3 ИНФОРМАЦИОННАЯ И ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ, ТЕЛЕМЕХАНИКИ И СВЯЗИ

УДК 625+ 681.518.5

МЕТОД ЛОГИЧЕСКОЙ ОБРАБОТКИ ДИАГНОСТИЧЕСКИХ ДАННЫХ УСТРОЙСТВ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА ОСНОВЕ КВАНТОВАНИЯ СИГНАЛОВ

Р. Б. АБДУЛЛАЕВ
Ташкентский государственный транспортный университет, Республика Узбекистан

В современное время стационарные системы автоматического контроля, технического диагностирования и мониторинга играют важнейшую роль в обеспечении технологических процессов во многих отраслях жизнедеятельности человечества, в т. ч. и транспорта [1]. К примеру, в отрасли железнодорожного транспорта системы технического диагностирования и мониторинга (СТДМ) используются для контроля технического состояния устройств автоматики, объектов сети электроснабжения, искусственных сооружений и прочей отраслевой инфраструктуры. Подобные устройства позволяют в некоторой степени отражать картину технического состояния объектов диагностирования, прогнозировать их дальнейшее техническое состояние, систематизировать действия обслуживающего персонала по выявлению и предотвращению отказов, аварий и т. д. [2]. Отсюда, очевидно, что системы мониторинга предназначены для повышения безотказности и отказоустойчивости устройств и систем организации движения поездов, в т. ч. в некоторой косвенной степени влияют на безопасность движения поездов, позволяя в ряде случаев фиксировать критические отклонения рабочих параметров объектов диагностирования.

На железных дорогах постсоветских государств, к примеру, в отрасли железнодорожной автоматики и телемеханики (ЖАТ), эксплуатируются ряд СТДМ. Из российских разработок СТДМ ЖАТ получили широкое применение на сети железных дорог такие системы, как «Аппаратно-программный комплекс диспетчерского контроля» (АПК-ДК), «Автоматизированная система диспетчерского контроля» (АСДК) и «Автоматизированная система диагностирования и контроля устройств сигнализации, централизации и блокировки» (АДК-СЦБ) [3]. На железной дороге Узбекистана из собственных разработок начата эксплуатация системы «ZarafshON» [4].

Эксплуатация СТДМ дает ряд преимуществ в сфере технической эксплуатации и обслуживания устройств ЖАТ, позволяя автоматизировать ряд измерений их рабочих параметров. Однако зачастую системы мониторинга накапливают большие объемы диагностических данных и в существующей парадигме их анализа и обработки фиксируют до 90–95 % ложных диагностических ситуаций (инцидентов). Совершенствование возможно путем использования логических методов анализа диагностических данных и использования систем поддержки принятия решений на их основе.

Использование систем логической обработки данных и поддержки принятия решений техническим персоналом значительно поспособствовало бы сокращению числа отказов, времени на поиск и устранение причин отказов, продлению срока службы устройств ЖАТ и, в определенной степени, – обучению персонала в выявлении причин отказов и принципов функционирования устройств ЖАТ. Внедрению подобных подсистем в СТДМ ЖАТ препятствует необходимость обработки больших потоков данных, что составляет определенную нагрузку на вычислительные комплексы и приводит к большим затратам времени на обработку.

В целях устранения недостатков существующего способа логического анализа предлагается квантование диапазона диагностических данных по пороговым значениям данных, при котором диагностируемое устройство находится в том или ином состоянии. Тем самым можно сократить длину вектора диагностических данных и, соответственно, уменьшить затраты вычислительных ресурсов на процессы обработки.

Рассмотрим пример квантования диапазона значимых величин напряжения (тока) путевого реле и принцип замены измеренных величин на векторы данных с малой длиной. На рисунке 1 приведе-

ны основные принципы квантования уровней напряжения питания путевого реле по основным пороговым значениям параметров. Для этого условно приведены кривая $U(t)$, $I(t)$ и по вертикальной шкале уровни основных напряжений реле.

В целях сокращения байтов данных при логической обработке предлагается объединять некоторые байты данных, формируемые при каждом шаге квантования и входящих в один и тот же диапазон параметра реле (выделены фигурной скобкой) и далее, представлять этот диапазон байтов данных одним коротким вектором данных. Например, на рисунке 1 условно выделен диапазон рабочего напряжения реле $U_р$, при котором реле надежно притягивает свой якорь, не находится в режиме перегрузки, формирует информацию о свободности рельсовой цепи. При этом все байты данных, формируемые при каждом шаге квантования данного диапазона, будут заменены вектором 101. Таким образом заменяются все полученные от измерительных контроллеров байты диагностических данных на векторы с малой длиной в зависимости от принадлежности тому или иному параметрическому диапазону.

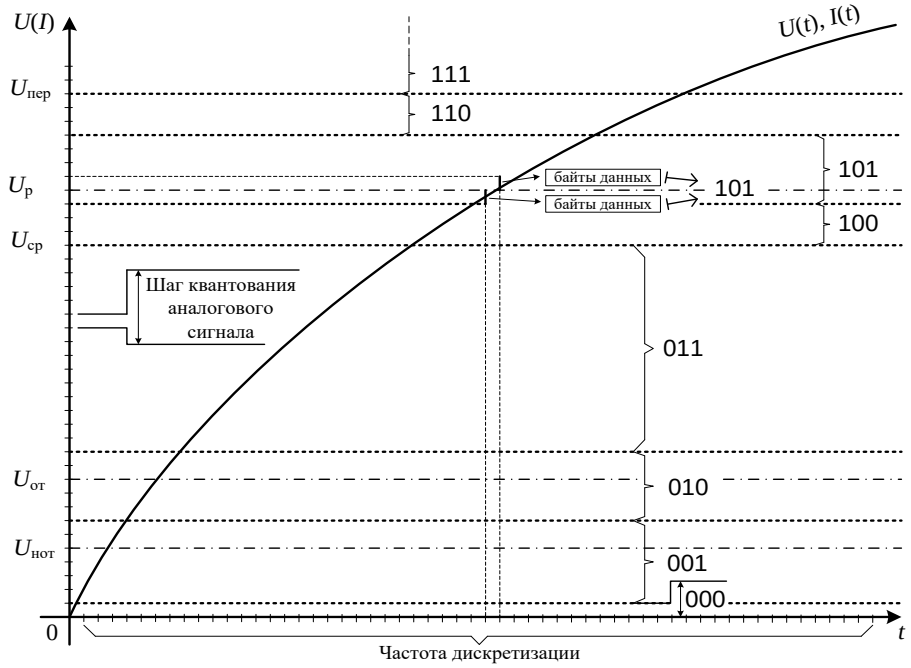

Рисунок 1 – Принципы квантования уровней напряжения (тока) питания путевого реле по наиболее значимым диапазонам напряжений (токов) устройства

Длина формируемого вектора данных может выбираться различной в зависимости от специфики диагностируемого устройства и необходимости отражения полной картины режимов его работы, состояний и т. д. Далее, для защиты от аппаратных и программных сбоев сформированный вектор можно закодировать любым помехоустойчивым кодом, к примеру, полиномиальными кодами [5].

Сокращение массива данных позволит снизить нагрузку на вычислительное устройство при обработке комплекса алгоритмов логического анализа диагностических данных, сократить время на их обработку, использовать малое количество контрольных разрядов при кодировании нового вектора данных, что упростит алгоритм их вычисления. Так как диагностические данные от измерительных контроллеров поступают в центральный модуль несинхронно, то и замена определенных байтов данных на векторы данных малой длины может осуществляться между опросами других измерительных контроллеров, что очевидно, не потребует выделения дополнительного времени.

Список литературы

1 **J. Guo, X. Wang.** Future prospects on the intelligent monitoring technologies for railway signaling systems in China / X. Y. Wang, J. Guo, Zhang and Y. Yang // 6th IET Conference on Railway Condition Monitoring (RCM 2014). – Birmingham, 2014. – Pp. 1–5.

2 **Ефанов, Д. В.** Функциональный контроль и мониторинг устройств железнодорожной автоматики и телемеханики / Д. В. Ефанов. – СПб. : ФГБОУ ВО ПГУПС, 2016. – 171 с.

3 **Молодцов, В. П.** Системы диспетчерского контроля и мониторинга устройств железнодорожной автоматики и телемеханики : учеб. пособие / В. П. Молодцов, А. А. Иванов. – СПб. : Петербургский гос. ун-т путей сообщения, 2010. – 140 с.

4 Проект «ЗАРАФШОН» [Электронный ресурс]. – Режим доступа : https://mikroelektronika.plus. – Дата доступа : 21.09.2021.

5 Polynomial Code with Detecting the Symmetric and Asymmetric Errors in the Data Vectors / R. Abdullaev [et al.] // Proceedings of 17th IEEE East-West Design & Test Symposium (EWDTS`2019), Batumi, Georgia, September 13–16. – 2019. – P. 157–161. – DOI: 10.1109/EWDTS.2019.8884451.

УДК 621.38

ГАРМОНИЗАЦИЯ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ОТВЕТСТВЕННЫМИ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

К. А. БОЧКОВ, П. М. БУЙ, А. Ю. КУЛАЖЕНКО
Белорусский государственный университет транспорта, г. Гомель

В настоящее время актуальным остается вопрос о том, каким образом соотносятся сферы информационной и функциональной безопасности для автоматизированных систем управления ответственными технологическими процессами и, в частности, какова их роль в процессе обеспечения безопасности движения поездов на железнодорожном транспорте.

Общие вопросы требований по информационной безопасности сформулированы в СТБ 34.101.1-2014 (IEC 15408-1:2009) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» [1]. Предметом защиты в этом направлении является сама информация, а точнее такие ее основные свойства, как конфиденциальность, целостность и доступность. В соответствии с [2], безопасность информации – это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Предметом обеспечения функциональной безопасности является безотказность и безопасность работы автоматизированных систем управления ответственными технологическими процессами железнодорожного транспорта, которая может быть нарушена путем реализации атак как на информацию и ее носители, которые необходимы для штатной работы системы, так и на сам процесс функционирования, приводя систему к опасным отказам. Для систем, критичных к функциональной безопасности, всегда определяются критерии опасных отказов, которые приводят к авариям, угрозе жизням людей, экологическим бедствиям.

Для подавляющего большинства современных объектов информационных технологий актуальными являются исключительно вопросы информационной безопасности, т. к. задачами этих объектов является хранение, обработка и/или предоставление информации. К таким объектам можно отнести персональные компьютеры, мобильные устройства пользователей, Internet of Things (IoT) и т. п.

Концепция информационной безопасности Республики Беларусь указывает на то, что повсеместное функционирование объектов транспорта с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности [3]. Но безопасность людей, социальной и экологической сферы не является предметом информационной защиты. Методы и средства, обеспечивающие исключительно информационную безопасность, не в силах решить эти задачи. Особенно это актуально для автоматизированных систем управления ответственными технологическими процессами (АСУ ОТП), которые широко применяются на железнодорожном транспорте. Основную роль в обеспечении безопасности движения поездов выполняют системы железнодорожной автоматики и телемеханики (СЖАТ). Такие системы в своем составе используют информационную инфраструктуру и на них должны выполнятся мероприятия по обеспечению информационной безопасности. Но в таких системах не информация должна являться главным объектом защиты, а в случае железнодорожного транспорта, это, в первую очередь, обеспечение безопасности движения поездов. Атака на инфокоммуникационные системы и/или на информацию при обнаружении будет заблокиро-