

Возможны следующие случаи, связанные с неисправностями модулей:

- 1) неисправность одного модуля ввода сигналов с двумя сигналами ПК и МК в одном блоке (модуль ввода сигналов 1);
- 2) неисправность одного модуля ввода сигналов с одним сигналом ПК или МК, второй модуль исправен (модуль ввода сигналов 2 и 3);
- 3) одновременная неисправность двух модулей ввода сигналов (модуль ввода сигналов 2 и 3).

Состояние сигнала при неисправном модуле ввода сигналов обозначим  $\{H\}$ . Состояние сигнала 0 или 1 при исправном модуле ввода сигналов обозначим  $\{*\}$ .

В первом и в третьем случае состояние сигналов МК и ПК неизвестно  $\{HH\}$  (МК = H, ПК = H) и стрелка однозначно будет находиться в положении без контроля.

Во втором случае неисправность может быть в модуле ввода сигналов 2 или в модуле ввода сигналов 3.

При неисправности второго модуля ввода сигналов, осуществляющего ввод сигнала ПК  $\{*H\}$ , и исправности третьего модуля ввода сигналов, осуществляющего ввод сигнала МК при наличии активного сигнала (единица) МК  $\{1H\}$ , можно утверждать, что стрелка находится в минусовом положении. При отсутствии активного сигнала МК  $\{0H\}$  возникает ситуация «Нет контроля стрелки. Возможно стрелка в плюсовом положении».

При неисправности третьего модуля ввода сигналов, осуществляющего ввод сигнала МК  $\{H*\}$ , и исправности первого модуля ввода сигналов, осуществляющего ввод сигнала ПК при наличии активного сигнала (единица) ПК  $\{H1\}$ , можно утверждать, что стрелка находится в плюсовом положении. При отсутствии активного сигнала ПК возникает ситуация «Нет контроля стрелки. Возможно стрелка в минусовом положении».

Таким образом, для обеспечения безопасности движения поездов системы железнодорожной автоматики и телемеханики в процессе предварительной обработки информации о сложных объектах контроля (стрелка, светофор, рельсовая цепь и другие) должны хранить, передавать и обрабатывать в совокупности показания всех датчиков и индикаторов неисправностей сложного объекта контроля как показано выше.

#### Список литературы

- 1 Правила технической эксплуатации железных дорог Российской Федерации : утв. приказом Минтранса России от 23 июня 2022 г. – № 250. – 517 с.
- 2 ГОСТ 33894-2016. Системы железнодорожной автоматики и телемеханики на железнодорожных станциях. – Введ. 2017-11-01. – М. : Стандартинформ, 2017. – 26 с.
- 3 ГОСТ 33896-2016. Системы диспетчерской централизации и диспетчерского контроля движения поездов. – Введ. 2017-11-01. – М. : Стандартинформ, 2017.
- 4 СТО РЖД 1.19.003-2010. Автоматизированные системы диспетчерского управления движением поездов. – Введ. 2017-11-01. – М., 2010. – 43 с.
- 5 СП 235.1326000.2015. Свод правил. Железнодорожная автоматика и телемеханика. Правила проектирования: утв. приказом. Минтранса России № 205 от 06.07.2015 г. Дата введения : 01.07.2015 г. – М. : Минтранс России, 2015. – 145 с.

УДК 65.011.56

## НОВЫЕ ТРЕБОВАНИЯ К СИСТЕМАМ УПРАВЛЕНИЯ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

*И. В. КАСПАРОВ*

*Самарский государственный университет путей сообщения, филиал в г. Нижний Новгород,  
Российская Федерация*

Развитие железнодорожного транспорта на современном этапе требует новых подходов к созданию и эксплуатации жизненно важных систем управления и обеспечения безопасности движения поездов. Длительное время системы железнодорожной автоматики и телемеханики представляли собой достаточно разрозненные устройства, которые не имели единых требований в области функциональной безопасности и надежности, а также кибербезопасности.

Переход к созданию современных комплексных систем интервального регулирования движения поездов является очень актуальным, так как постоянно происходит усложнение задач перевозочного процесса, поэтому необходима унификация требований, разработка единой методологии оценки киберзащищенности объектов управления, разработка и внедрение методики прогнозирования предельного состояния элементов инфраструктуры.

Специалистами выработан ряд требований, которые предъявляются к системам управления [1–3]:

- использование систем интервального регулирования на перегонах без напольных светофоров с исключением специализации направления движения;
- наличие режима автоматического интервального регулирования по главным станционным путям в выбранном направлении движения с возможностью, при этом, автономного управления маршрутами на остальных путях станций;
- возможность резервирования главных путей станции устройствами интервального регулирования АБ при неисправности ЭЦ;
- обеспечение цифровой увязки микропроцессорной ЭЦ с системами интервального регулирования АБ;
- наличие цифрового интерфейса с системой контроля маневровой автоматической локомотивной сигнализации и интеграцией АРМ МАЛС и МПЦ;
- возможность передачи по радиоканалу дополнительной информации для резервирования и дублирования основных каналов управления движением поездов (АЛСН, АЛС-ЕН, временные ограничения скорости и т. д.);
- наличие цифрового интерфейса с системами верхнего уровня, в том числе с возможностью реализации функций линейного пункта ДЦ в системах МПЦ;
- интеграция с системой интеллектуального оповещения работающих на путях и информирования пассажиров;
- встроенная диагностика технического состояния микропроцессорной аппаратуры, позволяющая выявлять неисправные узлы системы, вести статистику отказов и сбоев, а также иметь сопряжения с системами контроля параметров других устройств СЦБ;
- резервирование каналов межстанционной связи кольцевой архитектурой с использованием интегрированных в систему объектных контроллеров концентраторов связи, что значительно увеличивает функциональность, работоспособность и живучесть системы в случае повреждения кабеля;
- применение помехозащищенных рельсовых цепей тональной частоты с дополнительной кодовой защитой в целях электромагнитной совместимости с современным тяговым подвижным составом;
- разработка новой технологии АЛСО с «подвижными» блок-участками в системах интервального регулирования на перегонах;
- применение двухканальной автоматической локомотивной сигнализации АЛС-ЕН и АЛСН с возможностью переключения частот кодирования программным способом;
- разработка новой технологии с возможностью реконфигурации логики преследования ложной занятой рельсовой цепи;
- увязка с системами пересчета вариантных графиков.

Для повышения безопасности и эффективности работы железнодорожного транспорта в настоящее время широко используются технические средства автоматизированного и автоматического управления различными техническими процессами, активно внедряются программно-управляемые системы на основе микропроцессоров и робототехнические комплексы с элементами искусственного интеллекта [4]. Однако при этом возрастает вероятность проведения сетевых кибернетических и компьютерных атак на них. Широкое использование территориально-распределительных компьютерных сетей и специфика современных протоколов позволяют скрывать следы и источники атаки. Для снижения негативного влияния этих воздействий необходимо внедрять технологии кибербезопасности. Сейчас вопросы кибербезопасности стали особо актуальны, прежде всего, в связи с использованием стандартного системного и прикладного программного обеспечения в сочетании с применением сетевых протоколов семейства TCP/IP. Несмотря на положительный экономический эффект такого подхода, механическое тиражирование этих технологий приводит к наследованию их слабых сторон. С точки зрения кибербезопасности – это уязвимости (свойства информационных систем), которые злоумышленник может использовать для реализации атаки.

Еще одним немаловажным фактором является интеграция с системой передачи данных и реализация интерактивности информационных сервисов. Это приводит к увеличению поверхности атак (возможных точек для нападения) и расширению количества потенциальных источников негативного информационного воздействия.

В современном мире свою лепту вносит также и геополитика. Железнодорожный транспорт должен быть устойчив к негативным воздействиям со стороны других государств, в которых создаются и развиваются военные подразделения, ориентированные на действия в киберпространстве.

Объектами кибератак на железнодорожном транспорте могут являться бортовые программно-аппаратные системы управления локомотивами, микропроцессорные системы железнодорожной автоматики и телемеханики и электроснабжения.

Нарушение штатного режима работы микропроцессорных информационно-управляющих систем способно значительно снизить эффективность работы участка железной дороги. Так, например, системы интервального регулирования движения на скоростных и высокоскоростных участках активно используют радиоканал. В случае негативного воздействия на него, например, с использованием средств подавления диапазона ISM или GSM, определение скорости движения и многих других параметров становится невозможным. Это потребует перехода на движение по сигналам автоблокировки и приведет к увеличению интервала попутного следствия, а, следовательно, и снижению пропускной способности участка.

Более опасные угрозы связаны с возможностью нарушения безопасности движения поездов из-за вмешательства в алгоритмы работы стационарных устройств микропроцессорных систем ЖАТ и бортовых устройств безопасности на локомотивах. Превышение максимально допустимой скорости, задание враждебных маршрутов, изменение состояния сигналов на станции и перегонах чреват очевидными последствиями вплоть до крушения.

Необходимо максимально использовать достижения науки и техники для развития и широкого внедрения на железнодорожном транспорте технологий кибербезопасности.

Все программно-управляемые микропроцессорные системы железнодорожного транспорта нужно обязательно проверять на функциональную безопасность, отсутствие незадекларированных возможностей и несанкционированного доступа. Схемотехнические решения и программное обеспечение таких систем уже на стадии проектирования должны учитывать возможность проведения различного рода кибератак.

Следует постепенно переходить на полный цикл производства таких систем с использованием отечественной элементной базы. Нужно внедрять принципы открытого программного продукта и разрабатывать новые альтернативные варианты управления движением поездов при безусловном сохранении существующих ручных режимов управления, которые будут незаменимы в случае широкого проведения кибератак.

#### Список литературы

- 1 **Шабельников, А. Н.** Компоненты киберфизических систем в составе КСАУ СП / А. Н. Шабельников, А. В. Суханов // Автоматика, связь, информатика. – 2020. – № 1. – С. 17–19. – DOI : 10.34649/ AT.2020.1.1.002.
- 2 WHITE PAPER: On Artificial Intelligence : A European approach to excellence and trust / European Commission. Brussels, 2020. URL: [https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust\\_en](https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en).
- 3 **Семион, К. В.** Стратегия цифровой трансформации / К. В. Семион // Автоматика, связь, информатика. – 2019. – № 4. – С. 5–6.
- 4 **Каспаров, И. В.** Применение новых телекоммуникационных технологий на железнодорожном транспорте / И. В. Каспаров // Образование, наука, транспорт в XXI веке: опыт, перспективы, инновации : материалы V междунар. науч.-практ. конф. – Самара : СамГУПС, 2015. – С. 314–316.

УДК 621.391

## ПОВЫШЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СЕТИ СВЯЗИ ДИСТАНЦИИ СИГНАЛИЗАЦИИ И СВЯЗИ

*Д. В. КЛЮЧНИК*

*Минское отделение Белорусской железной дороги*

*В. О. МАТУСЕВИЧ, С. В. КИСЕЛЕВА*

*Белорусский государственный университет транспорта, г. Гомель*

В последние годы сети связи железной дороги активно обновляются, прокладываются волоконно-оптические кабельные линии связи, внедряется соответствующее оборудование передачи данных. Однако в эксплуатации остается большое количество медных магистральных кабельных линий связи. Так, по Молодечненской дистанции сигнализации и связи доля таких линий достигает 40 %. Эксплуатация медных магистральных кабелей будет продолжаться еще не менее 10–15 лет. Для уплотнения каналов связи и передачи данных на таких участках в настоящее время используется аппаратура аналоговых систем передачи типа К-60П, П-302-П, К12+12, SUKTN-12N-W, выпущенная в 1980-х годах. Вся эта аппаратура реализована на аналоговой