ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНЫМ АТАКАМ В СФЕРЕ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Бакуркин Р.С.[1], Безродный Б.Ф.[2], Коротин А.М.[3]

В данной статье предлагается подход к классификации микропроцессорных систем управления (МПСУ) в сфере железнодорожного транспорта и рассматриваются возможные способы их киберзащиты, в том числе предлагается способ защиты информации, передаваемой между станцией и локомотивом по радиоканалу DMR–RUS. Среди МПСУ предлагается выделить три основных группы систем – МПСУ подвижного состава, стационарные МПСУ и системы связи. Для стационарных МПСУ рассматриваются возможные способы защиты от компьютерных атак. На примерах микропроцессорной системы электрической централизации и системы управления объектами электроснабжения, учитывая их назначение и функциональные особенности, рассматриваются пассивный способ мониторинга компьютерных атак с помощью специализированного сенсора и возможность применения программно–аппаратных комплексов для организации защищенных соединений. Для защиты каналов связи между стационарными системами и системами подвижного состава, организованных на базе применения радиоканала DMR–RUS, предлагается рассмотреть обобщенную модель передачи информации по радиоканалу и разработать специальный уровень безопасности – уровень системы контроля целостности и обеспечения достоверности (СКЦПД), который позволит удостоверится, что поездная информация получена от легитимной станции или локомотива. Также отмечается, что из–за особенностей МПСУ, не всегда возможно применить традиционные способы защиты от компьютерных атак и приходится адаптировать известные или разрабатывать новые способы защиты.

***Ключевые слова**: информационная безопасность, кибербезопасность, АСУ ТП в железнодорожном транспорте, МПСУ, способы защиты МПСУ, DMR–RUS, СКЦПД.*

DOI 10.21681/2311-3456-2016-4-29-35

Введение

За последнее время во всём мире значительно увеличилось количество компьютерных атак на объекты критической инфраструктуры государств и крупных компаний. Системы управления в сфере железнодорожного транспорта (ЖТ) не стали исключением. По данным американского центра по безопасности индустриальных систем (US ICS-CERT) за 2015 8% всех инцидентов, связанных с безопасностью критической инфраструктуры, приходились на транспортные системы [1].

Уровень опасности также возрастает в связи с расширением области применения самих микропроцессорных систем управления (МПСУ). На сегодняшний день в ОАО «РЖД» используется около 60 разных типов МПСУ, а общее количество микропроцессорных систем составляет примерно 40000.

Как правило, безопасность объектов критической инфраструктуры строится на базе определенных требований и рекомендаций, специфичных для конкретной сферы деятельности, а также особенностей процесса эксплуатации систем. В рамках статьи предлагается систематизировать первый опыт проведения исследований защищенности МПСУ ЖТ, выбрать способы их защиты от компьютерных атак. Целью систематизации является определение типовых МПСУ и путей обеспечения их кибербезопасности.

1. Определение типовых МПСУ

Среди МПСУ, применяемых в сфере железнодорожного транспорта, можно условно выделить три основные группы систем – системы железнодорожного подвижного состава, системы объектов железнодорожной инфраструктуры и системы связи.

К системам железнодорожного подвижного состава относятся МПСУ, расположенные непосредственно на борту подвижного состава (МПСУ подвижного состава). Такие МПСУ, в первую очередь, отвечают за управление подвижным составом, обеспечение безопасности движения, передачу информации с борта локомотива в системы объектов железнодорожной инфраструктуры. К ним можно отнести:

- микропроцессорные системы управления и диагностики (МПСУиД);
- локомотивные устройства безопасности;
- системы взаимодействия с локомотивом (СВЛ ТР).

К системам объектов железнодорожной инфраструктуры относятся МПСУ, распложенные непосредственно на станциях, перегонах и сор-

1 Бакуркин Роман Сергеевич, ОАО «НИИАС», г. Москва, r.bakurkin@vniias.ru
2 Безродный Борис Федерович, доктор технических наук, профессор, ОАО «НИИАС», г. Москва, b.bezrodnyi@vniias.ru
3 Коротин Александр Михайлович, ОАО «НИИАС», г. Москва, a.korotin@vniias.ru

тировочных горках (стационарные МПСУ). Основное назначение таких систем заключается в управлении движением поездов на станциях и перегонах, обеспечении безопасности движения, формировании и расформировании составов. К таким МПСУ относят:

- системы электрической централизации (ЭЦ);
- системы диспетчерской централизации (ДЦ);
- системы горочной централизации (ГЦ);
- системы автоблокировки (АБТЦ);
- системы управления объектами электроснабжения.

К системам связи относятся системы, использующиеся для организации канала связи между МПСУ и (или) их компонентами. Такие системы могут быть расположены как на железнодорожном подвижном составе, так и на стационарных объектах. Выделяют два основных типа систем связи:

- системы, обеспечивающие взаимодействие между стационарными МПСУ и (или) их компонентами (в случае распределенных систем);
- системы, обеспечивающие взаимодействие между стационарными МПСУ и МПСУ подвижного состава.

В первом случае для обеспечения связи используются проводные каналы передачи данных [2], к которым, как правило, относят витую пару, коаксиальный кабель и оптоволокно. Для взаимодействия между стационарными МПСУ и МПСУ подвижного состава применяются беспроводные или комбинированные каналы передачи данных. В качестве беспроводных каналов передачи данных используется, как правило, радиоканал (Wi-Fi, GSM, GSM-R, TETRA, DMR).

2. Выбор способов защиты МПСУ от компьютерных атак

Все вышеперечисленные системы участвуют в перевозочном процессе, а это значит, что выполнение требуемых от систем функций при всех предусмотренных условиях применения должно осуществляться без возникновения недопустимого риска причинения вреда жизни или здоровью людей, имуществу и окружающей среды. Это обеспечивается методами функциональной безопасности, но при этом защита систем от компьютерных атак не учитывается. Такие атаки могут нарушить процесс обеспечения функциональной безопасности и привести к серьезным негативным последствиям, таким как нарушение безопасности движения ЖТ, снижение эффективности процесса перевозок, операционные и/или финансовые потери.

Защита систем от компьютерных атак обеспечивается методами, относящимися к кибербезопасности. Для каждой системы выбор таких методов является уникальным, и как правило, основывается на результатах исследований киберзащищенности систем. Исследования киберзащищенности проводятся с целью выявления существующих уязвимостей системы, выработки рекомендаций по их устранению и правильному использованию встроенных или дополнительных средств защиты. При выборе мер защиты учитываются особенности функционирования систем, чтобы выбираемые меры не оказывали отрицательного влияния на штатный режим функционирования, соотносились с существующими мерами функциональной безопасности и иными применяемыми мерами безопасности. Более подробно связь между функциональной и кибербезопасность описывается в статье [3].

Следует отметить, что системы связи не обеспечивают конфиденциальность и целостность передаваемой информации и отвечают только за доступность информации и канала связи. Таким образом, в случае передачи через системы связи информации, требующей обеспечения целостности и конфиденциальности, соответствующие меры кибербезопасности должны быть реализованы непосредственно в стационарных МПСУ и МПСУ подвижного состава.

Рассмотрим возможные способы защиты нераспределенных (не использующих для взаимодействия между своими компонентами внешние системы связи) стационарных МПСУ от компьютерных атак. В качестве примера такой системы может быть рассмотрена система электрической централизации.

Современные системы электрической централизации имеют схожую между собой структуру и, как правило, состоят из следующих основных компонентов (рис.1):

- Центральный процессор (ЦП);
- Система контроллеров напольных устройств (СКНУ);
- Автоматизированное рабочее место дежурного по станции (АРМ ДСП).

Главным компонентом системы является ЦП, реализующий логику работы системы и процесс обеспечения безопасности при движении поездов. ЦП осуществляет обработку данных таким образом, чтобы обеспечить безопасное управление напольными устройствами с учетом всех взаимозависимостей. Кроме того, ЦП обеспечивает трансформацию команд, полученных от АРМ, в ко-

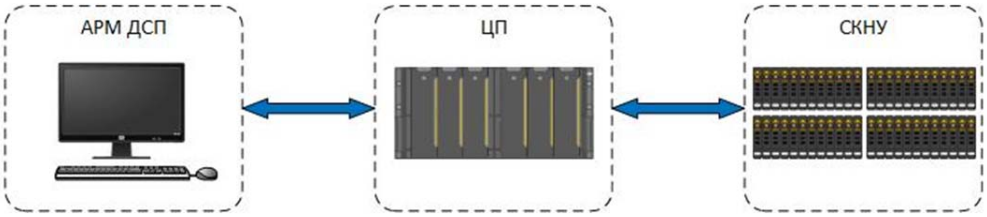

***Рис.1**. Основные компоненты системы ЭЦ*

манды, которые передаются напольным устройствам (стрелкам, светофорам и т.д.).

Непосредственное управление напольными устройствами, а также отслеживание их состояния, осуществляется через СКНУ, которые обеспечивают выполнение команд, полученных от ЦП, и сбор данных с напольных устройств.

Управление системой осуществляется с АРМ ДСП, созданного на базе промышленной ЭВМ.

Учитывая особенности систем электрической централизации, одним из возможных способов обеспечения защиты является применение пассивного сенсора мониторинга компьютерных атак.

Сенсор мониторинга компьютерных атак предназначен для анализа протоколов взаимодействия между компонентами системы и выявления инцидентов кибербезопасности. Применение данного сенсора позволяет своевременно выявлять атаки на систему и осуществлять расследование инцидентов кибербезопасности. На рисунке (рис.2) представлено расположение сенсора в локальной сети системы.

В локальной сети системы электрической централизации сенсор располагается между двумя основными компонентами - АРМ ДСП и ЦП, таким образом обеспечивая мониторинг сетевого траффика и своевременное оповещение в случае выявления инцидентов между данными компонентами. В зависимости от архитектуры системы и применяемых протоколов, возможно также подключение сенсора между ЦП и СНК.

Так как между компонентами системы циркулирует ответственная информация и осуществляется передача команд управления, то активное влияние (блокирование, фильтрация и др. активные действия) на сетевой трафик между ними не допускается. Сенсор функционирует посредством зеркалирования (копирования) сетевого траффика и, таким образом, осуществляет пассивный мониторинг, не оказывая влияния на траффик между компонентами.

Для выявления инцидентов кибербезопасности в сенсоре применяются специализированные алгоритмы их анализа и обнаружения. Сенсор обладает следующими основными функциональными возможностями:

- обнаружение аномалий в сетевом траффике;
- агрегация инцидентов безопасности и построение цепочек потенциально опасных событий;
- протоколирование действий операторов, событий и состояний контролируемой системы;
- обеспечение безопасного хранения запротоколированных событий контролируемой системы даже в случае ее компрометации.

Применение сенсора для обеспечения кибербезопасности конкретной системы микропроцессорной централизации рассмотрено в статье В.А. Гросса [4] на примере системы МПЦ EBILock 950.

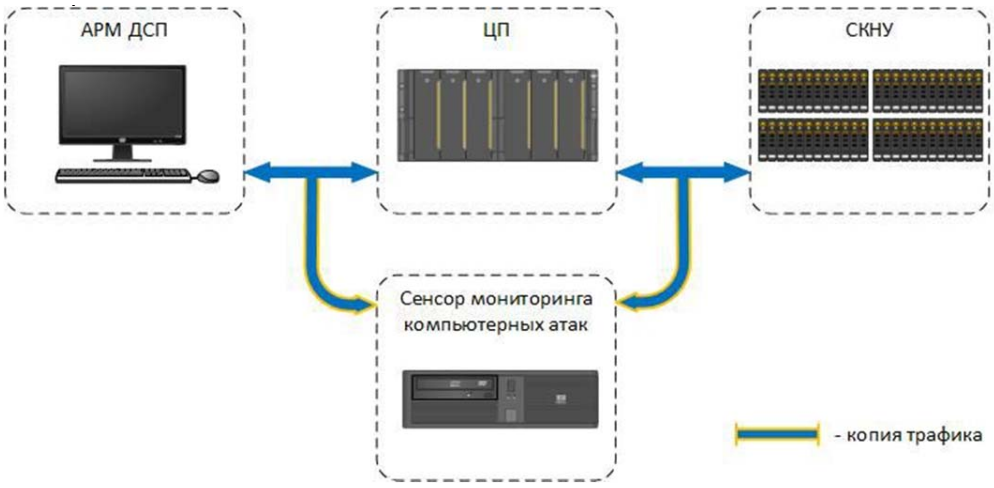

***Рис.2**. Расположение сенсора мониторинга компьютерных атак в локальной сети системы ЭЦ*

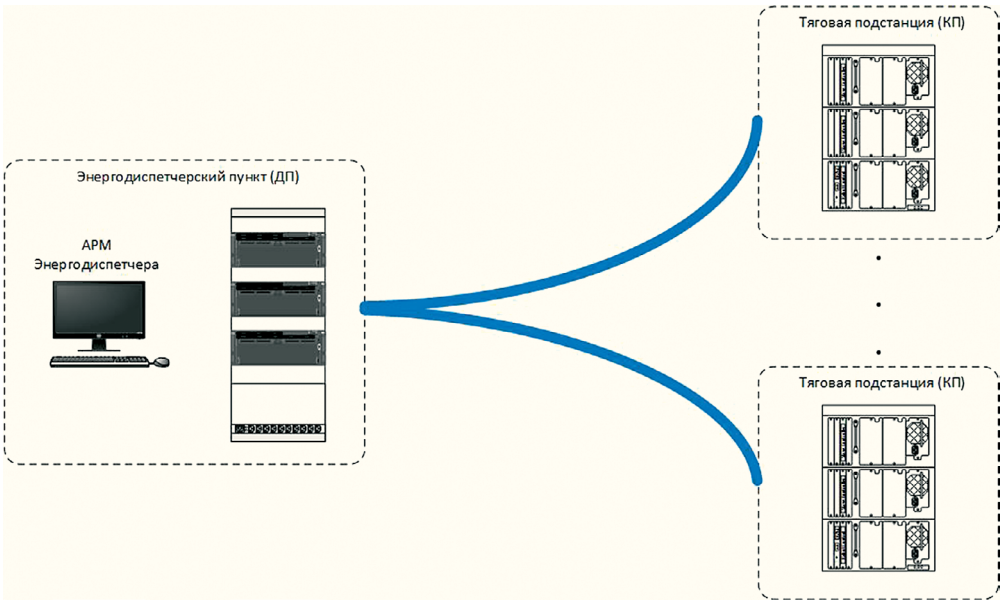

***Рис.3**. Типовая схема системы управления объектами электроснабжения*

Описанный выше способ не может использоваться для блокирования и противодействия компьютерным атак и применяется только для выявления инцидентов кибербезопасности. Как было сказано выше, это связано с критичностью передаваемой между компонентами системы информации и, как следствие, невозможностью оказания активного влияния на сетевой трафик (блокирование, фильтрация).

Далее предлагается рассмотреть способ защиты распределенных стационарных МПСУ от компьютерных атак. В качестве примера возьмем систему управления объектами электроснабжения.

Системы управления объектами электроснабжения предназначены для управления объектами электроснабжения железнодорожного транспорта, расположенными на тяговых подстанциях и постах секционирования. Такие системы, как правило, состоят из одного диспетчерского пункта (ДП) и нескольких контролируемых пунктов (КП). Типовая схема системы представлена на рисунке (рис.3).

В состав ДП входят автоматизированное рабочее место (АРМ) энергодиспетчера, с которого осуществляется непосредственное управление объектами электроснабжения, и сервер базы данных, который хранит в себе всю текущую информацию о данных объектах. КП состоит из специализированного оборудования, осуществляющее прием команд управления от ДП и дальнейшую их трансформацию в команды, поступающие непосредственно на объекты управления, а также осуществляет обратную связь с ДП путем передачи и трансформации информации, полученной от объектов управления.

Для защиты от компьютерных атак, направленных на канал связи между распределенными компонентами системы (ДП и КП), предлагается применить программно-аппаратный комплекс (ПАК) для организации защищенного шифрованного VPN-соединения. Данный ПАК установляется в ДП и всех КП, и путем взаимодействия ПАК ДП со всеми ПАК КП организуется защищенный канал связи. Ниже (рис.4) представлена типовая схема системы управления объектами электроснабжения с применением ПАК.

Используемый ПАК должен обеспечивать минимальное вмешательство в существующую инфраструктуру системы и не оказывать влияния на передаваемую информацию.

Аналогичный способ защиты может использоваться и при взаимодействии стационарных МПСУ с МПСУ подвижного состава. Однако, следует отметить, что применение VPN в некоторых системах связи может ограничиваться их пропускной способностью. В частности, система связи между станцией и локомотивом, построенная на базе радиоканала DMR-RUS, обладает низкой пропускной способностью и применение в ней VPN-соединения невозможно. В связи с этим, в случае отсутствия конфиденциальной информации в МПСУ, для защиты передаваемой информации возможно использование системы обеспечения целостности и подтверждения достоверности информации [5].

Текущая модель передачи информации по радиоканалу, как правило, содержит два уровня – уровень приложения, на котором происходит обмен информацией между железнодорожными

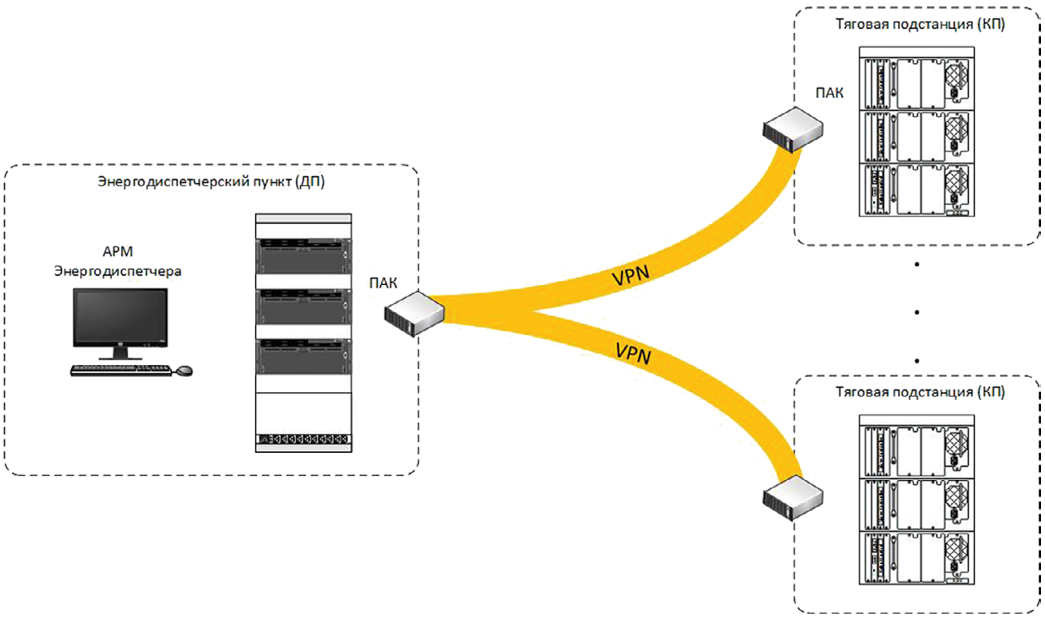

***Рис.4**. Типовая схема системы управления объектами электроснабжения с применением ПАК при организации защищенного соединения*

системами управления, и канальный уровень, или уровень радиоканала, который используется для передачи информации уровня приложения между радиостанциями. Системы связи на базе радиоканала, участвующие в управлении движением поездов, согласно европейскому стандарту EN 50129-2, считаются открытыми системами передачи данных, и, как следствие, требуют дополнительных мер защиты.

Для обеспечения целостности и достоверности передаваемой по радиоканалу информации предлагается разработать и реализовать дополнительный уровень модели, расположенный между уровнем приложения и канальным уровнем и обеспечивающий необходимый уровень защиты. На рисунке (рис.5) представлена пред-

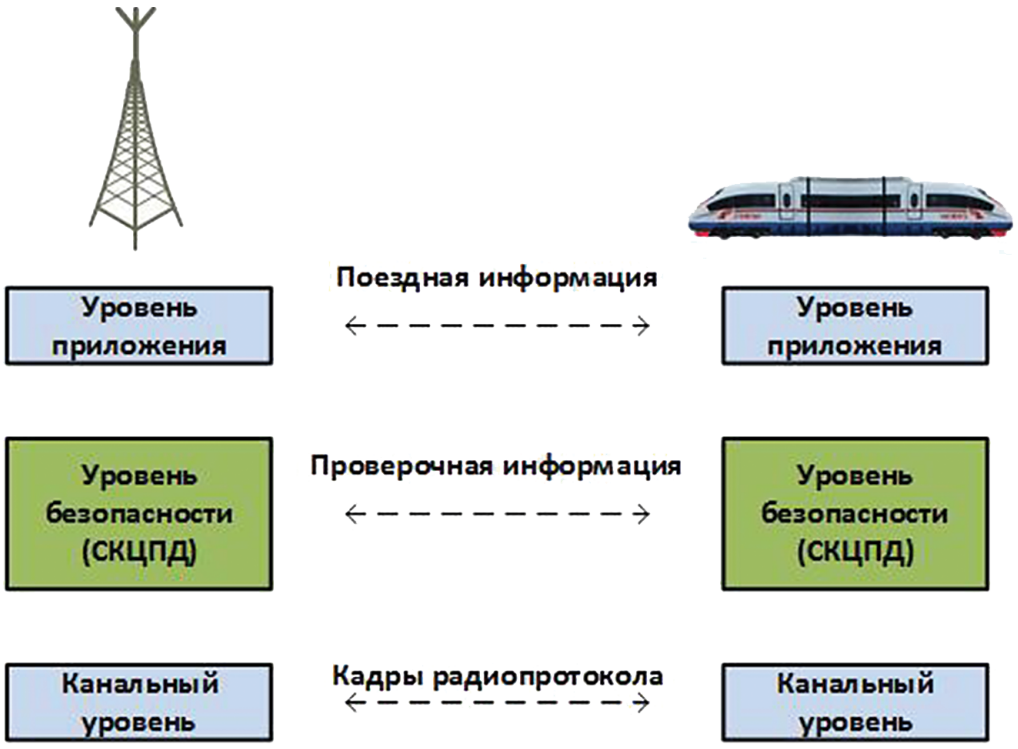

***Рис.5**. Предлагаемая модель передачи поездной информации по радиоканалу с ограниченной пропускной способностью*

лагаемая модель передачи поездной информации по радиоканалу с ограниченной пропускной способностью.

Предлагаемый уровень будем называть уровнем безопасности, или уровнем системы контроля целостности и обеспечения достоверности (СКЦПД). Предполагается, что программно-аппаратные компоненты СКЦПД, установленные на станции и локомотиве, будут обмениваться специально сформированной проверочной информацией (ЭЦП или коды аутентификации (имитовставка, HMAC)), подтверждающей, что поездная информация получена от легитимной станции или локомотива.

Заключение

Таким образом, рассмотренные в статье способы противодействия компьютерным атакам на МПСУ, позволят повысить уровень киберзащищенности систем, однако, необходимо учитывать, что применяемые для этого средства защиты также нужно поддерживать в актуальном состоянии и осуществлять их техническую поддержку. На сегодняшний день, для систем железнодорожного подвижного состава и объектов железнодорожной инфраструктуры уже проводятся исследования киберзащищенности [6-12], для централизованных и распределенных МПСУ были предложены описанные выше решения по обеспечению кибербезопасности. Тем не менее, применение таких решений в ряде случаев невозможно в связи с ограниченными функциональными возможностями и характеристиками систем, например, с ограничениями пропускной способности канала связи между системами и (или) их компонентами, что было проиллюстрировано на примере системы передачи информации между станцией и локомотивом на базе радиоканала DMR-RUS. Поэтому, для защиты информации, передаваемой в рамках такой системы, предлагается разработать систему контроля целостности и обеспечения достоверности информации (СКЦПД). В дальнейшем представляется целесообразным провести исследования по выбору оптимального способа построения СКЦПД, а также разработать и реализовать саму систему.

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им. Н.Э.Баумана, г. Москва, v.tsirlov@bmstu.ru*

Литература

1. ICS-CERT. ICS-MM201512 November-December // ICS-CERT Monitor Newsletters. 2015. 10 p. URL: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.
2. Зюко А.Г., Кловский Д.Д., Коржик В.И., Назаров М.В. Теория электрической связи. Учебник для вузов. / Под ред. Д.Д. Кловского. М.: Радио и связь, 1999. 432с.
3. Barnert Tomasz, Kosmowski Kazimierz T., Piesik Emilian, Śliwiński Marcin. Security aspects in functional safety analysis // Journal of Polish Safety and Reliability Association, 2014, Vol. 5, No 1, 8 p., URL: http://jpsra.am.gdynia.pl/upload/SSARS2014PDF/VOL1/SSARS2014-BarentKosmowski.pdf.
4. Гросс В.А. Повышение киберзащищенности МПСУ ЖАТ // Автоматика, связь, информатика. 2016. № 5. С. 12-15.
5. Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». М.: Радио и связь, 1999. 325 с.
6. Шубинский И.Б., Макаров Б.А. Немного о кибербезопасности // Автоматика, связь, информатика. 2014. № 8. С. 15-18.
7. Шубинский И.Б., Макаров Б.А. О киберзащищенности информационных систем управления движением поездов // Автоматика, связь, информатика. 2014. № 11. С. 9-12.
8. Макаров Б.А. Актуальность кибербезопасности на железнодорожном транспорте // Вестник Института проблем естественных монополий: Техника железных дорог. 2015. № 3 (31). С. 10-15.
9. Гордейчик С.В. Кибербезопасность микропроцессорных систем ЖАТ // Автоматика, связь, информатика. 2015. № 4. С. 4-6.
10. Гордейчик С.В., Грицай Г.С., Баранов Д.С. Модель киберугроз МПЦ // Автоматика, связь, информатика. 2015. № 7. С. 18-20.
11. Gordeychik S., Timorin A., Gritsai G. The Great Train Cyber Robbery // Schedule 32. Chaos Communication Congress (Congress Center Hamburg, Germany, December 27-30, 2015). URL: https://media.ccc.de/v/32c3-7490-the_great_train_cyber_robbery.
12. Розенберг Е.Н. Системы диагностики и их киберзащищенность // Автоматика, связь, информатика. 2015. № 10. С. 20-21.
13. Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУ ТП // Вопросы кибербезопасности. 2015. № 2 (10). С. 56-59.

COUNTERACTION TO COMPUTER ATTACKS IN RAILWAY TRANSPORT

Bakurkin R.[4], Bezrodnyi B.[5], Korotin A.[6]

We suggest to distinguish three main groups of systems: MPCS of rolling stock, stationary MPCS and communication systems. We consider possible ways of protection against computer attacks for stationary MPCS. By the examples of microprocessor system of electric centralization and systems of power supply facilities considering its purpose and functional characteristics we show passive way of computer attacks monitoring with specialized sensor and the possibility of the use of hardware and software complexes for organization of secure connections. To protect links between stationary systems and systems of rolling stock, based on the use of DMR-RUS radio channel, we propose to consider generalized model of transmission of information by radio channel and to develop special level of security – the level of integrity monitoring and reliability verification system (IMRVS), which would help to make sure that the train information was got from legitimate station or locomotive. It was also noted that because of MPCS characteristics it is not always possible to use traditional ways of protection against computer attacks or to develop new ways of protection.

***Keywords**: Information security, cybersecurity, ICS in railway transport, MPCS, the ways of MPCS protection, DMR-RUS, IMRVS.*

Reference

1. ICS-CERT. ICS-MM201512 November-December, ICS-CERT Monitor Newsletters. 2015. 10 p. URL: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.
2. Zyuko A.G., Klovskiy D.D., Korzhik V.I., Nazarov M.V. Teoriya elektricheskoy svyazi. Uchebnik dlya vuzov. Pod red. D.D. Klovskogo. M.: Radio i svyaz', 1999. 432 p.
3. Barnert Tomasz, Kosmowski Kazimierz T., Piesik Emilian, Śliwiński Marcin. Security aspects in functional safety analysis // Journal of Polish Safety and Reliability Association, 2014, Vol. 5, No 1, 8 p., URL: http://jpsra.am.gdynia.pl/upload/SSARS2014PDF/VOL1/SSARS2014-BarentKosmowski.pdf.
4. Gross V.A. Povyshenie kiberzashchishchennosti MPSU ZhAT, Avtomatika, svyaz', informatika. 2016. No 5, pp. 12-15.
5. Konyavskiy V.A. Upravlenie zashchitoy informatsii na baze SZI NSD «Akkord». M.: Radio i svyaz', 1999. 325 P.
6. Shubinskiy I.B., Makarov B.A. Nemnogo o kiberbezopasnosti, Avtomatika, svyaz', informatika. 2014. No 8, pp. 15-18.
7. Shubinskiy I.B., Makarov B.A. O kiberzashchishchennosti informatsionnykh sistem upravleniya dvizheniem poezdov, Avtomatika, svyaz', informatika. 2014. No 11, pp. 9-12.
8. Makarov B.A. Aktual'nost' kiberbezopasnosti na zheleznodorozhnom transporte, Vestnik Instituta problem estestvennykh monopoliy: Tekhnika zheleznykh dorog. 2015. No 3 (31), pp. 10-15.
9. Gordeychik S.V. Kiberbezopasnost' mikroprotsessornykh sistem ZhAT, Avtomatika, svyaz', informatika. 2015. No 4, pp. 4-6.
10. Gordeychik S.V., Gritsay G.S., Baranov D.S. Model' kiberugroz MPTs, Avtomatika, svyaz', informatika. 2015. No 7, pp. 18-20.
11. Gordeychik S., Timorin A., Gritsai G. The Great Train Cyber Robbery, Schedule 32. Chaos Communication Congress (Congress Center Hamburg, Germany, December 27-30, 2015). URL: https://media.ccc.de/v/32c3-7490-the_great_train_cyber_robbery.
12. Rozenberg E.N. Sistemy diagnostiki i ikh kiberzashchishchennost', Avtomatika, svyaz', informatika. 2015. No 10, pp. 20-21.
13. Gordeychik S.V. Missiotsentricheskiy podkhod k kiberbezopasnosti ASU TP. Voprosy kiberbezopasnosti. 2015. N 2 (10), pp. 56-59.

4 Roman Bakurkin, OAO «NIIAS», Moscow, r.bakurkin@vniias.ru
5 Boris Bezrodnyi, Dr.Sc., Professor, OAO «NIIAS», Moscow, b.bezrodnyi@vniias.ru
6 Alexander Korotin, OAO «NIIAS», Moscow, a.korotin@vniias.ru