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-

вана, но если она не будет обнаружена (например, действия нарушителя будут признаны законными) или будет направлена исключительно на технологический процесс в обход информационной инфраструктуры (например, электромагнитный терроризм), то могут пострадать люди или может быть нанесен вред окружающей среде. Это будет нарушением критериев опасного отказа. В таком случае преобладающими становятся вопросы функциональной безопасности.

Функциональная безопасность – свойство объекта железнодорожного транспорта, связанного с безопасностью, выполнять требуемые функции безопасности при всех предусмотренных условиях в течение заданного периода времени [4].

Для автоматизированных систем управления ответственными технологическими процессами железнодорожного транспорта, как, впрочем, и для многих подобных систем других отраслей необходимо обеспечивать как информационную, так и функциональную безопасность. Зачастую, классические методы, обеспечивающие функциональную безопасность и современные методы, обеспечивающие информационную безопасность, частично перекрывают зоны своей ответственности, которая, касается, например, обеспечения доступности и целостности информации и реализуется организационными мероприятиями. Известный специалист в области функциональной безопасности профессор Скляр В. В. для того, чтобы избежать дублирования требований для объектов защиты, рекомендует гармонизировать требования по информационной и функциональной безопасности, сформировать общий жизненный цикл, а также увязать процессы управления безопасностью и условия безопасности объекта защиты. Также, по аналогии с функциональной безопасностью, для которой определены уровни полноты безопасности (SIL), определяются пять (от 0 до 4) уровней информационной безопасности (SL) [5]. При такой гармонизации требований процессы обеспечения информационной и функциональной безопасности будут происходить параллельно. Причем, исходя из назначения и характеристик объекта защиты в общем жизненном цикле обеспечения информационной и функциональной безопасности определяется приоритет.

Примером гармонизации требований по функциональной и информационной безопасности на общем жизненном цикле является стандарт ОАО РЖД 02.049-2014 [6], устанавливающий требования к функциональной и информационной безопасности программного обеспечения АСУТП и техническими средствами железнодорожного транспорта. Вместе с тем он в основном базируется на нормативных документах Российской Федерации и не полностью учитывает принятые Евразийской экономической комиссией (ЕЭК) технические регламенты таможенного союза по железнодорожному транспорту ТР ТС 001–003. Кроме того, оценка соответствия требованиям функциональной и информационной безопасности программного обеспечения АСУТП в отрыве от безотказности аппаратных средств не позволяет определить достигнутый уровень полноты безотказности всего АПК систем железнодорожной автоматики и телемеханики.

Совокупность угроз информационной и функциональной безопасности потенциально реализуются через кибератаки. Кибератака в соответствии с [3] – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. В контексте термина «кибератака» обеспечение информационной и функциональной безопасности можно обозначить термином «кибербезопасность». При таком подходе можно говорить о двухмерной модели кибербезопасности, включающей как информационную, так и функциональную составляющую (рисунок 1).

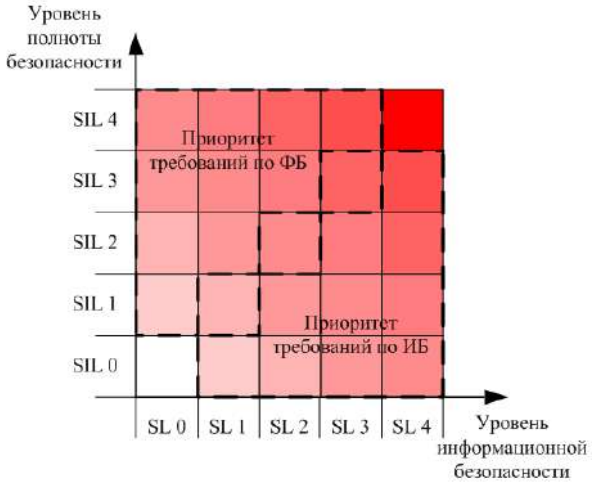

Рисунок 1 – Двухмерная модель кибербезопасности АСУ ОТП железнодорожного транспорта

Чем выше уровень SIL, тем меньше допускается угроз функциональной безопасности. Аналогичным образом необходимо привязать уровни информационной безопасности к допустимому уровню соответствующих угроз. Источником

классификации уровней информационной безопасности может послужить классификация типовых информационных систем и перечень требований к системе защиты информации, представленные в приказе ОАЦ от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [6]. При необходимости обеспечить требуемые уровни SIL и SL требуется реализовать такие условия функционирования и использовать средства защиты информации, при которых уровень угроз кибербезопасности будет находиться в безопасной зоне как по информационной, так и по функциональной безопасности, учитывая приоритеты их обеспечения для конкретного объекта защиты.

Исходя из этой двухмерной модели, обеспечение кибербезопасности заключается в соотношении угроз в сферах информационной и функциональной безопасности. При этом, для систем обеспечения безопасности движения поездов, к которым относятся современные микроэлектронные СЖАТ на основе аппаратно-программных комплексов (АПК), преобладающим является обеспечение функциональной безопасности.

Список литературы

1 СТБ 34.101.1-2014. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1: Введение и общая модель. – Взамен СТБ 34.101.1-2004 ; введ. 2014–09–01. – Минск : БелГИСС, 2014. – 60 с.

2 СТБ ISO/IEC 27001-2016. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Минск : БелГИСС, 2016. – 28 с.

3 О Концепции информационной безопасности Республики Беларусь : Постановление Совета безопасности Республики Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН Законодательство Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

4 ГОСТ 33432-2015. Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта. – Минск : БелГИСС, 2015. – 26 с.

5 **Скляр, В. В.** Обеспечение безопасности АСУТП в соответствии с современными стандартами : метод. пособие / В. В. Скляр. – М. : Инфра-Инженерия, 2018. – 384 с.

6 СТО РЖД 02.049-2014. Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта.

7 О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 : Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 // Эталон Online [Электронный ресурс] / Национальный Центр правовой информации Республики Беларусь. – Минск, 2020.

УДК 007.51: 621.317.1

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ И УЧЕТА АККУМУЛЯТОРНЫХ БАТАРЕЙ В ДИСТАНЦИИ СИГНАЛИЗАЦИИ И СВЯЗИ ЖЕЛЕЗНОЙ ДОРОГИ

А. В. ВЕСЕЛОВ
Полоцкая дистанция сигнализации и связи Белорусской железной дороги

В. Г. ШЕВЧУК
Белорусский государственный университет транспорта, г. Гомель

Устройства технологической связи Белорусской железной дороги относятся к потребителям особой группы электроприемников I категории электроснабжения. В качестве третьего независимого источника питания особой группы применяются источники вторичного электроснабжения 24, 48 и 60 В с аккумуляторными батареями (АКБ) различных типов. Поддержание АКБ в технически исправном состоянии, своевременное выявление батарей, параметры которых не соответствуют техническим требованиям, и их замена, составление перспективных планов замены АКБ на основе динамики изменения технических характеристик являются основными задачами обслуживающего персонала участков связи в дистанциях сигнализации и связи.

Разработано устройство автоматическое разрядное (УАР), предназначенное для автоматизированного контроля емкости аккумуляторных батарей (АКБ) с выводом результатов тестирования на дисплей и формированием файлов отчета результатов тестирования на карте памяти.