трафика различных классов. Последние версии протокола позволяют использовать логические порты, конфигурации пакетов и туннели, и они могут обрабатывать логические соединения.

ЛИТЕРАТУРА

1. Thomas D. Nadeau and Ken Gray. SDN: Software Defined Networks, Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. – 2013.

2. A. Al-Shabibi. Programmable virtual networks: From network slicing to network virtualization, July 2013. http://www.slideshare.net/nvirters/virt-july2013meetup.

В.О.КАЗЮЧИЦ[1], С.С.ДИК[1], С.М.БОРОВИКОВ[1], А.В. БУДНИК[2]

ИНТЕГРАЦИЯ В СИСТЕМУ «АРИОН-ПЛЮС» МОДУЛЕЙ ОЦЕНКИНАДЕЖНОСТИ И ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ТЕХНИЧЕСКИХ СИСТЕМ

[1]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

[2]Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь

На рынке программных комплексов (ПК) представлен ряд зарубежных и отечественных ПК, позволяющих проводить автоматизированный расчет надежности сложных технических систем, в том числе радиоэлектронной аппаратуры и электрорадиоизделий. Наиболее распространенными среди зарубежных ПК являются: RELEX (Relex software Corporation, США); A.L.D.Group (Израиль); Risk Spectrum (Relcon AB, Швеция); ISOGRAPH (Великобритания).

Среди отечественных ПК, которые применяются на ряде предприятий: ПК АСОНИКА-К (МИЭМ-ASKsoft); ПК АСМ (ПК для автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем, ОАО «СПИК СЗМА»); ПК «Универсал» (для расчетов надежности и функциональной безопасности технических устройств и систем, ФГУП «ВНИИ УП МПС РФ»).

Ранее (2016 год) в БГУИР была разработана система автоматизированного расчета показателей надежности ЭУ, предназначенная для расчета надежности с учетом календарного периода эксплуатации, т.е. с учетом периодов наработки и периодов хранения (ожидания перед использованием по назначению). Кроме того, система позволяет учесть циклический характер работы ЭУ, т.е. учесть прогнозное число циклов «включено-выключено» в течение заданной суммарной наработки. Указанная система разработана на базе ранее созданной белорусской системы АРИОН [1,2]. Поэтому новой системе дано название «АРИОН-плюс».

В 2017 году с использованием методов анализа надежности и эффективности сложных технических систем [3] были разработаны модули оценки показателей надежности и эффективности функционирования систем. Разработанные модули предназначены для оценки надежности сложных технических систем, использующих в своем составе структурное резервирование составных частей. Определение показателя надежности системы выполняется по результатам анализа возможных технических состояний системы. Для выполнения анализа используется модель в виде структурной схемы надежности системы. Эта схема строится с учетом сформулированных условий работоспособности исследуемой системы и ее структурной схемы (электрической или деления). Для анализа также необходима информация о вероятностях работоспособного или неработоспособного состояний составных частей системы. Анализ возможных состояний системы и расчет итогового показателя надежности системы выполняется автоматически с учетом построенной структурной схемы надежности.

По вопросу использования системы «АРИОН-плюс» обращаться по e-mail: bsm@bsuir.by или же в ауд. 37 первого учебного корпуса БГУИР.

ЛИТЕРАТУРА

1. Разработка программного комплекса автоматизированной оценки надежности электронных устройств и систем: отчет по НИР (заключительный) / Белорусский государственный университет информатики и радиоэлектроники ; рук. С. М. Боровиков ; исполнители : С. М. Боровиков [и др.]. – Минск, 2016. – 45с. – Библиогр.: С. 42. – № ГР 20121425.

2. Система автоматизированной оценки надежности электронных устройств «АРИОН–плюс» / С. М. Боровиков [и др.] // Современные средства связи: материалы XXI

международной научно-технической конференции, Минск, 20-21 октября 2016. – Минск, БГАС, 2016. – С. 238-240.

3. Надежность технических систем : справочник / Ю. К. Беляев [и др.] ; под ред. И. А. Ушакова. – М. : Радио и связь, 1985. – 608 с.

Н.Е.МАТЕЙКО[1], С.И.ПОЛОВЕНЯ[1]

ИССЛЕДОВАНИЕ ПРОТОКОЛОВ БЕЗОПАСНОСТИ IOT В СИСТЕМЕ SMART HOUSE

[1]*Учреждение образования «Белорусская государственная академия связи, г. Минск, Республика Беларусь*

На сегодняшний день Интернет вещей (IoT) все больше и больше захватывает мир. Общение с неживыми вещами стало реальностью. В 2015 году количество устройств, подключенных через Интернет, превысило число людей, живущих на земле почти вдвое. Ожидается, что эта тенденция будет расти экспоненциально, и к 2025 году - количество устройств, достигнет примерно 75 миллиардов [1], что составляет отношение людей к подключенным устройствам как 1:10. Фактически, основная проблема, которая замедляет проникновение IoT в текущий мир - это безопасность.

Самым распространенным приложением IoT является умный дом (Smart home). Умный дом - технология, где все устройства в доме общаются друг с другом, чтобы добиться автоматизации. Интеллектуальная домашняя автоматизация полностью полагается на безопасную связь между устройствами и домашним контроллером.

Проанализируем существующие протоколы безопасности, которые используются в умном доме:

- **Z-wave** - это собственная технология автоматизации умного дома (smart home). Он был разработан компанией Sigma Designs 2005 года и быстро стал одним из самых популярных протоколов домашней автоматизации, поддерживая более чем 450 компаний по всему миру. Сетевая инфраструктура Z-Wave имеет ячеистую топологию, и устройства сети могут общаться непосредственно друг с другом. Безопасность между устройствами обеспечивается за счет симметричного протокола шифрования Advanced Encryption Standard (AES). Значительным преимуществом Z-Wave является его функциональная совместимость. Все устройства данного протокола работают со всеми другими устройствами Z-Wave, независимо от типа, версии или бренда.

В настоящее время на рынке существует более 1700 различных совместимых с Z-Wave устройств, что дает потребителям доступ к широкому спектру возможностей для автоматизации своего дома. Также, частота протокола значительно ниже частоты, используемой большинством других беспроводных устройств, поэтому у нее меньше шансов на вмешательство.

В Республике Беларусь такой протокол появился недавно, и уже сумел завоевать популярность за счет повышенного уровня безопасности, приемлемой стоимости и легкой управляемости сети.

- **ZigBee** во многом похож на Z-Wave и также является популярным протоколом беспроводной домашней автоматизации. Альянс ZigBee был учрежден в 2002 году. Сейчас в него входят более 300 компаний. Данный протокол был первоначально разработан для коммерческого использования, но теперь он считается стандартом автоматизации как в жилых, так и коммерческих условиях. Этот протокол использует радиочастотную связь и поддерживает ячеистую топологию сети, которая обеспечивает более широкий диапазон и более быструю связь между устройствами. Для обеспечения безопасной связи, спецификация ZigBee регламентирует безопасность на уровнях NWK и APS.

В настоящее время данный протокол имеет более 1500 продуктов, сертифицированных как совместимые с концентратором ZigBee. Стандарт ZigBee позволяет создавать датчики с низким энергопотреблением. Фактически, он настолько эффективен, что можно управлять устройством на одном и том же наборе батарей в течение нескольких лет. Домашняя автоматизация также предлагает функцию Green Power, которая полностью исключает необходимость в аккумуляторах.

В нашей стране данная технология уже сумела внедриться в такие компании как Белтелеком, Гипросвязь и многие медицинские учреждения. Одним из недостатков этого протокола является то, что он работает в той же полосе частот, что и Wi-Fi, создавая при этом помехи.

- **Insteon** - это технология домашней автоматизации, где устройства общаются синхронно по сети с двойной сеткой, объединяющую радиочастотную беспроводную сеть и электрическую