УДК 51-74

МЕТОДОЛОГИЯ АУДИТА ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ЭКСПЛУАТИРУЕМЫХ СИСТЕМ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ

Ирина Александровна Можаева, к.т.н. (ООО «НТЦ СЗМА»),
Александр Абрамович Нозик, к.т.н. (АО «СПИК СЗМА»),
Александр Владимирович Струков доцент, к.т.н. (АО «СПИК СЗМА»)

В отличие от экспертизы промышленной безопасности, целью которой является определение соответствия объектов экспертизы промышленной безопасности, указанных в ФЗ №116 (пункт 1, ст. 13), предъявляемым к ним требованиям промышленной безопасности, целью аудита эксплуатируемых систем противоаварийной автоматической защиты (ПАЗ) является оценка степени их пригодности для выполнения возложенных на них задач.

Работы по аудиту систем ПАЗ включают в себя:

- получение достоверных сведений и оценка фактического технического состояния оборудования систем ПАЗ;
- получение объективной информации о соответствии систем ПАЗ действующим и перспективным нормативным требованиям;
- разработка рекомендаций по приведению систем ПАЗ, включая документацию к ним и процедуры эксплуатации, к требованиям норм и правил.

Аудит эксплуатируемых систем ПАЗ опасных производственных объектов (ОПО) – это независимое обследование системы ПАЗ на эксплуатируемых ОПО специалистами, квалифицированными в области промышленной и функциональной безопасности.

В общем виде порядок проведения аудита эксплуатируемых систем ПАЗ показан на рис.1.

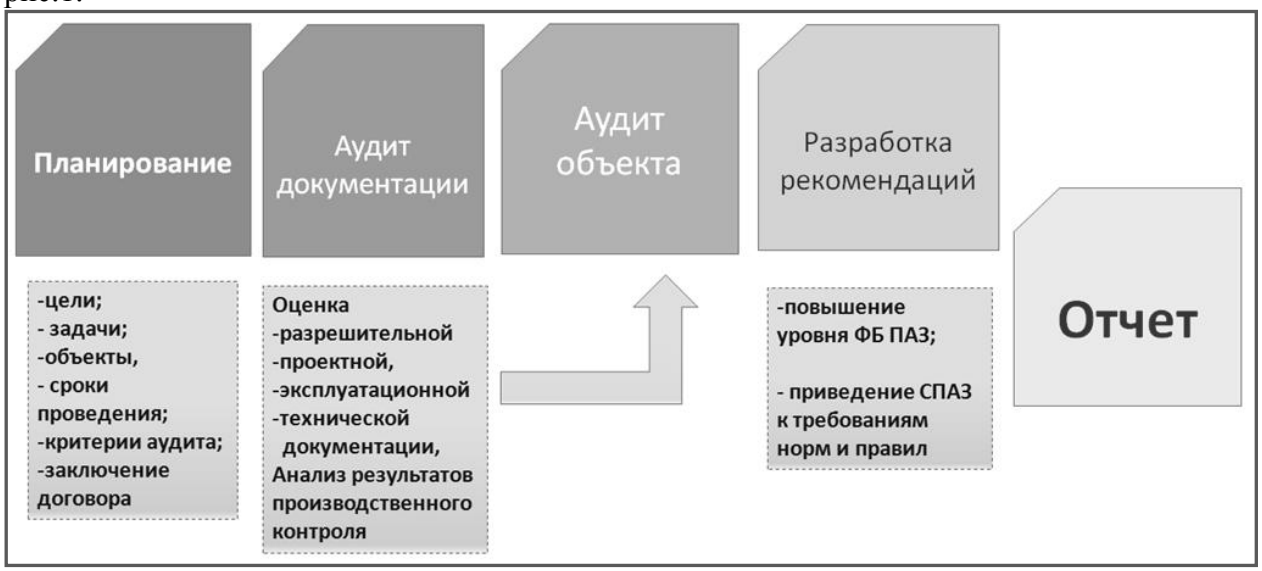

Рисунок 1 – Порядок проведения аудита эксплуатируемых систем ПАЗ

Если по результатам аудита системы ПАЗ выявляются отклонения от требований нормативных документов, например, Федеральных норм и правил (ФНиП), то требуется проведение анализа опасности и работоспособности (АОР) либо технологической части объекта, либо контуров безопасности, реализующих соответствующие функции безопасности.

Результатом этих работ может быть дооснащение объекта средствами контроля, автоматического регулирования, устройствами взрывопредупреждения и взрывозащиты, быстродействующими отсекателями, системами безопасной аварийной остановки объекта, оповещения, защиты и спасения людей или проведение других мероприятий.

При недостаточности этих мероприятий может быть принято решение о внедрении/доработке системы ПАЗ. При этом согласно требованиям ФНиП [1], должен быть проведен расчет надежности ПАЗ с учетом отказов двух типов – отказов типа «несрабатывание» и отказов типа «ложное срабатывание». Методы и средства проектирования/доработки систем ПАЗ выбирают на основе анализа опасностей, возникающих при эксплуатации технологических объектов, условий возникновения и развития возможных аварийных ситуаций, особенностей технологических процессов и аппаратурного оформления [2].

Центральным понятием международных стандартов серии МЭК 61508 и 61511 является концепция жизненного цикла функциональной безопасности (ЖЦ ФБ). Практика разработки и эксплуатации систем ПАЗ показала, что на всех этапах ЖЦ ФБ присутствуют типовые ошибки, выявление и устранение которых является одной из задач аудита ПАЗ.

Основные этапы ЖЦ ФБ систем ПАЗ (СПАЗ) показаны на рис.2.

Рисунок 2 – Этапы жизненного цикла систем ПАЗ

Каждый этап ЖЦ ФБ характеризуется входными и выходными мероприятиями и документами.

На рис. 3 показан этап 1 ЖЦ ФБ и его выходные и выходные мероприятия.

Рисунок 3 – Этап 1 жизненного цикла систем ПАЗ

Основными типовыми ошибками реализации этапа 1 ЖЦ ФБ являются:

- использование упрощённого перечня нормативной документации;
- отсутствие обоснования приемлемого уровня риска.

Для устранения указанных ошибок необходимо использование полного перечня нормативной документации и обоснование приемлемого уровня риска.

На рис. 4 показан этап 2 ЖЦ ФБ, его выходные и входные мероприятия и основные нормативные документы, используемые при его реализации.

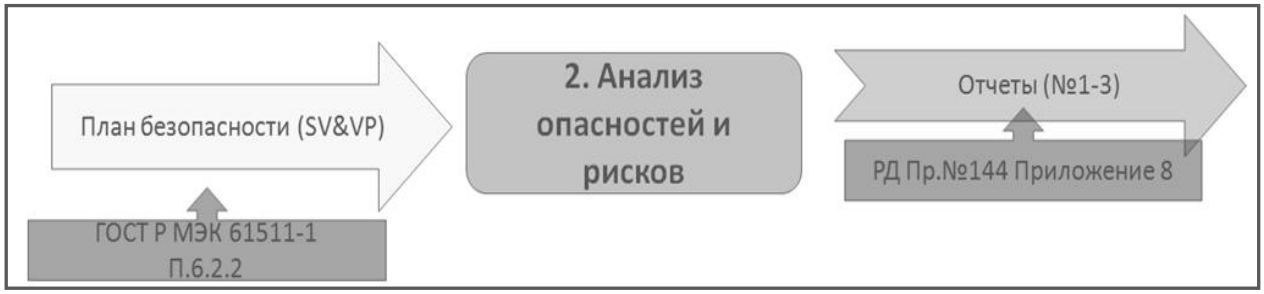

Рисунок 4 – Этап 2 жизненного цикла систем ПАЗ

Основными типовыми ошибками реализации этапа 2 ЖЦ ФБ являются исключение или формальный подход к анализу рисков, а также не включение в Декларацию о промышленной безопасности и планы ликвидации аварий результатов АОР.

Для устранения указанных ошибок необходимо:

- использование нормативных документов по анализу рисков;
- уточнение целей и границ анализа опасностей;
- выполнение АОР технологического объекта [3];
- выполнение анализа требуемого уровня полноты безопасности (УПБ/SIL) слоя защит (ПАЗ);
- выполнение анализа опасности с учётом риска, возникающего при отказе контура безопасности;
- включение результатов анализа АОР в Декларацию промышленной безопасности и планы ликвидации аварий.

На рис. 5 показан этап 3 ЖЦ ФБ и его входные и выходные мероприятия

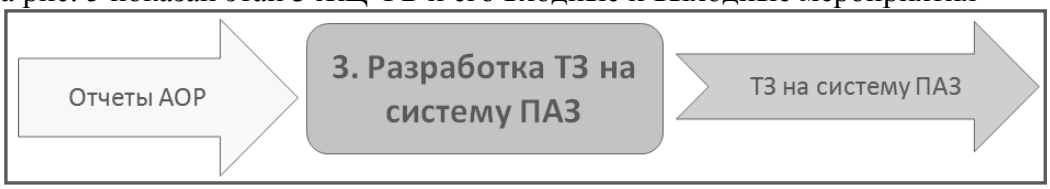

Рисунок 5 – Этап 2 жизненного цикла систем ПАЗ

Основными типовыми ошибками реализации этапа 3 ЖЦ ФБ являются:

- выбор и внедрение технических средств с ограниченной диагностикой и непредсказуемым поведением вследствие отказов;
- отсутствие учёта требований положения (состояния) исполнительного механизма при отказе аппаратных средств или потере питания;
- отсутствие полноты независимости системы ПАЗ от других систем, не связанных с безопасностью (отсутствие сегментации управляющих сетей, общие электрические цепи с основной системой управления (СУ), невозможность запуска алгоритмов ПАЗ без человеко-машинного интерфейса основной СУ);
- отсутствие учёта специфики аппаратных средств системы ПАЗ (отсутствие аппаратной фильтрации входных сигналов, обработка сигналов по мажоритарной схеме, автоматическое периодическое кратковременное тестирование выходных сигналов);
- отсутствие полных, однозначных и верифицируемых описаний алгоритмов логических схем блокировки для прикладного программирования.

Для устранения указанных ошибок необходимо осуществить:

- подбор технических средств, соответствующих требованиям к надёжности (в том числе, в терминах УПБ/SIL) и быстродействию;
- подтверждение соответствия контуров безопасности требованиям к надёжности (в том числе, в терминах УПБ/SIL) и быстродействия расчётом;
- внесение изменений в проект для учёта требований к положению (состоянию) исполнительного механизма при отказе аппаратных средств или потере питания;

- внесение изменений в проект для обеспечения полноты независимости системы ПАЗ от других систем, не связанных;

- внесение изменений в проект для учёта специфики аппаратных средств ПАЗ (аппаратная фильтрация входных сигналов, обработка сигналов по мажоритарной схеме, автоматическое периодическое кратковременное тестирование выходных сигналов).

Для 5-го этапа ЖЦ ФБ (сборка и программирование системы ПАЗ) характерны следующие типовые ошибки:

- использование в качестве исходных данных для программирования неполных, неоднозначных и неверифицируемых описаний алгоритмов;

- программирование без учёта необходимости безопасной реакции системы ПАЗ при отказе различных аппаратных средств;

- возможность недетерминированного отключения алгоритмов безопасности (ПАЗ) из небезопасной системы (основной СУ);

- несоответствие маркировки нормативным требованиям и проектным решениям или отсутствие маркировки.

Для устранения указанных ошибок необходимо выполнить:

- устранение несоответствия между конструкторской документацией и фактическим состоянием аппаратной части;

- устранение несоответствия между ЛСБ и фактическим состоянием прикладного ПО;

- доработку прикладного ПО с учётом необходимости обеспечения безопасной реакции системы ПАЗ при отказе различных аппаратных средств;

- доработку прикладного ПО для исключения возможности недетерминированного отключения алгоритмов безопасности (ПАЗ) из небезопасной основной СУ.

При планировании испытаний (этап 6 ЖЦ ФБ) к типовым ошибкам относят отсутствие плана и методик испытания системы ПАЗ и формальное описание методики испытания функций безопасности.

Для устранения этих ошибок необходимо разработать следующие документы:

- Методики проверочных испытаний;
- Программу и методики автономных испытаний;
- Методики индивидуальных испытаний для внешних устройств;
- Программы и методики комплексных и приёмочных испытаний.

Предварительные заводские автономные испытания (этап 7 ЖЦ ФБ) характеризуются такими типовыми ошибками как пропуск стадии заводских (автономных) испытаний центральной части системы ПАЗ и отсутствие формализованной сверки загруженного программного обеспечения с проектной документацией. Для устранения этих ошибок необходимо проведение автономных (заводских) испытаний центральной части системы ПАЗ (в случае выполнения реконструкции (глубокой модификации) системы ПАЗ) и формализованная сверка загруженного прикладного ПО.

При проведении монтажа системы ПАЗ (этап 8 ЖЦ ФБ) возникают следующие типовые ошибки:

- нарушение технологии монтажа (негерметичные кабельные вводы, отсутствие крепления кабелей, прокладка кабелей с нарушением требований электромагнитной совместимости, отсутствие герметичности в импульсных линиях, прямое отступление от схем монтажа и т.д.);

- отсутствие формализованной проверки функций безопасности «от трубы до трубы»;

- отсутствие исполнительной документации (As-build);

- отсутствие оценки функциональной безопасности системы ПАЗ экспертом с необходимой степенью независимости;

- отсутствие приёмо-сдаточной рабочей комиссии, уполномоченной приказом заказчика;

- выполнение пусковых операций (появление установленных опасностей) до подтверждения соответствия функциональной безопасности системы ПАЗ и приёмки её в промышленную эксплуатацию.

Для устранения этих ошибок необходимо осуществить:

- устранение нарушений технологии;
- подготовку исполнительной документации;
- проведение формализованной проверки (испытания) функций безопасности «от трубы до трубы»;
- оценку функциональной безопасности системы ПАЗ экспертом с необходимой степенью независимости;
- создание приёмо-сдаточной рабочей комиссии, уполномоченной приказом заказчика, подтверждения соответствия функциональной безопасности системы ПАЗ;
- выполнение пусковых операций после подтверждения соответствия функциональной безопасности системы ПАЗ и приёмки её в промышленную эксплуатацию.

В процессе промышленной эксплуатации и технического обслуживания систем ПАЗ (этап 9 ЖЦ ФБ) ошибочно допускается пуск и эксплуатация ОПО с неактивными функциями безопасности в системе ПАЗ (деблокирование) и внесение изменений (модификация) системы ПАЗ без всестороннего анализа влияния на безопасность.

Для устранения этих ошибок необходимо осуществить:

- пуск и эксплуатацию ОПО, эксплуатацию системы ПАЗ с активными функциями безопасности (без отключения функций безопасности/защиты);
- проведение проверочных испытаний;
- учёт запросов функций безопасности и отказов компонентов системы ПАЗ;
- выполнение документированного анализа влияния на безопасность вносимых изменений (модификации) в систему ПАЗ;
- периодический аудит систем ПАЗ ОПО**.**

В табл.1 приведены отдельные несоответствия (типовые проектные ошибки), связанные с несоблюдением требованием ФНиП [1] и способы устранения.

Таблица 1 – Типовые проектные ошибки

Типовая проектная ошибка	Способ устранения
Системы ПАЗ не функционируют независимо от системы управления технологическим процессом. Нарушение работы системы управления влияет на работу системы ПАЗ	Доработать проект системы ПАЗ для обеспечения независимости функционирования ПАЗ, устранить общие точки отбора, датчики, барьеры искробезопасности, модули, блоки питания, цифровые шины (использующиеся для выполнения функций безопасности)
Для взрывоопасных технологических процессов проектируются системы ПАЗ, не предупреждающие возникновение аварии при отклонении от предусмотренных технологическим регламентом на производство продукции предельно допустимых значений параметров процесса во всех режимах работы	На основании анализа рисков технологического процесса разработать логические схемы блокировок, предупреждающие возникновение аварии во всех режимах работы процесса
Методы создания систем ПАЗ определяются без обоснования с помощью анализа опасности и работоспособности контуров безопасности с учётом риска, возникающего при отказе контура безопасности	Выполнить обоснование проектных решений по системе ПАЗ с помощью анализа опасности и работоспособности контуров безопасности с учётом риска, возникающего при отказе контура безопасности
В системе ПАЗ используются датчики, которые используются в других подсистемах АСУТП ОПО	В проекте системы ПАЗ исключить использование датчиков, которые используются в других подсистемах АСУТП ОПО
Достаточность резервирования и его тип в системе ПАЗ не обосновывается разработчиком проекта	В проекте системы ПАЗ обосновать степень резервирования и его тип

Типовая проектная ошибка	Способ устранения
В системе ПАЗ используются исполнительные устройства, которые применяются в других подсистемах АСУТП ОПО	В проекте системы ПАЗ исключить использование исполнительных устройств подсистем АСУТП ОПО
Не определены вероятности для типов отказов: отказов типа «несрабатывание» и отказов типа "ложное срабатывание»	В проекте системы ПАЗ установить показатели надёжности для двух типов отказов данных систем: отказы типа «несрабатывание» и отказы типа «ложное срабатывание»
Системы ПАЗ для объектов, имеющих в составе технологические блоки I и II категорий взрывоопасности, строятся на базе программируемых логических контроллеров, не способных функционировать по отказобезопасной структуре и не проверенных на соответствие требованиям функциональной безопасности	В проекте на систему ПАЗ выбирать контроллеры, способные функционировать по отказобезопасной структуре и проверенные на соответствие требованиям функциональной безопасности
В случае отключения электроэнергии или прекращения подачи сжатого воздуха для питания системы ПАЗ не обеспечивается перевод технологического объекта в безопасное состояние	Определить безопасное состояние исполнительных механизмов на основании анализа опасности и работоспособности. Внести изменения в проектную документацию

При проведении аудита эксплуатируемых систем ПАЗ ОПО используются формализованные опросные листы, составляемые опытными специалистами в области проектирования и эксплуатации систем ПАЗ и учитывающие особенности конкретного ОПО.

В этих опросных листах указываются сведения о классе опасности исследуемого объекта, категория опасности, приводится перечень технологических блоков с категориями взрывоопасности. Определяются наличие и полнота документации на технологический объект (наличие Декларации промышленной безопасности, утвержденного технологического регламента и перечня функций безопасности ПАЗ с указанием требуемых уровней полноты безопасности и т.д.).

Определяются сведения о системах ПАЗ, выделенных системах сигнализации и оповещения, системах контроля загазованности и пожаротушения.

Собираются сведения о наличии рабочей документации на системы ПАЗ (наличие схем питания и заземления, логических схем блокировок и защит, отчета по анализу риска инструментальной части ПАЗ).

Данные о наличии эксплуатационной документации на системы ПАЗ должны включать сведения о наличии:

- руководства пользователя системы ПАЗ;
- руководства по эксплуатации и техническому обслуживанию КТС системы ПАЗ;
- методики проверочных испытаний;
- журнала учёта отказов системы ПАЗ;
- журнала учёта модификаций системы ПАЗ и внесения изменений в прикладное ПО;
- плана-графика работ по плановому обслуживанию системы ПАЗ;
- отчёта работ по плановому обслуживанию.

В опросных листах указываются сведения о производителях и моделях оборудования КТС системы ПАЗ по датчикам, решающему устройству и исполнительным механизмам.

В опросных листах указываются показатели функциональной безопасности систем ПАЗ:

- показатели надёжности, безопасности (вероятностные характеристики для ложного срабатывания и несрабатывания);
- показатели быстродействия систем ПАЗ (цикл, время реакции, время срабатывания исполнительных механизмов);

- соответствие показателей надёжности и быстродействия рискам технологического процесса ОПО, приоритетность команд системы ПАЗ по отношению к командам управления технологическим оборудованием ОПО, формируемым АСУТП или оперативным персоналом АСУТП;

- отсутствие конфликта между системами ПАЗ на ОПО (срабатывание одной системы ПАЗ не должно приводить к созданию на объекте ситуации, требующей срабатывания другой такой системы);

- исключение срабатывания систем ПАЗ от кратковременных сигналов нарушения нормального хода технологического процесса;

- обеспечение перехода технологического объекта в безопасное состояние при прекращении питания КТС системы ПАЗ;

- наличие/отсутствие общей шины передачи данных для системы управления и ПАЗ;

- использование датчиков и ИМ в системе ПАЗ и системы управления одновременно;

- максимальный заданный уровень полноты безопасности функции безопасности систем ПАЗ.

Также в опросных листах должны быть данные о надежности, предоставляемые производителями компонентов ПАЗ, сведения о применении мер по снижению числа отказов по общей причине, наличии ЗИП и контрольных проверках функций безопасности.

В опросные листы могут быть включены сведения о полученных предписаниях Ростехнадзора.

Таким образом, аудит функциональной безопасности эксплуатируемых систем ПАЗ представляет собой широкий спектр инжиниринговых задач, которые решаются на всех этапах жизненного цикла функциональной безопасности.

ЛИТЕРАТУРА

1. Приказ Ростехнадзора от 11.03.2013 N 96 «Об утверждении Федеральных норм и правил в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств».

2. Приказ Ростехнадзора от 21.11.2013 N 559 «Об утверждении Федеральных норм и правил в области промышленной безопасности «Правила безопасности химически опасных производственных объектов».

3. ГОСТ Р 51901.11-2005. Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство.