АВТОМАТИКА И ТЕЛЕМЕХАНИКА

УДК 656.2.08

К. А. БОЧКОВ, доктор технических наук, П. М. БУЙ, кандидат технических наук, Белорусский государственный университет транспорта, г. Гомель

ОСОБЕННОСТИ АТТЕСТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ЛОКАЛЬНЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

Рассматриваются особенности аттестации систем защиты информации локальных систем железнодорожной автоматики и, в частности, микропроцессорной централизации «*i*путь» в Республике Беларусь. Анализируется набор необходимой документации о системе защиты на объекте оценки для проведения аттестации. Указываются сложности проведения аттестации систем железнодорожной автоматики, находящихся в эксплуатации на Белорусской железной дороге и не имеющих отдельных подсистем, обеспечивающих информационную безопасность, в силу отсутствия подобных требований в процессе их проектирования и внедрения в производство. Поднимается вопрос о достаточности существующих мер функциональной безопасности локальных систем железнодорожной автоматики для обеспечения их информационной безопасности.

В настоящее время на Белорусской железной дороге большинство эксплуатируемых систем железнодорожной автоматики построено на базе реле первого класса надежности. Основная задача таких систем заключается в обеспечении функциональной безопасности на высоком уровне с интенсивностью опасных отказов от 10^{-8} до 10^{-13} $с^{-1}$. Вопросы информационной безопасности для релейных систем железнодорожной автоматики, согласно [1], не рассматривались. Хотя с помощью организационных мероприятий, предусмотренных правилами технической эксплуатации данных систем, исключались попытки несанкционированного доступа (НСД) к их аппаратам управления. Кроме того, логика работы систем строились таким образом, что ею исключались любые запрещенные действия субъектов или действия субъектов, приводящих к формированию недопустимых по условиям безопасности движения управляющих воздействий.

На смену релейным системам железнодорожной автоматики в последнее время внедряются микропроцессорные системы, построенные на базе аппаратно-программных комплексов. К таким системам относится микропроцессорная централизация (МПЦ) «*i*путь», которая уже несколько лет успешно функционирует на станции Ипуть. Для этой и подобных ей локальных систем железнодорожной автоматики, согласно постановлению Совета Министров Республики Беларусь № 625 «О некоторых вопросах защиты информации» от 26 мая 2009 года, неизбежным становится вопрос аттестации их систем защиты информации.

В перечень документов, необходимых для проведения аттестации, помимо документации на систему и сведений о разработчике, входят следующие документы о системе защиты на объекте оценки:

– правила разграничения доступа в информационной системе;

– модель нарушителя правил разграничения доступа в информационной системе;

– состав и структура системы защиты информации;

– наличие сертификатов соответствия либо экспертных заключений на средства защиты информации;

– задание по безопасности на информационную систему;

– проектная и эксплуатационная документация на систему защиты информации, другие данные, влияющие на обеспечение защиты информации;

– инструкция по обеспечению защиты информации в информационной системе;

– инструкция о порядке применения средств защиты информации в информационной системе;

– программа проведения приемочных испытаний системы защиты информации;

– акт и протоколы приемочных испытаний системы защиты информации;

– протоколы испытаний средств защиты информации;

– протокол оценки задания по безопасности.

Эксплуатируемые в настоящее время системы МПЦ в большинстве своем не имеют в составе отдельно выделенную систему защиты, обеспечивающую информационную безопасность объекта. Однако в микропроцессорные системы железнодорожной автоматики заложены все принципы защиты от НСД и правила обработки управляющих воздействий, которые присущи релейным системам. Кроме того, микропроцессорные системы данного класса управляют стрелками и сигналами на отдельных станциях, т. е. их функционирование носит локальных характер. Однако возможны ситуации, когда подобные локальные системы могут быть выполнены в качестве линейных станций в системе диспетчерского управления через системы диспетчерской централизации (ДЦ). При этом возможны ситуации включения таких

станций в системы ДЦ как по каналам телеуправления (ТУ) и телесигнализации (ТС), так и только по каналам ТС для крупных станций или станций со значительной маневровой работой.

Указанная выше станция Ипуть с количеством стрелок 18, оборудованная системой МПЦ «*i*путь», включена в ДЦ только по каналу ТС как локальная станция с местным управлением дежурными по станции (ДСП). Логика и алгоритмы функционирования локальных станций и организационно-технические мероприятия, реализованные в МПЦ «*i*путь», исключают попытки НСД к автоматизированному рабочему месту (АРМ) ДСП. Тем не менее, необходимо проведение аттестации системы защиты информации МПЦ «*i*путь», что вынуждает формировать соответствующую документацию, разрабатывать задание по безопасности данной системы и проводить ее оценку.

В таблицах 1 и 2 соответственно приведены правила разграничения доступа (ПРД) и модель нарушителя ПРД в информационной системе МПЦ «*i*путь».

Таблица 1 – **Правила разграничения доступа в информационной системе МПЦ «*i*путь»**

Действия субъектов согласно ПРД	Субъекты информационной системы					
	Начальник станции	Дежурный по станции	Начальник участка СЦБ	Старший электромеханик	Электромеханик	Диспетчер отделения дороги
Получение информации о поездной обстановке на станции	+	+	+	+	+	+
Получение специальной технологической информации по станции	+	+	–	–	–	–
Получение диагностической информации о системе МПЦ по фиксированным запросам	–	–	+	+	+	–
Управление объектами станции с обеспечением условий безопасности движения поездов	+	+	–	–	–	–
Техническое обслуживание объектов управления на станции	–	–	+	+	+	–
Обслуживание технических средств МПЦ	–	–	+	+	+	–

Сертификатов соответствия либо экспертных заключений на средства защиты информации МПЦ «*i*путь», а также проектной и эксплуатационной документации на систему защиты информации нет. Это обусловлено тем, что в процессе своей работы она не хранит и не обрабатывает информацию, которая подлежит защите. Однако система МПЦ «*i*путь» относится к классу А2 типовых объектов информатизации, согласно [2]; ею обрабатывается информация, содержащая сведения, отнесенные в установленном порядке к служебной информации ограниченного распространения, исключительно в силу специфики отрасли. Любая информация о поездной обстановке на станции, положении стрелок и сигналах светофоров может быть легко получена путем визуального наблюдения за станцией.

Таблица 2 – **Модель нарушителя правил разграничения доступа в информационной системе МПЦ «*i*путь»**

Действия нарушителей ПРД	Нарушители ПРД						
	Начальник станции	Дежурный по станции	Начальник участка СПБ	Старший электромеханик	Электромеханик	Диспетчер отделения дороги	Посторонний субъект
Получение информации о поездной обстановке на станции	–	–	–	–	–	–	+
Получение специальной технологической информации по станции	–	–	+	+	+	+	+
Получение диагностической информации о системе МПЦ	+	+	–	–	–	+	+
Управление объектами станции с целью выполнения запрещенной операции	+	+	+	+	+	+	+
Доступ к объектам управления на станции	–	–	+	+	+	+	+
Доступ к объектам управления на станции с целью приведения их в негодность	+	+	+	+	+	+	+
Доступ к техническим средствам МПЦ с целью приведения их в негодность	+	+	+	+	+	+	+
Изменение или удаление программного обеспечения системы МПЦ	+	+	+	+	+	+	+
Установка на ПК системы МПЦ постороннего программного обеспечения	+	+	+	+	+	+	+
Доступ в помещения станции	–	–	–	–	–	–	+

Отсутствие целостной системы информационной безопасности в МПЦ «*i*путь» объясняется тем, что в процессе разработки не ставились задачи по ее организации.

К сожалению, разработка задания по безопасности, его оценка и сама аттестация требуют существенных финансовых вложений. Но не эта проблема является главной. До недавнего времени

в Республике Беларусь отсутствовала аккредитованная организация, способная провести указанную работу, и при этом компетентная в системах железнодорожной автоматики и принципах их функционирования. Кроме того, для разработки задания по безопасности, его оценки и проведения аттестации необходимы три такие организации.

Задание по безопасности, согласно [3], должно содержать требования безопасности, а также определять функциональные и гарантийные меры безопасности, реализация которых обеспечивала бы соответствие объекта установленным требованиям. Несмотря на все мероприятия по защите от НСД, реализуемые в локальных микропроцессорных системах железнодорожной автоматики, и особенности их функционирования, разработка задания по безопасности данных систем с использованием [4, 5] является достаточно сложной и трудоемкой задачей в силу излишней формализованности и громоздкости данных стандартов. Все это вызвало ряд затруднений в процессе аттестации МПЦ «*i*путь».

Было бы целесообразным для разработки задания по безопасности локальной системы железнодорожной автоматики, ее оценки и аттестации системы защиты информации разработать перечень специализированных требований безопасности к подобным системам и провести классификацию этих систем по классам безопасности, каждому из которых будет соответствовать свой набор требований. Так, например, ДЦ, которая является системой более высокого уровня, использует удаленные каналы передачи управляющих воздействий и получения информации о состоянии объектов управления. Поэтому к таким системам должны предъявляться более жесткие требования информационной безопасности, чем к локальным системам МПЦ.

Список литературы

1 **Калютчик, С. П.** Особенности организации работ по обеспечению информационной безопасности на Белорусской железной дороге / С. П. Калютчик // Вестник БелГУТа: Наука и транспорт. – 2006. – № 1-2 (12-13). – С. 70–74.

2 **СТБ 34.101.30-2007.** Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация. – Введ. впервые 2008–04–01. – Мн. : БслГИСС, 2008. – 6 с.

3 **СТБ 34.101.1-2004.** Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1: Введение и общая модель. – Взамен СТБ 34.101.1-2001 ; введ. 2005–02–01. – Мн. : БелГИСС, 2005. – 35 с.

4 **СТБ 34.101.2–2004.** Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные требования безопасности. – Взамен СТБ 34.101.2-2001 ; введ. 2005–02–01. – Мн. : БелГИСС, 2005. – 90 с.

5 **СТБ 34.101.3–2004.** Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 3: Гарантийные требования безопасности. – Взамен СТБ 34.101.3-2001 ; введ. 2005–02–01. – Мн. : БелГИСС, 2005. – 112 с.

Получено 06.05.2011

K. A. Bochkov, P. M. Bui. Features of the railway automatics local system's certification of the protection's systems of information.

The features of the railway automatics local system's certification and, in particular, of microprocessor centralization "*i*путь" of the protection's systems of information in Republic of Belarus. The set of the necessary documentation about system of protection on object of an estimation for realization of certification is analyzed. The complexities of realization of certification of railway automatics systems which is taking place in operation by the Byelorussian railway and not having separate subsystems, ensuring information safety, by virtue of absence of the similar requirements are specified during their designing and introduction in manufacture. The question on sufficiency of existing measures railway automatics local systems functional safety for maintenance of their information safety rises.