УДК 622.529.55

В.Н. ИВАНИЛОВ, ***канд. техн. наук, ст. науч. сотрудник,***
Е.И. СОВЕТОВА, ***ст. науч. сотрудник, МакНИИ,***
В.В. ИВАНИЛОВ, ***студент, ДонНТУ; Макеевка***

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ СИСТЕМ ШАХТНОЙ АВТОМАТИЗИРОВАННОЙ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ

Приведены материалы, раскрывающие принципы проектирования и разработки программного обеспечения средств электрических, электронных, программируемых электронных систем, предназначенных для поддержания безопасного режима работы и защиты работников шахты.

Ключевые слова: автономный элемент, аппаратные средства, программное обеспечение, противоаварийная защита, электронные системы.

В современных условиях применение технологий, машин, механизмов, оборудования, транспортных и других средств производства, имеющих системы автоматического контроля и управления технологическими процессами и состоянием производственной среды, построенные с применением электронных программируемых систем, обусловлено выполнением функций противоаварийной защиты (далее – ПАЗ) и автоматического контроля параметров безопасности [1]. При этом необходимо формировать информацию о появлении опасных и вредных производственных факторов, предаварийных и аварийных ситуаций, а также создании автоматических предупреждающих действий с целью поддержания безопасного режима работы людей.

Целью статьи является ознакомление научных, инженерно-технических работников угольной отрасли с разработанными нормативными требованиями безопасности к программному обеспечению электронных устройств систем шахтной автоматизированной противоаварийной защиты.

Разработанные требования вошли в СОУ-Н 10.1.00174088.028:2011 «Требования и регламент оценки автоматизированных средств и систем противоаварийной защиты» [2] и заключаются в следующем.

Электрические, электронные, программируемые электронные системы шахтной автоматизированной системы противоаварийной защиты монтируют из отдельных автономных элементов таких систем (аппаратура

© В.Н. Иванилов, Е.И. Советова, В.В. Иванилов, 2013

контроля метана, скорости и направления движения воздуха и т.п.) или из элементов таких систем, встроенных в горношахтное оборудование (далее – ГШО), и, как правило, персональных компьютеров или промышленных контроллеров.

Систему шахтной автоматизированной противоаварийной защиты в каждом отдельном случае необходимо разрабатывать с однозначно определенной архитектурой построения и типом интерфейсного соединения, обеспечивающим двусторонний обмен информацией, например, RS485, Profibus, Fieldbus и др.

Допускается использовать существующие интерфейсные каналы ГШО (токовые, частотные, потенциальные и т.п.) для обмена информацией между ними и поверхностной частью системы ПАЗ с последующим ее преобразованием в соответствие с требованиями программно-аппаратного интерфейса, принятого в системе.

В каждом отдельно взятом случае требования к выбору операционной системы и прикладному программному обеспечению (ПО) определяются заказчиком и разработчиком системы ПАЗ.

Программное обеспечение должно соответствовать требованиям ГОСТ 19.001-77 и должно обеспечивать:

– безопасность собственно ПО;

– безопасность системы, гарантируемую средствами ПО.

Безопасность собственно ПО должна обеспечиваться одним из следующих видов программной избыточности: функциональной, структурной, временных прерываний или информационной.

Безопасность системы, гарантируемая средствами ПО, реализуют с использованием одного из следующих уровней безопасности:

– аппаратного, основанного на самопроверяющихся схемах или применении схем с отказоустойчивыми элементами. Самопроверяющиеся схемы, при возникновении в них неисправностей, должны формировать на своих выходах сигнал защитного отключения;

– информационного с организацией защиты от ошибок информации, передаваемой по каналам связи. Основными методами защиты должны быть применение памяти с аппаратным контролем паритета и использование корректирующих кодов (с контролем на четность, равновесных, с повторением, с суммированием, арифметических, кодов Хэмминга и др.) при накоплении и передаче информации;

– программного с применением программных средств тестирования, верификации или самопроверяющихся программ, защищенных от отказов за счет использования структурного резервирования аппаратуры и ПО. В этом случае должны использоваться способы параллельной обработки ин-

формации в нескольких вычислительных каналах или с помощью последовательных нескольких частей программы в одном вычислительном канале;

– интерфейсного.

ПО должно обеспечивать решение задач обнаружения искажения алгоритмов функционирования, ограничения последствий этого искажения в пределах участка программы (программного модуля) и восстановления правильного результата.

ПО должно быть устойчиво, что должно обеспечиваться одним из следующих видов программной избыточности:

– временной, основанной на выделении специальных интервалов времени для организации процедур контроля и восстановления;

– информационной с резервированием информационных массивов и применением корректирующих кодов для передачи информации. В случае разрушения основного информационного массива программа должна обращаться к резервному, который используется до полного восстановления основного информационного массива;

– структурной, состоящей в использовании дополнительных программных модулей, не отвечающих за основной вычислительный процесс, и предназначенных для определения или исправления ошибок в работе. Это могут быть программы проверки результатов вычислений, тесты аппаратной части или же несколько версий одной программы, дублирующих друг друга. Тестовые процедуры должны быть встроены в систему безопасности ПО при его разработке.

ПО системы ПАЗ должно обеспечивать:

– защиту от несанкционированного вмешательства в программные средства, обеспечивающие безопасность системы ПАЗ.

– накопление информации с созданием нескольких резервных копий, защищенных от несанкционированного доступа;

– возможность доступа к накопленным данным о безопасности технологических процессов с размежеванием прав пользователей в режиме прямого доступа, без остановки защитных функций системы.

В ПО системы ПАЗ следует предусматривать возможность метрологической калибровки аппаратного состава системы ПАЗ, имеющего аналоговый интерфейсный протокол обмена.

Средствами ПО системы ПАЗ необходимо осуществлять контроль сообщений о невыполнении защитных функций элементами автономных элементов системы ПАЗ и формировать дополнительное управление защитным действием на устройство ГШО, не выполнившее защитные функции, заложенные в его конструкцию.

Эту функцию вводят во время разработки новых поколений автономных элементов системы с учетом особенностей управления ГШО. Для устройств ГШО, которые находятся в эксплуатации и не имеют таких характеристик, рекомендуется введение таких защитных функций в ходе выполнения капитального ремонта ГШО.

Кроме того, средства ПО шахтной системы ПАЗ должны:

– быть тестируемыми и диагностируемыми;

– обеспечивать возможность настройки и самодиагностики без прерывания своего функционирования, сохранять работоспособность после перезагрузок, вызванных сбоями/отказами технических средств, и целостность при собственных сбоях;

– быть защищены от компьютерных вирусов, от несанкционированного доступа, от потерь и искажений при хранении, вводе, выводе, возникновении сбоев при обработке информации и от возможности случайных изменений;

– не иметь свойств и характеристик, не описанных в своей документации (не задекларированных возможностей).

ВЫВОДЫ

В результате применения разработанных требований безопасности к программному обеспечению электронных систем шахтной автоматизированной противоаварийной защиты предприятия угольной отрасли будут обеспечены системами защиты, имеющими более высокие параметры функциональной безопасности, что позволит уменьшить действие опасных и вредных производственных факторов на здоровье горняков.

СПИСОК ЛИТЕРАТУРЫ

1. Правила безопасности в угольных шахтах: НПАОП 10.0-1.01-10.– Офиц. изд. – К.: Охрана труда, 2010. – 430 с. – (Нормативно-правовой документ Госгорпромнадзора Украины).

2. Требования и регламент оценки автоматизированных средств и систем противоаварийной защиты: СОУ-Н 10.1.00174088.028:2011 – Офиц. изд. – Макеевка: МакНИИ, 2012. – 54 с. – (Нормативный документ Минэнергоугля Украины).

Получено: 16.10.2013

Наведено матеріали, що розкривають принципи проектування та розроблення програмного забезпечення засобів електричних, електронних, програмованих електронних систем, призначених для підтримки безпечного режиму роботи і захисту працівників шахти.

Ключові слова: автономний елемент, апаратні засоби, програмне забезпечення, протиаварійний захист, електронні системи.

The materials have been set out which reveal the designing and development principles of the software of devices of electrical, electronic, programmable electronic systems intended to support safe operation and protection of mine workers.

Keywords: independent device, hardware facilities, software, accident-prevention protection, electronic systems.