УДК 004.056:621.396
DOI 10.21685/2587-7704-2018-3-2-2

Open Access | RESEARCH ARTICLE

Стенд для исследования атак нарушителя на передачу данных в нелицензируемом диапазоне 433 МГц

М. В. Власов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Д. В. Малашкин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. П. Иванов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Разработана структура учебно-лабораторного стенда для исследования атак нарушителя на компоненты телекоммуникационной системы. Проведено тестирование работоспособности разработанного стенда. Экспериментально получена зависимость коэффициента правильного приема пакета от соотношения сигнал/помеха.

Ключевые слова: атака нарушителя, телекоммуникационная система, нелицензируемый диапазон частот, учебно-лабораторный стенд.

A bench to research intruder attacks on data transmission in the unlicensed band of 433 MHz

M. V. Vlasov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

D. V. Malashkin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. P. Ivanov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. A structure of the educational laboratory bench to research intruder attacks on components of the telecommunication system has been developed. Testing of the developed bench operation has been conducted. The dependence of the correct packet reception ratio on the signal-to-interference ratio was experimentally obtained.

Keywords: intruder attack, telecommunication system, unlicensed frequency band, educational laboratory stand.

Защита информационного пространства России от современных угроз является одним из приоритетных направлений национальной безопасности. Как заявил президент России В. В. Путин на открытии заседания Совета безопасности России, надежная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России в самом широком смысле этого слова [1].

Обеспечение безопасности сетей связи – одна из важнейших задач в общем контексте мероприятий по обеспечению безопасности как на государственном уровне, так и для отдельно взятых орга-

низаций [2]. Это один из приоритетов Доктрины информационной безопасности (ИБ) России [3]. Наличие информационных потерь, вызванных воздействием атак на компоненты телекоммуникационных систем (ТКС), приводит к увеличению риска ошибочных и несвоевременных решений при формировании управляющих воздействий и к снижению эффективности систем управления и связи [4].

В этой связи подготовка специалистов в области ИБ должна включать в себя изучение принципов работы систем радиосвязи и приобретение практических навыков по обеспечению их безопасности.

Модернизация лабораторной базы для подготовки специалистов по защите информации предполагает создание новых учебно-лабораторных комплексов для исследования помехозащищенности ТКС, что позволит сформировать необходимые практические навыки и выработать требуемые компетенции для будущей деятельности студентов. Особенно важно формирование высокого уровня компетенций при подготовке к разработке и эксплуатации защищенных ТКС [5].

В соответствии с современными требованиями ФГОС ВО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» выпускник вуза должен быть готов к решению следующих профессиональных задач [6]:

– сопровождение разработки, исследование ТКС, сетей и устройств, технических и программно-аппаратных средств защиты и обработки информации в ТКС;

– определение требований по защите информации, анализ защищенности ТКС и оценка рисков нарушения их ИБ;

– сравнительный анализ сетей и систем передачи информации по показателям ИБ, обеспечения требуемого качества обслуживания.

Целью данной работы является создание стенда для проведения лабораторного практикума по дисциплине «Сети и системы передачи информации» и научно-исследовательской работы студентов специальности 10.05.02 по исследованию атак на компоненты ТКС, выявление наиболее опасных с практической точки зрения видов атак и сценариев поведения нарушителя.

Все атаки нарушителя на компоненты ТКС можно классифицировать следующим образом [4]:

– атака, направленная на перехват передаваемой информации;

– атака, направленная на блокирование приема информации;

– атака, направленная на модификацию передаваемой информации;

– атака, направленная на фальсификацию передаваемой информации.

На начальном этапе разработки учебного стенда была реализована атака, направленная на блокирование приема информации [7].

Обобщенная схема учебного стенда приведена на рис. 1.

Рис. 1

В состав учебного стенда входят следующие компоненты:

– источник данных;

– передатчик;

– приемник;

– получатель данных;

– источник атаки.

В качестве источника данных используется программируемая плата Arduino MEGA 2560, с помощью которой осуществляется генерирование информации, формирование пакета данных, управле-

ние характеристиками передатчика, передача пакетов данных в передатчик. Передатчиком является радиомодуль FS1000A, который служит для передачи данных по радиоканалу в нелицензируемом диапазоне частот 433 МГц. В качестве приемника используется радиомодуль MX-RM-5V, с помощью которого осуществляется прием данных от передатчика и их передача получателю данных. Получателем данных является программируемая плата Arduino MEGA 2560, которая осуществляет прием данных от приемника, выделяет информационную часть из пакета данных и обрабатывает информацию. В качестве источника атаки используется генератор высокочастотный программируемый Г4-164, который генерирует сигнал на той же несущей частоте, что и передающее устройство.

Тестирование разработанного стенда проводилось в лабораторных условиях. При тестировании были выставлены следующие параметры:

– на передатчике:

– скорость передачи данных: 2000 бит/с;

– количество передаваемых пакетов за один тест: 500;

– модуляция сигнала: амплитудная;

– на источнике атак:

– модуляция сигнала: амплитудная;

– глубина модуляции: 50 %;

– модулирующий сигнал полосой в 1 кГц.

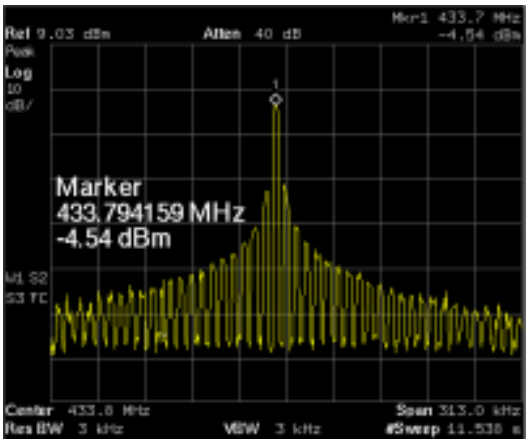
К передатчику, приемнику, источнику атак и спектроанализатору были подключены одинаковые антенны – четвертьволновые штыри. Уровень сигнала не изменялся, изменялся уровень атаки (помехи). Тестирование производилось в условиях влияния помех окружающей среды – перемещения людей по аудитории и воздействия белого шума.

В ходе тестирования была успешно проверена работа следующих компонентов стенда:

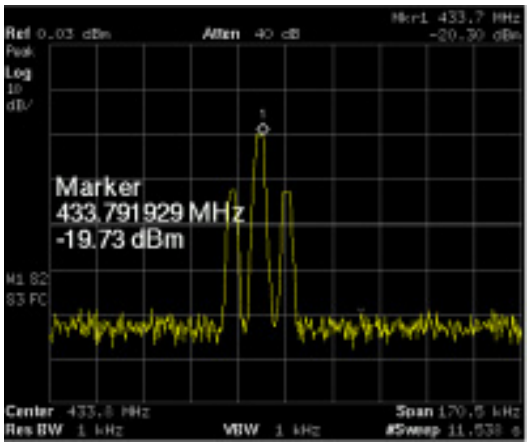
– передатчика. На рис. 2а показан спектр формируемого сигнала на выходе передатчика;

– источника атак / генератора помех. На рис. 2б показан спектр формируемого сигнала на выходе генератора помех;

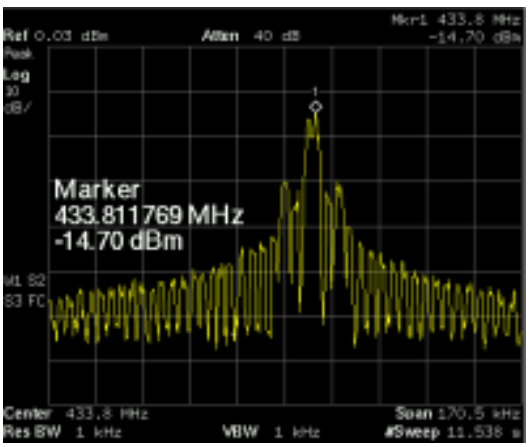
– приемника. На рис. 2в показан спектр сигнала на входе генератора помех.



а)



б)



в)

Рис. 2

Также в ходе тестирования была получена зависимость вероятности правильного приема пакета от соотношения сигнал/помеха, которая приведена на рис. 3.

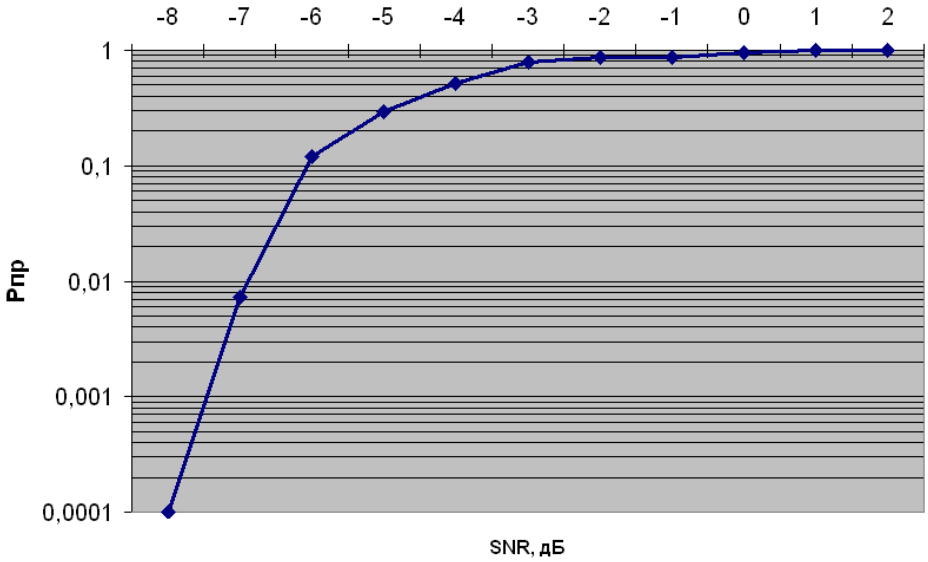


Рис. 3

Разработанный стенд по исследованию атак на компоненты ТКС представляет упрощенную модель канала связи при воздействии преднамеренных атак. Он позволит будущим специалистам по защите информации получить представление о принципах работы систем радиосвязи, а также даст возможность осуществить перехват данных в сети связи. Использование стенда во время научно-исследовательской работы поможет будущим специалистам в формировании навыков решения профессиональных задач в рамках эксплуатационной и экспериментально-исследовательской деятельности, а также в формировании профессиональных компетенций.

Библиографический список

1. Заседание Совета безопасности, посвященное вопросам противодействия угрозам национальной безопасности в информационной сфере. – URL: http://kremlin.ru/events/president/news/46709 (дата обращения: 14.10.2018).
2. Алексеев, В. М. Обеспечение информационной безопасности систем и сетей передачи информации : учеб. пособие / В. М. Алексеев, Ю. Ю. Горюнов, А. П. Иванов. – Пенза : Пенз. филиал РГУИТП, 2012. – 108 с.
3. Доктрина информационной безопасности Российской Федерации. – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 14.10.2018).
4. Иванов, А. П. Анализ моделей атак нарушителя на компоненты телекоммуникационных систем / А. П. Иванов, Е. Д. Кашаев // Информация и безопасность. – 2013. – № 3. – С. 439–440.
5. Иванов, А. П. Учебный стенд для исследования помехоустойчивости аппаратуры передачи данных / А. П. Иванов // Университетское образование (МКУО-2014) : сб. ст. XVIII Междунар. науч.-метод. конф., посвящ. 200-летию со дня рождения М. Ю. Лермонтова (г. Пенза, 10–11 апреля 2014 г.) / под ред. А. Д. Гулякова, Р. М. Печерской. – Пенза : Изд-во ПГУ, 2014. – С. 180–181.
6. Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (уровень специалитета) : Приказ Министерства образования и науки РФ от 16 ноября 2016 г. № 1426. – URL: http://fgosvo.ru/uploadfiles/fgosvospec/100502.pdf (дата обращения: 14.10.2018).
7. Власов, М. В. Разработка стенда для исследования атак нарушителя на компоненты телекоммуникационных систем / М. В. Власов, Д. В. Малашкин, А. П. Иванов // Информационные технологии в науке и образовании. Проблемы и перспективы : сб. науч. ст. Всерос. межвуз. науч.-практ. конф. (г. Пенза, 14 марта 2018 г.) / под ред. Л. Р. Фионовой. – Пенза : Изд-во ПГУ, 2018. – С. 202–204.

Власов, М. В.
Стенд для исследования атак нарушителя на передачу данных в нелицензируемом диапазоне 433 МГц / М. В. Власов, Д. В. Малашкин, А. П. Иванов // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-2.