УДК 656.257 + 004.056

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ СИСТЕМ МИКРОПРОЦЕССОРНЫХ И РЕЛЕЙНО-ПРОЦЕССОРНЫХ ЦЕНТРАЛИЗАЦИЙ НА СЕТИ ОАО «РЖД». ПЕРСПЕКТИВЫ И ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СРЕДСТВ ЗАЩИТЫ

МОИСЕЕВ Владимир Валерьевич, главный инженер Центра компьютерных железнодорожных технологий кафедры «Автоматика и телемеханика на железных дорогах»; e-mail: moiseev@crtc.spb.ru

Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург

В статье изложены основные аспекты обеспечения киберзащищенности ряда систем железнодорожной автоматики и телемеханики, разработки коллектива ЦКЖТ ФГБОУ ВО ПГУПС. Рассмотрены основные проблемные положения в сфере разработки и проектирования распределенных систем микропроцессорной централизации, включая нормативное обеспечение. Представлены перспективные отечественные средства защиты информации, и выполнен анализ требований по кибербезопасности к системам микропроцессорной и релейно-процессорной централизации, а также представлена практическая реализация ряда мероприятий по повышению уровня киберзащищенности систем железнодорожной автоматики и телемеханики. Рассмотрен ряд технических решений в области киберзащищенности при реализации распределенных систем управления на железнодорожном транспорте на примере микропроцессорной централизации МПЦ-МПК.

Ключевые слова: микропроцессорная централизация; релейно-процессорная централизация; информационная безопасность; кибербезопасность; киберзащищенность; система обнаружения вторжений; распределенная система управления.

DOI: 10.20295/2412-9186-2022-8-03-266-275

▼ Введение

Современное развитие железнодорожной отрасли характеризуется переходом на микропроцессорные устройства и аппаратуру, который можно квалифицировать общим термином — цифровизация. Это обусловлено конкурентными преимуществами, которыми обладают микропроцессорные системы железнодорожной автоматики и телемеханики (ЖАТ) и наличием ряда издержек и значительно больших эксплуатационных расходов при дальнейшем использовании устаревших (в том числе релейных) технологических решений. Также стоит отметить, что железнодорожные компании ищут новые возможности для повышения эффективности работы железнодорожного транспорта и снижения расходов [1], такая работа в области цифровых технологий проводится в ОАО «РЖД» и затрагивает все элементы и системы инфраструктуры холдинга [2].

Изменение роли человека в процессе организации перевозок и перевод многих процессов в цифровую плоскость имеет как большое количество положительных аспектов, так и ряд отрицательных.

Текущая ситуация с кибербезопасностью в мире показывает значительный рост количества компьютерных атак и увеличение инцидентов в области транспортной инфраструктуры и предприятий гражданского сектора, что требует самого пристального внимания к решению задач по обеспечению безопасного функционирования критически важных отраслей экономики [3]. Немаловажным фактором является и сложная геополитическая ситуация в мире, учитывая, что в задачи железнодорожного транспорта входит обеспечение бесперебойности перевозок и живучести в случае негативных воздействий со стороны других государств (включая киберпространство

и возможные атаки в нем). Учитывая общемировые тенденции и проводимые мероприятия в киберпространстве (подготовка, учения, разработка средств защиты и т. д.) в зарубежных странах [4], отечественные разработчики микропроцессорных систем ЖАТ стоят перед решением ряда сложнейших задач, которые ранее не были так актуальны для данного направления в науке и технике.

Прошедшие годы текущего века показали бурный рост в области развития цифровых технологий, особенно в области проектирования и строительства инфраструктур. Не исключением стал и железнодорожный транспорт [5], вследствие чего возрастает зависимость железнодорожной отрасли от компьютерных технологий, ее киберзащищенность (кибербезопасность) [6]. Согласно ГОСТ Р 56205—2014[1], кибербезопасность — это действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов. При этом главная цель киберзащиты — это уменьшение риска травмирования или угрозы здоровью населения, а также разглашения информации, сбоя в работе критически важных объектов инфраструктуры, к которым относится железнодорожный транспорт.

На основе предъявляемых требований к микропроцессорным системам ЖАТ специалисты Центра компьютерных железнодорожных технологий ФГБОУ ВО ПГУПС (ЦКЖТ ПГУПС) в тесном сотрудничестве с рядом отечественных разработчиков и экспертов в области информационной безопасности разработали и провели испытания ряда программно-аппаратных средств киберзащиты для систем микропроцессорной централизации (МПЦ) и релейно-процессорной централизации (РПЦ) на основе отечественных комплексов и средств защиты информации. Это позволит решать задачи по внедрению устройств и систем ЖАТ с учетом выполнения условий по киберзащите.

[1] ГОСТ Р 56205—2014. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. — Ч. 1-1. Терминология, концептуальные положения и модели.

1. Нормативное обеспечение кибербезопасности систем ЖАТ

Безопасность железнодорожного транспорта как части критической инфраструктуры государства при проведении в отношении нее компьютерных атак регулируется положениями Федерального закона от 26 июля 2017 г. № 187[2].

Одним из важных аспектов надежной и безопасной работы железнодорожной инфраструктуры является киберзащищенность систем и средств управления железнодорожными перевозками, к которым относятся системы ЖАТ. Основным нормативным документом в области защиты информации для систем ЖАТ как составной части инфраструктуры железнодорожного транспорта является приказ ФСТЭК[3] от 14 марта 2014 г. № 31, который относит системы ЖАТ к автоматизированным системам управления технологическими процессами (АСУТП) на железнодорожном транспорте. На основе требований выше указанных документов Центром кибербезопасности АО «НИИАС» для ОАО «РЖД» был разработан ряд методических документов в области киберзащищенности микропроцессорных систем управления движением поездов [7].

Данные нормативные документы позволяют учитывать особенности систем обеспечения управления движением поездов, главной целью их создания является формализация подхода при оценке киберзащищенности микропроцессорных систем управления и обеспечения безопасности движения поездов, определение порядка устранения выявленных несоответствий, сопровождение систем на всех стадиях жизненного цикла.

Все системы ЖАТ (как вновь проектируемые, так и разрешенные к применению на сети

[2] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[3] Приказ ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (в ред. Приказов ФСТЭК России от 23 марта 2017 г. № 49, от 9 августа 2018 г. № 138, от 15 марта 2021 г. № 46).

железных дорог ОАО «РЖД») должны соответствовать требованиям киберзащищенности и информационной безопасности к микропроцессорным системам управления и проходить подтверждение соответствия в установленном порядке. Как правило, они должны быть дополнены встроенными средствами защиты от несанкционированного доступа, а также должна быть выполнена актуализация программной документации с последующей сертификацией программного обеспечения (ПО) [8].

Учитывая, что в микропроцессорных системах ЖАТ в большинстве случаев построение сетей связи основывается на стандартных промышленных протоколах и способах организации связи, одним из основополагающих документов для обеспечения кибербезопасности сетей связи ЖАТ является ГОСТ Р МЭК 62443-2-1—2015[4], который определяет элементы (устройства), необходимые для встраивания в системы управления и обеспечения безопасности движения поездов и правила разработки таких элементов.

На основании вышеперечисленных нормативных документов и регламента взаимодействия структурных подразделений и функциональных филиалов ОАО «РЖД» с разработчиками и поставщиками систем управления и обеспечения безопасности движения поездов проводится аудит и оценка соответствия требованиям кибербезопасности систем ЖАТ с предоставлением экспертного заключения Центра кибербезопасности АО «НИИАС», по результатам которого определяется уровень и степень киберзащищености систем ЖАТ, а также перечень необходимых мероприятий.

2. Реализация требований по обеспечению кибербезопасности в системах ЖАТ разработки ЦКЖТ ПГУПС

На основе обобщения и анализа мирового опыта разработки специализированных методов и средств обеспечения кибербезопасности АСУТП [9, 10], а также определения уязвимостей и недостатков в их работе, с учетом разработанных технических решений по системам МПЦ-МПК и ЭЦ-МПК, которые внедряются уже более 20 лет, коллектив ЦКЖТ ПГУПС разработал модель угроз и способы защиты для внедряемых систем ЖАТ на основе требований информационной и функциональной безопасности.

Учитывая, что ориентировочное соотношение устраненных и выявленных уязвимостей в зарубежных системах (в частности, в продукции таких крупных производителей, как Siemens, Honeywell, Schneider Electric) составляет около 65 %, т. е. около 35 % известных уязвимостей не имеют решения из-за технических особенностей (технической реализации) [11], для систем ЖАТ разработки ЦКЖТ ПГУПС были определены три основных направления по устранению возможных уязвимостей и минимизации рисков:

1. Разработка дополнительных организационно-технических мероприятий для повышения уровня киберзащищенности систем ЖАТ.

Данные мероприятия позволяют в первую очередь исключить доступ к критически важному оборудованию систем ЖАТ, снизить риски внешнего воздействия, обеспечить контроль и протоколирование доступа к используемому оборудованию.

2. Доработка ПО систем МПЦ-МПК и ЭЦ-МПК.

Дополнительная адаптация ПО систем ЖАТ по требованиям нормативных документов позволяет минимизировать затраты на изменение аппаратных средств систем ЖАТ, повысить степень конфиденциальности информации, обеспечивает снижение рисков воздействия от внутреннего нарушителя системы ввиду разграничения прав доступа.

3. Применение новых, технических программно-аппаратных решений.

Изменение конфигурации систем ЖАТ под новые программно-аппаратные решения в области киберзащиты позволяет не только повысить общий уровень кибербезопасности, но и перейти на другую структуру управления и контроля объектами транспортной инфраструктуры (распределенную конфигурацию)

[4] ГОСТ Р МЭК 62443-2-1—2015. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. — Ч. 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики.

без снижения общего уровня безопасности и надежности систем ЖАТ.

Реализация всех трех направлений в едином комплексе мероприятий позволила снизить риски нарушения безопасности движения поездов и срыва процесса перевозок.

На основе замечаний специалистов Центра кибербезопасности АО «НИИАС» при проведении проверки систем МПЦ-МПК и ЭЦ-МПК на соответствие требованиям кибербезопасности для повышения киберзащищенности систем МПЦ-МПК и ЭЦ-МПК были реализованы следующие дополнительные мероприятия:

а) организационно-технические мероприятия повышения уровня киберзащищенности:

- ограничение физического доступа к оборудованию всех уровней систем МПЦ-МПК и ЭЦ-МПК (включая сетевое оборудование локальных вычислительных сетей) с контролем доступа. Защита от несанкционированного доступа к оборудованию, размещенному внутри шкафов, обеспечивается с помощью замков и сигнализации, срабатывающей при открытии дверей шкафов;
- использование только проводных интерфейсов в системе коммуникаций;
- пломбирование доступа к аппаратуре автоматизированных рабочих мест (АРМ);
- организация периодической проверки подключения сетевых и питающих кабелей на компьютерах, сетевых концентраторах, в вычислительных и силовых шкафах. Подключение должно соответствовать сетевой схеме из проектной документации, сетевые порты должны быть промаркированы;
- применение системы бесперебойного питания для ослабления уязвимости вследствие сбоев электропитания;
- применение полного резервирования программно-аппаратных средств для устранения уязвимости, связанных со сбоями и отказами программно-технических средств;
- контроль за работой МПЦ-МПК и ЭЦ-МПК на основе анализа протоколов работы систем, в которых ведется регистрация состояния объектов и действия персонала, с обязательной идентификацией по типу, дате и времени события, а также информации об источнике события;
- периодическая проверка целостности прикладного ПО, контроль файлов и папок ПО на соответствие предоставленным дистрибутивам. Проверяются как исполнимое ПО, так и технологические базы данных с периодичностью не реже 1 раза в год;

б) доработка ПО систем МПЦ-МПК и ЭЦ-МПК:

- использование системы паролей (различных уровней, например дежурный по станции, администратор и т. д.) для ограниченного доступа к настройкам операционной системы АРМ и к сетевому оборудованию, с заданием минимальной сложности пароля с определяемыми требованиями к количеству символов, сочетанию букв, цифр и специальных символов, для обеспечения однозначной аутентификации пользователей системы при всех видах доступа;
- блокирование неактивных (неиспользуемых) учетных записей пользователей АРМ после периода времени неиспользования;
- ограничение количества неуспешных попыток входа в систему, а также блокирование учетной записи пользователя при превышении пользователем количества неуспешных попыток входа в систему с АРМ или блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности);
- программная блокировка неиспользуемых портов в сетевых коммутаторах.

Дополнительно необходимо отметить, что изначально ПО систем МПЦ-МПК и ЭЦ-МПК основано на использовании ОС Linux с открытым исходным кодом для исключения возможности воздействия со стороны недекларированных возможностей и ослабления воздействия вредоносного ПО, а также использования закрытого протокола (собственной разработки) обмена данными.

При этом необходимо учитывать, что протокол разработки ЦКЖТ ФГБОУ ВО ПГУПС может применяться как в аналоговых, так и в цифровых (на основе волоконно-оптических линий) каналах связи, с поддержкой протоколов обмена данными типа X.25, IPX, TCP/IP, QNX Net (FLEET) и промышленных протоколов RS-485, RS-422 и т. д.;

в) применение новых технических решений в системах МПЦ-МПК и ЭЦ-МПК:

- интеграция в состав программно-аппаратных средств отечественной системы обнаружения вторжения (СОВ) для противодействия несанкционированному доступу и мониторинг работы локальной вычислительной сети (ЛВС) систем ЖАТ.

Реализация данной технической задачи для систем ЖАТ основывалась на том, что применяемые технические решения анализируют сетевой трафик по ряду позиций и выявляют подключение новых клиентских машин в сети ЛВС, сигнализируют о значительном превышении объемов данных, передаваемых в ЛВС, выявляют новые нехарактерные протоколы передачи данных в сети, осуществляют фильтрацию сетевых пакетов в различных режимах и т. д.

При анализе рынка отечественных СОВ был рассмотрен ряд разработчиков с опытом защиты сетевой инфраструктуры АСУ ТП (таких как АО НПО «Эшелон», ООО «Юзергейт» и т. д.), в системах МПЦ-МПК и ЭЦ-МПК было принято решение о применении российских программно-аппаратных комплексов «Рубикон-К» разработки АО НПО «Эшелон», которые выполняют функции межсетевого экрана, системы обнаружения вторжений и маршрутизатора, они сертифицированы ФСТЭК России и Минобороны РФ и обеспечивают необходимый уровень информационной безопасности, данный комплекс представлен на рис. 1, *а*, *б*.

а

б

Рис. 1. Программно-аппаратный комплекс:
а — «Рубикон-К mini», *б* — «Рубикон-К mini» в составе систем ЖАТ

Комплекс «Рубикон-К» обеспечивает оперативное сообщение об инцидентах в системе информационной безопасности ответственному персоналу (передачу в центры диагностики и мониторинга).

Настройка данного СОВ происходит с учетом требований Заказчика и предоставляемых каналов связи для передачи диагностической информации о работе СОВ, а установка данного СОВ выполняется в электротехнический шкаф центральной вычислительной системы МПЦ-МПК (ЭЦ-МПК) с подключением к коммутаторам линий ЛВС.

Простота установки и адаптации СОВ на базе «Рубикон-К», а также высокий класс защиты стали решающими факторами при принятии решения об их применении.

Можно констатировать, что применение данного программно-аппаратного комплекса позволяет оперативно отслеживать и принимать решения по всем случаям (инцидентам) несанкционированного доступа, но тем не менее данный вид защиты не гарантирует полного исключения угрозы остановки движения поездов на каком-либо участке или объекте (станции) по причине отключения систем централизации или автоблокировки из-за защитного отказа (сбоя), вызванного внешним вмешательством в работу систем ЖАТ.

Применение данного технического средства является одной из мер, повышающих киберзащищенность систем ЖАТ, но не является единственной и полностью достаточной;

- модернизация структуры линии связи на базе отечественных контроллеров защиты линии и применение распределенной структуры систем ЖАТ.

Большинство микропроцессорных систем ЖАТ в Российской Федерации имеют структуру с централизованным расположением оборудования, что означает исключение выходов каналов связи за пределы контролируемой зоны (поста ЭЦ). При организации распределенной структуры системы ЖАТ, например диспетчерской централизации или мультистанционной МПЦ, или интеграции системы автоблокировки в состав МПЦ, когда вычислительные средства МПЦ выполняют функцию автоблокировки, может возникать ситуация, требующая обеспечения киберзащиты каналов связи.

Данная задача решается путем применения дополнительных программных настроек в аппаратуре передачи данных, организации защищенных каналов (например, VPN-соединений) или применения контроллеров защиты линии для организации, защищенных волоконно-оптических линий передачи информации ограниченного доступа.

В качестве основного технического решения для систем ЖАТ разработки ЦКЖТ ФГБОУ ВО ПГУПС были выбраны контроллеры защиты линии типа FOBOS-100GL разработки ФГУП «РФЯЦ-ВНИИЭФ», данные контроллеры имеют сертификат ФСТЭК России и предназначены для создания защищенных волоконно-оптических систем передачи данных ограниченного доступа и защиты от утечки информации.

Контроллер защиты линии типа FOBOS-100GL, установленный в электротехнический шкаф центральной вычислительной системы МПЦ-МПК, представлен на рис. 2.

Контроллер защиты линии типа FOBOS-100GL выполняет следующие функции:

– постоянный контроль волоконно-оптических каналов на основе анализа коэффициента передачи с отключением передачи оптических сигналов при появлении дополнительных потерь (утечек или съемов информации);
– установка и контроль заданной мощности информационного оптического сигнала;
– активная защита линии связи от несанкционированных изменений конфигурации сети за пределами контролируемой зоны или попыток доступа к средствам защиты.

Применение данных контроллеров позволяет защитить от несанкционированного доступа как линии связи между различными АРМ систем ЖАТ, где применяются стандартизованные протоколы передачи данных (например, TCP/IP), так и линии связи с конечными исполнительными устройствами (промышленными контролерами), где применяется стандарт RS-485, Modbus и иные.

Рис. 2. Контроллер FOBOS-100GL

При функционировании FOBOS-100GL в составе волоконно-оптических систем передачи данных распределенной МПЦ-МПК, при имитации несанкционированного доступа к линии и вмешательства в работу канала, в соответствии с существующими требованиями по защите каналов передачи данных ограниченного доступа, происходит отключение передачи данных по линии и выдача сигнала «Тревога».

Существующий алгоритм работы контроллеров защиты линии приводит к прерыванию бесперебойного функционирования системы ЖАТ ввиду отсутствия поступления информации от удаленных объектов управления и контроля, что, в свою очередь, ведет к срыву перевозочного процесса. Тем не менее натурные совместные испытания устройств СОВ и контроллера защиты линии в составе системы МПЦ-МПК показали высокую эффективность работы, возможность организации защищенного канала удаленного управления и контроля и позволяет сделать вывод о достаточном уровне киберзащищенности.

Выполнение комплекса мероприятий по повышению киберзащищенности систем ЖАТ с проведением натурных испытаний выявило ряд существенных замечаний, из которых следует необходимость доработки проектной документации на данные системы с разработкой дополнительных технических решений по оборудованию и аппаратуре киберзащиты, а также изменений в алгоритмах работы контроллеров защиты линий.

3. Особенности кибербезопасности систем ЖАТ

Реализация требований кибербезопасности в области ЖАТ, а также особенность построения микропроцессорных систем АСУТП уже давно наметили явную необходимость выделения микропроцессорных систем управления ЖАТ как отдельного класса АСУТП.

Данная необходимость неоднократно обсуждалась в публикациях и при проведении научных совещаний и конференций [12].

Необходимо отметить, что системы ЖАТ как средства управления движением поездов являются системами реального времени, которые функционируют 24 часа в сутки и, соответственно, имеют сильную зависимость от непрерывности поступления информации об объектах контроля и управления (динамически изменяемой ситуации на полигоне управления). Следовательно, можно утверждать, что любое вмешательство в работу систем ЖАТ, вызвавшее блокирование работоспособности (сбой, перезагрузка, потеря информации, ложная информация и т. д.), уже достигло своей цели — срыва бесперебойной работы системы ЖАТ. Соответственно, угрозы, приводящие к снижению надежности процесса перевозок, не требуют высокого уровня квалификации

злоумышленника и могут быть реализованы с помощью несложного вредоносного ПО, без применения специальных программ и оборудования.

В то же время обнаружение программно-аппаратными средствами киберзащиты несанкционированного доступа в систему управления движением поездов любого уровня должно приводить к блокированию работы и исключению дальнейшего доступа злоумышленника до устранения уязвимости в ПО, что приводит к ситуации, когда любое несанкционированное проникновение (только своим фактом) означает успех атаки, так как приводит систему в состояние защитного отказа.

Существующее столкновение интересов при решении общей задачи киберзащищенности требует других подходов как в оценке модели угроз для систем ЖАТ и их классификации, так и необходимости иной интерпретации требований кибербезопасности к АСУТП на железнодорожном транспорте, данные особенности и предложения по их реализации рассматривались в ряде публикаций [13].

По мнению автора, именно проблема «как обнаружить?» несанкционированное вмешательство в микропроцессорные системы ЖАТ отходит на второй план, перед проблемой «что с этим делать?» в режиме реального времени, без нарушения перевозочного процесса и минимизации рисков, так как не существует таких средств киберзащиты, которые бы полностью исключали вероятность несанкционированного вмешательства в автоматическом режиме, без участия человека (оператора). Соответственно, требуется формализация процедур информирования и реагирования на инциденты обслуживающим (оперативным) персоналом, установление четких правил по обеспечению информационной безопасности во всех режимах функционирования систем ЖАТ и конкретных мероприятий по противодействию несанкционированному вмешательству (в случае его обнаружения) в работу устройств ЖАТ, разработка регламента взаимодействия всех подразделений железнодорожной компании при нарушении кибербезопасности систем, обеспечивающих управление перевозочным процессом.

Заключение

Коллектив ЦКЖТ ПГУПС разрабатывает, проектирует и внедряет системы ЖАТ уже более 25 лет. Требования и подходы к проектированию, применяемые ранее при создании микропроцессорных систем ЖАТ, в первую очередь основывались на обеспечении функциональной безопасности систем, электромагнитной совместимости устройств, исключении недекларированных возможностей в ПО. Задачи киберзащищенности систем ЖАТ решались параллельно без тщательной проработки и в значительной степени носили организационно-технический характер, например выделение отдельных каналов связи, изоляция каналов управления систем обеспечения безопасности движения поездов от сетей общего доступа и т. д., это обусловлено различием между подходами и методами обеспечения информационной безопасности и практикой решения задач при разработке систем, обеспечивающих безопасность движения поездов.

Только всестороннее и комплексное изучение этой сложной научно-технической задачи, выработка рациональных подходов при реализации позволят встроить процессы обеспечения кибербезопасности в существующие алгоритмы функционирования систем обеспечения безопасности движения поездов, при этом не снижая надежность функционирования систем ЖАТ. Особенно это актуально при применении многостанционной (распределенной) микропроцессорной системы централизации с интеграцией функций систем интервального регулирования движением поездов и реализации безопасного вычисления алгоритмов в «едином» аппаратно-программном пространстве (вычислительном центре), которое требует предоставления защищенных каналов связи, выходящих за пределы контролируемой зоны. Перспективным направлением в области обеспечения кибербезопасности систем ЖАТ является разработка комплексных систем диагностирования и мониторинга инфраструктуры с интегрированными функциями обнаружения вторжения и контроля защиты линий связи, применение такой аппаратно-программной платформы, которая обеспечит эксплуатирующий персонал

(инженеров центров диагностики и мониторинга) полным набором инструментов по оперативному управлению и защите всех информационно-управляющих систем. ▲

Библиографический список

1. Цифровые высокоскоростные ж/д магистрали как часть цифровой экономики. BIM-ГИС-технологии в проектах строительства ВСМ. Опыт Южной Кореи, Гонконга и др. стран. — URL: http://www.eurasiancommission.org/.
2. Бердышева Ю. А. Инструменты реализации цифровой трансформации железнодорожного транспорта / Ю. А. Бердышева, Е. А. Жаркова // Вестник Сибирского государственного университета путей сообщения: Гуманитарные исследования. — 2022. — № 1(12). — С. 5–8. — DOI: 10.52170/2618-7949_2022_12_5.
3. Privalov A. Evaluating the functioning quality of data transmission networks in the context of cyberattacks / A. Privalov, D. Titov, I. Kotenko et al. // Energies. — 2021. — Vol. 14. — № 16. — DOI: 10.3390/en14164755.
4. Метельков А. Н. Киберучения: зарубежный опыт защиты критической инфраструктуры / А. Н. Метельков // Правовая информатика. — 2022. — № 1. — С. 51–60. — DOI: 10.21681/1994-1404-2022-1-51-60.
5. Куприяновский В. П. BIM на железных дорогах мира - развитие, примеры, стандарты / В. П. Куприяновский, О. Н. Покусаев, А. А. Климов и др. // International Journal of Open Information Technologies. — 2020. — Т. 8. — № 5. — С. 57–80.
6. Ададуров С. Е. Международная кибербезопасность на железнодорожном транспорте: методологические подходы и нормативная методическая база / С. Е. Ададуров, С. В. Диасамидзе, А. А. Корниенко, А. А. Сидак // Вестник Научно-исследовательского института железнодорожного транспорта. — 2015. — № 6. — С. 9–15.
7. Безродный Б. Ф. Особенности кибербезопасности АСУ ТП на железнодорожном транспорте / Б. Ф. Безродный // Системы безопасности: Технический журнал. — 2020. — № 6. — С. 34–35.
8. Кибербезопасность микропроцессорных систем железнодорожной автоматики / Б. Ф. Безродный, И. А. Наседкин, Р. С. Бакуркин и др. // Автоматика, связь, информатика. — 2020. — № 12. — С. 4–8. — DOI: 10.34649/AT.2020.12.12.002.
9. Гарбук С. В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты / С. В. Гарбук, Д. И. Правиков, А. В. Полянский, И. В. Самарин // Вопросы кибербезопасности. — 2019. — № 3(31). — С. 63–71. — DOI: 10.21681/2311-3456-2019-3-63-71.
10. Lakhno V. Development of the intelligent decision-making support system to manage cyber protection at the object of informatization / V. Lakhno, Yu. Boiko, A. Mishchenko et al. // Eastern-European Journal of Enterprise Technologies. — 2017. — Vol. 2. — № 9(86). — Pp. 53–61. — DOI: 10.15587/1729-4061.2017.96662.
11. Гордейчик С. В. Кибербезопасность микропроцессорных систем управления на железнодорожном транспорте. Научное издание / С. В. Гордейчик. — М.: Горячая Линия — Телеком, 2021. — 120 с.
12. Макаров Б. А. Актуальность кибербезопасности на железнодорожном транспорте / Б. А. Макаров // Вестник Института проблем естественных монополий: Техника железных дорог. — 2015. — № 3(31). — С. 10–15.
13. Ададуров С. Е. Реагирование на инциденты информационной безопасности в микропроцессорных системах железнодорожной автоматики и телемеханики / С. Е. Ададуров, А. П. Глухов, А. А. Сидак и др. // Двойные технологии. — 2018. — № 2(83). — С. 76–81.

TRANSPORT AUTOMATION RESEARCH, 2022, Vol. 8, No. 3, pp. 266–275
DOI: 10.20295/2412-9186-2022-8-03-266-275

Provision of Cyber Security for Microprocessor and Relay Processor Interlocking Systems on Russia Railway JSC. Prospects and Practical Application of the Remedies

Information about author

Moiseev V. V., Chief Engineer of Computer Railway Technology Center, Department of Automation and Remote Control on Railways. E-mail: moiseev@crtc.spb.ru

Emperor Alexander I St. Petersburg State Transport University, Saint Petersburg

Abstract: The article expounds major aspects of cyber protection provision for railway automation and remote control system series, the developments made by staff of Computer railway technology center of Emperor Alexander I St. Petersburg State Transport University. Major topical provisions in the sphere of development and designing of microprocessor interlocking distributed systems, including regulatory provision, are considered. Promising domestic informational safety remedies are presented and analysis of requirements on cyber safety for microprocessor and relay processor interlocking systems is made as well as practical realization of measure series on cyber safety level rise for railway automation and remote control systems is presented. A number of technical solutions in the field of cyber security in the implementation of distributed control systems in railway transport are considered using the example of microprocessor interlocking system MPC-MPK.

Keywords: microprocessor interlocking; relay processor interlocking; informational safety; cyber security; cyber protection; intrusion detection system; control distributed system.

References

1. *Tsifrovye vysokoskorostnye zh/d magistrali kak chast' tsifrovoy ekonomiki. BIM-GIS-tekhnologii v proektakh stroitel'stva VSM. Opyt Yuzhnoy Korei, Gonkonga i dr. stran* [Digital high-speed railway lines as part of the digital economy. BIM-GIS-technologies in high-speed railway construction projects. Experience of South Korea, Hong Kong and other countries]. Available at: http://www.eurasiancommission.org/. (In Russian)
2. Berdysheva Yu. A. Instrumenty realizatsii tsifrovoy transformatsii zheleznodorozhnogo transporta [Tools for the implementation of the digital transformation of railway transport]. *Vestnik Sibirskogo gosudarstvennogo universiteta putey soobshcheniya: Gumanitarnye issledovaniya* [Bulletin of the Siberian State University of Railway Transport: Humanitarian Research]. 2022, I. 1(12), pp. 5–8. DOI 10.52170/2618-7949_2022_12_5. (In Russian)

3. Privalov A., Titov D., Kotenko I. Evaluating the functioning quality of data transmission networks in the context of cyberattacks. Energies. 2021, vol. 14, I. 16. DOI: 10.3390/en14164755.
4. Metel'kov A. N. Kiberucheniya: zarubezhnyy opyt zashchity kriticheskoy infrastruktury [Cyber teachings: foreign experience in protecting critical infrastructure]. *Pravovaya informatika* [Legal informatics]. 2022, I. 1, pp. 51–60. DOI: 10.21681/1994-1404-2022-1-51-60. (In Russian)
5. Kupriyanovskiy V. P., Pokusaev O. N, Klimov A. A. *BIM na zheleznykh dorogakh mira — razvitie, primery, standarty* [BIM on the railways of the world — development, examples, standards]. International Journal of Open Information Technologies. 2020, vol. 8, I. 5, pp. 57–80. (In Russian)
6. Adadurov S. E., Diasamidze S. V., Kornienko A. A., Sidak A. A. Mezhdunarodnaya kiberbezopasnost' na zheleznodorozhnom transporte: metodologicheskie podkhody i normativnaya metodicheskaya baza [International cybersecurity in railway transport: methodological approaches and normative methodological base]. *Vestnik Nauchno-issledovatel'skogo instituta zheleznodorozhnogo transporta* [Bulletin of the Research Institute of Railway Transport]. 2015, I. 6, pp. 9–15. (In Russian)
7. Bezrodnyy B. F. Osobennosti kiberbezopasnosti ASU TP na zheleznodorozhnom transporte [Features of cybersecurity of APCS in railway transport]. *Sistemy bezopasnosti: Tekhnicheskiy zhurnal* [Security Systems: Technical Journal]. 2020, I. 6, pp. 34–35. (In Russian)
8. Bezrodnyy B. F., Nasedkin I. A., Bakurkin R. S. Kiberbezopasnost' mikroprotsessornykh sistem zheleznodorozhnoy avtomatiki [Cybersecurity of microprocessor systems of railway automatics]. *Avtomatika, svyaz', informatica* [Automation, communication, informatics]. 2020, I. 12, pp. 4–8. DOI 10.34649/AT.2020.12.12.002. (In Russian)
9. Garbuk S. V., Pravikov D. I., Polyanskiy A. V, Samarin I. V. Obespechenie informatsionnoy bezopasnosti ASU TP s ispol'zovaniem metoda prediktivnoy zashchity [Ensuring information security of automated process control systems using the predictive protection method]. *Voprosy kiberbezopasnosti* [Cybersecurity Issues]. 2019, I. 3(31), pp. 63–71. DOI 10.21681/2311-3456-2019-3-63-71. (In Russian)
10. V. Lakhno, Yu. Boiko, A. Mishchenko Development of the intelligent decision-making support system to manage cyber protection at the object of informatization. Eastern-European Journal of Enterprise Technologies. 2017, vol. 2, I. 9(86), pp. 53–61. DOI 10.15587/1729-4061.2017.96662.
11. Gordeychik S. V. *Kiberbezopasnost' mikroprotsessornykh sistem upravleniya na zheleznodorozhnom transporte* [Cybersecurity of microprocessor control systems in railway transport. Scientific publication]. Moscow: Goryachaya Liniya – Telekom Publ., 2021. 120 p. (In Russian)
12. Makarov B. A. Aktual'nost' kiberbezopasnosti na zheleznodorozhnom transporte [The relevance of cybersecurity in railway transport]. *Vestnik Instituta problem estestvennykh monopoliy: Tekhnika zheleznykh dorog* [Bulletin of the Institute for Natural Monopoly Problems: Railway Engineering]. 2015, I. 3(31), pp. 10–15. (In Russian)
13. Adadurov S. E, Glukhov A. P., Sidak A. A. Reagirovanie na intsidenty informatsionnoy bezopasnosti v mikroprotsessornykh sistemakh zheleznodorozhnoy avtomatiki i telemekhaniki [Responding to information security incidents in microprocessor systems of railway automation and telemechanics]. *Dvoynye tekhnologii* [Dual technologies]. 2018, I. 2(83), pp. 76–81. (In Russian)