ИСПЫТАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ТЕХНИЧЕСКОГО РЕГЛАМЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ ТР 2013/027/BY

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Грицкевич В.И.

Бойправ О.В. – к.т.н.

Целью испытаний является проверка функций безопасности маршрутизаторов Cisco ASR920 и ASR1001 на предмет соответствия заявленным функциональным (полный перечень представлен в СТБ 34.101.2) и гарантийным требованиям безопасности (полный перечень представлен в СТБ 34.101.3), а также требованиям СТБ 34.101.73. Задачей испытаний является подтверждение того, что все заявленные в заданиях по безопасности требования к объектам оценки (маршрутизаторам) реализованы. Объект оценки считается выдержавшими испытания, если в нём реализованы все заявленные требования. Результаты испытаний объекта оценки отражаются в техническом отчете и протоколе.

Испытания данных маршрутизаторов проводятся на испытательном стенде, состав и структура которого соответствует схеме, приведенной на рисунке 1, где ПЭВМ 1, ПЭВМ 2, ПЭВМ 3, ПЭВМ 4, ПЭВМ Управления, маршрутизатор R1 (маршрутизатор Cisco ASR920 или ASR1001 (зависит от того, какой маршрутизатор испытывается)), маршрутизатор R2 (Cisco ASR 920), маршрутизатор R3 (Cisco ASR 920), а также концентраторы сетевые SW1 (TP-Link TL-SG1008D), SW2 (D-Link DGS-1008D) и SW3 (TP-Link TL-SG1008D) соединяются в соответствии со схемами кабелями UTP категории 5. Конфигурирование маршрутизаторов происходит либо с помощью CLI-интерфейса, либо с помощью протоколов telnet или ssh (определяется методикой испытаний).

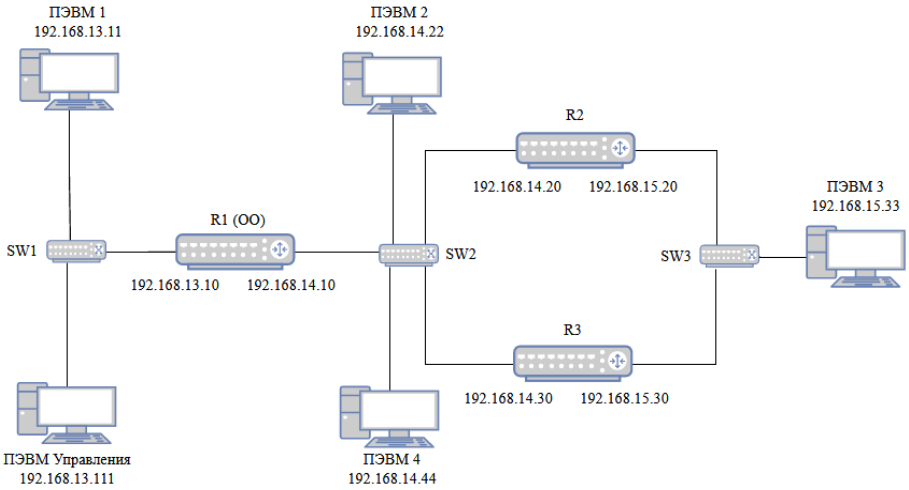

Рис. 1 – Схема испытательного стенда

Полный перечень заявленных функциональных требований безопасности представлен в заданиях безопасности для Cisco ASR920 и Cisco ASR1001. Ниже представлены наиболее важные из них, а также методика проверки требований:

- FIA_ATD.1 «Определение атрибутов пользователя» - на R1 создаются пользователи с различными уровнями привилегий (пример команды: username admin privilege 10 password admin);
- FIA_UAU.2 «Аутентификация до любых действий пользователя» - производятся попытки получить доступ к R1, используя корректный идентификатор и некорректный пароль;
- FIA_AFL.1 «Обработка отказов аутентификации» - на R1 задаётся блокировка на 120с при достижении двух неудачных попыток аутентификации в течении 120с (команда: login block-for 120 attempts 2 within 120);
- FDP_IFF.1 «Простые атрибуты безопасности» - добавляются надёжные стационарные маршруты (пример: ip route 192.168.15.0 255.255.255.0 192.168.14.20), настраивается управление сетевыми потоками (пример: deny ip host 192.168.13.11 any log), просматривается журнал аудита (show logging);
- FPT_FLS.1 «Сбой с сохранением безопасного состояния» - во время работы R1 прерывается подача электропитания с целью подтверждения того, что им невозможно управлять во время сбоя подачи электропитания, а также проверяется утверждение, что после загрузки маршрутизатор требует повторной аутентификации;
- FAU_GEN.1 «Формирование данных аудита» - просматривается журнал аудита (show logging) на наличие следующих записей: запуск средств аудита; использование доверенного канала и идентификатор

инициатора; попытка открытия сеанса связи пользователя; запросы на выполнение операции над объектом, изменения атрибутов безопасности; управление информационными потоками для информации контроля, полученной из недостоверных источников: адрес отправителя, адрес получателя, тип протокола; изменение в установке меток времени;

- FAU_SAR.3 «Выборочный просмотр данных аудита» - выполняется поиск данных аудита на основе значения даты, времени, идентификатора пользователя, IP-адреса отправителя (пример команды: show logging | include “Jun 4”).

Полный перечень заявленных гарантийных требований безопасности представлен в заданиях безопасности для Cisco ASR920 и Cisco ASR1001. Ниже представлены наиболее важные из них, а также методика проверки требований:

- ADV_ARC.1 «Описание архитектуры безопасности» - эксперту необходимо убедиться, что маршрутизатор спроектирован таким образом, что его функциональные возможности безопасности невозможно обойти, а также, что описание архитектуры безопасности составлено на уроне необходимой детализации;

- ADV_TDS.1 «Базовый проект» - эксперту необходимо убедиться, что проект содержит все необходимые компоненты и описания для подсистем, реализующих функциональные требования безопасности;

- ASE_CCL.1 «Утверждение о соответствии» - эксперту необходимо проанализировать задание по безопасности маршрутизатора;

- ASE_OBJ.2 «Задачи безопасности» - проверяется формулировка и обоснование задач безопасности;

- ASE_SPD.1 «Определение проблемы безопасности» - проверяется наличие описания угроз.

Перечень заявленных требований СТБ 34.101.73 представлен в заданиях по безопасности маршрутизаторов. Проверка требований стандарта СТБ 34.101.73 осуществлялась путём анализа результатов проверки функциональных требований безопасности.

По окончании испытаний маршрутизаторов Cisco ASR920 и ASR1001 были составлены следующие документы: технический отчет о результатах оценки и протокол испытаний. В протоколе испытаний указаны точное наименование, состав и конфигурация ОО на момент проведения оценки (испытаний).

В результате проведения испытаний маршрутизаторов Cisco ASR920 и ASR1001 было установлено, что они соответствуют всем заявленным функциональным и гарантийным требованиям безопасности, а также требованиям СТБ 34.101.73.

Список использованных источников:

1. Информационные технологии. Средства защиты информации. Информационная безопасность: ТР 2013/027/BY. Введ. 01.01.2014. – Минск: Госстандарт Республики Беларусь: 2013.

2..Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности: СТБ 34.101.2-2014. – Введ. 28.01.2014. – Минск: Госстандарт Республики Беларусь: 2013.

3. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности: СТБ 34.101.3-2014. – Введ. 28.01.2014. – Минск: Госстандарт Республики Беларусь: 2013.

4. Задание по безопасности ЗБ.Cisco-ASR900-IOS XE 3.16.001–2017 «Программное обеспечение Cisco IOS XE версии 3.16 маршрутизаторов Cisco серии ASR 900».

5. Задание по безопасности ЗБ.Cisco-ASR1000-IOS XE 3.16.002–2017 «Программное обеспечение Cisco IOS XE версии 3.16 маршрутизаторов Cisco серии ASR 1000».

6. Методика испытаний маршрутизаторов серии Cisco ASR 900 с программным обеспечением IOS XE версии 3.16 МИ.СКЛ 04-2018.

7. Методика испытаний маршрутизаторов серии Cisco ASR 1000 с программным обеспечением IOS XE версии 3.16 МИ.СКЛ 05-2018.