УДК 004.056+629.1.04 Вестник УрФО № 3(33) / 2019, с. 73–81

Шевяков И. А., Соколов А. Н.

DOI: 10.14529/secur190309

КОНЦЕПЦИЯ СТЕНДА ДЛЯ ИССЛЕДОВАНИЯ КИБЕРБЕЗОПАСНОСТИ УСТРОЙСТВ НА ШИНЕ FLEXRAY «ПОДКЛЮЧЕННОГО» ТРАНСПОРТНОГО СРЕДСТВА, ОСНОВАННАЯ НА ИСПОЛЬЗОВАНИИ ИНТЕРФЕЙСНЫХ ПЛАТ

В статье предложена концепция стенда для исследования уязвимостей устройств на шине FlexRay так называемого «подключенного» транспортного средства (ТС), при функционировании которого используются цифровые системы передачи данных. Ос-новные проблемы кибербезопасности этих объектов связаны с возможностью ком-прометации данных, которыми обмениваются устройства автомобиля в процессе его функционирования. Актуальность исследования кибербезопасности таких устройств связано с необходимостью обеспечения безопасности движения. Для моде-лирования воздействий на шину, в частности подмены и инжекции сигналов злоу-мышленниками, предложено использование интерфейсных плат, разработанных для изучения шины FlexRay, программируемых в среде разработки Labview.

Ключевые слова: *«подключенное» транспортное средство, шина FlexRay, кибер-безопасность, интерфейсная плата, среда разработки Labview.*

THE CONCEPT OF THE STAND FOR THE STUDY OF CYBERSECURITY OF DEVICES ON THE FLEXRAY BUS OF THE "CONNECTED" VEHICLE, BASED ON THE USE OF INTERFACE BOARDS

The article proposes the concept of a stand for researching the vulnerabilities of devices on the FlexRay bus, the so-called "Connected" vehicle , the operation of which uses digital data transmission systems. The main problems of cybersecurity of such objects are related to the possibility of compromising the data exchanged between the vehicle devices during its operation. The relevance of the study of cybersecurity of such devices is associated with the need to ensure traffic safety. To simulate the effects on the bus, in particular, the substitution and injection of signals by intruders, it is proposed to use interface cards designed to study the FlexRay bus, programmed in the Labview development environment.

Keywords: *connected car, FlexRay, cybersecurity, interface board, Labview.*

Современные транспортные средства (ТС) широко контролируются сетевыми компьютерами, и недавние исследования показали, что эти системы уязвимы для злоумышленников, получивших доступ к внутренним автомобильным сетям [1] и удаленных внешних злоумышленников [2]. Исследование автомобильной киберфизической безопасности является сложной задачей из-за высоких барьеров для входа и в связи с отсутствием автомобильных испытательных стендов с открытым исходным кодом. При исследовании автомобильных сетей, в частности, возникают проблемы, связанные с отсутствием документации о специальных запатентованных протоколах, используемых производителями автомобилей. Это вынуждает каждую исследовательскую группу «с нуля» создавать свое программное обеспечение для автомобильных испытательных стендов и часто заключать ограничительные соглашения с производителями автомобилей для получения доступа к документации, необходимой для создания такого испытательного стенда. Такой подход предотвращает распространение их испытательного программного обеспечения.

В настоящее время на рынке существуют продукты, которые имеют возможности работы с форматами данных автомобильных сетей, в частности, сети FlexRay. В этой сети работают устройства, отвечающие за контроль шасси, тормозную систему и систему активной безопасности ТС. Требования к отказоустойчивости и кибербезопасности таких устройств весьма высоки.

В работе представлена концепция стенда для исследования аспектов автомобильной безопасности, который может обеспечить анализ, понимание и тестирование автомобильных киберфизических систем. Стенд позволяет быстро приступить к изучению автомобильных киберфизических систем, предоставляя платформу для обратного проектирования и тестирования посредством реальных экспериментов по настройке лабораторной сети или систем автомобиля.

Стенд состоит из интерфейсной платы (например, NI PCI-8517/2) для ПК и программ, написанных с использованием среды разработки Labview. К плате подключаются как реальные блоки управления, так и их имитаторы на основе микроконтроллеров или устройств стандарта PXI. Программное обеспечение включает в себя множество функций, облегчающих обратный инжиниринг протокола, и позволяет производить мониторинг и передачу сообщений FlexRay, которые могут использоваться для выполнения функций диагностики и отладки сети общего назначения.

Шина FlexRay

Бортовая шина передачи данных FlexRay была разработана в качестве основополагающего элемента электронного управления автомобилем и впервые применена для организации подключения тормозной системы с другими компонентами [3]. Шина позволяет осуществлять взаимодействия контроллеров тормозов, других подсистем, включая датчики, интегрированную систему управления шасси (integrated chassis management, ICM) и блок электронного управления (Electronic Control Unit, ECU), осуществляющий мониторинг и управление двигателем и трансмиссией. Система электронной стабилизации (electronic stability program, ESP) управляет тормозной системой, обеспечивая в критических случаях устойчивость автомобиля за счет торможения одного определенного колеса. Некоторые другие вспомогательные системы, включая функцию остановки-старта адаптивного круиз-контроля, также имеют доступ к ESP, и в некоторых случаях могут активировать торможение.

Все коммуникационные процессы требуют высокой полосы пропускания, отказоустойчивости, способности работать в режиме реального времени и масштабируемости. Этими свойствами обладает шина FlexRay, обеспечивающая два независимых канала для передачи данных, каждый из которых может передавать до 10 Мбит/с. Бортовая и промышленная шина предыдущего поколения CAN, получившая широкое распространение, в том числе и для решения подобных задач, обеспечивает пропускную способность лишь около 1 Мбит/с.

Для работы с шиной, в частности, для формирования тестовых вредоносных сигналов, предлагается использовать устройство PCI-8517/2, разработанное компанией National Instruments [4] (рис. 4).

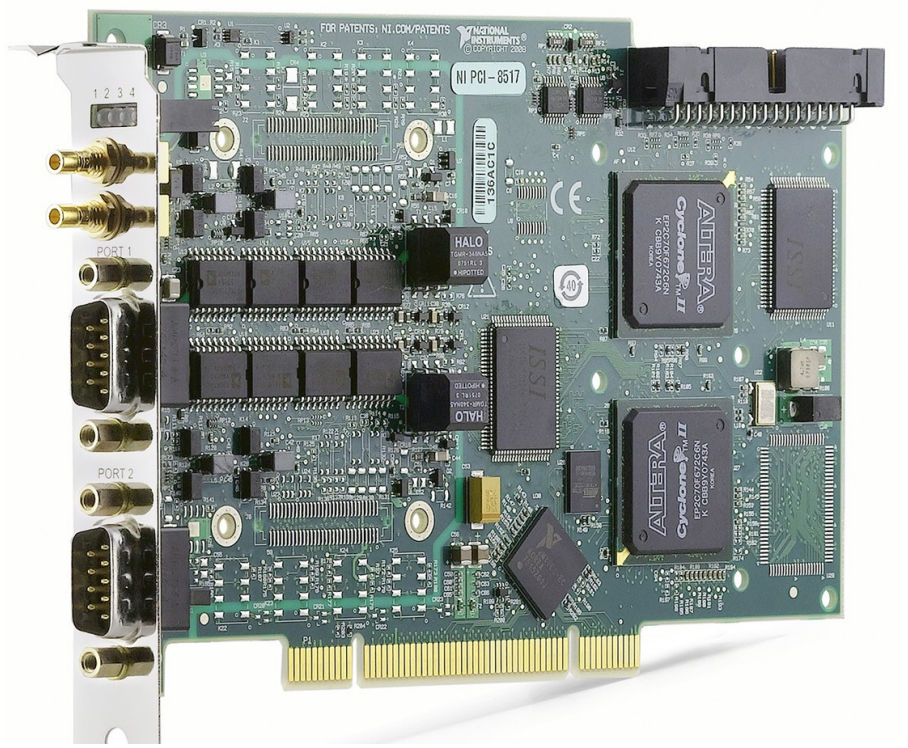

Рис. 1. Интерфейсная плата PCI-8517/2

PCI-8517/2 – это 2-х портовое интерфейсное устройство FlexRay, предназначенное для разработки приложений FlexRay и позволяющее ПК подключаться и обмениваться данными по шине FlexRay. PCI-8517/2 содержит два полнофункциональных интерфейса для устройств FlexRay для обеспечения возможности подключения отдельного блока управления двигателем (ECU) к интерфейсу в случае недоступности других узлов холодного пуска. Кроме того, для соединения двух отдельных сетей FlexRay можно использовать интерфейсы по отдельности, сохраняя при этом полную производительность на каждом из них.

Модель стенда для изучения уязвимостей шины FlexRay

В общем виде стенд представляет собой ПК с установленной платой расширения, к которой подключены модули контроля устройств на шине FlexRay. Структура предлагаемого стенда приведена на рис. 2.

Устройства стенда соединены в соответствии с топологией пассивной звезды. Возможны варианты использования других топологий при использовании дополнительных плат расширения или других активных устройств FlexRay. В качестве устройств шины предлагается использовать программно-аппаратную эмуляцию на основе платформы PXI (рис. 3).

Платформа состоит из шасси и вставляемых в неё различных плат расширения, с помощью которых можно генерировать различные цифровые и аналоговые сигналы, а также обрабатывать их в среде Labview, которая специализирована для работы с устройствами стандартами PXI. Также возможно использование платы 8517/2 с интерфейсом PXI для использования в шасси с остальными блоками, что позволяет сделать исследовательский стенд более компактным.

Подготовка данных для интерфейса

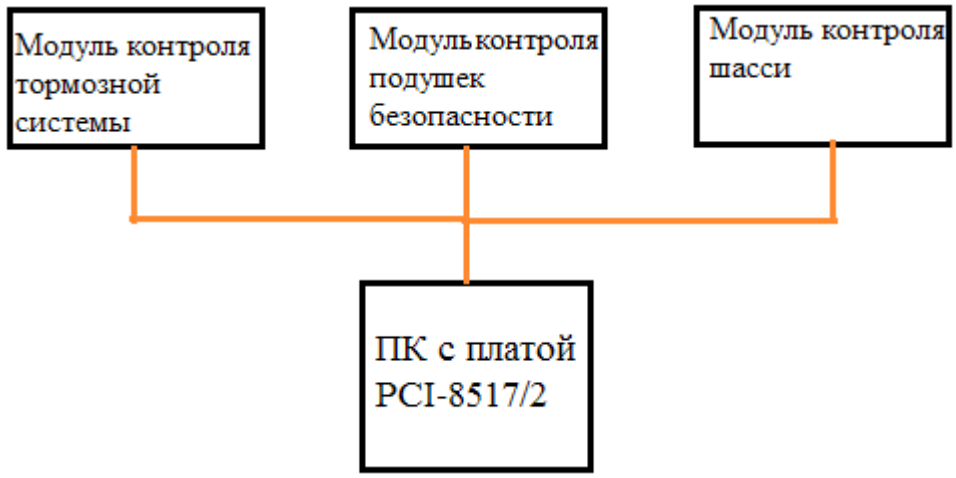

Рис. 2. Структура стенда для исследования киберугроз шины FlexRay

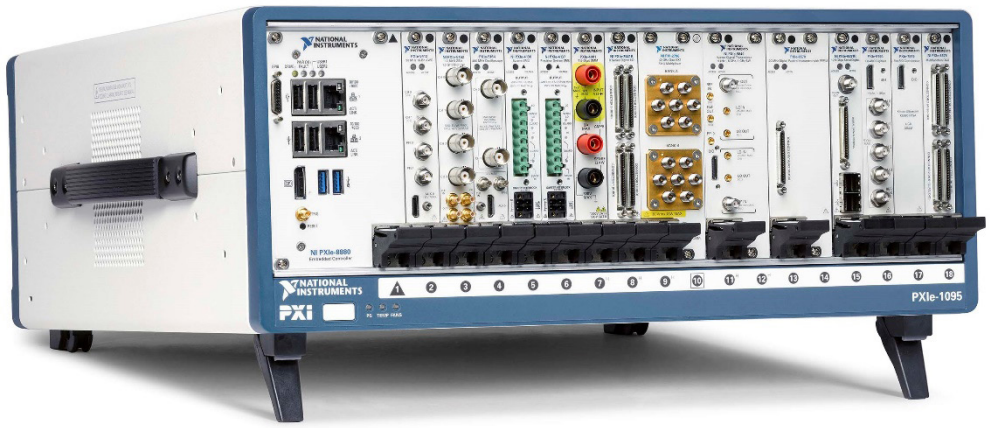

Рис. 3. Шасси стандарта PXI с установленными интерфейсными платами

Для подготовки данных, которые будут передаваться через интерфейсную плату в сеть, используется редактор баз данных NI-XNET – инструмент для создания и обслуживания встроенных сетевых баз данных. NI-XNET использует стандарт FIeld Bus EXchange (FIBEX) – стандартизированный формат файлов на основе XML, определенный консорциумом ASAM и применяемый для описания автомобильных сетей. Формат базы данных FIBEX совместим со многими различными автомобильными протоколами, что делает его достаточно гибким. FIBEX становится стандартом для определения сетей FlexRay «де-факто» и быстро внедряется для сетей CAN. Базы данных FIBEX обычно создаются проектировщиками автомобильных сетей и передаются инженерам, работающим над определенным аспектом ТС.

С помощью файла FIBEX и интерфейса NI-XNET (рис. 4) можно взаимодействовать с сетью автомобиля без необходимости настраивать интерфейсы и сигналы вручную.

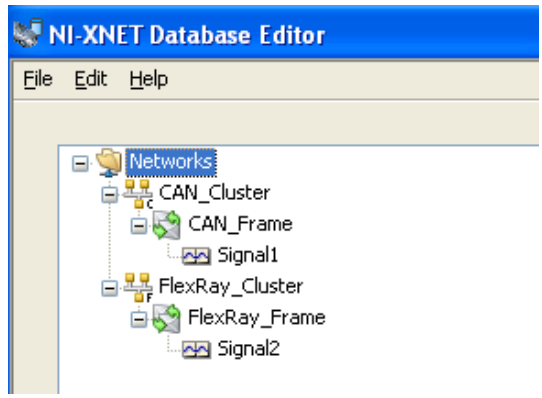

Рис .4. Внешний вид окна NI-XNET.

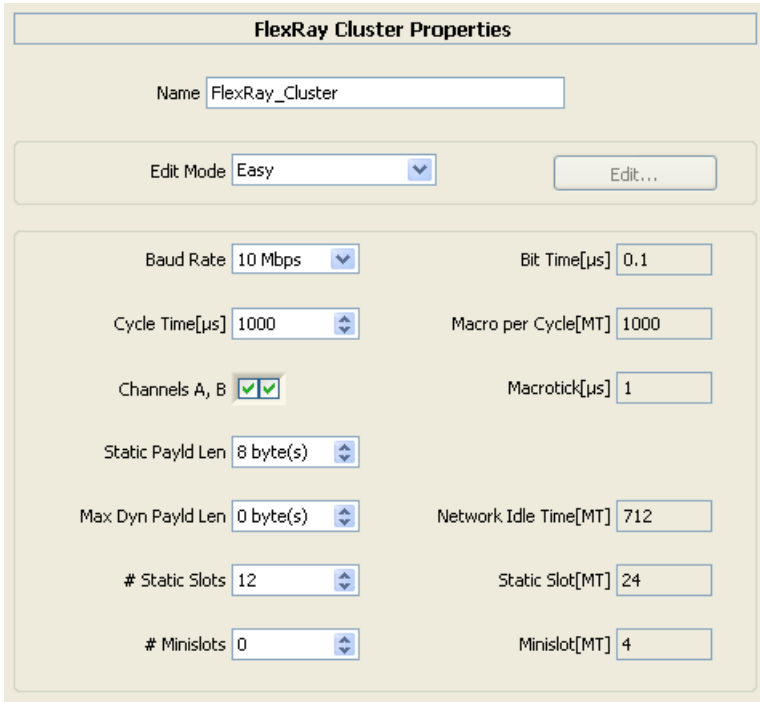

Рис. 5. Окно настройки параметров кластера.

Основным объектом базы данных является кластер. Для FlexRay существует около 30 глобальных сетевых параметров, которые нужно установить для кластера (рис. 5). Редактор баз данных NI-XNET включает режим Easy View, где устанавливаются 6 наиболее важных параметров. Другие параметры выбираются автоматически для получения работающей сети. Если имеется уже готовая

база данных, например, предоставленная производителем автомобильной электроники, для установки отдельных параметров можно использовать экспертное представление. FIBEX поддерживает несколько кластеров на одну базу данных, таким образом, в

При использовании файла базы данных с NI-XNET указывается путь к файлу или его псевдоним. Псевдоним обеспечивает более короткое и удобочитаемое имя для использования в приложении.

После создания базы данных в графиче-

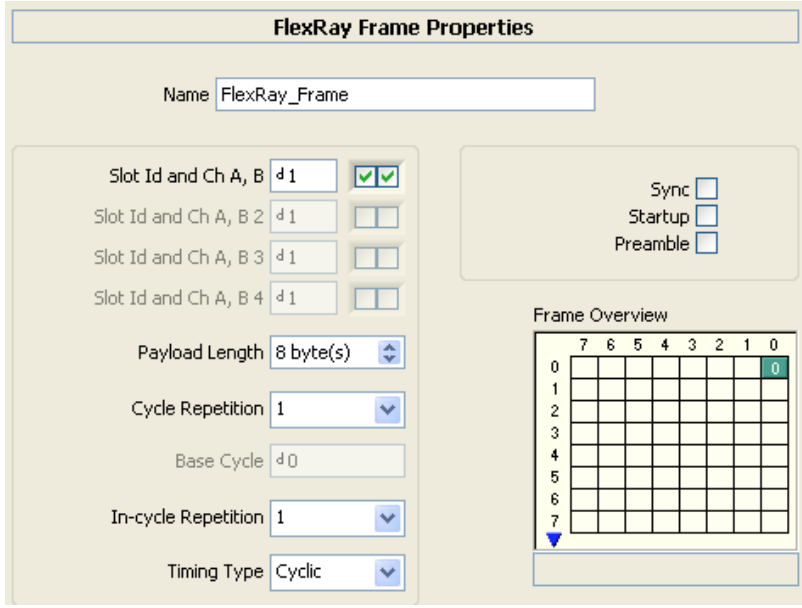

Рис. 6. Окно настройки параметров кадра

одной базе данных можно описать все сети автомобиля.

Каждый кластер может содержать произвольное количество кадров (frame). Кадр – это отдельное сообщение, которым обмениваются в кластере.

Основными свойствами кадра являются его идентификатор (идентификатор слота для FlexRay) и длина полезной нагрузки, которая в случае FlexRay может быть любым четным значением от 0 до 254.

Каждый кадр (рис. 6) содержит произвольное количество сигналов, которые являются основными единицами обмена данными в сети.

Сигналы (рис. 7) имеют следующие параметры:

• *начальный бит* – начальная позиция сигнала в кадре;

• *количество битов* – длина сигнала в кадре;

• *тип данных* – со знаком, без знака или с плавающей запятой;

• *порядок байтов* – младший или старший порядковый номер;

• *коэффициент масштабирования и смещение* – для преобразования физических данных в двоичное представление.

ском коде размещаются элементы, инициализирующие интерфейсную плату и считывающую базу данных. Выбор базы данных (рис.8) происходит в элементе, изображённом в нижней части рис. 9. Инициализация передачи данных из базы в сеть осуществляется с помощью элементов из верхней части рис. 9.

Исследовательские возможности стенда позволяют моделировать и изучать автомобильные сети с моделями защитных устройств, которые предназначены для предотвращения и пресечения несанкционированного доступа к автомобильной сети. С помощью стенда можно тестировать следующие устройства и системы безопасности:

• *брандмауэр* (предотвращение передачи неавторизованных пакетов в автомобильную сеть) [5];

• *систему обнаружения вторжений* в автомобильную сеть [6];

• *пакетное шифрование* (защита данных в автомобильной сети от перехвата и вставки пакетов) [5];

• *аутентификацию ECU* (предотвращение взаимодействия неавторизованных ECU с автомобильной сетью, например, ECU, установленного злоумышленником) [5];

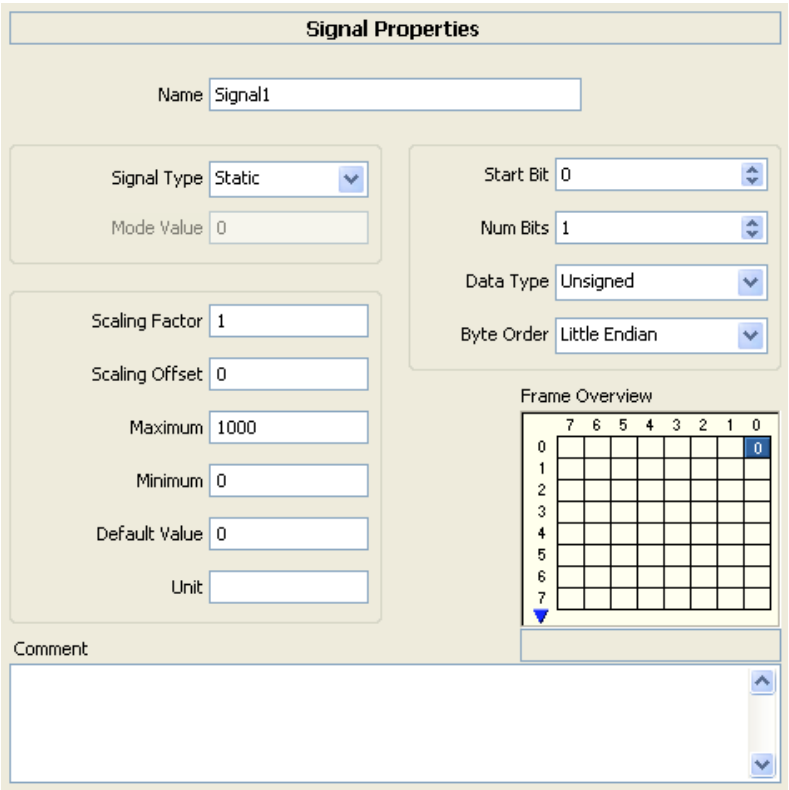

Рис. 7. Окно настройки параметров сигнала

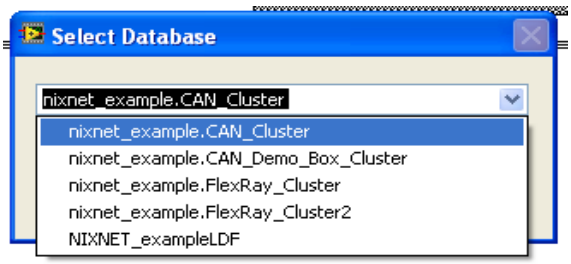

Рис. 8. Выбор файла базы данных для инициализации работы интерфейсного устройства

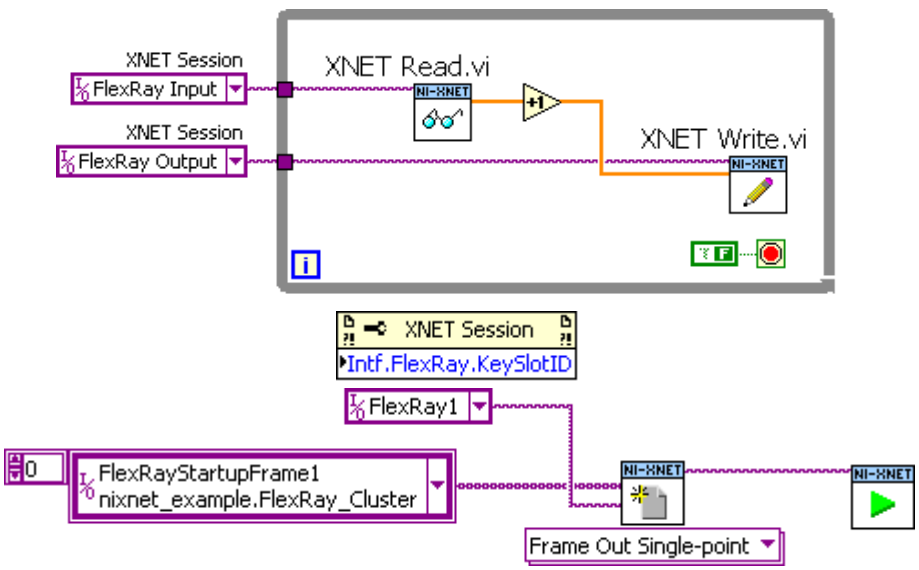

Рис. 9. Элементы программы, инициализирующие интерфейсную плату

• *устройства безопасности ECM* (обнаружение компрометированных ECU и аутентификаций) [7].

На стенде возможно изучение и таких аспектов автомобильной безопасности, как:

• *безопасная передача данных в беспроводном режиме* (контроль и тестирование беспроводных компонентов, встроенных в автомобили);

• *брандмауэры входящего трафика* (защита автомобильной сети от доступа нежелательного входящего трафика);

• *безопасность сетей Car2X* (изучение уязвимостей сетей car2X с целью обеспечения их безопасности).

Приведем некоторые примеры учебного использования испытательного стенда, связанные с тестированием безопасности автомобиля:

• *лабораторное задание по обеспечению безопасности автомобильной сети* – обнаружение сетевой активности и попытки захвата сети (например, управление боковым зеркалом, блокировкой / разблокировкой дверей);

• *упражнение по программированию интерфейсной платы* для приема и передачи пакетов по сети FlexRay;

• *тестирование автомобильной безопасности* для реализации системы обнаружения вторжений на интерфейсной плате для сети FlexRay.

Существуют другие учебные применения лабораторной сети, не связанные с тестированием автомобильной безопасности, например, исследования встроенной операционной системы, сетевые лабораторные занятия и др.

Заключение

В работе представлена концепция стенда для изучения аспектов кибербезопасности «подключенных» ТС, в частности безопасности устройств, передающих данные по шине FlexRay. Описаны принципы функционирования шины, форматы сигналов и пакетов сигналов, передаваемых по шине. В качестве основы для стенда предложено использовать интерфейсную плату NI PCI-8517/2, программируемую в среде Labview, с помощью которой плата может считывать формат сигналов FIBEX, формировать и передавать в сеть сигналы FlexRay.

Предложенная модель стенда является расширяемой, благодаря возможностям:

• использования интерфейсных плат, позволяющих генерировать и принимать сигналы других автомобильных сетей, таких как LIN, CAN;

• упрощённого создания сигналов для этих сетей, благодаря редактору NI-XNET и среды программирования Labview.

Литература

1. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In Security and Privacy (SP), 2010 IEEE Symposium, p. 447–462.

2. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security, SEC'11, Berkeley, CA, USA, 2011.

3. FlexRay Automotive Communication Bus Overview. – URL: https://www.ni.com/ru-ru/innovations/white-papers/06/flexray-automotive-communication-bus-overview.html (дата обращения: 02.09.2019).

4. PCI-8517. – URL: http://www.ni.com/ru-ru/support/model.pci-8517.html (дата обращения: 02.09.2019).

5. M. Wolf, A. Weimerskirch, and C. Paar. Security in automotive bus systems. In Proceedings of the Workshop on Embedded Security in Cars (escar), 2004.

6. U.E. Larson and D.K. Nilsson. Securing vehicles against cyber-attacks. 2008.

7. G. Lee, H. Oguma, A. Yoshioka, R. Shigetomi, A. Otsuka, and H. Imai. Formally verifiable features in embedded vehicular security systems. In Vehicular Networking Conference (VNC), 2009 IEEE, p. 1–7.

ШЕВЯКОВ Игорь Андреевич, преподаватель кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sheviakovia@susu.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

SHEVIAKOV Igor Andreevich, teacher of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sheviakovia@susu.ru

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru