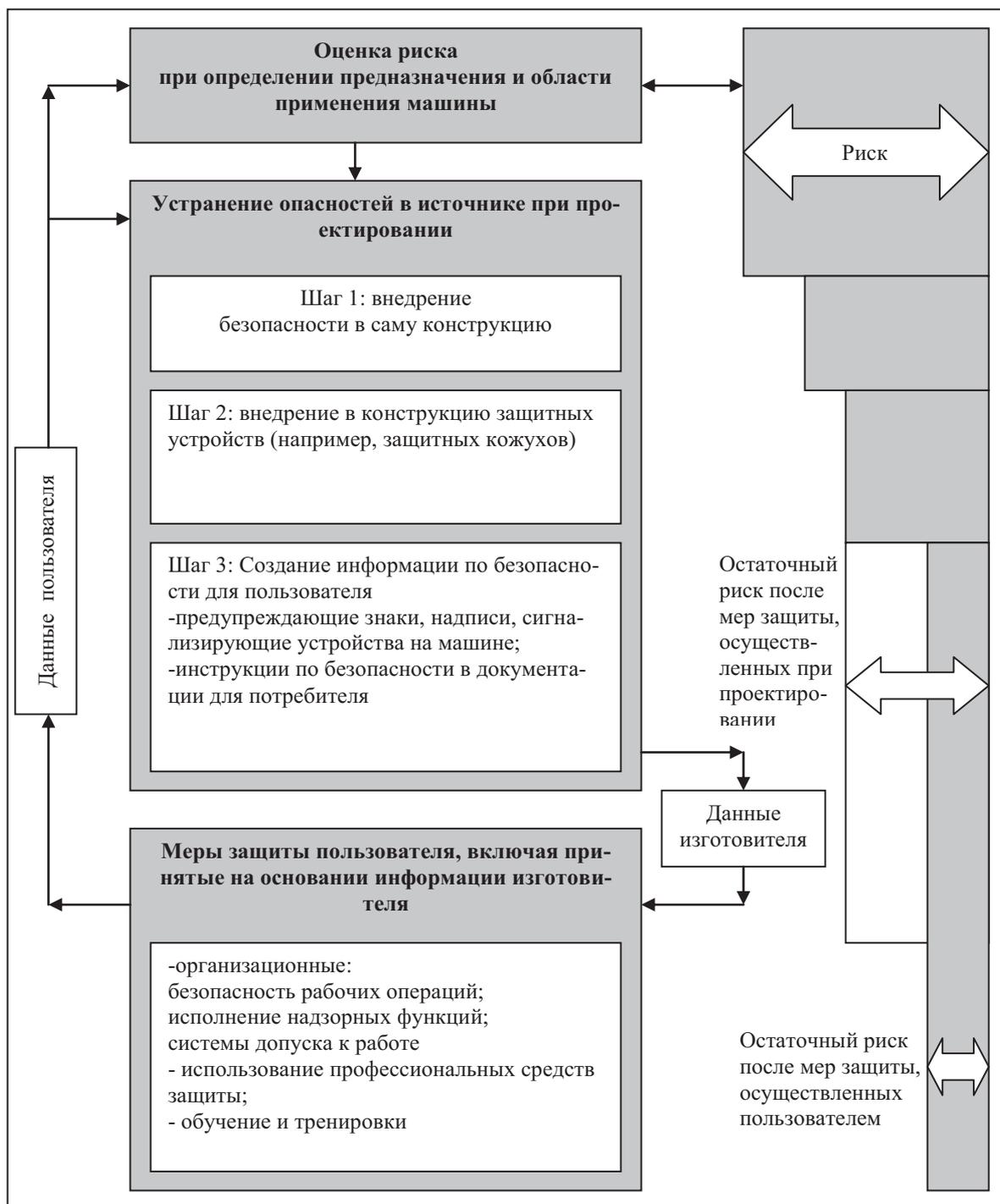


Рис. 3. Алгоритм снижения риска на стадии создания и эксплуатации компонента «машина»

Таким образом, анализ опасностей выполняют качественными и количественными методами и, определив при этом необходимость снижения риска, используют встроенные системы функциональной безопасности, которые диагностируют опасные состояния и осуществляют при необходимости безопасные операции.

### Список литературы

1. Переездчиков И.В. Анализ опасностей промышленных систем человек-машина-среда и основы защиты. М.: Кнорус, 2011. 784 с.
2. Северцев Н.А. Метод количественного анализа опасности сложных систем на основе теории множеств // Вопросы теории безопасности и устойчивости систем. 2006. № 8. С. 5-17.
3. Переездчиков И.В. Методология анализа опасности сложных технических систем на базе четких и нечетких множеств// Химическое и нефтегазовое машиностроение. 2005. № 7. С. 39-41.
4. ГОСТ Р 51901.13-2005. Менеджмент риска. Анализ дерева неисправностей. М., 2005. 16с.