Учредитель

ФГБОУ ВО «Новосибирский государственный технический университет»

Журнал зарегистрирован 01.03.2021 Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство о регистрации ПИ № ФС 77-80320

Адрес издателя и редакции: 630073, г. Новосибирск, пр. К. Маркса, 20.
E-mail: office@publish.nstu.ru и digital-tech-security@mail.ru
Web site: http://publish.nstu.ru и http://journals.nstu.ru/digital-tech-security/

Publisher and editorial office adress: 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation

До номера 1 (100) 2021 г. включительно журнал выходил под названием «Сборник научных трудов НГТУ» (ISSN 2307-6879)

16+

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ

ISSN 2782-2230

№ 4 (103) **2021**

СОДЕРЖАНИЕ

Выпускающий редактор *И.П. Брованова*
Корректор *Л.Н. Киншт*
Компьютерная верстка *С.И. Ткачева*

Лицензия № ИД 04303 от 20.03.01. Подписано в печать 23.12.2021. Выход в свет 27.12.2021
Формат 60×84/16. Бумага офсетная. Тираж 300 экз. Уч.-изд. л. 5,58
Печ. л. 6,0. Изд. № 230. Заказ № 49. Цена свободная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20

Publisher and editorial adress: 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation
E-mail: office@publish.nstu.ru, digital-tech-security@mail.ru
Web site: http://publish.nstu.ru, http://journals.nstu.ru/digital-tech-security/

DIGITAL TECHNOLOGY SECURITY

ISSN 2782-2230

№ 4 (103) **2021**

CONTENTS

Editor *L.N. Kinsht*
Publishing Editor *I.P. Brovanova*
Computer imposition *S.I. Tkacheva*

License № ID 04303 from 20.03.01. Signed in print December 23, 2021
Date of publication December 27, 2021. Format 60 × 84 1/16
Offset Paper. Circulation is 300 copies. Educational-ed. liter. 5,58. printed pages 6,0
Publishing number 230. Order number 49

It is printed in printing house of Novosibirsk State Technical University
630073, Novosibirsk, 20 K. Marx Prospekt

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 4 (103). – 9–19

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

УДК 004.616-71 DOI: 10.17212/2782-2230-2021-4-9-19

MODELING OF A HARDWARE AND SOFTWARE COMPLEX "POLIGRAF" BASED ON FREELY DISTRIBUTABLE MICROCONTROLLER PLATFORMS*

VIKTOR A. MASHTAKOV[1], VIKTOR M. BELOV[2]

[1] *20 Karl Marx Avenue, Novosibirsk, 1630073, Russian Federation, Novosibirsk State Technical University, master's student of the Department of Information Security. E-mail: vitya.mashtakov@gmail.com*
[2] *20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, Novosibirsk State Technical University, doctor of technical sciences, professor of the Department of Information Security. E-mail: vmbelov@mail.ru*

This article is devoted to the modeling of the software and hardware complex (SHC) "Polygraph" on the basis of freely distributed microcontroller platforms. In the work, the analysis of primary sources was carried out and the most promising microcontroller platform for the purposes of visual modeling and training to work on such devices was chosen. Within the framework of modeling tasks, on the basis of a number of criteria, the most optimal automated system for the design of devices has been determined. Using the chosen toolkit, the authors modeled the first educational test version of "Polygraph" with the ability to display some parameters measured by real SHC. The article considered the connection of the following sensors of the SHC "Polygraph": pulse, body temperature and respiratory rate. Based on the work done, it was concluded that this development is promising and relevant for design purposes and training in work on devices such as "Polygraph".

Keywords: component, polygraph, microcontroller platform, sensor, software and hardware complex, computer-aided design system, photoplethysmography, model

INTRODUCTION

Currently, law enforcement agencies, government agencies, as well as some commercial enterprises use a device called "Polygraph" when hiring. It is used to select applicants for vacancies, investigate various kinds of offenses, etc. Let's try to give the most general definition of this technical device. "Polygraph", in our opin-

* *Received 10 November 2021.*

ion, is a technical device designed for simultaneous simultaneous measurement of psychophysiological characteristics of a person (respiration indicators, skin conductivity, heart rate, etc.) and presentation of measurement results in digital or analog form to determine the reliability of information received from of the interrogated person [1, 2]. Today, in the era of universal digitalization of world socio-economic relations, everyone who wants to use a polygraph faces several serious problems: the high cost of the device and the high cost of its maintenance. This article discusses the possibility of modeling SHC "Polygraph" on the basis of freely distributed microcontroller platforms: analysis of primary sources is carried out in order to select the most optimal microcontroller platform (MP) and computer-aided design (CAD) system according to certain criteria; the simulation results are shown after connecting a number of sensors.

1. THEORY

A. Task Statement

To The task is to simulate a model of SHC "Poligraf" in one of CADs, with subsequent presentation of the design results in the form of a structural model, with a description of the principle of the device.

B. Selection of Microcontroller Platform

At the moment, the most widely known and popular among the developers and ordinary users are two platforms: Arduino and Raspberry Pie. The platforms are recognized for their simplicity and ease of use, as well as rather simple to learn basic functions, even if the user is using any of them for the first time. In order to understand which platform is better to use, it is necessary to conduct a comparative analysis. The analysis was based on the following criteria: ease of use and interaction with the platform; complexity of programming language and development tools; platform flexibility and the ability to adapt to different projects; demand for power supply systems; system crash tolerance [2].

– The Raspberry Pi is a computer that can run a Linux operating system that supports multitasking. Various devices can be connected to the USB ports, e.g. for wireless connection to the Internet. The platform is very powerful and can function as a complete personal computer (PC) [3].

– The Arduino can read analog signals in real time better than the Raspberry Pi. Arduino's versatility allows it to operate with practically any type of chips and sensors. The Raspberry Pi is much more selective with analog sensors: additional hardware is required.

– Arduino is less demanding on the power system of the devices. The recommended power supply for Arduino UNO is 7-12V, which can be stabilized to 5V.

The Raspberry Pi platform requires strictly 5V input, so it requires a power filter with 1A current [4].

– Arduino's development environment is much easier to use than Linux for instance, to be able to create a program for a flashing LED on the Raspberry Pi, it requires an operation system (OS) and certain program code libraries. On the other hand with the Arduino, it is possible to write a similar program using only eight lines of program code. Because the Arduino is not meant to run many applications or the OS, it is possible to simply plug in the platform and start working.

– The Arduino can work with any power supply and PC. The Arduino can be switched on/off at will during operation, which makes it different from the Raspberry Pi, whose OS can be damaged if the board is switched off without a proper shutdown session.

Based on all the above mentioned advantages and disadvantages of the discussed platforms, it follows that Arduino has an undeniable advantage in the realization of hardware-software projects, including the solution of our task [5].

C. CADs Selection

Once the microcontroller platform has been defined, it is necessary to choose the software for further design of the device. The choice of a suitable system was made on the basis of the following factors: the breadth of software functionality; the ability to perform all stages of development; the possibility of connecting third-party libraries; the ability to simulate the external impact on the designed device.

Among different software, the most promising for solving the problem is the Proteus software. The main advantages and features of Proteus functionality are as follows:

- the widest functionality for working with microcontroller platforms in comparison with all existing analogs;
- proteus contains over than 6000 electronic elements with full reference data and also demonstration projects;
- USBCONN and COMPIM tools that allow to connecting virtual device to the USB and COM ports of computer;
- the possibility to perform all the stages of development of an electronic device based on a microcontroller in a single environment;
- possibility to write, debug and test the firmware even before the prototype is physically built;
- a preinstalled set of models of most electronic components sorted by type;
- a wide selection of third-party component libraries that are created by enthusiasts around the world and are freely available;
- an electronic circuit simulator that can be used to see how a device behaves in operation;

- simulators of sensors and tools of external influence: it is possible to change the sensor readings, watching how the system reacts to it;
- applying the available Proteus features and capabilities, it is possible to not only fully meet the needs of the project, but also to obtain the necessary opportunities for experimentation and complete debugging of the device under development, avoiding unnecessary costs and errors.

2. EXPERIMENTAL RESULTS

The "Polygraph" device consists of two units - analog and digital. The analog part is a set of sensors, which receive the primary signal from the user. Then the signal goes to the digital part, where the signal is digitized and transmitted to the PC. The model of the device is shown in Fig. 1.

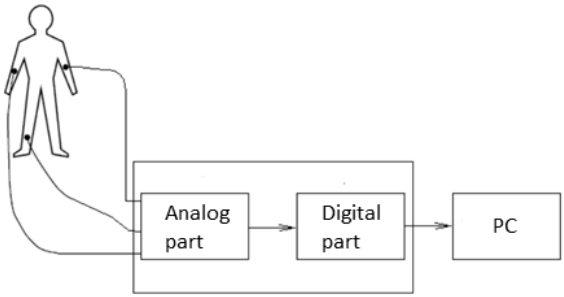


Fig. 1. Device model

Рис. 1. Модель устройства

All sensors are connected to the microcontroller platform through analog inputs, the values received from the sensors are displayed in the terminal window. An oscilloscope is added to the pulse sensor for clarity. The sensor readings are randomly generated, thus simulating real measurement conditions.

The results of the device design are shown in Fig. 2, 3 and 4 on the example of three sensors – a body temperature sensor, a pulse sensor and a flex sensor is connected to the platform. Flex sensor in the future will be attached to the chest and will read the breathing rate of the test subject.

As a temperature sensor, the most common and affordable option was chosen – the TMP36 sensor [6, 7]. This sensor uses solid-state electronics technology to detect temperature. That is, there is no mercury or bimetallic plates. Instead, they have thermistors. In thermistors, as the temperature increases, the voltage in the diode

rises, technically the voltage difference at the base and emitter in the transistor. Accurate voltage sensing makes it possible to produce an analogue signal proportionally to the temperature [8].

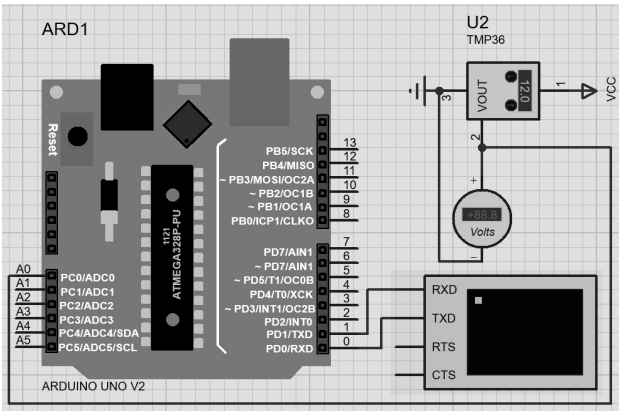


Fig. 2. Temperature sensor model

Рис. 2. Модель датчика температуры

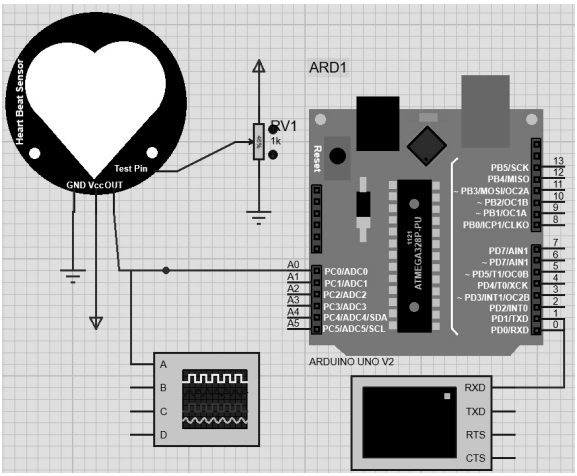


Fig. 3. Pulse sensor model

Рис. 3. Модель датчика пульса

A photoplethysmograph was chosen for the pulse sensor as the most available and common for this purpose today. This is an analog sensor based on the method of photoplethysmography – the change in the optical density of the blood volume in the area of the body being measured, due to the change in the blood flow through the vessels depending on the phase of the cardiac cycle. The sensor contains a light source and a photodetector, the voltage of which varies depending on the blood volume during cardiac pulsations.

The pulse sensor amplifies the analog signal and normalizes it with respect to the point of average value of the sensor supply voltage. The sensor reacts to intensity changes in light. If the light intensity hitting the sensor stays constant, the signal values will stay near the midpoint of the ADC range. If a greater intensity of study is recorded, the signal curve goes up, if less intensity, the curve goes down, on the contrary.

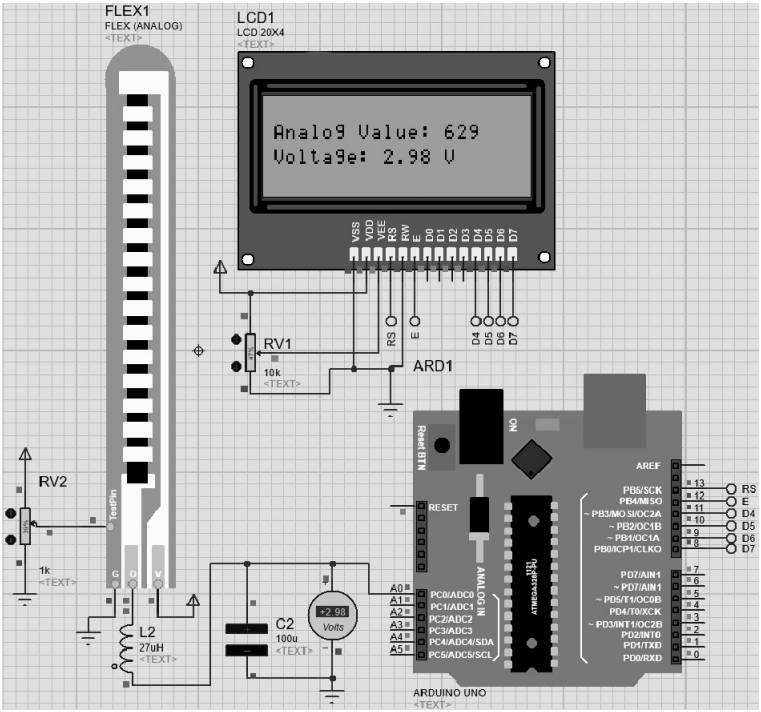


Fig. 4. Flex sensor model

Рис. 4. Модель гибкого датчика

Flex sensor is built on resistance carbon elements. The fact that it is a varying print resistor means that it could be made quite long on a slim, elastic base plate. When the base plate is bent, there is some resistance at the output of the sensor, corresponding with the bending radius. In other words, flexible sensors are analog resistors that work as part of a variable analog voltage divider.

The results obtained from the sensors are displayed in the program in the virtual terminal window and are shown in Fig. 5, 6, 7 and 8.

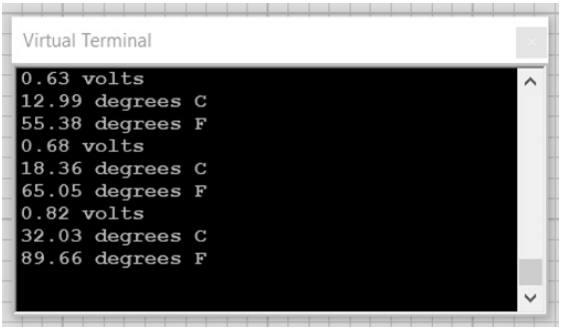


Fig. 5. Temperature sensor results

Рис. 5. Результаты датчика температуры

The temperature sensor is connected to the analog input of the Arduino and, depending on the temperature of the object, outputs different voltage values which are converted into temperature readings [9].

Fig. 6. Pulse sensor results

Рис. 6. Результаты датчика пульса

The heart rate sensor is also connected to the analog input of the Arduino and records the number of heartbeats [10]. Also an oscilloscope is connected to the pulse sensor circuit, for visual display of time parameters and voltage values of the pulse sensor. These parameters are shown in Fig. 6.

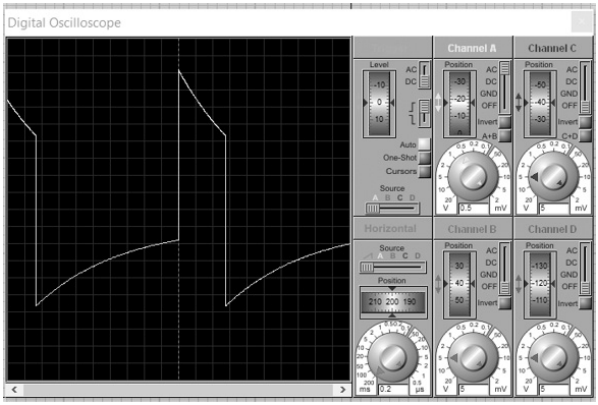


Fig. 7. Time parameters and voltage values of the pulse sensor

Рис. 7. Временные параметры и значения напряжения импульсного датчика

The value of its intensity is proportional to the change in blood filling of the tissue under study during contraction and relaxation of the heart muscle.

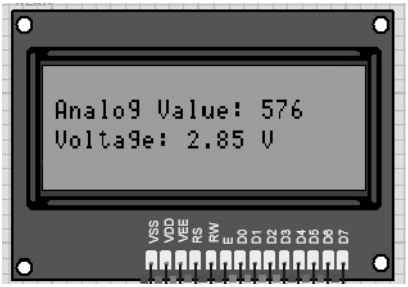


Fig. 8. Flex sensor results

Рис. 8. Результаты гибкого датчика

The flex sensor is connected to the analog input of the Arduino and, depending on the bending radius of the object, outputs different resistance.

CONCLUSIONS

In the course of this research the following tasks were solved: comparative analysis of the most popular freely distributed microcontroller platforms for modeling SHC "Poligraf"; determination of the optimal microcontroller platform and software for visual modeling and training on them; construction of the first training test version of "Poligraf", which displays some parameters measured by real devices. This research shows the promise and relevance of this model for teaching and designing devices such as "Poligraf". Further efforts in work should be directed, in our opinion, on increasing the number of measured parameters, studying and improving metrological characteristics of model samples of the device and increasing reliability of the information provided by the interviewed persons.

REFERENCES

1. Sal'kova A. Slomannye zhizni: mozhno li verit' "detektoru lzhi"? [Can we trust the lie detector?]. *Gazeta.Ru*, 2019, 14 April. (In Russian). Available at: https://www.gazeta.ru/science/2019/04/14_a_12299647.shtml (accessed 02.12.2021).

2. *Poligrafy na rossiiskom rynke* [Polygraphs on the Russian market]. Available at: http://www.bnti.ru/index.asp?tbl=05.13 (accessed 02.12.2021).

3. Monk S. *Programming Arduino: getting started with sketches*. New York, McGraw-Hill/TAB Electronics, 2011. 162 p.

4. Margolis M. *Arduino cookbook*. Oreilly, 2014. 800 p.

5. Petracca M., Passaro P., Gioia E. AMBER: advanced mother board for embedded systems pRototyping. *EURASIP Journal on Embedded Systems*, 2017, vol. 2017, p. 32. DOI: 10.1186/s13639-017-0080-z.

6. Sinha A., Pavithra M., Sutharshan K.R., Subashini M. A MATLAB based on-line polygraph test using galvanic skin resistance and heart rate measurement. *Australian Journal of Basic and Applied Sciences*, 2013, vol. 7 (11), pp. 153–157.

7. USB Polygraph. *Juangg Projects*, 2019, June 09. Available at: https://juangg-projects.blogspot.com/2019/06/usb-polygraph.html (accessed 02.12.2021).

8. Tsapenko M. *Izmeritel'nye informatsionnye sistemy: struktury i algoritmy, sistemotekhnicheskoe proektirovanie* [Measuring information systems: structures and algorithms, system engineering design]. 2nd ed. Moscow, Energoatomizdat Publ., 1985. 439 p.

9. *Datchik temperatury TMP36 i Arduino* [Temperature sensor TMP36 and Arduino]. Available at: https://arduino-diy.com/arduino-datchik-temperatury-TMP36 (accessed 02.12.2021).

10. Smirnov V.A. *Biofizicheskie osnovy pletizmografii. Registratsiya i analiz fotopletizmogramm* [Biophysical basis of plethysmography. Registration and analysis photoplethysmogram]. Blagoveshchensk, 2014. 10 p.

Viktor A. Mashtakov, master's student of Novosibirsk State Technical University. The main direction of scientific research is the development of automated production systems. E-mail: vitya.mashtakov@gmail.com

Viktor M. Belov, doctor of technical sciences, professor, professor of the Department of Information Protection of Novosibirsk State Technical University. The main direction of scientific research is the application of mathematical methods in various fields of science, technology, society. He has more than 600 scientific publications. E-mail: vmbelov@mail.ru

DOI: 10.17212/2782-2230-2021-4-9-19

Моделирование программно-аппаратного комплекса «полиграф» на базе свободно распространяемых микроконтроллерных платформ*

В.А. Маштаков[1], В.М. Белов[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистрант кафедры защиты информации. E-mail: vitya.mashtakov@gmail.com*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доктор технических наук, профессор кафедры защиты информации. vmbelov@mail.ru*

Настоящая статья посвящена моделированию программно-аппаратного комплекса (ПАК) «Полиграф» на базе свободно распространяемых микроконтроллерных платформ. Проведен анализ первоисточников и выбрана наиболее перспективная для целей наглядного моделирования и обучения работе на такого рода устройствах платформа микроконтроллера. В рамках задач моделирования на основе ряда критериев определена оптимальная для моделирования устройств автоматизированная система. Используя выбранный инструментарий, авторы смоделировали первую учебную тестовую версию «Полиграфа» с возможностью отображения некоторых параметров, измеряемых реальными ПАК. В статье рассмотрены подключения следующих датчиков ПАК «Полиграфа»: пульса, температуры тела и частоты дыхания; сделан вывод, что данная модель является перспективной и актуальной для целей обучения работе и проектирования устройств типа «Полиграф».

Ключевые слова: компонент, полиграф, микроконтроллерная платформа, датчик, программно-аппаратный комплекс, система автоматизированного моделирования, фотоплетизмограф, модель

* *Received 10 November 2021.*

СПИСОК ЛИТЕРАТУРЫ

1. *Салькова А.* Сломанные жизни: можно ли верить «детектору лжи»? // Газета.Ру. – 2019. – 14 апреля. – URL: https://www.gazeta.ru/science/2019/04/14_a_12299647.shtml (дата обращения: 02.12.2021).

2. Полиграфы на российском рынке. – URL: http://www.bnti.ru/index.asp?tbl=05.13 (дата обращения: 02.12.2021).

3. *Monk S.* Programming Arduino: getting started with sketches. – New York: McGraw-Hill/TAB Electronics, 2011. – 162 p.

4. *Margolis M.* Arduino cookbook. – Oreilly, 2014. – 800 p.

5. *Petracca M., Passaro P., Gioia E.* AMBER: advanced mother board for embedded systems pRototyping // EURASIP Journal on Embedded Systems. – 2017. – Vol. 2017. – P. 32. – DOI: 10.1186/s13639-017-0080-z.

6. A MATLAB based on-line polygraph test using galvanic skin resistance and heart rate measurement / A. Sinha, M. Pavithra, K.R. Sutharshan, M. Subashini // Australian Journal of Basic and Applied Sciences. – 2013. – Vol. 7 (11). – P. 153–157.

7. USB Polygraph // Juangg Projects. – 2019. – June 09. – URL: https://juangg-projects.blogspot.com/2019/06/usb-polygraph.html (accessed: 02.12.2021).

8. *Цапенко М.* Измерительные информационные системы: структуры и алгоритмы, системотехническое проектирование: учебное пособие. – 2-е изд., перераб. и доп. – М.: Энергоатомиздат, 1985. – 439 с.

9. Датчик температуры TMP36 и Arduino. – URL: https://arduino-diy.com/arduino-datchik-temperatury-TMP36 (дата обращения: 02.12.2021).

10. *Смирнов В.А.* Биофизические основы плетизмографии. Регистрация и анализ фотоплетизмограмм: методические указания для самоподготовки студентов / Амурская государственная медицинская академия. – Благовещенск, 2014. – 10 с.

Для цитирования:

Mashtakov V.A., Belov V.M. Modeling of a hardware and software complex "Poligraf" based on freely distributable microcontroller platforms // Безопасность цифровых технологий. – 2021. – № 4 (103). – С. 9–19. – DOI: 10.17212/2782-2230-2021-4-9-19.

For citation:

Mashtakov V.A., Belov V.M. Modeling of a hardware and software complex "Poligraf" based on freely distributable microcontroller platforms. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 4 (103), pp. 9–19. DOI: 10.17212/2782-2230-2021-4-9-19.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 4 (103). – 20–36

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.17212/2782-2230-2021-4-20-36

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТА ДАННЫХ В СИСТЕМАХ «УМНЫЙ ДОМ»*

И.Л. РЕВА[1], А.Б. АРХИПОВА[2], Р.В. САМОЙЛЕНКО[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры защиты информации. E-mail: reva@corp.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры защиты информации. E-mail: arhipova@corp.nstu.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: ro999@yandex.ru*

Идея умных домов существует уже несколько десятилетий и с тех пор неоднократно описывалась разными авторами. Однако в определениях последних 20 лет почти всегда присутствуют три аспекта. Во-первых, домашние устройства должны быть подключены не только друг к другу, но также и к Интернету. Во-вторых, необходим интеллектуальный способ управления системой, например, центральный шлюз или интеллектуальные приложения для смартфонов. Наконец, в системе должна быть определенная степень домашней автоматизации. Программно-аппаратный комплекс, удовлетворяющий данным требованиям, можно назвать системой «умного дома». Важное практическое значение имеет сейчас система обеспечения безопасности «умного дома», которая должна включать в себя меры по защите IT-инфраструктуры, обеспечивающие личную безопасность жителей, их здоровья, санитарного состояния помещения, а также сохранность материальных ценностей. Из этого следует, что довольно актуальной является проблема отсутствия тщательного исследования угроз информационной безопасности и проработки защиты всего программно-аппаратного комплекса системы «умный дом». При решении данной задачи в статье проведен анализ основных типов и характеристик системы «умный дом», выявлены их ключевые уязвимости. Также проведено исследование уязвимостей аппаратного обеспечения системы «умный дом». Проведена качественная оценка рисков информационной безопасности умного дома и выработаны защитные меры для их снижения; разработан и исследован прототип фрагмента системы безопасности «умный дом». При экспериментальном исследовании угроз и уязвимостей

* Статья получена 01 ноября 2021 г.

разработанного прототипа фрагмента системы «умный дом» была подробно изучена угроза перехвата критически важной информации системы. По результатам разработки и исследования «Инспектора безопасности» были сделаны выводы об эффективности применения модуля обнаружения вторжения.

Ключевые слова: информационная безопасность, безопасность системы «умный дом», модель угроз, оценка рисков, инспектор безопасности, система обнаружения вторжения, система безопасности, критически важная информационная система

ВВЕДЕНИЕ

Процессы цифровизации потребностей населения страны обусловлены чрезвычайно стремительным распространением и развитием устройств IT-инфраструктуры, которые успешно применяются для обеспечения комфортного быта граждан в многоквартирных и частных домах.

IT-технологии дают возможность создать умный дом, который представляет собой комплекс программно-аппаратных систем, непосредственно управляющих всеми компонентами инженерных коммуникаций, реализованных в жилом помещение. Согласно исследованиям компании IDC, на 2020 год объем мирового рынка устройств для умного дома составил 801,5 млн штук, увеличившись по сравнению с 2019 годом на 4,5 %. В отчете IDC отмечено, что рынок оборудования для умного дома будет сохранять положительную динамику до 2025 года и к концу периода превысит 1,4 млрд единиц [1]. Однако важно учитывать, что информация, хранящаяся и используемая в системах автоматизации жилого помещения, является частью индивидуальной критической информационной инфраструктуры, поэтому чем больше растет популярность умного дома, тем серьезнее становится проблема информационной безопасности такого комплекса.

Важное практическое значение обеспечения безопасности умного дома имеют меры по защите IT-инфраструктуры, обеспечивающие личную безопасность жителей, их здоровья, санитарного состояния помещения, а также сохранность материальных ценностей.

Из этого следует, что довольно актуальной является проблема отсутствия тщательного исследования угроз информационной безопасности и проработки защиты всего программно-аппаратного комплекса системы «умный дом». Всё больше появляется случаев, когда реальные устройства были скомпрометированы, что демонстрирует важность обеспечения высокой безопасности в этой области. Fernandes использовали несколько уязвимостей в Samsung SmartThings с сопутствующими приложениями, например, чтобы отключить определенные функции и вызвать ложную пожарную тревогу [2]. Schwartz провели тестирование методом «черного ящика» на 16 устройствах умного

дома и восстановили пароли на восьми из них [3]. Более того, были дополнительные сообщения о взломах реальных пользователей и компаний. Эти атаки варьируются от получения доступа к радионяням до доступа к внутренним серверам казино через аквариумный термометр. Поэтому очевидной становится работа, связанная с исследованием вопросов в области защиты информации устройств умного дома.

1. ОСНОВНАЯ ИДЕЯ

Идея умных домов существует не менее 70 лет и с тех пор неоднократно определялась разными авторами [4–8]. Однако в определениях последних 20 лет почти всегда присутствуют три аспекта. Во-первых, домашние устройства должны быть подключены не только друг к другу, но также и к Интернету. Во-вторых, необходим интеллектуальный способ управления системой (например, центральный шлюз или интеллектуальные приложения для смартфонов). Наконец, в системе должна быть определенная степень домашней автоматизации.

Программно-аппаратный комплекс, удовлетворяющий данным требованиям, можно назвать системой «умный дом».

В умных домах в основном используются три разных типа устройств – датчики, исполнительные механизмы и смешанные устройства. Датчики (например, термометры, датчики света или кнопочные переключатели) предоставляют информацию о реальном мире в сеть умного дома. Приводы (например, лампочки, интеллектуальные замки или кофеварки) берут за основу эту информацию и выполняют действия в соответствии с некоторыми предустановленными правилами автоматизации или ручными инструкциями. Наконец, смешанные устройства – это более мощные устройства с датчиками и исполнительными механизмами (например, развлекательные системы или системы наблюдения). В дополнение к этому в большинстве типов умных домов есть центральный шлюз, который соединяет дом и позволяет устройствам обмениваться данными. Персональные компьютеры и смартфоны обычно не считаются устройствами умного дома.

Если рассматривать систему «умный дом» как объект защиты информации, то его можно представить как помещение, оборудованное комплексом средств вычислительной техники, с использованием информационных технологий, которые способны функционировать автоматически, решая задачу обеспечения комфортного и безопасного проживания человека (рис. 1).

Вышеуказанная IT-система способна анализировать потребности человека и подстраиваться под них путем формирования и сохранения условий для повседневной жизнедеятельности человека, а также обеспечения личной

защищенности, уменьшения вероятности причинения вреда здоровью граждан и их материальным ценностям. Из этого можно сделать вывод, что целью управления системой «умный дом» является поддержание условий проживания, которые отвечают всем требованиям безопасности, а также обеспечение необходимого уровня комфорта, что достигается путем проактивного управления инженерными коммуникациями внутри здания, в том числе посредством взаимодействия с окружающей средой.

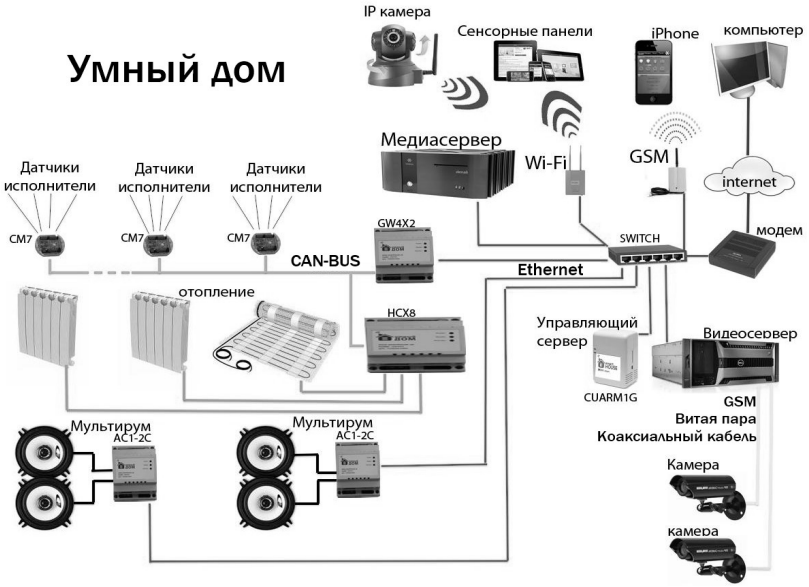


Рис. 1. Типовая система «умный дом»

Fig. 1. Typical Smart Home System

2. СТРУКТУРА УМНОГО ДОМА

Использование программно-аппаратного комплекса «умный дом» дает возможность гарантировать комфортную и высокоэффективную эксплуатацию, избежать риска причинения ущерба, вызывающего отказ или поломки всех систем жизнеобеспечения здания.

Выше подчеркивалось, что понятие «умный дом» объединяет в себе помещения в зданиях разнообразного назначения с целостной IT-системой кон-

троля состояния всех подсистем, обеспечивающих безопасность и комфортное нахождение в здание.

На рис. 2 более подробно изображена структура системы «умный дом».

Рис. 2. Структура и основные модули системы «умный дом»

Fig. 2. Smart home system structure and main modules

Есть несколько способов объединить все системы жизнеобеспечения и создать умный дом, удобный для эксплуатации конечным пользователем. Наиболее популярны четыре архитектуры, используемые для умных домов, каждая из которых имеет свои недостатки и преимущества [9].

3. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ УМНОГО ДОМА

В этом разделе проанализированы различные атаки на систему «умный дом» и классифицированы по требованиям безопасности, на которые они нацелены. Мы ориентируемся на три основных требования:

– конфиденциальность;

– целостность;

– доступность.

Согласно статистическим исследованиям компании Dr.WEB, за последние годы прослеживается динамично увеличение атак на подобные системы, результат приведен на рис. 3.

В контексте анализа умного дома под конфиденциальностью подразумевается такое состояние IT-системы управления умным домом, при котором отсутствует возможность утечки информации через подсистемы. Пример реализации угрозы – утечка персональной информации или утечка информации о конфигурации IT-систем умного дома.

Рис. 3. Динамика зафиксированных атак на устройства интернета вещей согласно статистическим исследованиям компании Dr.WEB

Fig. 3. Dynamics of recorded attacks on the Internet of Things devices according to the statistical studies of Dr.WEB

Целостность информации – это достоверность и полнота информации, получаемая системой от различных датчиков и устройств, установленных в системе. Например, при получении неверной информации о присутствии в помещении человека происходит ложное срабатывание системы контроля доступа.

Доступность информации применительно к умному дому – это состояние информации или ресурсов IT-системы, при котором субъекты или сама система, имеющие права доступа, могут реализовать различные действия в соответствии со сценарием работы (выключать / включать датчики, открывать замки и т. д.).

Проанализировав все возможные варианты угроз информационной безопасности умного дома, можно составить перечень наиболее возможных, тем самым создав модель угроз (табл. 1), которая в дальнейшем будет использоваться для оценки рисков.

Таблица 1

Table 1

Модель угроз информационной безопасности умного дома

Smart home information security threat model

№	Тип атаки	Уязвимость	Возможные последствия
1	Хакерские атаки на центральный сервер	Подключение сети умного дома к Интернету. Отсутствие (неэффективность) механизмов защиты периметра сети	Нарушение работы либо выход из строя центрального сервера, а следовательно, и всей системы. Нарушение конфиденциальности, целостности и доступности информации (КЦД)

Продолжение табл. 1

Continuation of the Tab. 1

№	Тип атаки	Уязвимость	Возможные последствия
2	Влияние вирусных и троянских программ на работу системы	Подключение сети умного дома к Интернету. Отсутствие (неэффективность) механизмов защиты периметра сети	Сбои в ПО системы, а следовательно, нарушение работы либо вывод из строя аппаратуры системы. Нарушение КЦД информации, находящейся внутри сети
3	Перехват информации, передаваемой по проводным и беспроводным каналам связи	Возможность доступа злоумышленника к проводным каналам или к зоне устойчивого перехвата радиосигналов сети. Отсутствие (неэффективность) механизмов защиты трафика	Нарушение конфиденциальности информации, передаваемой по каналу. Возможен захват управления системой
4	Доступ злоумышленника с правами администратора на центральный сервер с помощью хищения паролей и других реквизитов разграничения доступа	Отсутствие (неэффективность) механизмов аутентификации и идентификации	Нарушение КЦД информации, находящейся внутри сети
5	Доступ к сети неавторизованных пользователей	Отсутствие (неэффективность) механизмов аутентификации и идентификации	Нарушение КЦД информации, находящейся внутри сети
6	Наличие нарушителей в числе обслуживающего персонала (охранники, наладчики, уборщики и др.)	Отсутствие (неэффективность) организационных мероприятий по отбору и контролю за персоналом	Нарушение КЦД информации. Возможны сбои в системе из-за неправильного обслуживания оборудования. Уровень опасности зависит от степени доступа инсайдера к системе
7	Ошибки пользователя	Отсутствие (неэффективность) механизмов защиты системы от неправильных действий пользователей	Нарушение КЦД информации. Возможны сбои в системе из-за неправильного использования оборудования

Окончание табл. 1

End of the Tab. 1

№	Тип атаки	Уязвимость	Возможные последствия
8	Кража (злоумышленный вывод из строя аппаратуры) системы «умный дом»	Отсутствие (неэффективность) – физической охраны объекта	Нарушение КЦД информации
9	Перебои в сети электропитания	Отсутствие системы автономного электропитания	Дезорганизация работы системы
10	Стихийные бедствия (пожар и др.)	Отсутствие (неэффективность) механизмов защиты	Дезорганизация работы системы
11	Поломка аппаратуры системы	Низкая надежность оборудования, низкая квалификация персонала	Нарушение КЦД информации
12	Ошибки программного обеспечения	Использование нелицензионного ПО, низкая квалификация персонала, отсутствие (неэффективность) тестирования закупаемого ПО	Нарушение КЦД информации
13	Утечка информации через побочные электромагнитные излучения и наводки (ПЭМИН)	Наличие ПЭМИ компьютерной техники. Выход проводников, в которых могут быть наводки излучений, за пределы контролируемой зоны	Нарушение конфиденциальности информации, обрабатываемой на ЭВМ
14	Утечка информации по акустоэлектрическому каналу	Наличие акустоэлектрических преобразователей (датчики ОС, ПС)	Нарушение конфиденциальности информации

4. ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УМНОГО ДОМА

Угрозы информационной безопасности IT-системы «умный дом» в первую очередь зависят от выбранных способов и технологий построения данной системы, так как на определение возможных угроз влияет состав оборудования. Для оценки рисков информационной безопасности умного дома использовались угрозы, представленные в предыдущих разделах. Их реализа-

ция может привести к нарушению информационной безопасности умного дома, построенного по классической технологии.

При оценке рисков системы умного дома использовался качественный метод для обоснования и оценки угроз, их привязки к уязвимостям системы, определения вероятности их возникновения и потенциального влияния на всю систему умного дома. Во время проведения оценки рисков оценивалась соответствующая вероятность и воздействие, связанные с каждой идентифицированной угрозой, по пятиуровневой шкале (1–5), после чего рассчитывалось значение риска.

Для анализа применялся подход на основе анализа угроз безопасности информационных систем, уязвимостей и уровней риска. Следовательно, архитектура умного дома рассматривается по аналогии с информационной системой и, таким образом, разделяется на подкатегории, содержащие программное обеспечение, оборудование, информацию (или данные), протоколы связи (включая радиосвязь) и людей (в качестве конечных пользователей или представителей, например поставщиков).

При анализе можно разделить систему на следующие шесть частей:

- подключенные датчики / устройства (S);
- внутренний шлюз (GW);
- облачный сервер (CS);
- API (API);
- мобильное устройство;
- приложения для мобильных устройств.

Каждая из вышеперечисленных частей была проанализирована в поисках уязвимостей и угроз, связанных с оборудованием, программным обеспечением, информацией, коммуникациями и человеческими аспектами в структурированном виде. Если риск был идентифицирован, ему присваивался уникальный дескриптор (идентификатор).

Каждый риск представлен следующими шестью атрибутами: уникальным идентификатором, объяснением уязвимости, объяснением угрозы, значением вероятности, значением стоимости последствий и в результате значением риска. Значения как вероятности, так и последствий рассчитываются с использованием анализа статистических данных атак на информационную систему. Значения риска были рассчитаны путем умножения средней вероятности и значений последствий, что дает значение риска в диапазоне 1…25. Однако самые низкие значения риска, измеренные в этом исследовании, составили 3,5, а самые высокие – 15,44. Более подробная информация о значениях риска, вероятности и последствий представлена в табл. 2.

Таблица 2

Table 2

Минимальное и максимальное значения вероятности, последствий и риска

Minimum and maximum values of probability, consequences and risk

Исследуемый параметр	Минимум	Максимум
Значение вероятности	1.0	4,75
Значение последствий	2.0	4.0
Значение риска	3.5	15,44

Исходя из значений риска каждый риск можно отнести к одному из следующих трех классов серьезности: низкий, средний, высокий. Классы серьезности были определены следующим образом:

- низкий, если значение риска < 6, т. е. событие маловероятно или риск имеет незначительное влияние;
- средний, если значение риска ≥ 6 и значение риска < 10;
- высокий, если значение риска ≥ 10.

Таким образом, что касается пятиуровневой шкалы, низкий риск требует, чтобы один из факторов вероятность / воздействие был низким или, если они равны, оба должны быть ниже 2,5. Средний риск включает два самых высоких значения для одного из факторов вероятности / воздействия, только если другой фактор ниже 3,0. Высокий риск требует, чтобы оба фактора были выше 3. Из 32 рисков 9 были классифицированы как низкие, 19 как средние и 4 как высокие по степени серьезности. В табл. 3 показана классификация серьезности каждого риска, разделенного на шесть категорий подсистем, а также на пять категорий угроз. Категория угроз, которая включает в себя большинство рисков, – это категория, связанная с программным обеспечением, которая включает 13 рисков. Категории угроз, касающиеся информации, коммуникации и человека, содержат по 5 рисков каждая, в то время как аппаратные угрозы содержат 4 риска. Наиболее серьезные риски встречаются в категории людей.

В табл. 3 представлена классификация серьезности риска на низкий / средний / высокий на основе соответствующего значения риска. Риски разделены на пять столбцов, по одному для каждой категории угроз, и шесть строк, по одной для каждой категории подсистем.

Таблица 3

Table 3

Классификация серьезности риска

Classification of risk severity

Идентификатор	Программное обеспечение	Аппаратное обеспечение	Информация	Передача данных	Человек
Датчики / устройства	0 / 0 / 0	0 / 1 / 0	1 / 0 / 0	1 / 0 / 0	N / A
Шлюз	0 / 3 / 0	0 / 1 / 0	0 / 2 / 0	0 / 1 / 0	N / A
Облачный сервер	0 / 1 / 0	1 / 0 / 0	1 / 0 / 0	0 / 1 / 0	N / A
Мобильные устройства	1 / 0 / 0	1 / 0 / 0	1 / 0 / 0	1 / 0 / 0	N / A
Программы	0 / 3 / 1	0 / 0 / 0	0 / 0 / 0	0 / 0 / 0	N / A
API	0 / 4 / 0	0 / 0 / 0	0 / 0 / 0	1 / 0 / 0	N / A
Общее	1 / 11 / 1	2 / 02 / 0	3 / 2 / 0	3 / 2 / 0	0 / 2 / 3

5. РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПРОТОТИПА ФРАГМЕНТА ЗАЩИТЫ СИСТЕМЫ «УМНЫЙ ДОМ»

В этом разделе описывается процесс разработки модуля безопасности для обнаружения вредоносной активности в сети умного дома, так как выявление атак является первоочередной и наиболее проблемной задачей. Модуль мы называли «Инспектор безопасности», он интегрирован с популярной платформой Smart Hub, использующей открытый исходный код. Описана структура Security Supervisor (Инспектор безопасности) и то, как она взаимодействует с Home Assistant на абстрактном уровне, также описана фактическая реализация системы защиты.

При создании прототипа фрагмента защиты системы «умный дом», был использован интеллектуальный концентратор в качестве места для размещения диспетчера безопасности. Было проанализировано несколько умных хабов и выбран Home Assistant из-за его популярности, доступности и открытости. Таким образом, был разработан диспетчер безопасности так, чтобы он соответствовал архитектуре Home Assistant, даже несмотря на то что общие

принципы программного обеспечения можно адаптировать к любой системе интеллектуального концентратора.

Как уже отмечалось выше, модуль ориентирован на обнаружение угроз безопасности системы «умный дом», в дальнейших исследованиях при успешных испытаниях «Инспектора безопасности» планируется изучить возможные реакции системы на обнаруженные атаки и разработать оптимальный способ их предотвращения.

Home Assistant имеет простую модульную архитектуру программного обеспечения (рис. 4) [13]. Он состоит из центрального ядра, пользовательского интерфейса, домашней автоматизации и компонентов для связи с интеллектуальными устройствами в доме. На рис. 4 заштрихованные области – части исходного кода Home Assistant, а незаштрихованные – внешние библиотеки и физические устройства.

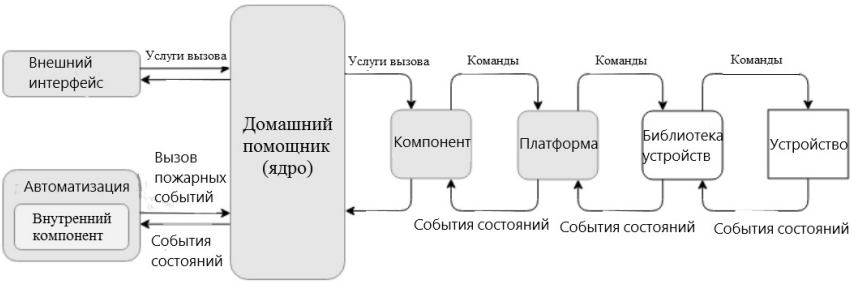


Рис. 4. Архитектура домашнего помощника [13]

Fig. 4. Home Assistant Architecture [13]

Ядро Home Assistant состоит из Event Bus и State Machine. Event Bus позволяет другим частям Home Assistant активировать и прослушивать события, чтобы сообщать об изменениях друг другу. State Machine хранит текущее состояние умного дома, и изменения состояний упрощаются с помощью событий, отправляемых по шине EventBus.

Связь с устройствами умного дома осуществляется через компоненты и платформы. Компоненты объекта – это элементы, которые обеспечивают связь с определенным типом устройства (например, светом или переключателем). Они содержат общие функции для типа устройства. Платформы расширяют компоненты сущности, чтобы они были совместимы с устройствами определенных марок. Фактическая связь с устройством осуществляется через внешние сторонние библиотеки. Платформы передают команды, состояния и события этим библиотекам через вызовы API. Модульность, обеспечивае-

мая компонентами сущностей и платформами, упрощает разработчикам добавление поддержки для большего количества устройств.

Заключительная часть Home Assistant – это домашняя автоматизация, управляющая пользовательскими настройками и внутренними компонентами, которые используют триггеры событий вместе с информацией из ядра для активации команд. Примером автоматизации может быть включение света, когда пользователь приходит домой, а на улице темно.

ЗАКЛЮЧЕНИЕ

Результатом настоящей работы является исследование защищенности IT-систем умного дома путем выявления угроз и уязвимостей информационной безопасности умного дома, а также применения натурного моделирования для проверки работоспособности предлагаемых решений по защите умного дома.

Для достижения указанной цели в ходе работы были решены следующие задачи:

- при решении задачи анализа основных типов и характеристик системы «умный дом» были выявлены их ключевые уязвимости, проведено исследование уязвимостей аппаратного обеспечения системы;
- проведена качественная оценка рисков информационной безопасности умного дома и выработаны защитные меры для их снижения;
- разработан и исследован прототип фрагмента системы «умный дом»;
- при экспериментальном исследовании угроз и уязвимостей разработанного прототипа фрагмента системы «умный дом» была подробно изучена угроза перехвата критически важной информации системы.

По результатам разработки и исследования Инспектора безопасности были сделаны выводы об эффективности применения модуля обнаружения ботнета. Также следует подчеркнуть оптимальное использование ресурсов прототипом безопасности, что доказывает оптимальность подбора комплектующих для создания модуля обнаружения. В дальнейших исследованиях запланировано усовершенствование модуля обнаружения вредоносной активности и разработка полноценной системы для предотвращения атак на программно-аппаратный комплекс «умный дом».

СПИСОК ЛИТЕРАТУРЫ

1. IDC forecasts double-digit growth for smart home devices as consumers embrace home automation and ambient computing [Прогноз продаж умных

устройств]. – IDC, 2021. – URL: https://www.idc.com/getdoc.jsp?containerId=prUS47567221 (accessed: 03.12.2021).

2. *Fernandez E., Jung J., Prakash A.* Security analysis of new intelligent home applications // Proceedings of the IEEE Symposium on Security and Privacy (SP). – San Jose, CA, 2016. – P. 636–654. – DOI: 10.1109/SP.2016.44.

3. Opening Pandora's box: effective techniques for reverse engineering IoT devices / O. Shwartz, Y. Mathov, M. Bohadana, Y. Elovici, Y. Oren // Smart Card Research and Advanced Applications, CARDIS 2017. – Cham: Springer, 2018. – P. 1–21. – DOI: 10.1007/978-3-319-75208-2_1.

4. *Полоцкий Р.Е.* Что такое «умный дом»? // Алгоритм безопасности. – 2017. – № 4. – С. 4–7.

5. *King N.* Smart home – definition. – Intertek Research & Testing Centre, 2003. – URL: https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf (accessed: 03.12.2021).

6. Организация информационного взаимодействия элементов системы «умный дом» / В.С. Афонин, А.Г. Зрюмова, А.А. Кузнецов, Р.А. Забеляев, Р.А. Дьякин // Ползуновский альманах. – 2017. – № 4-3. – С. 170–172.

7. *Robles R.J., Kim T.-h.* Applications, systems and methods in intelligent home technologies: a review // International Journal of Advanced Science and Technology. – 2010. – Vol. 15. – P. 37–48.

8. *Sandström G.* Smart homes and user values: long-term evaluation of IT-services in residential and single family dwellings: Doctoral thesis. – Stockholm: KTH, 2009. – 164 p. – URL: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A281689&dswid=-7783 (accessed: 08.12.2021).

9. *Росляков А.В.* Интернет вещей. – Самара: ПГУТИ, 2014. – 342 с.

10. *Снегуров А.В., Ткаченко Е.А., Кравченко А.Д.* Риски информационной безопасности систем, построенных по технологии «Умный дом» // Восточно-Европейский журнал передовых технологий. – 2011. – Т. 4, № 3. – С. 30–34.

11. *Fall K.*, *Stevens W.* TCP/IP illustrated. Vol. 1. The protocols. – 2nd ed. – Upper Saddle Rive: Addison-Wesley, 2012. – 1056 p. – (Addison-Wesley Professional Computing Series).

12. Overview of intrusion detection in the internet of things / B. Bogaz, R.S. Miani, G.G. Garpelon, S.T. Kawakani, S.C. de Alvarenga // Journal of Network and Computer Applications. – 2017. – Vol. 84. – P. 25–37. – URL: http://www.sciencedirect.com/science/article/pii/S1084804517300802 (accessed: 08.12.2021).

13. *Anderson R.* Security engineering: a guide to building dependable distributed systems. – 3rd ed. – New York: Wiley, 2020. – 1232 p.

Рева Иван Леонидович, кандидат технических наук, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность, информационные технологии, приборостроение. E-mail: reva@corp.nstu.ru

Архипова Анастасия Борисовна, кандидат технических наук, доцент кафедры защиты информации Новосибирского государственного технического университета. Основные направления научных исследований: программное обеспечение научных задач, управление в социально-экономических системах, информационная безопасность. E-mail: arhipova@corp.nstu.ru

Самойленко Роман Вадимович, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность. E-mail: Cherkaev@corp.nstu.ru

DOI: 10.17212/2782-2230-2021-4-20-36

Analysis of threats to information security and data protection in the "Smart house systems"*

I.L. Reva[1], A.B. Arhipova[2], R.V. Samoylenko[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, Associate Professor of the Department of Information Security. E-mail: reva@corp.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, Associate Professor of the Department of Information Security. E-mail: arhipova@corp.nstu.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: ro999@yandex.ru*

The idea of smart homes has been around for several decades and has been described by different authors many times since then. However, there are almost always three aspects in the definitions of the last 20 years. First, home devices must be connected, not only to each other, but also to the Internet. Second, an intelligent way to manage the system is needed, such as a central gateway or smart smartphone apps. Finally, there must be some degree of home automation in the system. A hardware and software complex that meets these requirements can be called a "smart home" system. The system of ensuring the security of the "smart home" is now of great practical importance, which should include measures to protect the IT infrastructure, ensuring the personal safety of residents, ensuring their health, the sanitary condition of the premises, as well as the safety of material assets. It follows from this that the problem of the lack of a thorough study of information security threats and the elaboration of protection of the entire software and hardware

* *Received 01 November 2021.*

complex of the "smart home" system is quite urgent. When solving this problem, an analysis of the main types and characteristics of smart home systems was carried out, and their key vulnerabilities were identified. Also, a study of vulnerabilities in the hardware of smart home systems was carried out; A qualitative assessment of the information security risks of a "smart home" has been carried out and protective measures have been developed to reduce them; A prototype of a fragment of the “smart home” security system has been developed and studied. In an experimental study of threats and vulnerabilities of the developed prototype of a fragment of the "smart home" system, the threat of interception of critical information of the system was studied in detail. Based on the results of the development and research of the Security Inspector, conclusions were drawn about the effectiveness of the use of the intrusion detection module.

Keywords: information security, smart home security, threat model, risk assessment, security inspector, intrusion detection system, security system, critical information system

REFERENCES

1. *IDC forecasts double-digit growth for smart home devices as consumers embrace home automation and ambient computing*. IDC, 2021. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS47567221 (accessed 03.12.2021).

2. Fernandez E., Jung J., Prakash A. Security analysis of new intelligent home applications. *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2016, pp. 636–654. DOI: 10.1109/SP.2016.44.

3. Shwartz O., Mathov Y., Bohadana M., Elovici Y., Oren Y. Opening Pandora’s box: effective techniques for reverse engineering IoT devices. *Smart Card Research and Advanced Applications, CARDIS 2017*. Cham, Springer, 2018, pp. 1–21. DOI: 10.1007/978-3-319-75208-2_1.

4. Polotskii R.E. Chto takoe "umnyi dom"? [What is a smart home]. *Algoritm bezopasnosti*, 2017, no. 4, pp. 4–7.

5. King N. *Smart home – definition*. Intertek Research & Testing Centre, 2003. Available at: https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf (accessed 03.12.2021).

6. Afonin V.S., Zryumova A.G., Kuznetsov A.A., Zabelyaev R.A., D'yakin R.A. Organizatsiya informatsionnogo vzaimodeistviya elementov sistemy "umnyi dom" [Organization of information interaction of elements of the smart home system]. *Polzunovskii al’manakh = Polzunov Almanac*, 2017, no. 4-3, pp. 170–172.

7. Robles R.J., Kim T.-h. Applications, systems and methods in intelligent home technologies: a review. *International Journal of Advanced Science and Technology*, 2010, vol. 15, pp. 37–48.

8. Sandström G. *Smart homes and user values: long-term evaluation of IT-services in residential and single family dwellings*. Doctoral thesis. Stockholm, KTH, 2009. 164 p. Available at: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A281689&dswid=-7783 (accessed 08.12.2021).

9. Roslyakov A.V. *Internet veshchei* [Internet of things]. Samara: PGUTI Publ., 2014. 342 p.

10. Snegurov A.V., Tkachenko E.A., Kravchenko A.D. Riski informatsionnoi bezopasnosti sistem, postroennykh po tekhnologii "Umnyi dom" [Risk of information security systems based on technology "smart house". *Vostochno-Evropeiskii zhurnal peredovykh tekhnologii = Eastern-European Journal of Enterprise Technologies*, 2011, vol. 4, no. 3, pp. 30–34.

11. Fall K., Stevens W. *TCP/IP illustrated*. Vol. 1. *The protocols*. 2nd ed. Upper Saddle Rive, Addison-Wesley, 2012. 1056 p.

12. Bogaz B., Miani R.S., Garpelon G.G., Kawakani S.T., Alvarenga S.C. de. Overview of intrusion detection in the internet of things. *Journal of Network and Computer Applications*, 2017, vol. 84, pp. 25–37. Available at: http://www.sciencedirect.com/science/article/pii/S1084804517300802 (accessed 08.12.2021).

13. Anderson R. *Security engineering: a guide to building dependable distributed systems*. 3rd ed. New York, Wiley, 2020. 1232 p.

Для цитирования:

Рева И.Л., Архипова А.Б., Самойленко Р.В. Анализ угроз информационной безопасности и защита данных в системах «умный дом» // Безопасность цифровых технологий. – 2021. – № 4 (103). – С. 20–36. – DOI: 10.17212/2782-2230-2021-4-20-36.

For citation:

Reva I.L., Arkhipova A.B., Samoylenko R.V. Analiz ugroz informatsionnoi bezopasnosti i zashchita dannykh v sistemakh "Umnyi dom" [Analysis of threats to information security and data protection in the "Smart house systems"]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 4 (103), pp. 20–36. DOI: 10.17212/2782-2230-2021-4-20-36.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 4 (103). – 37–53

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.17212/2782-2230-2021-4-37-53

РАЗРАБОТКА ЛАБОРАТОРНОГО СТЕНДА ДЛЯ ИЗУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ*

Н.В. КУКУШКИНА[1], А.К. НОВОХРЁСТОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистрант кафедры вычислительной техники. E-mail: kukushkina.2020@stud.nstu.ru*

[2] *634050, РФ, г. Томск, пр. Ленина, 40, Томский государственный университет систем управления и радиоэлектроники, кандидат технических наук, доцент кафедры комплексной информационной безопасности электронно-вычислительных систем. E-mail: nak@fb.tusur.ru*

Объектом исследования настоящей статьи являются сетевые и узловые системы обнаружения вторжений. В качестве цели исследования ставится получение обзора по системам обнаружения вторжений, а также построение конструктивного варианта виртуального лабораторного стенда, предназначенного для обучения студентов (изучение тестовых характеристик систем обнаружения вторжений). В статье приведена краткая справка о системах обнаружения вторжений с учетом классификации по способу мониторинга и технологии обнаружения атак. На сегодняшний день системы обнаружения вторжений являются необходимым элементом комплексной системы защиты сетей как небольших, так и крупных организаций. Они позволяют повысить безопасность сети, защищая от внешних и внутренних нарушителей. Поэтому необходимость получения навыков установки, настройки и администрирования систем обнаружения вторжений является важной частью подготовки специалистов по информационной безопасности, что обусловливает необходимость непрерывной актуализации и модернизации средств обучения. В настоящей работе предлагается виртуальный лабораторный стенд, предназначенный для изучения систем обнаружения вторжений. Описаны его архитектура и параметры функционирования. С целью выбора системы обнаружения вторжений для виртуального лабораторного стенда был проведен сравнительный анализ имеющихся на рынке бесплатных и коммерческих систем обнаружения вторжений. Отдельно были рассмотрены узловые и сетевые системы обнаружения вторжений. Для обоих видов описаны их преимущества и недостатки. В результате для выбранной по результатам анализа системы обнаружения вторжений описаны функции и механизм работы. Кроме того, рассмотрены примеры пользовательских правил обработки событий безопасности.

* Статья получена 10 ноября 2021 г.

Ключевые слова: система обнаружения вторжений, система предотвращения вторжений, лабораторный стенд, сравнительный анализ, сетевые системы обнаружения вторжений, узловые системы обнаружения вторжений, Open Source Security, мониторинг событий

ВВЕДЕНИЕ

В настоящее время достаточно остро стоит вопрос организации безопасности сетей. Согласно исследованию компании Check Point [1], в 2021 году число кибератак в мире увеличилось на 40 % по сравнению с предыдущим годом. Кроме того, около 80 % взломов осуществляется внутри организации. Поэтому появляется необходимость своевременно обнаруживать и анализировать эти атаки, чтобы оптимально организовать безопасность сети. Одним из решений данной задачи является использование систем обнаружения вторжений.

1. ОСНОВНЫЕ СВЕДЕНИЯ О СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

1.1. ОПРЕДЕЛЕНИЯ И КЛАССИФИКАЦИЯ

Система обнаружения вторжений (IDS – Intrusion detection system, аналогичный русскоязычный термин – СОВ) – это программное либо программно-аппаратное средство, которое контролирует сети, хосты или приложения на предмет несанкционированной активности [2].

СОВ относятся к детективным механизмам защиты и используются для обнаружения различных видов вредоносных действий, которые могут поставить под угрозу безопасность компьютерной системы. К таким действиям относятся сетевые атаки на уязвимые сервисы, атаки на повышение привилегий, доступ неавторизованных пользователей к критически важным файлам, а также воздействия вредоносного ПО (компьютерных вирусов, троянов и червей). В случае обнаружения подобной активности системы обнаружения вторжений отправляют оповещение администратору безопасности, который затем может предпринять необходимые действия. Кроме того, СОВ может помочь спрогнозировать атаки в будущем. Например, злоумышленник может осуществлять некоторые предварительные действия, такие как сканирование портов.

Наиболее общая классификация СОВ производится по способу мониторинга. Выделяют СОВ уровня узла (HIDS – host-based IDS) и СОВ уровня сети (NIDS – network-based IDS) [3].

Датчиками узловых СОВ (УСОВ) являются программные модули, которые устанавливаются на защищаемые компьютеры в сети. Эти модули предназначены для отслеживания событий в журналах и обнаружения признаков подозрительной деятельности. Также они могут контролировать целостность файлов конфигурации системы и наличие в них несанкционированных изменений. Одним из недостатков узловых СОВ является их повышенная ресурсоемкость, наличие на защищаемом компьютере. Такая СОВ требует использования определенных вычислительных ресурсов. Помимо этого, она отслеживает только сетевые пакеты, принятые или отправленные компьютером, на котором она установлена.

Датчики сетевых СОВ (ССОВ) выявляют несанкционированное и аномальное поведение исключительно на основании сетевого трафика. Они стратегически расположены в различных точках сети для мониторинга входящего и исходящего трафика сетевых устройств. Однако сетевые СОВ слабо защищают от внутренних атак, так как чтобы обнаружить попытку вторжения, она должна попасть в сеть и зафиксироваться СОВ. Сетевые СОВ, как правило, не влияют на производительность компьютерной сети. Они устанавливаются либо «в разрыв» и пропускают через себя трафик в защищенную сеть, либо работают в режиме «зеркалирования», так или иначе являясь пассивными устройствами. Но в сильно распределенной или нагруженной сети сетевым СОВ может быть сложно обрабатывать весь трафик, и они могут пропустить вредоносные пакеты.

Также возможно классифицировать СОВ по технологии обнаружения [4]:

– на основании сигнатуры (подписи) атаки: атака описывается в виде сигнатуры, т. е. шаблона, характеризующего некоторое содержимое сетевого трафика. Такой метод также называется сигнатурным. Для установки факта вторжения собранный трафик сравнивается с данным шаблоном. Можно выделить также синтаксический разбор пакетов. Захваченные сетевые пакеты проходят через синтаксический анализатор и проверяются на соответствие атаке с помощью регулярных выражений;

– на основании аномального трафика: при обнаружении аномалий (резко изменившийся объем трафика, взаимодействие нетипичных узлов, использование непривычных протоколов и т. д.) источники событий (логи, сетевой трафик, действия пользователей) сопоставляются с профилями поведения. Атакой считается ситуация отклонения от этого профиля. Данный метод также называют эвристическим.

Итак, СОВ может оповещать о вредоносной активности, однако часто необходимо именно предотвратить вредоносную активность на ранней стадии. Для этих целей используются системы предотвращения вторжений (IPS – Intrusion prevention system, аналогичный русскоязычный термин – СПВ).

Программное обеспечение СОВ и СПВ являются ветвями одного и того же дерева и используют аналогичные технологии. Меры защиты СПВ можно отнести к превентивным, в отличие от СОВ, выполняющей детективные функции.

Нельзя сказать, что СПВ лучше СОВ или СОВ лучше СПВ, они имеют разные задачи и возможности. Выбор в каждом конкретном случае зависит от требуемых функций защиты, топологии сети и т. д. Для обеспечения комплексной безопасности наиболее эффективен вариант совместного использования средств СОВ и СПВ.

Известно, что использование СОВ регулируется законодательно. Так, например, информационные системы персональных данных (ИСПДн), в которых необходимо для персональных данных обеспечить 1-й или 2-й уровень защищенности, должны контролироваться СОВ. Существует специальный приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) № 638, который регулирует использование СОВ в государственных информационных системах (ГИС), ИСПДн и других системах. Выделено 6 классов защиты СОВ (6-й – самый низкий) [5]. Причем СОВ, соответствующие 1–3-му классу защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну. Методические документы, описывающие профили защиты, соответствующие данным уровням, не публикуются в открытом доступе, так как сами являются сведениями, составляющими государственную тайну. Федеральная служба безопасности (ФСБ) использует термин «система обнаружения атак» (СОА) вместо СОВ и выделяет 4 класса: А, Б, В, Г. Причем Г – самый низкий, и каждый следующий класс включает все требования к предыдущим. Требования ФСБ отсутствуют в открытом доступе.

1.2. ОБЗОР СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

На данный момент существует достаточно обширный выбор СОВ. В этом разделе попытаемся дать описание некоторых популярных на рынке защитных решений исходя из документации, прилагаемой к этим системам. Рассмотрим их архитектуру, принципы работы и особенности.

А. Узловые системы обнаружения вторжений

OSSEC (сокр. от Open Source Security), возможно, является ведущей УСОВ с открытым исходным кодом, доступной сегодня. Клиент-серверная архитектура OSSEC позволяет отправлять оповещения и журналы на централизованный сервер, где в дальнейшем может выполняться анализ, а также уведомление администратора, даже если хост-система отключена или скомпрометирована [6].

В отличие от OSSEC, Tripwire доступна как с открытым исходным кодом, так и с полноценной корпоративной версией [7]. Tripwire Open Source работает только в системах Linux и Unix, поддержка Windows отсутствует, однако она доступна в коммерческой версии для предприятий. Эта СОВ хорошо подходит для небольших децентрализованных систем.

Программный комплекс (ПК) Ребус-СОВ разработан российским Научно-исследовательским институтом «Центпрограммсистем» и предназначен для обнаружения и предотвращения вторжений. Он функционирует как на уровне узла, так и на уровне сети [8]. ПК Ребус-СОВ включает в себя средство противодействия вторжениям, средство сбора данных и обнаружения вторжений, консоль управления, сервер и агента.

Samhain обеспечивает централизованный сбор данных и анализ информации, собранной каждой отдельной машиной. Samhain обладает отличительной особенностью: она скрывает свои процессы от злоумышленников при помощи стеганографии [9]. В отличие от OSSEC, обработка событий происходит на самом клиенте, что имеет определенные последствия. С практической точки зрения необходимо соблюдать осторожность, чтобы не перегружать сервер и не мешать работе. С точки зрения безопасности наличие обрабатывающего механизма на агенте предоставляет злоумышленникам дополнительную цель.

VipNet IDS HS использует сигнатуры и правила, предоставляемые российской компанией ЗАО «Перспективный мониторинг». Данная СОВ состоит из трех компонентов: агента, сервера и консоли управления [10].

Б. Сетевые системы обнаружения вторжений

ССОВ Snort была выпущена компанией Sourcefire еще в 1998 году и стала своеобразным стандартом и ориентиром для будущих СОВ. Позднее, в 2013 году, компания Sourcefire была приобретена Cisco Systems. Snort является лидером в области ССОВ, но ее все еще можно использовать бесплатно. Преимущества технологии с открытым исходным кодом сосредоточены на более низких затратах и поддержке сообщества.

Поскольку Snort был создан очень давно, с развитием современных технологий и ростом трафика в сети версия 2 оказалась не способна обрабатывать высокоскоростной трафик в силу отсутствия многопоточности. Данный недостаток компенсирован в вышедшей в 2021 году версии Snort 3 [11].

СОА «Форпост» может обнаруживать компьютерные атаки и блокировать их источники на сетевом оборудовании в ручном или автоматическом режиме [12]. «Форпост» может поставляться в качестве программного обеспечения (устанавливаться на выделенные сервера заказчика) и в качестве заранее сконфигурированного аппаратно-программного комплекса.

OpenWIPS-NG – это СОВ уровня сети с открытым исходным кодом, которая в основном предназначена для беспроводных сетей [13]. WIPS (Wireless Intrusion Prevention System) переводится на русский язык как «беспроводная система предотвращения вторжений», поэтому эта ССОВ не только обнаруживает, но еще и противодействует вторжениям. OpenWIPS-NG находится на стадии разработки. Она появилась не так давно, поэтому на данный момент эта ССОВ имеет некоторые ограничения. Каждая установка включает в себя только один датчик. Кроме того, данная СОВ не имеет официальной полной документации.

Следующим в нашем списке является продукт под названием Zeek Network Security Monitor (ранее Bro) – это бесплатная ССОВ, которая является больше чем просто системой обнаружения вторжений. Zeek действует в два этапа: регистрация трафика и его анализ [14]. Модуль анализа Zeek состоит из двух элементов. Первый – это механизм событий, который отслеживает инициирующие события, такие как сетевые TCP-соединения или HTTP-запросы. Затем события дополнительно анализируются с помощью интерпретатора сценариев политики (скриптов, использующих собственный язык программирования Zeek Script), который решает, следует ли инициировать предупреждение и запускать действие. Это характеризует Zeek еще и как систему предотвращения вторжений.

С-Терра СОВ обнаруживает сетевые атаки и может использоваться для расследования инцидентов в сфере информационной безопасности [15]. Существует три варианта исполнения: 1) отдельный программно-аппаратный комплекс, 2) в составе С-Терра Шлюз и 3) установка на отдельную виртуальную машину. Возможно интегрирование другими продуктами С-Терра.

2. СРАВНЕНИЕ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Перед руководителями организаций закономерно встает вопрос выбора узловой или сетевой СОВ. Надежный режим безопасности будет включать в себя обе системы. Узловая СОВ может работать совместно с сетевой, обеспечивая дополнительное покрытие для чувствительных рабочих станций и регистрируя всё, что сетевая СОВ могла пропустить. Даже если вредоносные программы смогут проскользнуть мимо сетевой СОВ, их поведение будет обнаружено узловой СОВ.

В табл. 1 и 2 показано, что СОВ могут быть очень дорогими, но, к счастью, большинство лучших СОВ на рынке можно использовать бесплатно (с возможностью приобретения платных компонентов).

Таблица 1

Table 1

Сравнение узловых СОВ

Comparison of host-based IDS

Наименование СОВ	OSSEC	Open Source Tripwire	Ребус-СОВ	Samhain	ViPNet IDS HS
Производитель	Trend Micro	Tripwire, Inc.	НИИ Центр-программ-систем	Samhain Services	ИнфотеКС
Исполнение	ПО	ПО	ПО	ПО	ПО
Стоимость	Бесплатно	Бесплатно	От 48 204 руб.	Бесплатно	От 30 860 руб.
Поддержи-ваемые платформы	Unix, Linux, Windows, macOS	Unix, Linux	Linux, Windows	Unix, Linux, macOS	Linux, Windows
Метод обнаружения атак	Сигнатурный, эвристиче-ский	Сигнатур-ный	Сигнатурный, эвристи-ческий	Сигнатур-ный	Сигнатурный, эвристиче-ский
Наличие сертификата ФСТЭК	Нет	Нет	Есть	Нет	Есть
Активный ответ на атаку	Есть	Нет	Есть	Нет	Нет
Наличие графического интерфейса	Есть	Нет	Есть	Есть	Есть
Контроль целостности файлов	Есть	Есть	Нет	Есть	Есть
Обнаружение руткитов	Есть	Нет	Нет	Есть	Есть

Таблица 2

Table 2

Сравнение сетевых СОВ

Comparison of network-based IDS

Наименование СОВ	Snort	СОА Форпост	OpenWIPS-NG	Zeek	С-Терра СОВ
Производитель	Cisco Systems	ЗАО РНК	Thomas d'Otrepre	Институт Беркли, Калифорния	С-Терра СиЭсПи
Исполнение	ПО	ПО/ПАК	ПО	ПО	ПО/ПАК
Стоимость	Бесплатно	От 194 700 руб.	Бесплатно	Бесплатно	От 117 447 руб.
Поддерживаемые платформы	Unix, Linux, Windows	Linux, Windows	Linux	Linux, FreeBSD, macOS	Linux
Метод обнаружения атак	Сигнатурный	Сигнатурный, эвристический	Сигнатурный	Сигнатурный, эвристический	Сигнатурный, эвристический
Наличие сертификата ФСТЭК	Нет	Есть	Нет	Нет	Есть
Активный ответ на атаку	Возможен при использовании расширения snort_inline	Есть	Нет	Есть	Нет
Наличие графического интерфейса	Нет	Есть	Нет	Нет	Есть
Механизм детектирования	На основании правил	На основании правил	На основании правил	На основании скриптов на собственном языке	На основании правил

В табл. 1 среди бесплатных узловых СОВ выделяется OSSEC, поскольку она использует два метода обнаружения вторжений, может осуществлять активный ответ на атаку (что позволяет ей выиграть у Samhain) и, кроме того, является кроссплатформенной. Также можно сказать, что OSSEC не уступает по функционалу Ребус-СОВ и VipNet IDS HS, которые, в свою очередь, являются коммерческими продуктами. Open Source Tripwire предоставляет довольно узкий набор возможностей, так как большинство значимых функций производитель предлагает в аналогичном коммерческом решении.

На основании данных, представленных в табл. 2, можно сделать вывод, что СОВ с открытым исходным кодом Snort и Zeek обладают примерно одинаковыми возможностями. Помимо прочего, механизм детектирования с помощью скриптов Zeek обеспечивает создание большого количества журналов, при этом не разделяя трафик на «хороший» и «плохой», что позволяет фиксировать практически все события в сети и самостоятельно интерпретировать их с помощью уже упомянутых скриптов. СОВ Open WIPS-NG является самым слабым решением из всех представленных. Это объясняется тем, что проект находится на стадии разработки и многие запланированные функции еще не реализованы.

На российском рынке большинство СОВ поставляются вместе с аппаратной составляющей. Мощность коммерческих аппаратных решений заранее рассчитана и проверена, а внедрением занимаются специалисты. Поэтому можно легко предусмотреть запас, но вот стоят они недешево. Альтернативой служат решения open-source, зарекомендовавшие себя с хорошей стороны и при этом не требующие отчислений за программное обеспечение. Но все вопросы по внедрению ложатся на плечи системного администратора.

Для систем, где необходимо соответствие требованиям ФСТЭК и ФСБ (ГИС, ИСПДн и др.), требуется использовать сертифицированные решения, такие как VipNet IDS HS, СОА «Форпост», «Ребус-СОВ» и «С-Терра СОВ». К сожалению, бесплатных сертифицированных продуктов в России для таких систем нет. Данные СОВ могут использоваться в компаниях малого, среднего и крупного бизнеса. Они имеют широкий модельный ряд и могут быть интегрированы в различные системы.

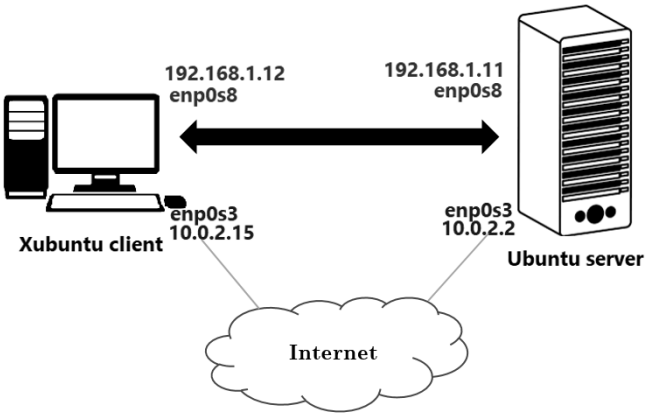
Все СОВ, перечисленные выше, имеют свои плюсы и минусы. Следовательно, лучшая СОВ для каждой отдельной организации будет зависеть от ее потребностей и обстоятельств, размера и топологии сети.

3. ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

На основании сравнения, приведенного в разделе 2, предложим лабораторный стенд, использующий для демонстрации СОВ OSSEC, которая является ярким представителем семейства узловых СОВ, имеет понятный синтаксис правил, осуществляет активный ответ на атаку и может быть установлена практически в любой операционной системе. Изучение конфигурирования и основ работы с СОВ позволит получить студентам ценные профессиональные компетенции.

В процессе обучения могут использоваться различные конфигурации лабораторных стендов. Остановимся на классическом варианте виртуального лабораторного стенда, состоящего из виртуальной машины-сервера и виртуальной машины-клиента. Несмотря на свою простоту, данный стенд имеет возможность добавления разнообразных платформ для аналитики полученных событий, а также возможность реализации многозадачности: в будущем планируется добавление сетевой СОВ на сервер для демонстрации мониторинга сети.

Локальная сеть виртуального лабораторного стенда состоит из сервера и клиента, которые имеют по два адаптера: внутренняя сеть и NAT. На сервере установлена операционная система Ubuntu 18.04, а на клиенте – Xubuntu 20.04. На рисунке представлена архитектура сети для работы с СОВ OSSEC.



Конфигурация сети для СОВ OSSEC

Network configuration for OSSEC IDS

СОВ OSSEC выполняет следующие функции:

– мониторинг целостности файлов;

– мониторинг журналов (собирает, анализирует и коррелирует системные журналы);

– обнаружение руткитов;

– настраиваемые оповещения в режиме реального времени;

– интеграция с существующей инфраструктурой;

– возможен активный ответ на атаку;

– централизованный сервер для управления массовой политикой;

– агентный и безагентный мониторинг (может быть использован для мониторинга брандмауэров, маршрутизаторов и др.).

Для СОВ OSSEC возможны четыре типа установки.

1. Сервер. При данном типе установки агенты передают сообщения журнала на сервер для обработки. Правила и декодеры устанавливаются только на сервере. Оповещения генерируются и распространяются с сервера.

2. Агент. Агенты OSSEC подключают локальные файлы журнала и пересылают сообщения на сервер OSSEC. Локальные сообщения мониторинга целостности файлов также пересылаются на сервер.

3. Гибрид. Гибридная установка – это и сервер, и агент. Как сервер, он обрабатывает журналы для нескольких агентов, а как агент – отправляет предупреждения на другой сервер.

4. Автономная установка. Это означает, что машина, на которую установлен OSSEC, не связана с сервером или агентами. Декодеры и правила также будут храниться на данном компьютере.

Для рассматриваемого лабораторного стенда использованы первые два типа установки для сервера и клиента соответственно.

СОВ OSSEC располагает собственным стандартным веб-интерфейсом, он достаточно скромен, но позволяет удобнее отслеживать события. На данный момент его разработка остановлена. Разработчики рекомендуют использовать для этих целей Kibana, Splunk или другие. В рамках же образовательного процесса данного веб-интерфейса вполне достаточно.

Правила OSSEC предоставляют собой мощный способ настройки оповещений. Каждый файл правил содержит несколько определений правил для различных приложений. В сочетании с правилами существуют декодеры, предназначенные для извлечения данных из необработанных событий, что позволяет OSSEC коррелировать разрозненные события, полученные из нескольких источников.

Используя правила OSSEC, мы можем настроить правила на основе имени пользователя, IP-адреса, имени хоста источника, URL-адреса, имени файла, времени суток, дня недели, совпавших правил, частоты и времени с момента последнего предупреждения.

В реальных системах также используется несколько способов работы с правилами:

– игнорирование правил (игнорирование определенных IP-адресов);

– повышение уровня значимости правила;

– изменение частоты появления некоторого правила до срабатывания связанного с ним правила;

– написание правил для пользовательских приложений;

– игнорирование событий изменения целостности определенных каталогов и др.

Для примера можно создать два правила, иллюстрирующих обработку событий неуспешной аутентификации (листинг 1). Правило 2501 захватывает событие, а правило 100100 будет срабатывать, если 5 раз выполнится правило 2501 в течение пяти минут для одного и того же пользователя.

Листинг 1 – Правила для обработки событий неуспешной аутентификации

```
<rule id="2501" level="8" overwrite="yes">
    <pcre2>FAILED LOGIN |authentication failure|</pcre2>
    <pcre2>Authentication failed for|invalid password
for|</pcre2>
    <pcre2>L0GIN FAILURE|auth failure: |authentication er-
ror|</pcre2>
    <pcre2>authinternal failed|Failed to authorize|</pcre2>
    <pcre2>Wrong password given for|login failed|Auth: Login
incorrect|</pcre2>
    <pcre2>Failed to authenticate user</pcre2>
    <decoded_as>fauth</decoded_as>
    <group>authentication_failed,</group>
    <description>User authentication failed.</description>
</rule>

<rule id="100100" level="10" frequency="5" timeframe="300">
    <if_matched_sid>2501</if_matched_sid>
    <same_user />
    <description>5 failed passwords within 5 minutes by same
user</description>
</rule>
```

OSSEC позволяет осуществлять активный ответ на события с помощью настройки секции <active-response> в конфигурационном файле. Используя

<active-response>, можно заблокировать пользователя, который вызвал срабатывание вышеописанного правила на 5 минут (листинг 2).

Листинг 2 – Конфигурация активного ответа

```
<active-response>
    <disabled>no</disabled>
    <command>disable-account</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>300</timeout>
</active-response>
```

Когда будет выполняться активный ответ на правило 100100, пользователь, который его вызвал, даже при вводе правильного пароля не сможет войти до истечения срока блокировки.

ЗАКЛЮЧЕНИЕ

По результатам сравнительного анализа можно сделать вывод, что эффективное решение для обеспечения безопасности должно включать возможность активного ответа на атаку, быть масштабируемым, кроссплатформенным и сочетать в себе разные методы обнаружения атак.

Статистика говорит, что трафик пользователей увеличивается каждый год на 50 %. К такой нагрузке следует быть готовым заранее. В том числе к обработке большого сетевого потока должны быть готовы системы обнаружения / предотвращения вторжений.

На самом деле сейчас редко используются решения СОВ в чистом виде. Чаще всего их интегрируют с СПВ, межсетевыми экранами и антивирусами. Следующим этапом развития подобных систем стало появление межсетевых экранов нового поколения (NGFW, Next Generation Firewall), которые выигрывают за счет параллельного анализа одного и того же трафика всеми средствами защиты.

Вместе с развитием технологий безопасности развиваются и кибератаки. Их становится сложно прогнозировать и предотвращать. Однако появляется возможность эффективно бороться с сетевыми атаками и обеспечивать дополнительный уровень безопасности компьютерных систем с помощью правильного инструмента СОВ, поддерживающего бизнес и IT-инфраструктуры.

БЛАГОДАРНОСТИ

Выражаем искреннюю благодарность доктору технических наук, профессору Виктору Матвеевичу Белову за высказанные замечания и оказанную поддержку при подготовке данной статьи.

СПИСОК ЛИТЕРАТУРЫ

1. Check Point Blog: web-сайт. – URL: https://blog.checkpoint.com/ (accessed: 03.12.2021).

2. *Andress J.* Foundations of information security: a straightforward introduction. – San Francisco: No Starch Press, 2019. – 248 p.

3. *Шелухин О.И., Сакалема Д.Ж., Филинова А.С.* Обнаружение вторжений в компьютерные сети (сетевые аномалии). – М.: Горячая линия – Телеком, 2018. – 220 с.

4. *Акбарова Ш.А., Ганиев А.А.* Классификация IDS // Молодой ученый. – 2017. – № 15 (149). – С. 1–3. – URL: https://moluch.ru/archive/149/41931/ (дата обращения: 03.12.2021).

5. Информационное письмо об утверждении требований к системам обнаружения вторжений / Федеральная служба по техническому и экспортному контролю. – ФСТЭК России, 2012. – 3 с.

6. OSSEC HIDS: website. – URL: https://www.ossec.net/about/ (accessed: 03.12.2021).

7. Tripwire: website. – URL: https://github.com/Tripwire/tripwire-open-source (accessed: 03.12.2021).

8. Программный комплекс обнаружения вторжений «Ребус-СОВ»: web-сайт. – URL: https://rebus-sov.ru/ (дата обращения: 03.12.2021).

9. The Samhain file integrity/intrusion detection / Samhain Labs. – URL: https://la-samhna.de/samhain/s_documentation.html (дата обращения: 03.12.2021).

10. ViPNet IDS HS – Система обнаружения компьютерных атак: web-сайт. – URL: https://infotecs.ru/product/vipnet-ids-hs-versiya-1.html#docs (дата обращения: 03.12.2021).

11. Snort Overview: website. – URL: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node2.html (accessed: 03.12.2021).

12. Система обнаружения атак «Форпост» версии 3.0 / Комапания «РНТ» Российские наукоемкие технологии. – URL: https://www.rnt.ru/ru/production/detail.php?ID=689 (дата обращения: 03.12.2021).

13. OpenWIPS-ng: website. – URL: https://openwips-ng.org/index.html (accessed: 03.12.2021).

14. Zeek: website. – URL: https://docs.zeek.org/en/lts/intro/index.html (accessed: 03.12.2021).

15. С-Терра СОВ. Версия 4.2: web-сайт. – URL: https://doc.s-terra.ru/rh_output/4.2/IDS/output/index.htm#t=mergedProjects%2F1main%2FFirst_Topic.htm (дата обращения: 03.12.2021).

Кукушкина Надежда Викторовна, магистрант кафедры вычислительной техники Новосибирского государственного технического университета. Область научных интересов – информационная безопасность автоматизированных систем. E-mail: kukushkina.2020@stud.nstu.ru

Новохрёстов Алексей Константинович, кандидат технических наук, доцент кафедры комплексной информационной безопасности электронно-вычислительных систем Томского государственного университета систем управления и радиоэлектроники. Область научных интересов – безопасность вычислительных сетей. E-mail: nak@fb.tusur.ru

DOI: 10.17212/2782-2230-2021-4-37-53

Development of the laboratory bench for studying intrusion detection systems*

N.V. Kukushkina[1], A.K. Novokhrestov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, master's student of the Computer Science Department. E-mail: kukushkina.2020@stud.nstu.ru*

[2] *Tomsk State University of Control Systems and Radioelectronics, 40 Lenin Avenue, Tomsk, 634050, Russian Federation, candidate of technical sciences, Associate Professor of the Department of Integrated Information Security of Electronic Computing Systems. E-mail: nak@fb.tusur.ru*

The research object of this article is network-based and host-based intrusion detection systems. The aim of the study is to obtain an overview of intrusion detection systems, as well as to build a constructive version of a virtual laboratory bench intended for teaching students (studying the test characteristics of intrusion detection systems). The article provides a brief reference on intrusion detection systems, taking into account the classification by the method of monitoring and the technology of detecting attacks. Today, intrusion detection system is a necessary element of a comprehensive network protection system for both small and large organizations. They improve network security by protecting against external and internal intrud-

* *Received 10 November 2021.*

ers. Therefore, the need to acquire skills in installing, configuring and administering intrusion detection systems is an important part of training information security specialists, which necessitates continuous updating and modernization of training tools. In this paper, we propose a virtual laboratory bench designed to study intrusion detection systems. Its architecture and functioning parameters are described. In order to select an intrusion detection system for a virtual laboratory bench, a comparative analysis of free and commercial intrusion detection systems on the market was carried out. Network-based and host-based intrusion detection systems were considered separately. For both types, their advantages and disadvantages are described. As a result, the functions and operation mechanism are described for the intrusion detection system selected based on the analysis results. In addition, examples of custom rules for handling security events are discussed.

Keywords: intrusion detection system, intrusion prevention system, laboratory bench, comparative analysis, network-based intrusion detection systems, host-based intrusion detection systems, Open Source Security, event monitoring

REFERENCES

1. Check Point Blog: website. Available at: https://blog.checkpoint.com/ (accessed 03.12.2021).

2. Andress J. *Foundations of information security: a straightforward introduction*. San Francisco, No Starch Press, 2019. 248 p.

3. Shelukhin O.I., Sakalema D.Zh., Filinova A.S. *Obnaruzhenie vtorzhenii v komp'yuternye seti (setevye anomalii)* [Detection of intrusions into computer networks (network anomalies)]. Moscow, Goryachaya liniya – Telekom Publ., 2018. 220 p.

4. Akbarova Sh.A., Ganiev A.A. Klassifikatsiya IDS [IDS classification]. *Molodoi uchenyi = Young Scientist*, 2017, no. 15 (149), pp. 1–3. (In Russian). Available at: https://moluch.ru/archive/149/41931/ (accessed 03.12.2021).

5. *Informatsionnoe pis'mo ob utverzhdenii trebovanii k sistemam obnaruzheniya vtorzhenii* [Intrusion detection system requirements statement letter]. Federal Service for Technical and Export Control, 2012. 3 p.

6. *OSSEC HIDS*: website. Available at: https://www.ossec.net/about/ (accessed 03.12.2021).

7. *Tripwire*: website. Available at: https://github.com/Tripwire/tripwire-open-source (accessed 03.12.2021).

8. *Programmnyi kompleks obnaruzheniya vtorzhenii "Rebus-SOV"* [Intrusion detection software "Rebus-SOV"]. Available at: https://rebus-sov.ru/ (accessed 03.12.2021).

9. *The Samhain file integrity/intrusion detection*. Samhain Labs. Available at: https://la-samhna.de/samhain/s_documentation.html (accessed 03.12.2021).

10. *ViPNet IDS HS*: website. (In Russian). Available at: https://infotecs.ru/product/vipnet-ids-hs-versiya-1.html#docs (accessed 03.12.2021).

11. *Snort Overview*: website. Available at: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node2.html (accessed 03.12.2021).

12. *"Forpost" version 3.0*. RNT Company. (In Russian). Available at: https://www.rnt.ru/ru/production/detail.php?ID=689 (accessed 03.12.2021).

13. *OpenWIPS-NG*: website. Available at: https://openwips-ng.org/index.html (accessed 03.12.2021).

14. *Zeek*: website. Available at: https://docs.zeek.org/en/lts/intro/index.html (accessed 03.12.2021).

15. *S-Terra SOV. Versiya 4*.2: website. (In Russian). Available at: https://doc.s-terra.ru/rh_output/4.2/IDS/output/index.htm#t=mergedProjects%2F1main%2FFirst_Topic.htm (accessed 03.12.2021).

Для цитирования:

Кукушкина Н.В., Новохрёстов А.К. Разработка лабораторного стенда для изучения систем обнаружения вторжений // Безопасность цифровых технологий. – 2021. – № 4 (103). – С. 37–53. – DOI: 10.17212/2782-2230-2021-4-37-53.

For citation:

Kukushkina N.V., Novokhrestov A.K. Razrabotka laboratornogo stenda dlya izucheniya sistem obnaruzheniya vtorzhenii [Development of the laboratory bench for studying intrusion detection systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 4 (103), pp. 37–53. DOI: 10.17212/2782-2230-2021-4-37-53.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 4 (103). – 54–71

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 621.382.232 DOI: 10.17212/2782-2230-2021-4-54-71

ОСОБЕННОСТИ ОБНАРУЖЕНИЯ И ИЗМЕРЕНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ШИРОКОПОЛОСНЫХ СИГНАЛОВ*

А.В. ИВАНОВ[1], С.Р. КОПЫЛОВА[2], С.А. РОЖКОВ[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент, заведующий кафедрой защиты информации. E-mail: andrej.ivanov@corp.nstu.ru*
[2] *630108, РФ, г. Новосибирск, ул. Плахотного, 10, Сибирский государственный университет геосистем и технологий, магистрант. E-mail: sve.copilova2011@yandex.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: rozhkov.2015@stud.nstu.ru*

Статья посвящена изучению технического канала утечки информации за счет побочных электромагнитных излучений. Кратко приведены методы обнаружения и измерения побочных электромагнитных излучений, а также широкополосных сигналов в общих случаях. Рассмотрены особенности обнаружения и измерения побочных электромагнитных излучений широкополосных сигналов (ПЭМИ ШПС) современных цифровых интерфейсов (например, DVI, HDMI, DisplayPort). Данные цифровые интерфейсы выбраны как наиболее актуальные в настоящее время против выходящих из массового пользования аналоговых (VGA). Проведён обзор основных подходов к выявлению подобных сигналов. Обнаружение и измерение сигналов ПЭМИ ШПС является нетривиальной задачей, поскольку сами по себе и сигналы ПЭМИ, и широкополосные сигналы имеют низкое отношение сигнал / шум. Подробно описан лабораторный стенд (альтернативная измерительная площадка), на котором проведены практические исследования по выявлению и измерению ПЭМИ ШПС на примере интерфейса HDMI. Продемонстрировано влияние экран-камеры на результаты исследований в случаях полного и частичного экранирования исследуемого объекта. Показано влияние величины полосы пропускания при измерениях ПЭМИ ШПС на отображаемый спектр такого сигнала. После достижения определенного значения данной величины отображаемый спектр становится четко различимым на фоне шумов. Произведено измерение уровней сигналов ПЭМИ ШПС двумя способами. Первый способ основывался на предположении о том, что спектр сигнала ПЭМИ ШПС сплошной. Во втором способе предполагалось, что спектр такого сигнала дис-

* Статья получена 02 ноября 2021 г.

кретный. По результатам этих измерений сделан вывод о фактическом характере спектра сигналов ПЭМИ ШПС.

Ключевые слова: информационная безопасность, широкополосные сигналы, побочные электромагнитные излучения, технические средства, безэховая камера, шумоподобный сигнал, техническая защита информации, измерение сигнала

ВВЕДЕНИЕ

Широкополосными (шумоподобными) сигналами (ШПС) называют такие сигналы, у которых произведение активной ширины спектра F на длительность T много больше единицы. Это произведение называется базой сигнала B. Для ШПС $B = FT >> 1$ [1, с. 5]. Другими словами, энергия любого широкополосного сигнала распределена в прямоугольнике на плоскости время–частота, площадь которого значительно больше единицы [2, с. 15].

Побочные электромагнитные излучения (ПЭМИ) – это электромагнитные поля, создаваемые в окружающем пространстве любыми техническими средствами во время их работы [3, с. 6]. Возникновение электромагнитных полей обусловлено протеканием тока в техническом устройстве.

ПЭМИ ШПС – это одна из современных угроз утечки информации по техническим каналам. Связана она с тем, что в современных технических средствах при обработке данных используются цифровые интерфейсы (например, DVI, HDMI, DisplayPort), а не аналоговые (VGA). Помимо этого, происходит возникновение паразитных излучений, т. е. как раз возникновение побочных электромагнитных излучений. Такое возникновение цифровых сигналов и паразитных излучений формирует возникновение ПЭМИ ШПС.

ШПС является слабым, так как уровень сигнала относительно шумов невысокий, или, другими словами, отношение сигнал / шум мало. Сигнал ПЭМИ, в свою очередь, тоже слабый из-за того, что является побочным, т. е. специально не созданным.

Исходя из вышесказанного сигналы ПЭМИ и ШПС имеют небольшой уровень относительно уровня шумов. В связи с этим возникает ряд проблем с обнаружением и измерением ПЭМИ ШПС. Рассмотрим данные особенности на примере сигналов видеоинтерфейсов, которые являются наиболее существенными в плане излучения по сравнению с остальными интерфейсами типовой автоматизированной системы.

1. ТЕХНОЛОГИЯ РАБОТЫ С СИГНАЛАМИ ПЭМИ

1.1. МЕТОДЫ И СПОСОБЫ ОБНАРУЖЕНИЯ И ИЗМЕРЕНИЯ ПЭМИ

1. Использование тестов

Основным методом обнаружения ПЭМИ является применение тестов.

Для реализации данного метода осуществляют сканирование всего исследуемого диапазона частот дважды. Сначала с выключенным тестовым сигналом в исследуемом техническом средстве (ТС), а затем уже с включенным сигналом [4].

При первом (с выключенным тестовым сигналом на ТС) сканировании исследуемого диапазона частот происходит фиксация и оцифровка мгновенных значений напряжений шумов за период контроля, затем полученные значения записываются в память прибора. При втором (тест включен) сканировании того же диапазона фиксируются и оцифровываются уже мгновенные значения уровней напряжения сигналов, превышающих ранее измеренные значения уровней шумов. После этого полученные значения записываются в память измерительного прибора. В дальнейшем на основе всех значений строят амплитудный спектр частот.

2. Обнаружение с помощью RTL SDR-приемника

В этом способе используется доступное оборудование – ТВ-тюнер на основе чипа RTL2832U, реализующий функции захвата и оцифровки радиосигналов. В статье И.Ю. Петрова «Обнаружение ПЭМИ с помощью RTL-SDR-приемника» описана работа такого приемника для обнаружения ПЭМИ [5].

Работа приемника происходит по следующему алгоритму:

1) антенну подключают к тюнеру;

2) после того как антенна приняла сигнала из эфира, дают указание чипу R820T выделить участок радиодиапазона и усилить его;

3) другому чипу передают этот же выделенный участок, который он оцифровывает и передает по USB на компьютер;

4) на компьютере установленная программа (GnuRadio, SDR# или др.) «настраивается» на выбранную частоту, выполняет демодуляцию указанным способом и отправляет получившийся звук на звуковую карту [5].

Использование ТВ-тюнера является уже устаревшим способом обнаружения ПЭМИ с помощью SDR. На сегодняшний день самая современная технология в семействе программно-определяемых радиоприемников – это DDC SDR (Digital Down Conversion, цифровое преобразование «вниз»). Ее особенность состоит в том, что сверхбыстрый аналогово-цифровой преобразователь с частотой преобразования порядка 100 млн выборок в секунду оцифровывает принимаемый радиосигнал, тем самым исключая необходимость гетеродина. Такой приемник не имеет зеркальных каналов [6].

3. Метод сравнения значений спектральных плотностей мощности в двух пространственно-размещенных точках

Данный метод основывается на измерении двух точек, которые располагаются в разных местах [7]. Первая расположена вблизи места располагаемого источника радиосигнала (вблизи ТС) на территории предприятия. Вторая точка является опорной и располагается удаленно от места первой. Решение об обнаружении канала утечки информации принимается, если значение спектральных плотностей мощности в первой точке больше, чем в опорной точке на заданную величину.

4. Корреляционный метод

Метод строится на использовании сертифицированной тестовой программы на компьютере, который подключается к исследуемому техническому средству. Такая тестовая программа реализована на применении «звуковой подкраски».

Алгоритм использования метода следующий:

1) после подключения компьютера к ТС и запуска программы происходит прием излучений;

2) в ручном режиме на основе полученных сигналов измерительный приемник настраивается на гармонику сигнала со «звуковой подкраской»;

3) найденный сигнал демодулируется, и определяется максимальная частота *f_max* на основе вычисленной демодулированной величины спектра;

4) в конце происходит формирование эталонного сигнала с частотой, равной максимальной частоте *f_max* сигнала.

В автоматическом режиме сканируется исследуемый диапазон. На текущей частоте сканирования определяют коэффициент корреляции принимаемого и эталонного сигналов и сравнивают их с пороговым значением, которое предварительно было рассчитано.

Результатом сравнения принятого и эталонного сигналов является принятие решения о наличии излучений в исследуемом техническом средстве [8].

1.2. МЕТОДЫ И СПОСОБЫ ОБНАРУЖЕНИЯ И ИЗМЕРЕНИЯ ШПС

Для обнаружения и измерения ШПС существует несколько способов, описанных в статьях Климова И.З., Чувашова А.М, Копысова А.Н, Богданова А.А. [9] и Денниса Хендлона [10].

В статье [9] один из способов основан на использовании корреляторов. Путем вычисления величины корреляционной функции в текущий момент времени определяется положение максимума, что соответствует решению задачи начальной синхронизации. Способ последовательного обнаружения

состоит в следующем. На каждом шаге сумма широкополосного сигнала и помех умножается на копию принимаемого сигнала. Сигнал, полученный в результате умножения на копию, накапливается в интеграторе. Накопленный сигнал сравнивается с порогом. Если сигнал превысил порог, то принимается решение о наличии сигнала. Если сигнал не обнаружен, то временное положение копии сигнала относительно входного сигнала изменяется на фиксированную величину, соответствующую длительности шага поиска, и процедура повторяется сначала. Если сигнал обнаружен – процедура обнаружения завершается [9].

В статье Денниса Хендлона [10] описан один из способов измерения ШПС. Вместо измерений частотной области Хендлон предлагает оцифровывать сигнал во временной области и затем уже обрабатывать оцифрованные данные. Также он предлагает разные методы измерения сигналов, а именно использование различного оборудования в зависимости от частот измерения. Для сигналов с полосой менее 80 МГц и центральной частотой менее 50 ГГц Хендлон предлагает использовать анализатор спектра. Для анализа сигналов с полосой менее 300 МГц – анализатор спектра в качестве понижающего преобразователя частоты, осциллограф – в качестве дискретизатора, а для анализа сигналов с полосой более 300 МГц можно использовать высокоскоростной осциллограф или комбинацию осциллографа с внешним преобразователем частоты [10].

1.3. ОСОБЕННОСТИ РАБОТЫ С ПЭМИ ШПС

Как уже было сказано выше, ПЭМИ ШПС – достаточно слабый сигнал, так как создавался с целью использования его для скрытия передачи информации за счет распределения энергии сигнала на большой период времени [11].

Из-за этих особенностей обнаружить и измерить ПЭМИ ШПС является достаточно трудным занятием.

Для выполнения этой задачи первое, что можно сделать, – это использовать такое оборудование, у которого отношение сигнал / шум меньше единицы. Такой способ позволит обнаружить сигнал в реальном времени без использования каких-либо тестовых программ на исследуемом техническом средстве. Минусом способа является высокая цена приемников.

Другой способ обнаружения ПЭМИ предполагает уменьшение уровня шумов. Данный способ поможет принять меньший по уровню сигнал. Так как теоретический предел приемника больше либо равен единице $U_{\text{с}} / U_{\text{ш}} \geq 1$, то домножив обе стороны на $U_{\text{ш}}$, получим неравенство $U_{\text{с}} \geq U_{\text{ш}}$, из которого

видно, что чем меньше уровень шума, тем меньший уровень сигнала мы можем принять [12, 13].

Здесь существует два различных варианта с понижением уровня шума:

1) уменьшение внешних шумов;

2) уменьшение собственных шумов приемного-тракта.

Для реализации первого пункта можно оборудовать специальную безэховую экранированную камеру, которая позволит исключить (или свести к минимуму) влияние другого оборудования в процессе измерения технического средства.

Второй способ имеет свои преимущества и недостатки. При сужении полосы пропускания приемника уменьшаются собственные шумы прибора. Минусом является то, что спектр сигнала не «перекрывается» полосой приемника, а значит, восстановить форму сигнала в реальном времени невозможно и измерение уровня сигнала будет некорректным.

Для правильного измерения сигнала в таком случае необходимо, чтобы он оставался стационарным во времени. Для этого используем тесты, которые обладают следующими свойствами: периодичные импульсные сигналы, которые позволят измерить сигнал по частям благодаря стационарности за всё время измерения. Далее остается лишь выбрать способ измерения, приняв спектр сигнала за сплошной или дискретный [14, 15].

2. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

2.1. ИССЛЕДОВАНИЕ ПЭМИ ШПС

Проверим теоретически описанные методы и способы обнаружения и измерения ПЭМИ ШПС на практике.

В проводимом исследовании использовалось следующее оборудование:

1) анализатор спектра СК4М-18;

2) программа управления СК4М-18 Graphit 2.6.1;

3) антенна измерительная дипольная активная АИ 5-0;

4) поворотный стол;

5) безэховая экранированная камера;

6) ноутбук;

7) исследуемый компьютер (интерфейс HDMI).

Проведем измерения с помощью представленного выше оборудования и сравним результаты измерений в разных случаях. В первом случае дверь в экран-камеру будет открыта, во втором случае будет полная экранировка.

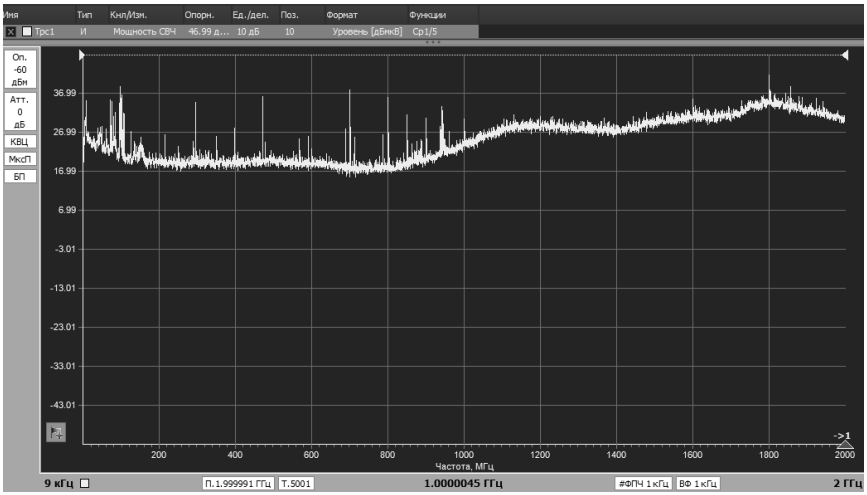


Рис. 1. Частотный спектр без использования экран-камеры

Fig. 1. Frequency spectrum without using a shielded camera

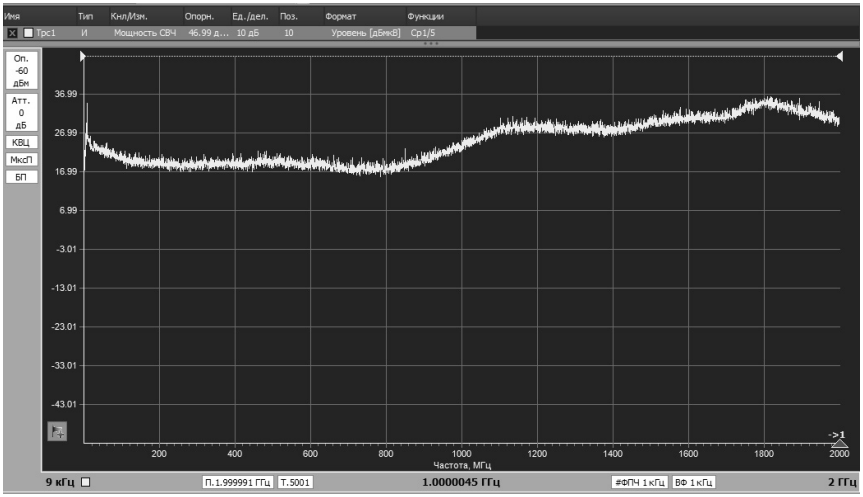


Рис. 2. Частотный спектр с применением экран-камеры

Fig. 2. Frequency spectrum with a shielded camera

На рис. 1 и 2 по оси *X* откладываются значения частот, выраженных в мегагерцах, а по оси *Y* отображается уровень сигнала (шума), выраженный в децибелах относительно 1 мкВ.

Если сравнить спектр, изображенный на этих рисунках, то видно, что спектр имеет одинаковые форму и уровень. До 1 ГГц уровень шума находится в пределах 16,99…26,99 дБмкВ, после 1 ГГц уровень становится на 10 дБмкВ больше. Но, несмотря на схожий уровень сигнала, на рис. 1 присутствуют побочные излучения, которые «проникают» сквозь открытую дверь, а впоследствии могут влиять на дальнейший ход обнаружения и измерения ПЭМИ ШПС, в то время как с закрытой дверью в экран-камере на графике спектра остаются лишь собственные шумы приемного тракта (рис. 2).

Далее в этой же экран-камере проведем измерение, но уже будем изменять полосу пропускания прибора. Чтобы добиться более четкой картины спектра, необходимо уменьшить уровень собственных шумов приемного тракта. Для этого будем постепенно сужать полосу пропускания прибора, каждый раз уменьшая ее в 10 раз, пока не добьемся явного изображения спектра сигнала. Возьмем картину спектра с двумя значениями полосы пропускания, равными 100 и 10 кГц (рис. 3 и 4 соответственно), а затем сравним их.

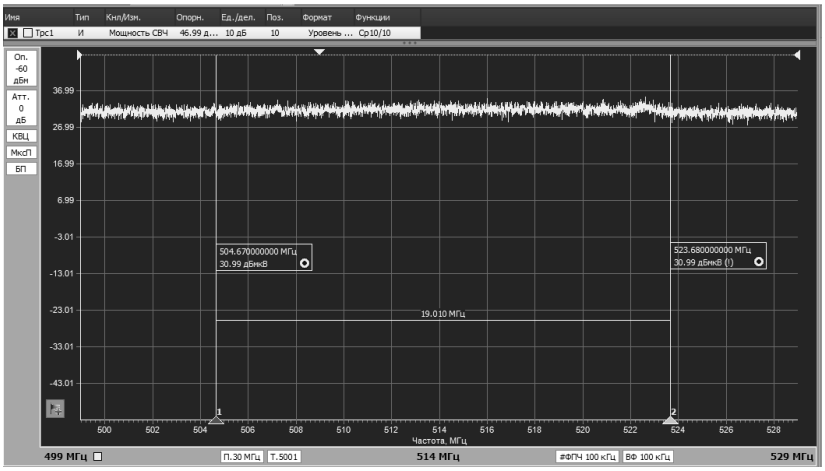


Рис. 3. Полоса пропускания приемника 100 кГц

Fig. 3. Receiver bandwidth is 100 kHz

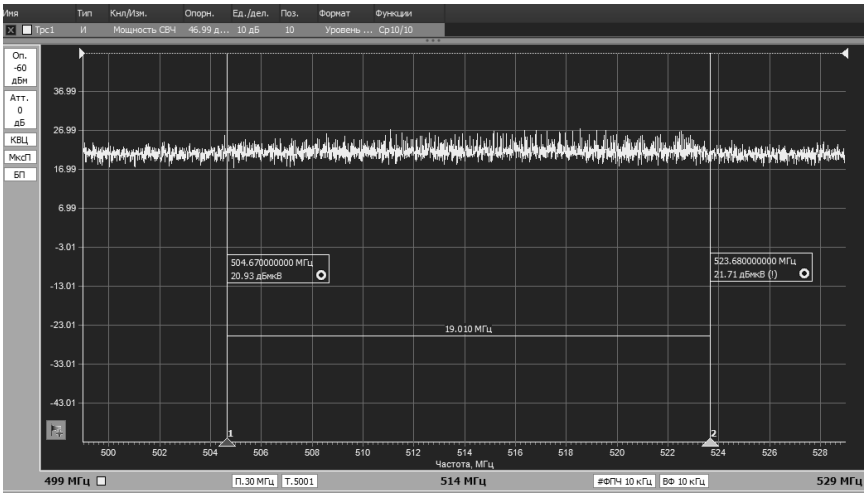


Рис. 4. Полоса пропускания приемника 10 кГц

Fig. 4. Receiver bandwidth is 10 kHz

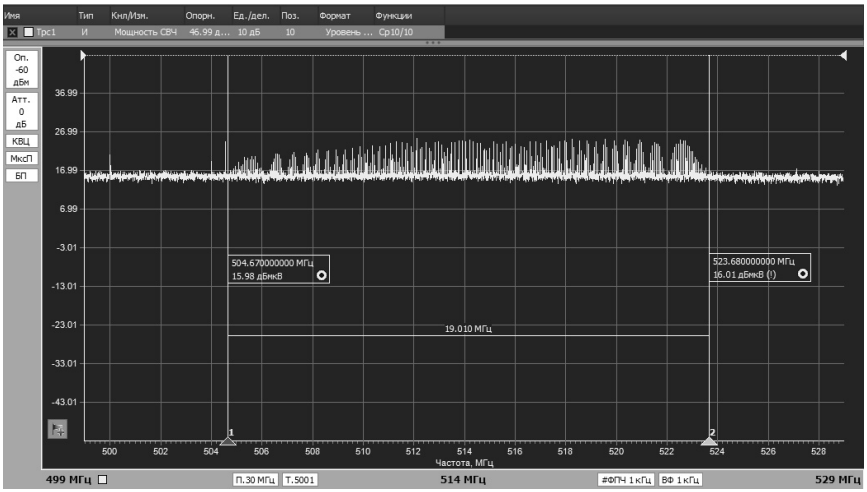


Рис. 5. Полоса пропускания приемника 1 кГц

Fig. 5. Receiver bandwidth is 1 kHz

В отличие от рис. 3, где сигнал еле различается на уровне шумов, на рис. 4 уже видна разница между сигналом и шумом. Общий уровень шума снизился на 10 дБмкВ. Но всё равно этого недостаточно, чтобы точно сказать об обнаружении ПЭМИ ШПС. Уменьшим полосу пропускания приемника с 10 до 1 кГц (рис. 5) и сравним полученные спектры сигнала.

Сигнал, как видно из рисунка, состоит из линейчатых спектральных составляющих, а не имеет сплошной спектр. С полосой пропускания 1 кГц можно сказать, что ПЭМИ ШПС обнаружен.

2.2. ИЗМЕРЕНИЕ ПЭМИ ШПС

Измерение побочных электромагнитных излучений широкополосных сигналов проводилось с использованием одного из методов обнаружения ПЭМИ – с использованием тестов. Тест сделал сигнал стационарным во времени, после чего его обнаружили, а затем измерили. Если посмотреть на рис. 6, то можно увидеть, что спектр сигнала имеет сплошную характеристику.

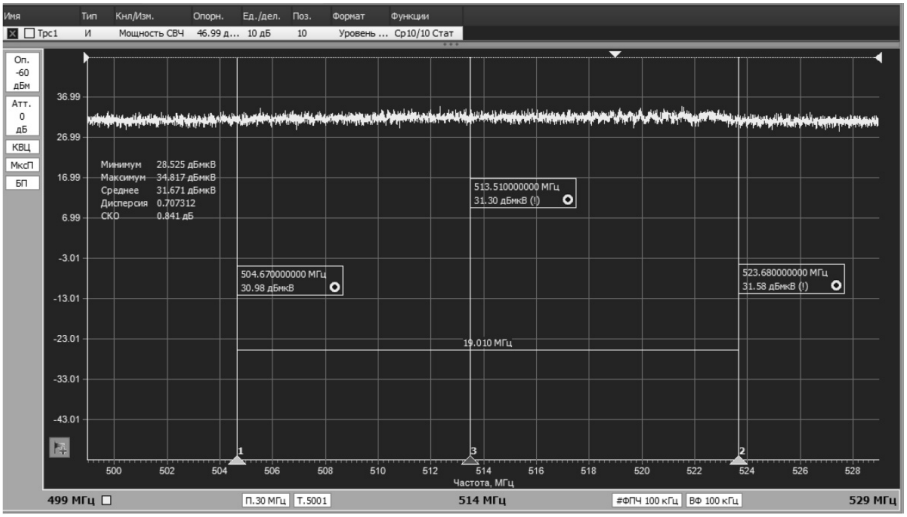


Рис. 6. Сплошной спектр

Fig. 6. Continuous spectrum

Для этого случая, когда огибающая функции спектральной плотности «плоская» $E_i \approx E_i + 1 \ldots \approx E_n$, рассчитываем значение напряженности по следующей формуле:

$$E_u = E_i \sqrt{\Delta f \Delta F}, \tag{1}$$

где E_u − интегральное значение напряженности в полосе Δf; E_i − измеренное значение напряженности поля с полосой приемника ΔF; Δf − ширина спектра; ΔF − полоса пропускания приемника.

Рассчитаем интегральное значение напряженности для данного случая.

1. Переведем измеренные значения E_1 из децибел в микровольты, используя следующую формулу:

$$E_i(\text{мкВ}) = 10^{\frac{E_i(\text{дБ})}{20}}. \tag{2}$$

Таким образом, $E_1 = 10^{\frac{31,3}{20}} = 36,73$ (мкВ).

2. Рассчитаем интегральное значение напряженности E_{u1}:

$$E_{u1} = 36,73 \sqrt{\frac{19\,010\,000}{100\,000}} = 506,4 \text{ (мкВ)}.$$

3. Переведем полученное значение обратно в децибелы по формуле (3):

$$E_{u1}(\text{дБ}) = 20 \log_{10} E_{u1}(\text{мкВ}). \tag{3}$$

Таким образом, $E_{u1} = 20 \log_{10} 506,4 = 54,09$ (дБ).

После расчета рассмотрим другой рисунок, с более узкой полосой пропускания. На рис. 7 видно, что спектр является дискретным, явно видны спектральные составляющие сигнала, которые подлежат измерению.

Для случая, когда спектр имеет дискретную форму, расчет интегрального значения напряженности происходит по следующей формуле (4):

$$E_u = \sqrt{\sum_{i=1}^{n} E_i^2}, \tag{4}$$

где $n = \Delta f / \Delta F$ − число измерений E_i.

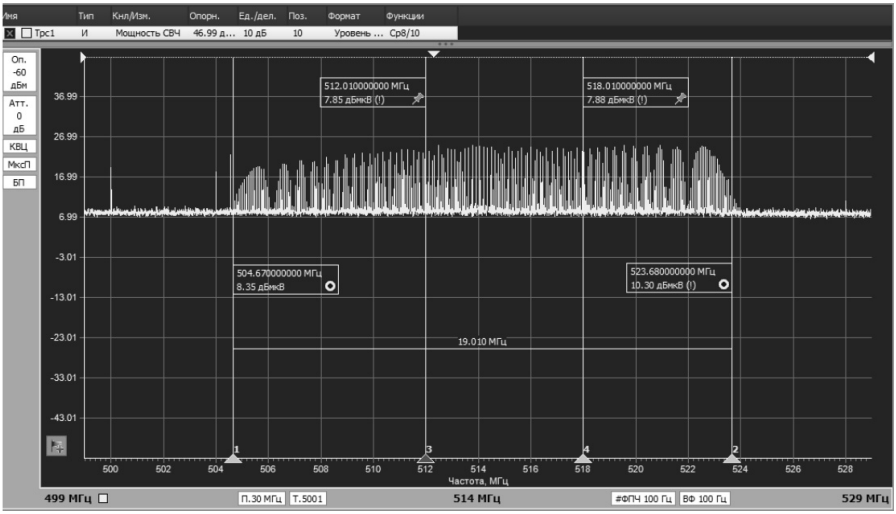


Рис. 7. Разбитие сигнала на участки (дискретный спектр)

Fig. 7. Splitting the signal into sections (discrete spectrum)

Для начала измерения для удобства разобьем исследуемый участок на 3 части (рис. 7). После разбиения запишем каждую частоту и соответственное ей полученное значение, которое превышает уровень шума. Далее проведем расчет: аналогично первому расчету сплошного спектра переведем значения из децибел в микровольты, используя формулу (2). Затем рассчитаем E_{u2} и переведем обратно в децибелы с помощью формул (4) и (3) соответственно:

$$E_{u2} = \sqrt{33090,28} = 181,91 \text{ (мкВ)}.$$

$$E_{u2} = 20\log_{10} 181,91 = 45,2 \text{ (дБ)}.$$

Сравнив интегральные значения напряженности в двух случаях, когда спектр сигнала имеет сплошную характеристику и когда он является дискретным, делаем вывод об ошибочности принятия спектра сигнала за сплошной.

Из полученного результата следует, что в данном примере уровень сигнала ошибочно завышен в 3 раза.

ЗАКЛЮЧЕНИЕ

Настоящая работа продемонстрировала, что, используя одни и те же настройки анализатора спектра, но либо изменяя полосу пропускания приемника, либо усредняя шумы, можно добиться уверенного обнаружения и измерения ПЭМИ ШПС. Усреднением шумов было достигнуто снижение общего уровня шумов на 10 дБмкВ и выделение на этом фоне исследуемого сигнала. В свою очередь, каждый раз сужая полосу пропускания приемного тракта в 10 раз, можно добиться четкой картины спектра сигнала. Шум при сужении полосы пропускания приемника также уменьшился в 3 раза. При полосе пропускания 100 кГц шум был равен 30 дБмкВ, а при полосе 1 кГц стал равен 15 дБмкВ. После обнаружения сигнала было произведено его измерение двумя способами. В первом способе характеристика спектра сигнала была сплошной (огибающая функции «плоская»), во втором – дискретной. На основе расчетов можно сделать вывод о существовании большой разницы в результатах при принятии решения о том, что огибающая спектральной функции имеет «плоскую» форму. Следовательно, при измерении ПЭМИ ШПС необходимо проводить измерение каждой спектральной составляющей отдельно, чтобы добиться корректного результата. Такая работа достаточно длительная и трудоемкая, поэтому требует автоматизации процесса.

СПИСОК ЛИТЕРАТУРЫ

1. *Барабашов Б.Г, Анишин М.М.* Широкополосные системы связи и сигналы: учебно-методическое пособие для студентов физического факультета по направлению Телекоммуникации. – Ростов н/Д.: ЮФУ, 2008. – 38 с. – URL: http://window.edu.ru/resource/749/70749/files/rsu803.pdf (дата обращения: 06.12.2021).

2. *Ипатов В.П.* Широкополосные сигналы. – Wiley, 2004. – 373 с.

3. *Иванов А.В.* Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок: учебное пособие. – Новосибирск: Изд-во НГТУ, 2018. – 64 с.

4. Патент 2617453 Российская Федерация, МПК G01R 29/08. Способ оценки параметров побочного электромагнитного излучения от элементов средств вычислительной техники / А.Б. Таранов, Е.И. Ларкин, Ю.Б. Иванов;

заявитель и патентообладатель Академия Федеральной службы охраны Российской Федерации (Академия ФСО России). – № 2015154172; заявл. 16.12.2015; опубл. 25.04.2017, Бюл. № 12. – 17 с. – URL: https://yandex.ru/patents/doc/RU2617453C1_20170425 (дата обращения: 06.12.2021).

5. *Петров И.Ю.* Обнаружение ПЭМИ с помощью RTL-SDR-приемника // Безопасность информационного пространства – 2017: XVI Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых. – Екатеринбург, 2018. – С. 119–122. – URL: https://elar.urfu.ru/bitstream/10995/65603/1/978-5-7996-2404-0_2018-39.pdf (дата обращения: 06.12.2021).

6. Исследование сигналов побочных электромагнитных излучений с применением SDR-приемников / Л.В. Меркулов, Д.К. Клоков, А.В. Иванов, И.Л. Рева // Наука. Технологии. Инновации. – Новосибирск, 2019. – Ч. 1. – С. 57–61.

7. *Былинкин А.А.* Многоканальное обнаружение радиосигнала с неизвестной структурой на фоне шумов // Вопросы защиты информации. – 2015. – № 2. – С. 42–47. – URL: https://www.elibrary.ru/item.asp?id=23583529 (дата обращения: 06.12.2021).

8. Патент 2340912 Российская Федерация, МПК G01R 29/08, H04B 17/00. Корреляционный способ распознавания побочного электромагнитного излучения и наводок средства вычислительной техники / В.В. Ёлкин; заявитель и патентообладатель ООО «Лаборатория Информационных Систем». – № 2006132681/09; заявл. 13.09.2006; опубл. 10.12.2008, Бюл. № 34. – 9 с.

9. Патент 2470459 Российская Федерация, МПК H04B 1/10, H04L 7/00, H03K 7/08. Способ обнаружения широкополосных сигналов и устройство для его реализации / И.З. Климов, А.М. Чувашов, А.Н. Копысов, А.А. Богданов; заявитель и патентообладатель Ижевский государственный технический университет имени М.Т. Калашникова. – № 2011120857/08; заявл. 24.05.2011; опубл. 20.12.2012, Бюл. № 35. – 10 с. – URL: https://elibrary.ru/item.asp?id=37504050 (дата обращения: 06.12.2021).

10. *Хендлон Д.* Эволюция измерений и анализа широкополосных сигналов // Компоненты и технологии. – 2009. – № 2. – С. 129–132. – URL: https://elibrary.ru/item.asp?id=15136069 (дата обращения: 06.12.2021).

11. *Кондратьев А.В.* Техническая защита информации. Практика работ по оценке основных каналов утечки. – М.: Горячая линия – Телеком, 2016. – 304 с.

12. *Kuhn M.G., Anderson R.J.* Soft tempest: hidden data transmission using electromagnetic emanations // Information Hiding: Second International Workshop, IH'98: proceedings. – Berlin; Heidelberg: Springer, 1998. – P. 124–142. – DOI: 10.1007/3-540-49380-8_10.

13. *Хорев А.А.* Технические каналы утечки информации, обрабатываемой средствами вычислительной техники // Специальная техника. – 2010. – № 2. – С. 39–57.

14. *Авдеев В.Б., Катруша А.Н.* Методика определения максимальной дальности перехвата побочного электромагнитного излучения при наклонных трассах его распространения // Специальная техника. – 2014. – № 5. – С. 8–16.

15. *Авдеев В.Б., Анищенко А.В.* Сравнительная оценка методических подходов к расчету отношения сигнал / шум в задачах контроля защищенности информации от утечки за счет побочных электромагнитных излучений // Специальная техника. – 2016. – № 1. – С. 54–63.

Иванов Андрей Валерьевич, заведующий кафедрой защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность, техническая защита информации. E-mail: andrej.ivanov@corp.nstu.ru

Копылова Светлана Романовна, магистрант Сибирского государственного университета геосистем и технологий. Основное направление научных исследований – техническая защита информации. E-mail: sve.copilova2011@yandex.ru

Рожков Семён Андреевич, ассистент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – техническая защита информации, акустические и виброакустические каналы утечки информации. E-mail: rozhkov.2015@stud.nstu.ru

DOI: 10.17212/2782-2230-2021-4-54-71

Features of detection and measurement of broadband TEMPEST signals*

A.V. Ivanov[1], S.R. Kopylova[2], S.A. Rozhkov[3]

1 *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, associate professor, head of the Information Security Department. E-mail: andrej.ivanov@corp.nstu.ru*
[2] *Siberian State University of Geosystems and Technologies Novosibirsk, 630108, Russian Federation, 10 Plahotnogo Street, master's student. E-mail: sve.copilova2011@yandex.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, assistant of the Information Security Department. E-mail: rozhkov.2015@stud.nstu.ru*

The article is devoted to the technical channels of Transient Electromagnetic Pulse Emanation (TEMPEST) information leakage. Methods of detection and measurement of TEMPEST, as well as broadband signals in general cases are briefly presented. The features of detection and measurement of broadband TEMPEST signals of modern digital interfaces (for example, DVI, HDMI, DisplayPort) are considered. These digital interfaces are selected as the most relevant at the moment, against analog ones that are coming out of mass use (VGA). The review of the main approaches to the identification of such signals is carried out. Detection and measurement of broadband TEMPEST signals is a non-trivial task, since both TEMPEST signals and broadband signals themselves have a low signal-to-noise ratio. A laboratory stand (an alternative measuring platform) is described in detail, where practical studies were carried out to identify and measure the broadband TEMPEST using the example of the HDMI interface. The influence of the shield camera on the results of research in cases of complete and partial screening of the object under study is demonstrated. The influence of the bandwidth value during measurements of the broadband TEMPEST on the displayed spectrum of such a signal is shown. After reaching a certain value of this bandwidth, the displayed spectrum becomes clearly distinguishable against the background of noise. The measurement of the signal levels of the broadband TEMPEST was carried out in two ways. The first method assumed that the spectrum of the broadband TEMPEST signal is continuous. In the second method, it was assumed that the spectrum of such a signal is discrete. Based on the results of these measurements, a conclusion was made about the actual nature of the spectrum of the signals of the broadband TEMPEST.

Keywords: information security, broadband signals, hardware, signal measurement, anechoic chamber, noise-like signal, technical security of information, TEMPEST

REFERENCES

1. Barabashov B.G, Anishin M.M. *Shirokopolosnye sistemy svyazi i signaly* [Broadband communication systems and signals]. Rostov-on-Don, Southern Federal University Publ., 2008. 38 p. Available at: http://window.edu.ru/resource/749/70749/files/rsu803.pdf (accessed 06.12.2021).

* *Received 2 November 2021.*

2. Ipatov V.P. *Shirokopolosnye signaly* [Spread spectrum and CDMA. Principles and applications]. Wiley, 2004. 373 p.

3. Ivanov A.V. *Otsenka zashchishchennosti informatsii ot utechki po kanalam pobochnykh elektromagnitnykh izluchenii i navodok* [Assessment of the security of information from leakage through the channels of side electromagnetic radiation and leads]. Novosibirsk, NSTU Publ., 2018. 64 p.

4. Taranov A.B., Larkin E.I., Ivanov Yu.B. *Sposob otsenki parametrov pobochnogo elektromagnitnogo izlucheniya ot elementov sredstv vychislitel'noi tekhniki* [Method of evaluating parameters of stray electromagnetic radiation from elements of computing equipment]. Patent RF, no. 2617453, 2017.

5. Petrov I.Yu. [Detection of compromising emanation using RTL-SDR receiver]. *Bezopasnost' informatsionnogo prostranstva – 2017: XVI Vserossiiskaya nauchno-prakticheskaya konferentsiya studentov, aspirantov, molodykh uchenykh* [Information Space Security 2017: All-Russian scientific and practical conference of students, postgraduates, young scientists]. Ekaterinburg, 2018, pp. 119–122. (In Russian). Available at: https://elar.urfu.ru/bitstream/10995/65603/1/978-5-7996-2404-0_2018-39.pdf (accessed 06.12.2021).

6. Merkulov L.V., Klokov D.K., Ivanov A.V., Reva I.L. Issledovanie signalov pobochnykh elektromagnitnykh izluchenii s primeneniem SDR priemnikov [Investigation of signals of side electromagnetic emanation using SDR receivers]. *Nauka. Tekhnologii. Innovatsii* [Science. Technologies. Innovations]. Novosibirsk, 2019, pt. 1, pp. 57–61.

7. Bylinkin A.A. Mnogokanal'noe obnaruzhenie radiosignala s neizvestnoi strukturoi na fone shumov [Multi-channel detection of radio signal with unknown structure against the noise background]. *Voprosy zashchity informatsii = Information Security Questions*, 2015, no. 2, pp. 42–47.

8. Elkin V.V. *Korre-lyatsionnyi sposob raspoznavaniya pobochnogo elektromagnitnogo izlucheniya i navodok sredstva vychislitel'noi tekhniki* []. Patent RF, no. 2340912, 2008.

9. Klimov I.Z., Chuvashov A.M., Kopysov A.N., Bogdanov A.A. *Sposob obnaruzheniya shirokopolosnykh signalov i ustroistvo dlya ego realizatsii* [Method of detecting broadband signals and device for realising said method]. Patent RF, no. 2470459, 2012.

10. Handlon D. Evolyutsiya izmerenii i analiza shirokopolosnykh signalov [The evolution of broadband signal measurement and analysis]. *Komponenty i tekhnologiii = Components and Technologies*, 2009, no. 2, pp. 129–132. (In Russian).

11. Kondrat'ev A.V. *Tekhnicheskaya zashchita informatsii. Praktika rabot po otsenke osnovnykh kanalov utechki* [Technical protection of information. The practice of work on the assessment of the main leakage channels]. Moscow, Goryachaya liniya – Telekom Publ., 2016. – 304 p.

12. Kuhn M.G., Anderson R.J. Soft tempest: hidden data transmission using electromagnetic emanations. *Information Hiding: Second International Workshop, IH'98*: proceedings. Berlin, Heidelberg, Springer, 1998, pp. 124–142. DOI: 10.1007/3-540-49380-8_10.

13. Khorev A.A. Tekhnicheskie kanaly utechki informatsii, obrabatyvaemoi sredstvami vychislitel'noi tekhniki [Technical channels of computer-processed information leakage]. *Spetsial'naya tekhnika = Special Equipment*, 2010, no. 2, pp. 39–57.

14. Avdeev V.B., Katrusha A.N. Metodika opredeleniya maksimal'noi dal'nosti perekhvata pobochnogo elektromagnitnogo izlucheniya pri naklonnykh trassakh ego rasprostraneniya [A technique for definition of the maximum stray electromagnetic pickup range at inclined propagation paths]. *Spetsial'naya tekhnika = Special Equipment*, 2014, no. 5, pp. 8–16.

15. Avdeev V.B., Anishchenko A.V. Sravnitel'naya otsenka metodicheskikh podkhodov k raschetu otnosheniya signal/shum v zadachakh kontrolya zashchishchennosti informatsii ot utechki za schet pobochnykh elektromagnitnykh izluchenii [Comparative assessment of methodological approaches to calculations of the signal-to-noise ratio in the tasks of monitoring of information protection against the leakage through stray electromagnetic radiation]. *Spetsial'naya tekhnika = Special Equipment*, 2016, no. 1, pp. 54–63.

Для цитирования:

Иванов А.В., Копылова С.Р., Рожков С.А. Особенности обнаружения и измерения побочных электромагнитных излучений широкополосных сигналов // Безопасность цифровых технологий. – 2021. – № 4 (103). – С. 54–71. – DOI: 10.17212/2782-2230-2021-4-54-71.

For citation:

Ivanov A.V., Kopylova S.R., Rozhkov S.A. Osobennosti obnaruzheniya i izmereniya po-bochnykh elektromagnitnykh izluchenii shirokopolosnykh signalov [Features of detection and measurement of broadband TEMPEST signals]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 4 (103), pp. 54–71. DOI: 10.17212/2782-2230-2021-4-54-71.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 4 (103). – 72–90

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.891.1.3 DOI: 10.17212/2782-2230-2021-4-72-90

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ SDR (SOFTWARE DEFINED RADIO) ДЛЯ ВОССТАНОВЛЕНИЯ СИГНАЛОВ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ВИДЕОТРАКТА*

А.В. ИВАНОВ[1], И.А. ОГНЕВ[2], Е.Е. НИКИТИНА[3], Л.В. МЕРКУЛОВ[4]

[1] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент, заведующий кафедрой защиты информации. E-mail: andrej.ivanov@corp.nstu.ru*
[2] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, аспирант кафедры защиты информации. E-mail: i.ognev.2016@corp.nstu.ru*
[3] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, аспирант кафедры защиты информации. E-mail: lizanikitinasj@gmail.com*
[4] *125993, г. Москва, Волоколамское шоссе, 4, Московский авиационный институт, магистрант кафедры технологии испытаний и эксплуатации. E-mail: Levmerkulov1@yandex.ru*

В настоящей статье представлены результаты восстановления сигналов побочных электромагнитных излучений видеотракта с применением SDR-приемника. Демонстрируется существование потенциального риска утечки конфиденциальной информации через технический канал утечки информации за счет побочных электромагнитных излучений видеотракта, минуя традиционные криптографические и физические методы защиты информации. Атака может быть реализована злоумышленником без специальных технических знаний и специального профессионального дорогостоящего оборудования. Представленный стенд позволяет упростить исследования, касающиеся побочных электромагнитных излучений, а также применять данную технологию для построения процесса обучения по этому направлению. В ходе работы приведено описание понятия технического канала утечки информации и краткое описание побочного электромагнитного излучения видеотракта. Далее кратко описаны технология SDR, выбранный приемник USRP B210 и кроссплатформенный программный пакет с открытым исходным кодом GNU Radio. Подробно описан демонстрационный стенд и приведены результаты восстановления изображения. Помимо этого, рассмотрены два этапа разработки демонстрационного стенда: с использованием имитационного сигнала и реального перехваченного сигнала. Демонстрационный стенд с имитационным сигналом способ-

* Статья получена 31 октября 2021 г.

ствует пониманию пользователем свойств побочных электромагнитных излучений, а также возможных препятствий на пути преобразования перехваченного сигнала в изображение. Исследования реального перехваченного сигнала проводились на мониторе с установленным разрешением 1280 × 1024 и частотой обновления экрана 60 Гц. Для подключения монитора был использован аналоговый интерфейс VGA (Video Graphics Array). Показана зависимость качества восстановленного изображения от установленной частоты дискретизации SDR-приемника.

Ключевые слова: информационная безопасность, побочные электромагнитные излучения, технические средства, автоматизированная система, программно-аппаратный комплекс, программно-определяемая радиосистема, Software Defined Radio, восстановление ПЭМИ видеотракта

ВВЕДЕНИЕ

В настоящее время проведение исследований, касающихся побочных электромагнитных излучений (ПЭМИ) технических средств, основывается на применении аппаратных комплексов, в основе которых лежат измерительные приемники или анализаторы спектра с набором измерительных антенн. Стоимость данного оборудования достаточно высока, что является препятствием как для исследователей в данной области, так и для построения учебного процесса по данному направлению.

На сегодняшний день успешное развитие радиоустройств под общим названием SDR (Software Defined Radio), или программно-определяемое радио, позволяет говорить о том, что такая техника дает достаточно серьезные возможности для исследователей радиосигналов за умеренную стоимость. Приемник на основе программно-определяемого радио способен сканировать широкий диапазон частот (до 6 ГГц у USRP B210) с полосой пропускания до 56 МГц и стоимостью приемника до 100 долларов, при этом обработка и анализ обнаруженных радиосигналов полностью производится при помощи персонального компьютера, на котором реализовано специальное ПО.

В настоящий момент различными учеными помимо исследований ПЭМИ видеотракта [1–3] проводятся исследования ПЭМИ интерфейса USB [4], лазерных принтеров [5], клавиатур с интерфейсом PS/2 [6] и т. д.

1. ТЕХНИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПЭМИ ВИДЕОТРАКТА

Технический канал утечки информации связан с неконтролируемым распространением информативного сигнала через физическую среду до технического средства, осуществляющего перехват информации [7]. Источники ПЭМИ видеотракта включают в себя порт вывода сигнала графического про-

цессора (GPU), кабели передачи видео (VGA, HDMI, DVI, Display Port и т. д.) и внутренние порты дисплея (LVDS и встроенный порт дисплея (eDP)) [8–10]. Основным устройством вывода визуальной информации в персональных компьютерах (ПК) является монитор. Практически все современные мониторы основаны на растровом изображении, это означает, что изображение передается по видеотракту к монитору построчно с определенной тактовой частотой [11].

В работе будем рассматривать интерфейс VGA как наиболее доступный и простой для исследования, но то же самое применимо и к современным цифровым интерфейсам (DVI, HDMI, Display Port).

Представим основные параметры, которые важны для дальнейшей работы.

1. Максимальная разрешающая способность – характеристика, связанная с размером отображаемого изображения. Максимальная разрешающая способность выражается в количестве точек по ширине и высоте отображаемого изображения. Например, для отображаемого изображения в разрешении 1280 × 1024 максимальная разрешающая способность будет составлять 1 310 720 точек.

2. Частота регенерации или обновления экрана (Гц).

3. Частота горизонтальной развертки монитора – характеристика, показывающая предельное число горизонтальных строк на экране монитора, которое может прочертить электронный луч за одну секунду.

4. Ширина полосы пропускания частот – параметр, характеризующий максимально возможное количество точек, отображаемых на экране за секунду (МГц).

Исследуемый монитор имеет следующие характеристики:

– разрешение экрана 1280 × 1024;

– частота обновления экрана 60 Гц.

Таким образом, требуемая ширина полосы пропускания монитора будет равна 1,05 × 1024 × 1280 × 1,3 × 60 = 107 МГц.

2. ТЕХНОЛОГИЯ SDR

Технология SDR (Software Defined Radio, программно-определяемое радио) – это технология, позволяющая с помощью программного обеспечения устанавливать или изменять рабочие радиочастотные параметры приемопередающего устройства.

Функциональная схема SDR (рис. 1) состоит:

– из программной части, предназначенной для выполнения значительной части функций по обработке сигналов и управления аппаратной частью;

– аппаратной части, предназначенной для выполнения функций, недоступных для программной реализации [12].

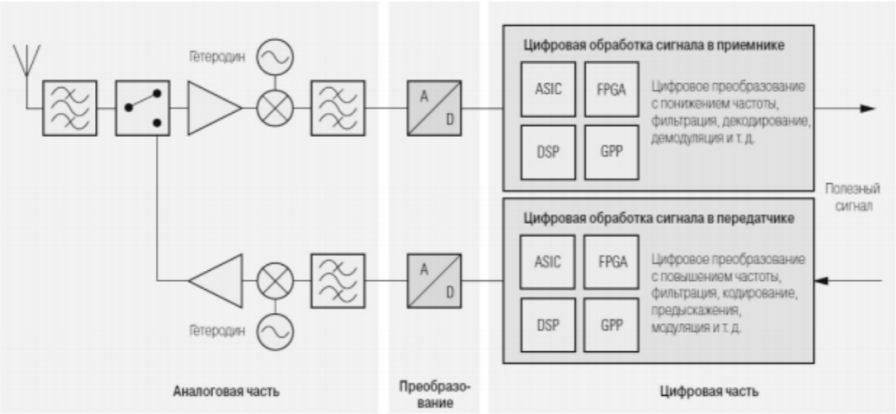


Рис. 1. Функциональная схема SDR

Fig. 1. Functional diagram SDR

Устройство SDR выполнено по модульной архитектуре. Модульная архитектура более гибкая и дает возможность заменять различные модули для достижения оптимальных результатов.

2.1. СИСТЕМА USRP

Для выполнения перехвата видеосигнала было использовано SDR-устройство серии USRP, а именно Ettus USRP B120.

Устройства серии USRP B210 представляют собой компактную и относительно недорогую аппаратную основу для технологии SDR. К достоинствам данного устройства можно отнести непрерывный частотный диапазон от 70 МГц до 6 ГГц, полосу пропускания шириной в 56 МГц, ПЛИС (программируемая логическая интегральная схема) Spartan 6, скоростное подключение USB 3.0 и возможность питания от шины.

Структура устройства USRP в совокупности с ПО GNU Radio представлена на рис. 2. Левый блок на рисунке представляет переднюю часть устройства, в задачи которой входит прием и передача радиосигналов. Верхний путь обозначает путь приема (R_x), нижний путь – путь передачи (T_x). Оба канала могут использоваться независимо друг от друга.

Таблица 1

Table 1

Параметры модели USRP B210

USRP B210 model parameters

Частотный диапазон	70 МГц … 6 ГГц
Ширина полосы пропускания	До 56 МГц
Разрядность АЦП	12 бит
Частота дискретизации	61,44 МГц
Чипсет	AD 9361
Способ связи	Дуплекс
Количество каналов приема	2
Количество каналов передачи	2
Интерфейс USB	3.0

Средний блок на рис. 2 представляет интерфейс преобразования аналогового сигнала в цифровой и наоборот. Передняя часть устройства подключается к материнской плате USRP, собранной на базе ПЛИС. На материнской плате USRP контроллером интегральной схемы выполняется преобразование аналоговых сигналов в цифровой и их смешивание в основной полосе.

Правый блок (рис. 2) представлен программной частью, реализованной на ПК в среде GNU Radio, где происходит последующая обработка сигнала. Подключение оформлено посредством интерфейса USB 3.0. При активном соединении программной и аппаратной частей система GNU Radio управляет дальнейшим процессом обработки сигналов.

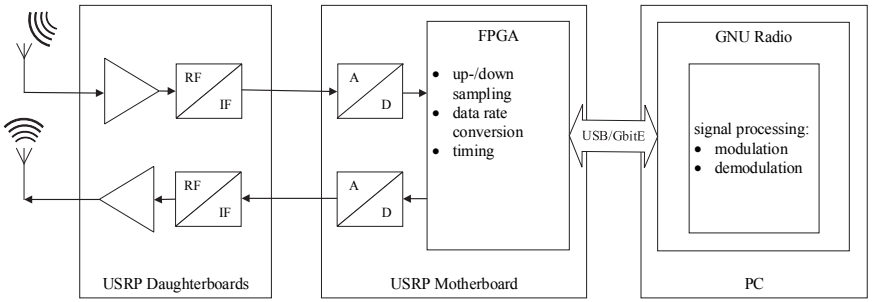


Рис. 2. Архитектура SDR-устройства модели USRP

Fig. 2. USRP SDR device architecture

2.2. GNU RADIO

Для цифровой обработки данных, полученных с SDR-устройства, на компьютере применяется кроссплатформенный программный пакет GNU Radio. Обработка данных производится в режиме реального времени.

Программа построена на модульной основе с учетом парадигмы ООП [13]. Каждый элемент программы является отдельным блоком со своей внутренней логикой. Каждый блок имеет вход и выход для подключения в общую схему, а также набор собственных параметров. Параметры могут задаваться статически (вводом определенного числа) или динамически (вводом переменной или выражений).

На рис. 3 показаны уровни обработки данных в среде GNU Radio.

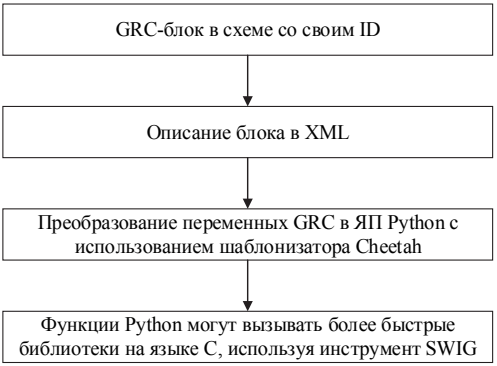


Рис. 3. Путь данных в среде GNU Radio

Fig. 3. GNU Radio data path

Верхний уровень блок-схемы – это уровень графического представления, на котором пользователь собирает функциональную схему. На этом уровне доступно взаимодействие с доступными параметрами блоков и их изменение.

Далее собранную схему необходимо сгенерировать. Система отправляет полученные сведения на следующий уровень, в описание блоков в формате XML.

3. СОСТАВ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА

В проводимом исследовании использовался ЖК-монитор Dell E2214H. Данный дисплей имеет максимальное разрешение экрана 1920 × 1080, частоту обновления 60 Гц, а также слоты для подключения DVI-D и VGA интерфейсов. Поскольку в эксперименте сделан акцент на изучение аналогового сигна-

ла, выберем интерфейс VGA, а также установим разрешение экрана 1280 × 1024 пикселей, кадровую частоту 60 Гц.

Программное обеспечение, на котором производится обработка получаемого сигнала и демонстрация результата, установлено на ноутбуке с работающей виртуальной машиной под управлением ОС Linux Ubuntu. К нему по интерфейсу USB 3.0 подключено SDR-устройство Ettus USRP B210, которое принимает и оцифровывает сигнал. Выборки сигнала, полученные от аппаратной части SDR, поступают в компьютер и обрабатываются в среде GNU Radio.

При разработке программного обеспечения для обнаружения и восстановления сигналов ПЭМИ видеоинтерфейса используются дополнительные модули, расширяющие базовые возможности GNU Radio, а также драйвер UHD, необходимый для успешного взаимодействия программной и аппаратной частей комплекса.

Таблица 2

Table 2

Характеристики используемых инструментов

Characteristics of the equipment used

Параметры монитора	
Модель	Dell E2214H
Разрешение экрана	1920 × 1080
Частота обновления	60 Гц
Видеоинтерфейс	VGA
Характеристики ОС хоста	
ОС	Windows 10
Процессор	Intel i5-3570
ОЗУ	10 Гб
Версия USB	3.0
Параметры виртуальной машины	
ОС	Ubuntu 18.04 LTS
Выделенный объем GPU	128 Мб
Выделенный объем ОЗУ	8 Гб
GNU Radio	3.7
UHD-драйвер	3.14.0

Окончание табл.2

End of the Tab.2

Устройство SDR	
Модель	Ettus USRP B210
ПЛИС	Spartan 6
Антенна	RX2
АЦП, разрядность	12 бит
АЦП, частота дискретизации	61,44 МГц

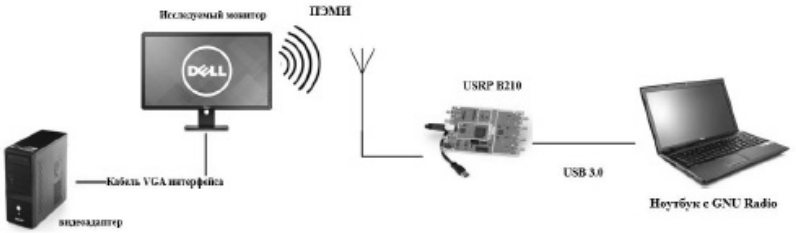


Рис. 4. Состав стенда

Fig. 4. Stand composition

На рис. 4 продемонстрирован макет программно-аппаратного комплекса.

4. ПРОВЕДЕНИЕ ЭКСПЕРИМЕНТА

4.1. СХЕМА С ИМИТАЦИОННЫМ СИГНАЛОМ

В этом разделе пойдет речь об имитации утечки по каналу ПЭМИ видеотракта. В схеме отсутствует SDR-приемник как средство перехвата реального сигнала. Вместо этого источником выступает заранее отобранное изображение. Изображение передается в виде цифрового сигнала, на который накладываются помехи, созданные программным генератором из блока GNU Radio. Задача данной модели состоит в демонстрации свойств ПЭМИ, а также возможных препятствий на пути преобразования перехваченного сигнала в изображение.

Схема, используемая на первом этапе эксперимента, представлена на рис. 5.

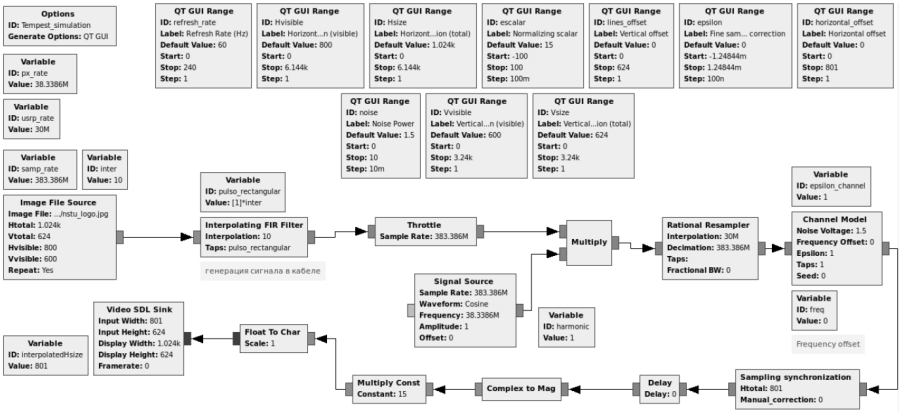


Рис. 5. Имитационная модель в GNU Radio

Fig. 5. Simulation model in GNU Radio

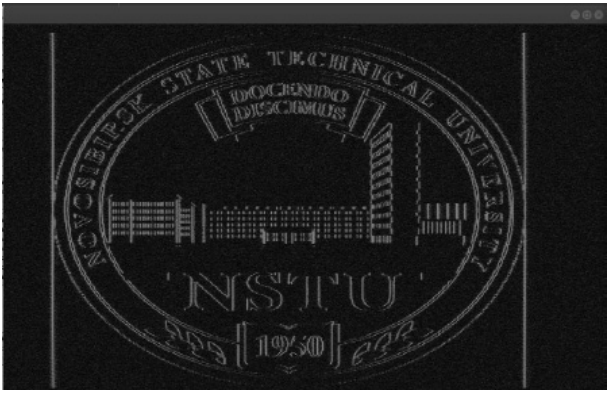


Рис. 6. Результат вывода изображения в имитационной схеме

Fig. 6. The result of displaying an image in the simulation circuit

Для тестирования был выбран классический логотип НГТУ. Результат работы программы показан на рис. 6.

4.2. ПРАКТИЧЕСКАЯ АТАКА

Отправной точкой в данной схеме является SDR Source – блок подключаемого устройства модели Ettus USRP B210. Сигнал с устройства в двоичной форме передается программе. Блоки данной схемы производят обработку сигнала и его преобразование в векторное изображение. Полная схема представлена на рис. 7.

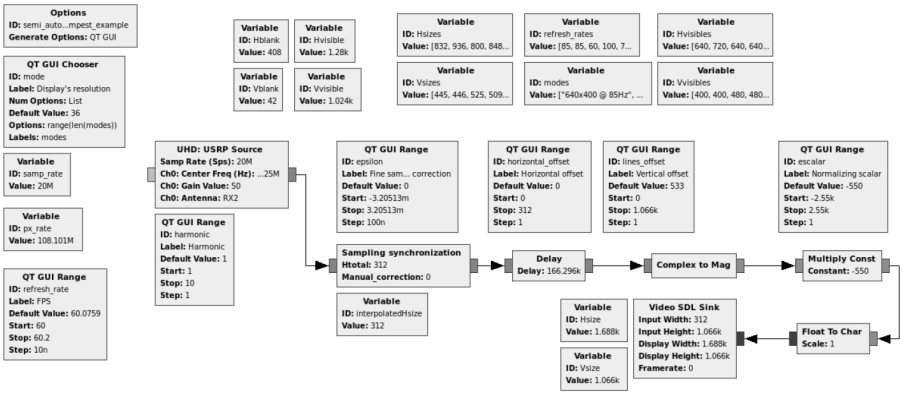


Рис. 7. Схема перехвата сигнала ПЭМИ

Fig. 7. Compromising radiation signal interception circuit

Как следует из теоремы Котельникова – Шеннона, для полного восстановления принимаемого видеосигнала необходимо, чтобы частота дискретизации приемника как минимум вдвое превышала значение частоты следования пикселей в сигнале видеоинтерфейса.

Чтобы определить диапазон исследуемых частот, на которых стоит ожидать появление информативного сигнала, необходимо знать разрешающую способность монитора и частоту обновления. Поскольку нам известны эти данные, применим следующее выражение для расчета:

$$f = (H \cdot L \cdot F_{\text{кадр}} \cdot 1{,}36) / 2 \,,$$

где H – разрешение монитора по высоте; L – разрешение монитора по ширине; $F_{\text{кадр}}$ – частота обновления монитора (кадровая частота).

Для исследуемого монитора имеем значение H = 1024, L = 120, $F_{кадр}$ = = 60 Гц. Коэффициент 1,36 применяется для учета кадровых гасящих импульсов, которые не входят в видимую зону изображения.

Подставив значения в вышеуказанное выражение, получим значение частоты 53,5 МГц. Полученный результат означает, что на этой частоте находится первая гармоника сигнала. Такой же сигнал появится на кратных частотах: 107,0 МГц, 160,4 МГц и т. д.

Следуя вышеуказанной теореме, можно сделать вывод, что частота дискретизации приемника должна быть не менее 107 МГц. Однако максимально возможная частота дискретизации используемого устройства SDR составляет 61,44 МГц, что ниже необходимого значения.

Известно, что в таком случае работает другое правило: чем выше частота дискретизации, тем качественнее изображение мы сможем восстановить.

Для подключения SDR-устройства был выбран интерфейс USB 3.0. Максимальная скорость передачи данных данного интерфейса равна 640 Мб/с. При передаче сигнала в GRC будет записываться комплексный I/Q сигнал 32 бит/с. Поскольку доступный диапазон значений I/Q потока содержится внутри отрезка [–1.0; 1.0], общий вес сигнала составит суммарно 64 бит/с, или 8 байт/с.

Скорость передачи данных от SDR-устройства к ПК можно вычислить, умножив вес одной входящей I/Q выборки на скорость обработки АЦП программного радио.

При выбранных частотах дискретизации (10, 16, 20 МГц) скорость передачи составит 80 Мбайт/с, 128 Мбайт/с и 160 Мбайт/с соответственно. Все эти значения не превышают предельную норму USB 3.0 в 640 Мбайт/с и, следовательно, допустимы для использования в исследовании.

Результаты восстановления сигнала ПЭМИ при частотах дискретизации 20, 16, 10 МГц показаны на рис. 8, 9 и 10 соответственно.

Скриншот рабочего стола исследуемого монитора представлен на рис. 11. На странице документа размещены две похожие буквы – ш и щ, оформленные крупным кеглем. Далее убывающим кеглем представлены русский алфавит и набор строчных гласных букв.

Полученные результаты доказывают, что при частоте дискретизации приемника 20 МГц и выше возможно перехватить довольно качественное и читаемое изображение. Использование интерфейса USB ниже 3.0 приведет к невозможности восстановить изображение достаточного качества для визуализации информации, так как скорость передачи USB 2.0 равна 60 Мбайт/с, что не позволит устанавливать частоту дискретизации выше 10 МГц. А как видно из рис. 10, изображение при частоте дискретизации 10 МГц практически нечитаемое.

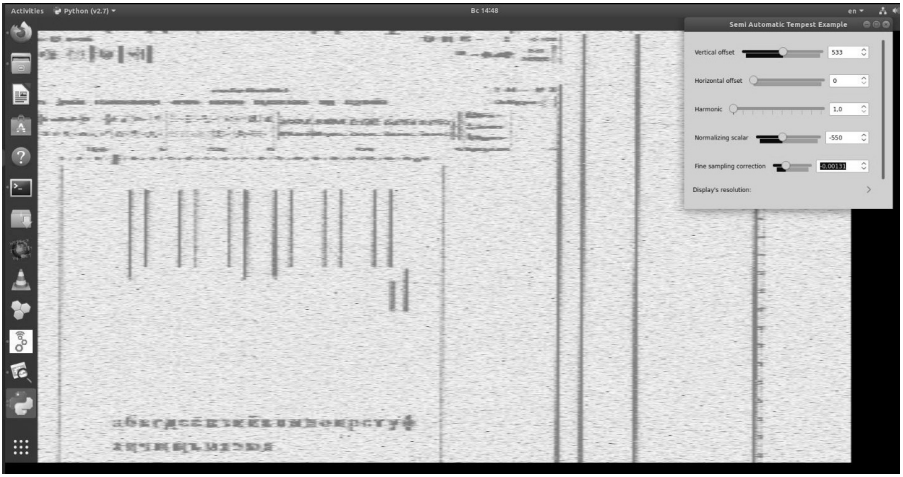


Рис. 8. Результат перехвата изображения с частотой дискретизации 20 МГц

Fig. 8. Image capture result with 20 MHz sampling rate

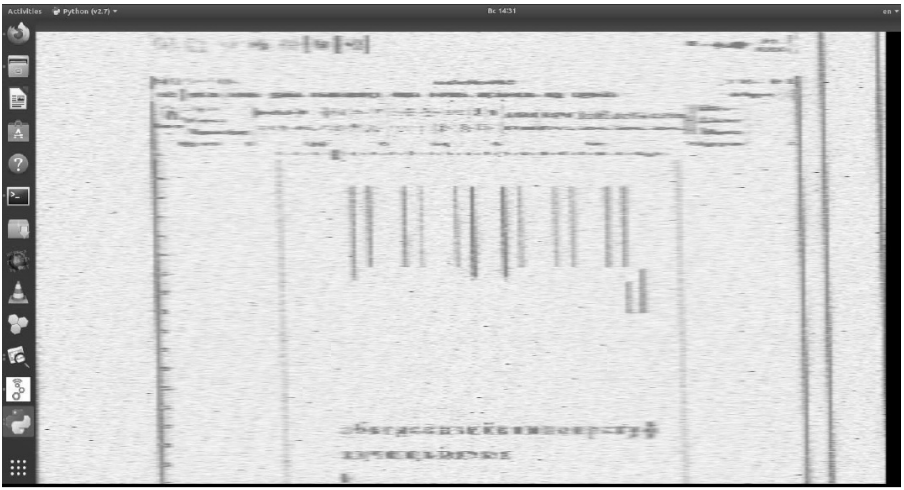


Рис. 9. Результат перехвата изображения с частотой дискретизации 16 МГц

Fig. 9. Image capture result with 16 MHz sampling rate

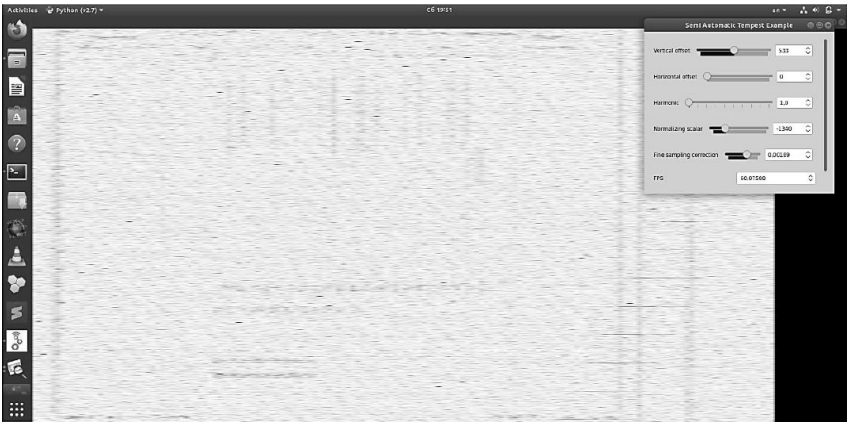


Рис. 10. Результат перехвата изображения с частотой дискретизации 10 МГц

Fig. 10. Image capture result with 10 MHz sampling rate

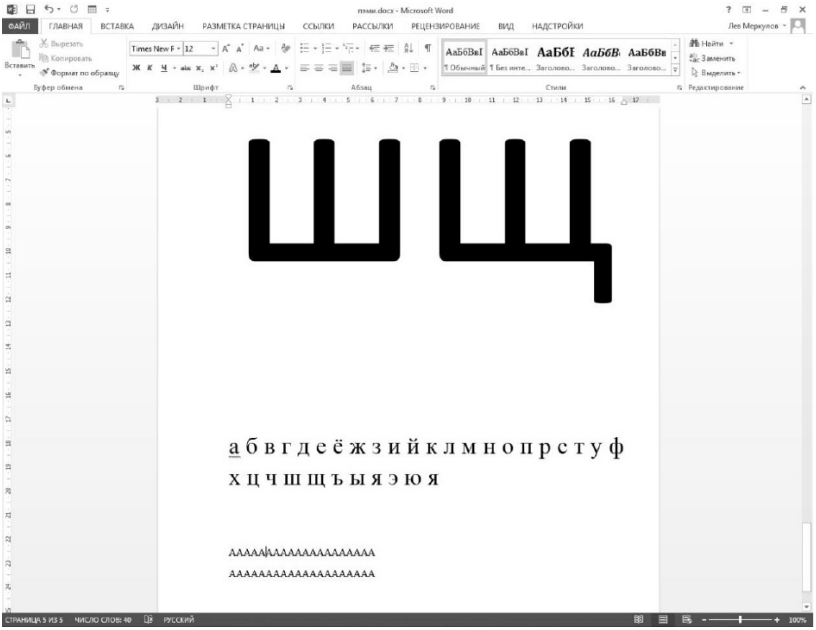


Рис. 11. Снимок рабочего стола исследуемого монитора

Fig. 11. A snapshot of the desktop of the monitor under study

Это показывает, что практическая атака может быть реализуема неподготовленным злоумышленником, не обладающим существенными специальными знаниями и, что также важно, дорогой профессиональной техникой. Более изощренный злоумышленник может использовать лучшее оборудование с более низким уровнем шума и более высоким усилением антенны для проведения такой атаки с большего расстояния.

ЗАКЛЮЧЕНИЕ

ПЭМИ видеотракта – это реальная угроза, которая существует с тех пор, как впервые были использованы мониторы. Рассмотренная в настоящей работе проблема VGA интерфейса не является исчерпывающей. На сегодняшний день известны случаи перехвата не только сигналов аналогового интерфейса, но и сигналов цифровых интерфейсов, например интерфейса HDMI [14] и DVI [15].

Текущий проект продемонстрировал, что практическая атака является жизнеспособной, и при этом злоумышленник необязательно должен иметь какие-либо предварительные знания о цели, и что развитие средств приема и обработки информации (в данном случае появление SDR-приемников) приводит к снижению стоимости затрат на реализацию подобных проектов.

СПИСОК ЛИТЕРАТУРЫ

1. *Meulemeester P. De, Scheers B., Vandenbosch G.A.E.* A quantitative approach to eavesdrop video display systems exploiting multiple electromagnetic leakage channels // IEEE Transactions on Electromagnetic Compatibility. – 2020. – Vol. 62 (3). – P. 663–672.

2. *Meulemeester P. De, Scheers B., Vandenbosch G.A.E.* Eavesdropping a (ultra-)high-definition video display from an 80 meter distance under realistic circumstances // 2020 IEEE International Symposium on Electromagnetic Compatibility and Signal/Power Integrity (EMCSI). – IEEE, 2020. – P. 517–522. – DOI: 10.1109/EMCSI38923.2020.9191457.

3. *Sayakkara A., Le-Khac N.-A., Scanlon M.* Accuracy enhancement of electromagnetic side-channel attacks on computer monitors // ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security. – ACM, 2018. – Art. 15. – P. 1–9. – DOI: 10.1145/3230833.3234690.

4. Compromising electromagnetic emanations of USB mass storage devices / A. Boitan, S. Halunga, V. Bîndar, O. Fratu // Wireless Personal Communications. – 2020. – P. 1–26.

5. *Ulaş C., Aşık U., Karadeniz C.* Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines // Computers and Security. – 2016. – Vol. 58. – P. 250–267. – DOI: 10.1016/j.cose.2016.02.001.

6. Study of compromising emissions of ps/2 keyboards by correlative methods / X.-I. Rognean, G. Rosu, A. Boitan, B. Trip, V. Butnariu, C. Kasmi, L.O. Fichte, O. Baltag // Revue Roumaine des Sciences Techniques. Serie Electrotechnique et Energetique. – 2020. – N 65. – P. 15–20.

7. *Хорев А.А.* Технические каналы утечки информации, обрабатываемой техническими средствами // Специальная техника. – 2004. – № 2. – С. 39–57. – URL: http://www.bnti.ru/showart.asp?aid=954&l-vl=4.03 (дата обращения: 06.12.2021).

8. *Kuhn M.G.* Compromising emanations: eavesdropping risks of computer displays. – Cambridge, 2003. – (Technical report / University of Cambridge, Computer Laboratory; no. 577).

9. *Sekiguchi H., Seto S.* Proposal of an information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer // 2008 IEEE Instrumentation and Measurement Technology Conference. – IEEE, 2008. – P. 1859–1863. – DOI: 10.1109/IMTC.2008.4547348.

10. *Kuhn M.G.* Compromising emanations of LCD TV sets // IEEE Transactions on Electromagnetic Compatibility. – 2013. – Vol. 55 (3). – P. 564–570.

11. *Marinov M.* Remote video eavesdropping using a software-defined radio platform: M.Phil in Advanced Computer Science / University of Cambridge, Computer Laboratory. – Cambridge, 2014. – 68 p.

12. *Силин А.* Технология Software Defined Radio: теория, принципы и примеры аппаратных платформ // Беспроводные технологии. – 2007. – № 2. – URL: https://wireless-e.ru/gsm/software-defined-radio/ (дата обращения: 07.12.2021).

13. GNU Radio. Guided tutorial introduction: website. – URL: https://wiki.gnuradio.org/index.php/Guided_Tutorial_Introduction (accessed: 07.12.2021).

14. *Wang S., Qiu Y., Tian J.* Method for evaluating digital video electromagnetic information leakage from video cable // Chinese Journal of Electronics. – 2021. – Vol. 30 (5). – P. 978–985. – DOI: 10.1049/cje.2021.07.009.

15. *Kubiak I., Przybysz A.* DVI (HDMI) and DisplayPort digital video interfaces in electromagnetic eavesdropping process // 2019 International Symposium on Electromagnetic Compatibility – EMC EUROPE. – IEEE, 2019. – P. 338–393. – DOI: 10.1109/EMCEurope.2019.8872097.

Иванов Андрей Валерьевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации Новосибирского государственного технического университета. Область научных интересов – техническая защита информации. E-mail: andrej.ivanov@corp.nstu.ru

Огнев Игорь Александрович, аспирант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – применение технологии SDR в информационной безопасности. E-mail: i.ognev.2016@corp.nstu.ru

Никитина Елизавета Евгеньевна, аспирант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – применение технологии SDR в информационной безопасности. E-mail: lizanikitinasj@gmail.co*m*

Меркулов Лев Владимирович, магистрант кафедры технологий испытаний и эксплуатации Московского авиационного института. Основное направление научных исследований – восстановление сигналов ПЭМИ с применением технологии SDR. E-mail: Levmerkulov1@yandex.ru

DOI: 10.17212/2782-2230-2021-4-72-90

Application of SDR (Software Defined Radio) technology for recovery of signals of side electromagnetic radiation of video tract*

A.V. Ivanov[1], I.A. Ognev[2], E.E. Nikitina[3], L.V. Merkulov[4]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, PhD in Technology, head of the Information Security Department. E-mail: andrej.ivanov@corp.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, graduate student of Information Security Department. E-mail: i.ognev.2016@corp.nstu.ru*

[3] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, graduate student of Information Security Department. E-mail: lizanikitinasj@gmail.com*

[4] *Moscow Aviation Institute, Volokolamskoe highway, 4, Moscow, 125993, Russian Federation, master's student of Test and Operation Technology Department. E-mail: Levmerkulov1@yandex.ru*

This article presents the results of recovering signals of spurious electromagnetic radiation of a video path using an SDR receiver. This work demonstrates the existence of a potential risk of leakage of confidential information through a technical channel of information leakage due to spurious electromagnetic radiation of a video path, bypassing traditional cryptographic and

* *Received 31 October 2021.*

physical methods of information protection. An attack can be carried out by an attacker without special technical knowledge and special professional expensive equipment. The presented stand makes it possible to simplify research related to spurious electromagnetic radiation, as well as to apply this technology to build a learning process in this domain. In the course of the work, a description of the concept of a technical channel of information leakage and a brief description of the side electromagnetic radiation of the video path are given. The following briefly describes the SDR technology, the selected USRP B210 receiver, and the cross-platform open source GNU Radio software package. The demonstration stand is described in detail and the results of image reconstruction are given. In addition, two stages of the development of a demonstration stand are considered: using a simulation signal and a real intercepted signal. A demonstration stand with simulation signals serves to develop a user's understanding of the properties of spurious electromagnetic radiation, as well as possible obstacles to converting an intercepted signal into an image. The studies of the real intercepted signal were carried out on a monitor with a set resolution of 1280×1024 and a screen refresh rate of 60 Hz. An analog VGA (Video Graphics Array) interface was used to connect the monitor. The dependence of the quality of the reconstructed image on the set sampling frequency of the SDR receiver is shown.

Keywords: information security, side electromagnetic radiation, technical devices, automated system, software and hardware complex, Software Defined Radio system, Software Defined Radio, recovery compromising radiation

REFERENCES

1. Meulemeester P. De, Scheers B., Vandenbosch G.A.E. A quantitative approach to eavesdrop video display systems exploiting multiple electromagnetic leakage channels. IEEE *Transactions on Electromagnetic Compatibility*, 2020, vol. 62 (3), pp. 663–672.

2. Meulemeester P. De, Scheers B., Vandenbosch G.A.E. Eavesdropping a (ultra-)high-definition video display from an 80 meter distance under realistic circumstances. *2020 IEEE International Symposium on Electromagnetic Compatibility and Signal/Power Integrity (EMCSI)*. IEEE, 2020, pp. 517–522. DOI: 10.1109/EMCSI38923.2020.9191457.

3. Sayakkara A., Le-Khac N.-A., Scanlon M. Accuracy enhancement of electromagnetic side-channel attacks on computer monitors. *ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM, 2018, art. 15, pp. 1–9. DOI: 10.1145/3230833.3234690.

4. Boitan A., Halunga S., Bîndar V., Fratu O. Compromising electromagnetic emanations of USB mass storage devices. *Wireless Personal Communications*, 2020, pp. 1–26.

5. Ulaş C., Aşık U., Karadeniz C. Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines. *Computers and Security*, 2016, vol. 58, pp. 250–267. DOI: 10.1016/j.cose.2016.02.001.

6. Rognean X.-I., Rosu G., Boitan A., Trip B., Butnariu V., Kasmi C., Fichte L.O., Baltag O. Study of compromising emissions of ps/2 keyboards by correlative methods. *Revue Roumaine des Sciences Techniques. Serie Electrotechnique et Energetique*, 2020, no. 65, pp. 15–20.

7. Khorev A.A. Tekhnicheskie kanaly utechki informatsii, obrabatyvaemoi sredstvami vychislitel'noi tekhniki [Technical channels of computer-processed information leakage]. *Spetsial'naya tekhnika = Special Equipment*, 2010, no. 2, pp. 39–57. Available at: http://www.bnti.ru/showart.asp?aid=954&l-vl=4.03 (accessed 06.12.2021).

8. Kuhn M.G. *Compromising emanations: eavesdropping risks of computer displays*. Cambridge, 2003. University of Cambridge, Computer Laboratory. Technical report, no. 577.

9. Sekiguchi H., Seto S. Proposal of an information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer. *2008 IEEE Instrumentation and Measurement Technology Conference*. IEEE, 2008, pp. 1859–1863. DOI: 10.1109/IMTC.2008.4547348.

10. Kuhn M.G. Compromising emanations of LCD TV sets. *IEEE Transactions on Electromagnetic Compatibility*, 2013, vol. 55 (3), pp. 564–570.

11. Marinov M. *Remote video eavesdropping using a software-defined radio platform*. M.Phil in Advanced Computer Science. University of Cambridge, Computer Laboratory, 2014. 68 p.

12. Silin A. Tekhnologiya Software Defined Radio: teoriya, printsipy i primery apparatnykh platform [Software Defined Radio technology. Theory, principles and examples of hardware platforms]. *Besprovodnye tekhnologii = Wireless Technologies*, 2007, no. 2. Available at: https://wireless-e.ru/gsm/software-defined-radio/ (accessed 07.12.2021).

13. *GNU Radio. Guided tutorial introduction*. Website. Available at: https://wiki.gnuradio.org/index.php/Guided_Tutorial_Introduction (accessed 07.12.2021).

14. Wang S., Qiu Y., Tian J. Method for evaluating digital video electromagnetic information leakage from video cable. *Chinese Journal of Electronics*, 2021, vol. 30 (5), pp. 978–985. DOI: 10.1049/cje.2021.07.009.

15. Kubiak I., Przybysz A. DVI (HDMI) and DisplayPort digital video interfaces in electromagnetic eavesdropping process. *2019 International Symposium on Electromagnetic Compatibility – EMC EUROPE*. IEEE, 2019, pp. 338–393. DOI: 10.1109/EMCEurope.2019.8872097.

Для цитирования:

Применение технологии SDR (Software Defined Radio) для восстановления сигналов побочных электромагнитных излучений видеотракта / А.В. Иванов, И.А. Огнев, Е.Е. Никитина, Л.В. Меркулов // Безопасность цифровых технологий. – 2021. – № 4 (103). – С. 72–90. – DOI: 10.17212/2782-2230-2021-4-72-90.

For citation:

Ivanov A.V., Ognev I.A., Nikitina E.E., Merkulov L.V. Primenenie tekhnologii SDR (Software Defined Radio) dlya vosstanovleniya signalov pobochnykh elektromagnitnykh izluchenii videotrakta [Application of SDR (Software Defined Radio) technology for recovery of signals of side electromagnetic radiation of video tract]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 4 (103), pp. 72–90. DOI: 10.17212/2782-2230-2021-4-72-90.

ПРАВИЛА ДЛЯ АВТОРОВ

УСЛОВИЯ ПРИЕМА СТАТЕЙ

Перед отправкой рукописи в редакцию авторы должны проверить свою статью с помощью системы «Антиплагиат». Принятый редакционной коллегией уровень оригинальности статей должен составлять не менее 85 %.

Все статьи и сопровождающие их материалы в журнал подаются через сайт журнала в электронном виде после регистрации всех авторов статьи. Регистрация обязывает каждого автора иметь международный идентификационный номер ORCID. Иные варианты подачи материалов не рассматриваются.

Автор (один из соавторов) в своем личном кабинете выбирает в меню пункт «Подать статью» и вводит все необходимые данные. Своих соавторов при этом он выбирает из списка зарегистрированных пользователей.

Рукопись статьи готовится в соответствии с правилами оформления в редакторе MS Word и прикрепляется в формате *.doc, *.docx.

Сканированные лицензионный договор с подписями авторов и экспертное заключение (цветной режим сканирования, разрешение не менее 600 dpi) необходимо также разместить на сайте журнала в разделе «Подать статью» в формате *.pdf, *.jpg, *.jpeg.

По окончании всех работ обязательно нажать кнопку «Отправить в редакцию».

В редакцию журнала предоставляются следующие материалы.

1. **Статья**, подготовленная в соответствии с правилами оформления, – печатная версия, 2 экземпляра, подписанных авторами.

2. **Контактная информация** (телефоны рабочий и сотовый, адреса электронной почты, место работы, адрес места работы, должность, ученая степень, ученое звание автора) – печатная версия, 2 экземпляра.

3. **Описание статьи для базы данных «Российский индекс научного цитирования (РИНЦ)»**, подготовленное в соответствии с правилами оформления, – печатная версия, один экземпляр.

4. **Лицензионный договор**, заполненный и подписанный.

5. **Электронная версия статьи, контактной информации, описания статьи для базы данных РИНЦ, сканированный лицензионный договор и экспертное заключение о возможности опубликования (в отдельных файлах на адрес редакции)**.

6. **Экспертное заключение о возможности опубликования**.

7. **Согласие на публикацию, обработку и распространение персональных данных авторов статей**.

Редакцией рассматриваются только те материалы авторов, которые полностью соответствуют вышеобозначенным требованиям. Неполный пакет материалов редакцией не рассматривается.

Подготовленные материалы направляются на почтовый адрес редакции: 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет (НГТУ), корп. 7, ком. 606, в редакцию журнала «Безопасность цифровых технологий».

Все рукописи рецензируются, по результатам рецензирования редколлегия принимает решение о целесообразности опубликования материалов.

ПРАВИЛА ОФОРМЛЕНИЯ

При подготовке документов для отправки в редакцию журнала авторам рекомендуется внимательно прочитать правила и посмотреть примеры оформления статей и всех необходимых сопутствующих документов. Редакция рассматривает статьи, подготовленные как на русском, так и на английском языке. Для опубликования статьи на английском языке необходимо дополнительно предоставить ее русскоязычный вариант, оформленный по правилам журнала (кроме зарубежных авторов).

Чтобы статья была направлена на рецензирование, Вам необходимо подготовить следующее:

1) **статью** в соответствии с правилами оформления (объем от 7 до 30 страниц);

2) **контактную информацию** в одном файле предоставить по каждому автору: ФИО полностью, ученая степень, ученое звание автора, должность, место работы, адрес места работы, телефон рабочий и сотовый, адрес электронной почты;

3) **описание статьи для базы данных «Российский индекс научного цитирования (РИНЦ)»**;

4) **лицензионный договор** заполнить, бланк лицензионного договора должен быть подписан только авторами (он доступен авторам также в личном кабинете); если авторов несколько, то необходимо добавить поля на всех авторов, и каждый должен поставить свою подпись;

5) **экспертное заключение** о возможности опубликования, принятое в Вашей организации;

6) авторы, не являющиеся сотрудниками НГТУ, предоставляют **сопроводительное письмо** на имя проректора по научной работе НГТУ (ссылка на страницу сайта НГТУ). Письмо нужно подготовить на бланке организации с подписью и печатью руководителя;

7) согласие на публикацию, обработку и распространение персональных данных авторов статей.

ОСНОВНЫЕ РАЗДЕЛЫ ЖУРНАЛА

Автоматизация и управление технологическими процессами и производствами.

Управление в социальных и экономических системах.

Методы и системы защиты информации, информационная безопасность.

RULES FOR AUTHORS

CONDITIONS FOR ACCEPTANCE OF ARTICLES

Before sending the manuscript to the editorial office, authors must check their article using the Antiplagiarism system. The level of originality of articles adopted by the Editorial Board should be at least 85 %.

All articles and their accompanying materials are submitted to the magazine through the magazine's website in electronic form after registration of all the authors of the article. Registration obliges each author to have an international ORCID. No other material supply options are considered.

The author (one of the co-authors) in his personal account selects the item "Submit article" in the menu and enters all the necessary data. At the same time, he selects his co-authors from the list of registered users.

The manuscript of the article is prepared in accordance with the design rules in the MS Word editor and attached in the format * .doc, * .docx.

Scanned license agreement with signatures of authors and expert opinion (color mode scanning, resolution not less than 600 dpi) can also be attached on the website of the magazine in the section "Submit article" in the format * .pdf, * .jpg, * .jpeg.

At the end of all works, be sure to click the "Send to Design" button.

The following materials are provided to the journal editor:

1. **The article**, prepared in accordance with the rules of design, is a private version, 2 copies signed by the authors.
2. **Contact information** (working and cellular phones, e-mail addresses, place of work, address of the place of work, position, scientific degree, academic title of the author) - printed version, 2 copies.
3. **The description of the article** for the database "**Russian Scientific Citation Index (RSCI)**," prepared in accordance with the rules of form-making, is a printed version, one copy.
4. **License agreement** completed and signed.
5. **Electronic version of the article**, contact information, description of the article for the RSCI database, scanned license agreement and expert opinion on the possibility of publication (in separate files to the editorial address).
6. **Expert opinion** on the possibility of publication.
7. **Consent to the publication, processing and dissemination of personal data of the authors of articles**.

The editors consider only those materials of the authors that fully meet the above requirements. Incomplete package of materials is not considered by the revision.

The prepared materials are sent to the postal address of the editorial office: 630073, Novosibirsk, pr. Karl Marx, 20, Novosibirsk State Technical University (NSTU), building 7, office 606, to the editors of the journal "Digital Technology Security."

All manuscripts were reviewed, and according to the results of the review, the editorial board decided on the appropriateness of publishing the materials.

FORMATTING RULES

When preparing documents for submission to the journal editor, authors are advised to carefully read the rules and see examples of the design of articles and all necessary related documents. The Drafting Committee considered articles prepared in both Russian and English. To publish the article in English, it is necessary to additionally provide its Russian-language version, drawn up according to the rules of the magazine (except for foreign authors).

For the article to be aimed at peer review, you need to prepare the following:

1) **the article** in accordance with the rules of design (volume from 7 to 30 pages);

2) **provide contact information** in one file for each author: full name, degree, academic title of the author, position, place of work, address of the place of work, telephone number of the worker and mobile, e-mail address;

3) **description of the article** for the database "Russian Scientific Citation Index (RSCI)";

4) fill out the **license agreement**, the form of the license agreement must be signed only by the authors (it is also available to the authors in the personal office), if there are several authors, then it is necessary to add fields on all authors and sign each of them;

5) **expert opinion** on the possibility of publication, adopted in your organization;

6) authors who are not employees of the NSTU provide a **companion letter** addressed to the vice-rector for scientific work of the NSTU (link to the page of the NSTU website). The letter should be prepared on the form of the organization with the signature and seal of the manager;

7) consent to the publication, processing and dissemination of personal data of the authors of articles.

JOURNAL SECTION

Automation and control of technological processes and productions.
Governance in social and economic systems.
Methods and systems of information protection, information security.