МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ
XXV МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ

Том 4

Харків 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЛЕКТРОНІКИ

МАТЕРІАЛИ 25-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

20 – 22 квітня 2021 р.

Том 4

КОНФЕРЕНЦІЯ

«ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ»

Харків 2021

УДК 004:[621.317+621.391](06)

25-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2021. – 176 с.

В збірник включені матеріали 25-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті».

Видання підготовлено факультетом інфокомунікацій
Харківського національного університету радіоелектроніки

61166 Україна, Харків, прос. Науки, 14
тел./факс.: (057) 7021397

E-mail: mref21@nure.ua

Харківський національний університет
радіоелектроніки (ХНУРЕ), 2021

Програмний комітет конференції

Снігуров А.В.	к.т.н., декан факультету ІК
Безрук В.М.	д.т.н, зав. каф. ІМІ
Лемешко О.В.	д.т.н., зав. каф. ІКІ
Захаров І.П.	д.т.н., зав. каф. ІМТ

УДК 004:621.391

ПРОБЛЕМИ ІНФОКОМУНІКАЦІЙ

МОДЕЛІ ПОШИРЕННЯ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ ДЛЯ АНАЛІЗУ ПОКАЗНИКІВ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ МЕРЕЖ ЗВ'ЯЗКУ 5 G

М. О. Чурсанов
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії
ім. В.В. Поповського, тел. (057) 702-13-20)
e-mail: mykyta.chursanov@nure.ua факс (057) 702-13-20

The next generation 5G / IMT-2020 technology, like any new technology, brings its own specific features to all aspects of the practice of its application. One of these particularly important aspects is electromagnetic compatibility. At the stage of preparation for the implementation of 5G radio networks, it is necessary to take early measures to effectively assess the EMC conditions for these networks based on a thorough analysis of the features of 5G technology, and by correctly and accurately assessing these conditions, successfully ensure the electromagnetic compatibility of radio equipment of new networks. The purpose of this work is to develop a radio wave propagation model for analyzing the electromagnetic compatibility of a 5G communication network.

Технологія нового покоління 5G/IMT-2020, як і будь-яка нова технологія, привносить свої специфічні особливості в усі аспекти, що стосуються практики її впровадження. Одним з таких особливо важливих аспектів є електромагнітна сумісність (EMC) [1-3]. На етапі підготовки до впровадження радіомереж технології 5G, необхідно завчасно потурбуватися про вжиття заходів щодо ефективної оцінки умов EMC для цих мереж на основі ретельного аналізу особливостей технології 5G, а правильно і точно оцінивши ці умови - успішно забезпечити EMC радіозасобів нових мереж. Метою даної роботи є проведення розробка моделі поширення електромагнітних хвиль для аналізу показників EMC мереж зв'язку 5 G. Одне з основних напрямків по створенню мобільного зв'язку 5G це освоєння частотних діапазонів вище 5 ГГц [2]. Найменше освоєний міліметровий діапазон (ММД) хвиль, тому саме в цьому діапазоні можливий розвиток стандарту 5G. Діапазон міліметрових хвиль вивчений ще не повністю. Тому становить інтерес дослідження можливостей мобільного зв'язку в цьому діапазоні хвиль.

Основні втрати передачі радіохвиль у вільному просторі визначаються виразом:

$$L_в = 92{,}4 + 20\lg(f) + 20\lg(R) \quad , [\text{дБ}] \qquad (1)$$

де R - відстань між передавачем і приймачем, f - частота.

Запропонована модель ослаблення сигналів в радіоканалах ММД, що враховує:

- ослаблення радіохвиль у вільному просторі;
- втрати енергії радіохвиль при поширенні через дощі;
- загасання сигналу ММД при поширенні через листя дерев;
- ослаблення сигналів при проходженні через щільні перешкоди (будівлі, споруди, тощо).

Модель представлена виразом:

$$L = L_в + kR(K_d Y^a + l_T V_T) + 0{,}2 f^{0{,}3} r^{0{,}6} + L_M \text{ ,[дБ]} \quad (2)$$

де k - коефіцієнт, що визначає наявність чи відсутність опадів, Y - інтенсивність опадів, мм/ч, K_d - параметр, що залежить від частоти, температури, поляризації дБч/м2, a - безрозмірний параметр, що залежить від частоти, температури, поляризації, l_T - питомий погонний коефіцієнт ослаблення сигналу ММД в тумані, V_T - коефіцієнт вмісту води в атмосфері, r - глибина шару листя, що перекриває, м, L_M - загасання сигналу в матеріалах, дБ.

У радіоканалах 5G можуть спостерігатися і часові завмирання [3]. Їх основною причиною є доплеровська зміна частоти при русі абонентів відносно один одного. Якщо мобільна станція переміщається, то через доплерівський зсув частоти сигнал зазнає спотворення. При наближенні абонентів зв'язку, зміна частоти визначиться виразом:

$$f = f_0 \left(\frac{C + U_{пр}}{C - U_{пер}} \right),$$

де f_0 - несійна частота, $U_{пр}$, $U_{пер}$ - швидкості руху приймача і передавача, C - швидкість поширення радіохвиль.

При віддаленні абонентів один від одного доплеровська зміна частоти визначається виразом:

$$f = f_0 \left(\frac{C - U_{пр}}{C + U_{пер}} \right).$$

Загасання сигналу в дощах визначається виразом:

$$L_d = K_d Y^a .$$

Список літератури:

1. 5G PPP Architecture Working Group white paper, "View on 5G Architecture," July 2016.

2. Бородин А. С. Сети связи пятого поколения как основа цифровой экономики / А.С. Бородин, А.Е. Кучерявый // Электросвязь .— 2017 .— №5 .— С. 47-51.

3. Бабков В.Ю. Сети мобильной связи. Частотно-территориальное планирование/ В.Ю. Бабков, М.А. Вознюк, П.А. Михайлов //М.: Горячая линия – Телеком. - 2007. - 224 с.

DECENTRALIZED LOAD BALANCING IN CLOUD COMPUTING TECHNOLOGIES

Master student Samad Habib Suhel
Supervisors - PhD Kadatskaja O.,Saburova S.
Kharkov National University of Radio Electronics
(61166, Kharkov, Nauka Avenue, 14, Info communication Engineering Department, tel. (057) 702-13-20),
E-Mail: tkc@kture.kharkov.ua fax (057) 702-13-20

In this work is studied of are load balancing algorisms cloud computing platform technologies. Presenting a review of the challenges related to SDN that are discussed the use of load balancing.

As emerging new technologies, such as cloud computing and with increasing their users, as well, managing the works is difficult. To address this issue, software-defined network (SDN) has been proposed, which makes network management more conformable. Order to maximize the efficiency and reliability of network resources due to limited network resources must be considered is load balancing issue that serves to distribute data traffic among multiple resources.
SDN controllers have a global view of the network and can produce more optimized load balances Load balancing is a technique to divide the workload onto
multiple resources in order to avoid overload on any of the resources . Maximizing throughput, minimizing response time and optimizing traffic are some of the load balancing

SDN load balancing methods are more accurate and have higher performance. In SDN associated research, load balancing issue is one of the most important issues because of industry concerns [1].The most significant qualitative parameters for load balancing in the SDN described.
Over the past years distributed computing has become much more advanced and there are many types of environments that are available for large scale applications. However scheduling applications in these environments still has a lot of issues, such as the decision process for allocating resources. Content aware load balancing uses the content requested to schedule a specific request.
Is evaluated a load balancing algorithm parameters are required and compare it with previous methods in order were indicated the better load balancing algorithm. The most significant qualitative parameters for load balancing in he SDN are described as follows.

An average number of synchronizations per minute-Cumulative frequency. Degree of Load Balancing, Energy Consumption, Execution Time, Forwarding Entries, Guaranteed Bit Rate (GBR), Latency, Migration, Cost, Response Time, Peak Load Ratio, For route Throughput, Workload, Root Mean Squared Error (RMSE).

Overload Ratio (OLR), in networks. In the LTE networks, OLR of a cell is defined in a specific period by employing its resource block utilization and QoS satisfaction of GBR User Equipments (UEs).
Packet Loss Rate: Packet loss happens when one or more packets of data do not reach their target. It usually results from network congestion. It is the percentage of packets lost regarding packets sent. Also, packet loss rate is the rate of packets loss
Detailed analysis of the resource topology of a load-balanced network infrastructure, as well as its attractors, trajectories, and state spaces, provides an open source toolkit that is compatible with available rendering metrics.

A new approach to load balancing is proposed as a Traffic Route Optimization (TMO) to dynamically balance the business time workload on a cloud computing platform. Analyzed the indicators of the probability of movement in the network with the optimization of the traffic route. To improve load balancing efficiency as well as network performance, there are major critical issues that need to be addressed.

The proposed strategy takes into account three factors that affect pheromone renewal, namely pheromone evaporation, task renewal, and incentives for successful tasks [2].The pheromone in the node decreases over time due to evaporation. It is proposed to use a local update strategy, where the pheromone is not equal to zero, in order to modify the pheromone at the slave nodes, in order to renew pheromones, this is an increase in the value of pheromones for subordinate nodes, which are associated with good conditions, and a decrease in those associated with bad parameters. Can set at least 2 requirements for performing tasks on a slave server: incentives, punishment. The first requirement is that the pheromone in this node increases if all tasks are performed with high quality network performance. The second requirement is that the pheromone in this node decreases if the tasks are performed with poor network performance.

By simulation of dynamic load balancing using traffic route optimization shown minimum number of iterations and the convergence time to achieve load balancing, which means that it is possible to achieve the optimal state using such parameter settings. Can later using this group of parameter settings for subsequent simulations. The degree of load balancing for the description of the results should match the level of balancing of the virtual machine in the cloud platform.

References

1.http://www.cablefree.net/wirelesstechnology/4glte/rsrp-rsrq-measurement-lte
2.http://www.techplayon.com/rsrp

ВИКОРИСТАННЯ СТЕКУ ПРОГРАМ ELK STACK ДЛЯ ВИРІШЕННЯ ПРОБЛЕМ, ЩО ВИНИКАЮТЬ У СФЕРІ ІНТЕРНЕТУ РЕЧЕЙ

Токар Д. І.
Науковий керівник – д.т.н., доцент Морозова О. І.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
61070, Харків, вул. Чкалова, 17, кафедра комп'ютерних систем,
мереж і кібербезпеки,
e-mail: d.tokar@student.csn.khai.edu, тел. (063) 667-98-50

The concept of the Internet of Things, the basic principles and the problems of the implementation are seen. It has been announced that the principle of IoT technology allows the solutions integration that are necessary for the function in in various spheres of activity and human life. Warehouse of ELK Stack components for IoT tasks was analyzed. It has been reported that software logs are created in information systems to collect statistics, useful data and others.

Глобальна інфраструктура інформаційного суспільства – Інтернет речей (Internet of Things, IoT), що забезпечує передові послуги за рахунок організації зв'язку між речами на основі інформаційних та комунікаційних технологій, що існують й розвиваються, міцно увійшла в нашу повсякденність. Ця концепція є невід'ємною частиною сучасного інфокомунікаційного суспільства. На основі IoT реалізовані значна кількість розумних додатків в різних сферах діяльності й життя людини. Найпоширенішим прикладом IoT є технологія «розумний будинок».

Поряд з вибором технологій, що є основою IoT, систем автоматизації та багато іншого, важливим завданням в рамках вибору архітектури IoT є вибір інформаційної системи, так званої IoT платформи, в складі якої розрізняють наступні ієрархічні рівні: базу даних, аналітику, візуалізацію, обробку та управління діями, управління пристроями, зв'язок та нормалізацію [1].

Таким чином, основне питання полягає в виборі платформи з розширеними можливостями збору, передачі, обробки інформації, забезпечення інформаційної безпеки, моніторингу та аналітики зібраних даних, що й визначає актуальність даної публікації.

Одним з продуктів, які оперативно можуть працювати з такою кількістю даних, слід зазначити стек ELK (Elasticsearch, Logstash та Kibana). Кожен з цих інструментів є повноцінним незалежним open source продуктом, а разом вони складають потужне рішення для широкого спектру завдань збору, зберігання та аналізу даних.

Для збору статистики, корисних даних тощо, в інформаційних системах створюються журнали програмного забезпечення. Кожна подія, кожна дія

користувача повинні бути записані в такий журнал. Це означає, що за годину може бути згенеровано десятки терабайт цих журналів.

Аналізатори журналів обирають за вхідні дані, що виробляються брандмауерами, маршрутизаторами, IDS та програмами, і перетворюють ці дані на дієвий інтелект. Протягом тривалого часу використовувалися основні інструменти, такі як grep, awk або perl, щоб виконують аналіз журналів. Однак зі зміною часу та масштабів додатків, попередніх методів вже не вистачає. Правильний аналіз журналів може допомогти інженерам DevOps, системним адміністраторам, інженерам із надійності веб-сайтів та розробникам приймати певні рішення.

Аналіз журналів допомагає оптимізувати або налагодити роботу системи та надати суттєві дані щодо вузьких місць у системі, особливо це стосується пристроїв IoT. Оскільки ці пристрої існують у великому географічному масштабі, то дані журналів зіграють вирішальну роль у розумінні поведінки системи. Схему використання журналу наведено на рис. 1.

Рисунок 1 – Схема використання журналів

Стек ELK складається з проектів з відкритим кодом, які беруть дані з будь-якого джерела та будь-якого формату, а потім здійснюють пошук, аналіз та візуалізацію в режимі реального часу. Він пропонує платформу управління журналами наступного покоління, яка вирішує проблеми, пов’язані з неоднорідністю та масштабом журналів. Особливо слід зазначити, що у зв’язку з тим, що великі інформаційні системи генерують величезну кількість службової інформації, яку потрібно десь зберігати, то налаштування сховища для логів на базі ELK Stack є дуже корисним.

Таким чином, можна зробити висновок, що для роботи в інфраструктурі IoT не потрібна велика система, яку можна віднести до категорії BigData і/або HighLoad. З іншого боку, звичні методи збереження та обробки інформації, такі, як запис в текстовий файл або SQL-базу, також не підходять, оскільки велика частина роботи відбувається з логами пристроїв, для яких зручно використовувати ELK Stack.

Література:

1. Five Things to Know About the IoT Platform Ecosystem [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://iot-analytics.com/5-things-know-about-iot-platform.

ВИКОРИСТАННЯ СЕНСОРНИХ МЕРЕЖ У РІЗНИХ СФЕРАХ ЖИТТЯ ТА ДІЯЛЬНОСТІ ЛЮДИНИ

Лісняк О.О.
Науковий керівник – доц., к.т.н. Токар Л.О.
Харківський національний університет радіоелектроніки
61166, Харьків, пр. Науки, 14, кафедра інфокомунікаційної інженерії ім В.В. Поповського, тел. +380509400704,
e-mail: oleksandr.lisniak@nure.ua

You can see the advantages of wireless sensor networks, basic concepts and principle of construction. A wide range of uses touch networks for human life and activities has been examined. The necessity for the usage of such networks in difficult conditions and in the absence of wired communications has been proven. Possibilities of using WSN in case for the transmission of various types of traffic and for the localization of large objects have been listed.

Під сенсорною мережею (WSN – WireleM Sensor Network або Ubiquitous Sensor Network – USN) розуміють мережу на основі стандартів IEEE 802.15. 4 / ZigBee / 6LoWPAN, з низькою швидкістю передачі даних і наднизьким енергоспоживанням. Така мережа за допомогою малогабаритних інтелектуальних сенсорів та пристроїв, які об'єднані в безпровідну мережу, утворює розподілену самоорганізовану мережу, переваги якої полягають в оперативності та економічності розгортання тривалої автономної роботи (при використанні відповідних алгоритмів), відсутності необхідності в технічному обслуговуванні та надійності роботи в жорстких умовах експлуатації і т.д.

У наш час сенсорні мережі вже отримали свою сферу використання в цивільній життєдіяльності та зайняли дуже важливу позицію повсякденного життя сучасної людини, що й обумовлює актуальність даної публікації.

Зараз сенсорні мережі задіяні у таких сферах як: моніторинг навколишнього середовища, охорона здоров'я, контроль руху об'єктів у просторі та багато інших.

Сучасні сенсорні мережі надають можливість розгортання в складних умовах, завдяки відсутності провідних комунікацій і мінімальних розмірів сенсорних пристроїв, технологія сенсорних мереж є надзвичайно гнучкою і практичною.

Використання WSN для передачі мови може бути затребуване в наступних програмах:

– організація зв'язку і передача голосових команд всередині обмеженої оперативної групи, в умовах великої територіальної розосередження і мобільності членів групи, а також забезпечення прихованої роботи і вимог довготривалої роботи передавачів без можливості підзарядки акумуляторів

(групи спеціального призначення, оперативного реагування, групи пожежних, пошуково-рятувальні групи, та інші);

– організація голосового зв'язку на основі вже існуючої інфраструктури WSN, з метою мінімізації витрат, але розгортання нової мережі для передачі голосу (наприклад, коли вже є розгорнута корпоративна мережа на обмеженій території);

– організація дешевого безпровідного голосового зв'язку на територіях з невеликим покриттям (наприклад: на території промислового підприємства, всередині будівель, в межах селища та інші).

Основними сферами використання сенсорних мереж для передачі телеметричного трафіку є:

– дослідження природи (стеження за атмосферними показниками, спостереження за рівнем води в водоймах, реєстрація вулканічної активності і тд);

– комунальне господарство (спостереження за водопостачанням, електроенергетикою і т.д.).

Можливості застосування сенсорних мереж для локалізації об'єктів дуже великі з огляду на невелику вартість розгортання системи і досить високу точність визначення місцеположення – сучасні пристрої забезпечують точність від декількох сантиметрів до одного метра та викорсистовуються в таких місцях як:

– морські порти і контейнерні майданчики (стеження за перебуванням та переміщенням контейнерів);

– склади і логістика (стеження за перебуванням та переміщенням автомобілів та вантажів на складських майданчиках), та ще багато інших

Зупинимося на деяких найбільш часто використовуваних варіантах застосування сенсорних мереж для автоматизації будівель:

– контроль стану навколишнього середовища всередині і зовні будинку (температура, тиск, вологість і т.д.);

– управління освітленням (наприклад, реагування освітлення на присутність людини);

– контроль доступу в приміщення;

– стеження за статусом місць загального користування;

– пожежна сигналізація.

Виходячи з цього впровадження безпровідних сенсорних мереж породжує цілий ряд нових моделей навантаження, для дослідження яких потрібно застосувати в якості базових: моделі самоподібних процесів, моделі тандемних мереж масового обслуговування та інші.

Перелік джерел:

1. А.В.Прокопьев. Самоподобие нагрузки в безпроводных сенсорных сетях для приложений сбора данных. 65-я Научно-техническая конференция. Апрель 2010. С-Петербург издательство СП6 ГЭТУ «ЛЭТИ».

2. А.Е.Кучерявый, А.И. Порамонов. Сети связи общего пользования. Тенденции развития и методы расчета. М:ФГУП ЦНИС. – 2008.

MODERN METHODS OF SECURE SOFTWARE CREATING

Andrii Zhuravka, Denis Zhuravka, Okwudili Gene Onukaogu
Науковий керівник – проф. Журавка А.В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20
e-mail: andy_zhuravka@ukr.net.

Security is a critical part of web applications and must be considered from the first stage of the development process. In fact, security is all about protecting your property from unauthorized actions, and several mechanisms are used to ensure it, including user identification, issuing or revoking access rights to important resources, as well as protecting information stored on the server and transmitted over the network. In all these cases, some fundamental platform is needed to provide basic security functionality. ASP.NET meets this need with built-in tools that you can use to secure your applications.

The ASP.NET security framework includes classes for authenticating and authorizing users, and for handling authenticated users in applications. It also includes a high-level model for managing users and roles, both programmatically and using administrative tools. Moreover, the .NET Framework itself provides a set of base classes for ensuring confidentiality and integrity through encryption and digital signatures.

While the security framework offered by .NET and ASP.NET is powerful enough, it is worth keeping the basic principles in mind and using these tools correctly at the right time. In too many projects, security concerns are belated; architects and developers don't think about it early on in a project. But if you do not take security into account from the very beginning, namely, when developing a design solution and an application architecture, then how can you correctly and timely use the protections offered by the .NET Framework?

Thus, it is important to consider safety issues from the first moment of operation. This is the only way to make the right security decisions during the architecture and design process.

Now let's look at the advanced concept of potential threats. Creating a secure architecture and design requires a deep understanding of the application environment. You will not be able to build secure software if you do not know who has access to the application and where the vulnerabilities are for attacks. Thus, the most important factor in creating a secure software architecture and design is a good understanding of environmental factors such as users, entry points and potential threats with attack points.

This is why threat modeling is becoming increasingly important in today's software development process. Threat modeling is a structured way of analyzing an application's environment in terms of potential threats, classifying threats and deciding on mitigation techniques. With this approach, decisions about security

technologies (such as authentication and SSL encryption) always have a valid basis - a potential threat.

However, threat modeling is important for another reason. As you may be aware, not all potential threats can be mitigated by the use of security technologies such as authentication and authorization. In other words, some of them are technically impossible to resolve at all.

For example, an online banking solution might use SSL to secure website traffic. But how can users know that they are indeed using a bank page and not a hacker fake website? So, the only way to be sure of this is to verify the certificate used to set up the SSL channel. But users must be warned about this, and therefore you must inform them in some way. Therefore, threat mitigation techniques are not only defense technologies. It includes a requirement that all users know how to validate a certificate. (Of course, you cannot force them to do this, but if the system is designed appropriately, you can still encourage most of them to do so). Threat modeling is an analysis technique that can help identify circumstances like these.

SSL (Secure Sockets Layer) technology encrypts communications over HTTP. SSL is supported by a wide range of browsers and ensures that the transmission of information between the client and the web server cannot be decrypted by intruders.

SSL is required to hide sensitive information such as credit card numbers and confidential information of an internal nature, but it is also important for user authentication. For example, if you create a signup page where a user submits their username and password, you must use SSL to encrypt this information. Otherwise, an attacker can intercept the user's identity and use it to penetrate the system.

The IIS web server provides SSL as a built-in, ready-to-use service. Since SSL works under HTTP, its implementation does not change the way that HTTP requests are handled. All encryption and decryption is handled by the SSL functionality of the web server software (in this case, IIS). The only difference is that the SSL secured address starts with https: //, not http: //. SSL traffic also goes through a different port (typically web servers use port 443 for SSL requests and port 80 for regular requests).

For a server to support SSL connections, it must have an X.509 certificate installed (the name X.509 was chosen to comply with the X.500 directory standard). To implement SSL, you need to purchase a certificate, install it, and configure IIS accordingly. All of these steps are detailed in the following sections.

Finally, while authentication and authorization are two critical factors in building secure applications, there is much more to consider. The point is that .NET has some useful functionality in store. One of the most important examples is support for cryptography - the science of encrypting data to ensure privacy and adding hash codes to detect tampering.

MODERN METHODS FOR DETECTING AND ANALYSIS OF MALWARE SOFTWARE

Andrii Zhuravka, Denis Zhuravka, David Ogamune
Науковий керівник – проф. Журавка А.В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20, e-mail: andy_zhuravka@ukr.net.

One of the most important tasks of computer security is the fight against malicious software (malware) and, in particular, the subtask of its detection. All detection methods can be divided into 2 types: methods for detecting known malware and methods for detecting unknown malware. In light of the current trends in the development of malware, the task of creating an effective means of detecting unknown malware is becoming more and more urgent. The author is working to create a similar tool.

The purpose of the development is to improve the detection efficiency by improving existing techniques. An analysis of the available techniques was carried out in order to identify their characteristics. The method for detecting unknown malware can be described using the following parameters: data obtained about the software under investigation, methods for obtaining this data, mathematical methods used for data analysis, and detected signs of harmfulness. The combination of these parameters determines the main characteristics of the technique: the level of errors of the first and second kind, resource intensity, computational complexity, algorithmic complexity (labor intensity of implementation), etc. Therefore, the constructed classification considers the techniques in the context of each of these parameters. Classification by the nature of the data received. By the nature of the data obtained, the methods are usually divided into structural analysis and behavioral analysis. Structural analysis takes into account the fact that some types of malware (for example, viruses) have distinctive features in their structure: the location of the entry point, specific command sequences, as well as many signs found in the so-called heuristic analysis. This type of analysis mainly detects indirect signs of malware, which do not directly indicate malware, but are rarely observed in useful software. In most cases, structural analysis is very fast (due to its low computational complexity). The main disadvantage of this approach is that not all types of malware are structurally different from useful software. Thus, not all types of malware can be detected by this method. Also, this category includes techniques that analyze the binary similarity of the software under investigation and known malicious programs. But in practice, these techniques do not give acceptable results. Behavioral Analysis examines the actions performed by software and their consequences. Such methods determine the harmfulness of programs by the same characteristics as a person - by their behavior. Ideally, a system that implements this approach is capable of protecting against any malware, but in practice it is

impossible to create such a system. On the one hand, tracking all software actions is an algorithmically complex, resource-intensive and, in some cases, impossible task. On the other hand, it is impossible to fully formalize the concept of "harmful behavior". In practice, such techniques monitor a limited set of actions performed by software and try to identify a limited set of signs of harmfulness in them. Thus, The advantages of behavioral analysis include the theoretical possibility of detecting any type of malware, as well as the possibility of detecting malware at the time of a malicious action, and the disadvantages - the practical impossibility of complete control of the system, resource consumption (the more control, the more the entire system slows down). Among the frequently discussed problems of behavioral analysis, one can indicate the issue of completeness of information obtained about software, as well as the problem of analyzing the flow of information with different requirements. The question of completeness of the information received mainly arises when trying to find out all the possible actions that the program can perform. This issue is especially acute when the so-called "temporary bombs" are detected. This type of malware performs malicious actions only under certain conditions, for example, on a specific date. Thus, if this condition is not met, the behavioral analyzer will not be able to detect such malware, and it will distribute itself freely. Some types of behavioral analysis impose their own requirements on the methods of analysis. So to study the flow of execution (for example, analyzing system calls on an end user's computer), methods are needed that will analyze it as data arrives for a guaranteed period of time. Otherwise, the antivirus will slow down the system, thereby interfering with the user. Classification by the method of obtaining data. The existing methods for detecting unknown malware can be divided into two categories by the method of obtaining data about the software under investigation: methods that execute and do not execute the program code. Techniques that do not execute program code are mainly used in structural analysis, so their main advantages and disadvantages are the same. The main drawback is the impossibility of detecting malware, the peculiarities of which appear only when the code is executed. The main advantages of this approach are high speed, low resource consumption and safety of use. In addition to the fact that these methods allow you to relatively quickly detect some types of malware, they can speed up the work of other methods. Thus, the method of determining changed files by checksums, also related to this type, allows you to speed up software analysis using other methods, for example, not to re-analyze the file if it has not been changed. Techniques that execute program code are mainly used in behavioral analysis. These techniques include collecting data while executing software on a real system (for example, a user's computer or honeypot), collecting data when executing software on emulators, and mixed methods. Therefore, each of these subspecies has its own advantages, disadvantages and areas of application.

ANALYSIS OF MODERN INTERNET INFORMATION SERVICES AND THEIR OPTIMAL SETTINGS

Andrii Zhuravka, Denis Zhuravka, Ethel Chila
Науковий керівник – проф. Журавка А.В.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20, e-mail: andy_zhuravka@ukr.net.

The main information services of the Internet are the World Wide Web, file transfer service, file sharing service. The main communication services include email, forum, chat, and IP telephony. Each Internet service has its own server program, client program, and its own protocol that ensures the interaction of the client program with the server. You can use any Internet service only if the corresponding software (client program) is installed and configured on your computer.

Obviously, there can be only two modes of communication in the network: the mode of direct communication in real time, when users are connected during communication. An analogue of such communication is a telephone conversation. Sometimes the term on-line is used to refer to this mode. Another mode is the off-line mode. An example of such communication in everyday life is sending a letter or telegram.

This system allows Internet and Intranet users to chat in real time. To receive this service, users must join channels that support different topics of discussion. Any characters entered through the IRC program appear on the screens of everyone else on your channel. It is the oldest and one of the most popular services on the Web. Its purpose is to support the exchange of emails between users. By its very nature, e-mail is an electronic messaging system in computer networks (in the offline mode). A mail server is a kind of post office where incoming and outgoing correspondence of registered users is received. The server and the e-mail client work under different protocols. The server program POP3 (Post Office Protocol), among other things, performs the function of protecting information. During a communication session, it establishes the identity of the user, provides communication with one personal box. No identification is required when running the client program. Its task is to send outgoing letters to the server and receive incoming ones. It uses the simpler SMTP (Simple Mail Transfer Protocol). Teleconference is a system for exchanging electronic messages on a specific topic between network subscribers (in the deferred communication mode - offline). Each participant receives all materials to one postal address (E: mail). Each subscriber e-mail is published on the teleconference server and reaches all participants.

Information services provide users with the ability to access certain information resources stored on the Internet. These resources are either files in one of the generally accepted formats, or various documents. The use of these

resources is provided through the appropriate services. This service is often referred to by the name of the protocol used: FTP (File Transfer Protocol). From the Network side, the service is provided by the so-called FTP servers, and from the user side - FTP clients. The purpose of the FTP server is to store a set of files of various purposes (usually in archived form). Most often these are program files: system and application software tools. But the sets can store files of any other formats: graphic, sound, MS Word documents, MS Excel, etc. All this information forms a hierarchical structure of folders (directories and subdirectories). A file sharing service is a service that provides the user with a place to store his files and round-the-clock access to them via the web, usually via the http protocol (and possibly via FTP). This service allows you to conveniently "change" files.

WWW is a distributed information system with hyperlinks, existing on the technical base of the world computer network Internet. This information system is a network of documents linked by hyperlinks. Such documents are called hypertext documents. Since links can point to any document on the Internet anywhere in the world, this system is called the World Wide Web. The smallest information unit of the WWW is a Web page, which is a collection of text, graphic and multimedia files linked by hyperlinks. A group of web pages, owned by the same owner and related to each other in content, make up a web site. A host is a computer that stores Web pages and Web sites is called a Web server. A client program designed to view Web sites is called a browser (from English browse - to view, scroll). Electronic payment systems allow you to pay for a wide range of services, in particular, to make utility bills. The scheme by which electronic payment systems work is extremely simple for the user. By registering in the system, you automatically open your account. Having credited the required amount of money to it in a convenient way, you can use it for settlements with partners of this system. This service provides interaction with a remote computer. It allows you to turn a user's computer into a remote terminal of another computer. Therefore, this service is also called remote terminal emulation. The terminal differs from an ordinary computer in that it does not perform its own calculations. Everything that is entered on the keyboard of the workstation is sent to the remote computer, and the results are sent back and displayed on the monitor of the workstation. As remote computers, machines running under the UNIX operating system are mainly used. Therefore, working in the remote terminal mode requires knowledge of the basic commands of this operating system. With the development of graphical operating systems such as Windows, the command mode has become less popular, and most users do not use the Telnet service recently.

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА СТАНДАРТОВ СЕТЕЙ IP-ТЕЛЕФОНИИ

Холобок В.И.
Научный руководитель – доц., к.т.н. Токарь Л.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Инфокоммуникационной
инженерии им. В.В. Поповского, тел. 0997492578
e-mail: vladyslav.kholobok@nure.ua

The basic principles of building IP-telephony networks, their advantages over traditional telephone networks are considered. The most commonly used protocols, the composition of the equipment of networks built on the basis of the H.323, SIP and MGCP protocols are described. Some typical problems associated with the use of these protocols are analyzed. A comparative characteristic of IP-telephony networks operating on the basis of the considered protocols is carried out.

На сегодняшний день сети IP-телефонии все больше вытесняют традиционные телефонные сети за счет легкости развертывания, низкой стоимости звонка, простоты конфигурирования, высокого качества связи и сравнительной безопасности соединения.

Для построения сетей IP-телефонии применяется несколько различных подходов, отличающиеся составом оборудования, принципами установления соединения, совместимостью устройств и др. Актуальность данной публикации определяется особенностями сетей, построенных на основе популярных протоколов VoIP.

Сети на базе протоколов H.323 ориентированы на интеграцию с телефонными сетями и могут рассматриваться как сети ISDN, наложенные на сети передачи данных. Основными устройствами сети являются: терминал (Terminal), шлюз (Gateway), привратник (Gatekeeper) и устройство управления конференциями (Multipoint Control Unit - MCU). Семейство протоколов H.323 включает в себя три протокола составляющие его основу:

- протокол RAS (Registration, Admission and Status) – протокол взаимодействия оконечного оборудования с Gatekeeper (привратником);
- H.225 – протокол управления соединениями;
- H.245 – протокол управления логическими каналами.

H.323 включает также такие стандарты кодирования речи, как G.711, G.722, G.723.1, G.728 и G.729, из которых G.711 является основным.

SIP – является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи (мультимедийных конференций, телефонных соединений и распределения мультимедийной информации), в основу которого заложены следующие принципы:

– персональная мобильность пользователей. Пользователи могут перемещаться без ограничений в пределах сети;

– масштабируемость сети;

– расширяемость протокола;

– интеграция в стек существующих протоколов Интернет;

– взаимодействие с другими протоколами сигнализации.

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. В качестве транспорта могут использоваться протоколы X.25, Frame Relay, AAL5, IPX и др.

Сети, построенные на основе протокола MGCP, созданы по принципу декомпозиции, согласно которому шлюз разбивается на отдельные функциональные блоки:

– транспортный шлюз - Media Gateway, который выполняет функции преобразования речевой информации.

– шлюз сигнализации - Signaling Gateway, который обеспечивает доставку сигнальной информации.

Весь интеллект функционально распределенного шлюза размещается в устройстве управления, функции которого, в свою очередь, могут быть распределены между несколькими компьютерными платформами. Одно из основных требований, предъявляемых к протоколу MGCP, состоит в том, что устройства, реализующие этот протокол, должны работать в режиме без сохранения информации о последовательности транзакций между устройством управления и транспортным шлюзом.

На сегодняшний день нет четкого стандарта, указывающего работу протоколов IP-телефонии.

На данный момент SIP протокол стал основополагающим в оборудовании IP-телефонии, в первую очередь за его лаконичность и простоту. Недостатком же протокола H.323 послужила его сложность и привязанность к медиа данным в отличии от SIP. Протокол MGCP поддерживает различные системы сигнализации сетей с коммутацией каналов, включая тоновую сигнализацию, ISDN, ISUP, QSIG и GSM. Закреплен как стандартный протокол IMS, наряду с SIP и Diameter. Используется в основном сетях провайдера IMS платформ.

Литература:

1. Романчева Н.И. Современные Интернет-технологии: Учебное пособие. - М.: МГТУ ГА. - 2007. – 104 с.

2. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-телефония. - М.: Радио и связь. - 2001. – 336 с.

3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер. - 2006 – 958 с.

USE OF DIRECTION FINDERS BY GOVERNMENT INTELLIGENCE AGENCIES

Pershyn I. V.
Scientific supervisor – D.Sc., prof. Kartashov V. M.
Kharkiv National University of Radio Electronics
MEIRES Department, 14, Nauky Ave., Kharkiv 61166, Tel. (057) 702-15-87
e-mail: yevhenii.pershyn@nure.ua

With the expansion of cellular technology over the last 15 years, there has been no way to accurately determine the location of a mobile terminal by government intelligence agencies, even with the help of telecom providers. The thesis is devoted to special devices called direction finders, which help the agencies to find a precise location of cellular terminals.

Every person has a mobile phone nowadays. Every criminal, even if they use secure applications to chat, rely on a standard phone with a subscriber identification module (a SIM card) and it is unlikely to find out the location of its phone. Intelligence agencies need to find the exact location of mobile terminals to detain criminals. They cannot ask a telecom provider to give them an accurate location immediately. Firstly, a precise location is not to be obtained from telecom providers in GSM networks. They can provide only a cell tower location information. Secondly, in order to ask the telecom provider, permission from court must be requested. An estimated location provided could be in a 1 km radius. There is a problem to find a more accurate location in the 1 km circle of the estimated location.

There is a way to solve the problem. Many different approaches to determining the origin of a radio transmission exist nowadays. One of them is a technique that allows finding the precise location of a mobile terminal. Every cellular phone has a transmitter that emits a signal to reach a base transceiver station. The technique is to receive this signal by a handheld device and to compare its receiving level from different locations. The higher the signal level the closer the handheld device is to the target terminal. However, several questions may arise:

- how to ask a target terminal what frequency it uses;
- how to filter out signals from other mobile terminals on the same frequency;
- how to be sure that the terminal is emitting signals continuously;
- how to determine from which direction the signal is coming.

Such cellular modules, which are used in mobile phones, can also be used in UAV to control their flight from a ground station on long distances. The technology of direction finding can be used by militaries too.

In order to answer the first three questions, the explanation follows. There is a technology that allows you to run a cellular stack on a software-defined radio platform. Running a specific protocol stack enables to run your own base transceiver station. If you specify a mobile country code (MCC), a mobile network code (MNC) and an absolute radio-frequency channel number (ARFCN) of a local telecom provider, you will be able to catch identifiers of mobile terminals around, authenticate them to be a service base transceiver station and send them to a specific ARFCN to have a clear channel for a direction finding procedure. It will not be very suspicious for the target terminal as you will use the same MCC and MNC codes as its SIM card provider. To be sure that the terminal is emitting signals continuously, the operator of the SDR based system establishes a special connection asking the target terminal to emit its maximum power continuously on a specific frequency. As soon as the signal transmission between this system and the target terminal is established, the direction finding device operator puts the required ARFCN value to the control software to tune the device. After that, the direction finder is able to see the signal coming from the target terminal continuously. Direction finders look like a portable device with or without a small display on it. The ones without a display usually have a Bluetooth module to be controlled remotely from a smartphone. Sound indication of the signal strength is audible in headphones.

To answer the fourth question, the procedure of direction finding is stated below. A directional antenna has to be connected to an antenna port of the direction finder. By rotating the antenna, to the left or right, the measured signal strength reading can be improved or reduced on the control software of the device, which allows the operator to hear an increased or decreased sound in its headphones. The signal strength will change depending on the distance and direction from the signal source. The maximum level of the signal indicated on a signal bar of the control software is correlated with the target terminal location. On some direction finders, it might be necessary to change a sensitivity value of the device when approaching the target terminal, but some devices have an automatic attenuation control feature. For the manual approach, the operator usually switches the attenuation level from 0 to 60 dB.

The operation range of such devices is usually from 0 to 500 meters. The accuracy achieved could be 1 meter. In a room with several people in possession of mobile terminals, it is possible to determine which of them emits a signal on the specific ARFCN. In a scenario with UAVs remotely controlled by means of cellular communications, it will be possible to determine the precise location of those that collapsed with the help of a direction finder. The cellular module inside the UAVs has to be active. The SDR based system runs a base transceiver station to attach a SIM card located in the cellular modem of the UAV. Then a team searches for the location of the UAV by means of direction finding.

АНАЛІЗ МЕТОДІВ МОДУЛЯЦІЇ У СТАНДАРТАХ IEEE 802.11

Греков І. С., Худяков А. Д.
Науковий керівник – доц., к.т.н. Токар Л.О.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14, кафедра ІКІ ім. В.В. Поповського,
тел. +380950578758, e-mail: grekovv76@gmail.com

802.11 WiFi can use different digital modulation schemes for data transmission. Environmental factors and protocol will define scheme selection. 802.11n, 802.11ac and 802.11ax use the same modulation principles as 802.11g, 802.11b and 802.11a. 802.11x can negotiate up to 1024QAM if the receiver sensitivity permits. In addition to modulation schemes, 802.11n, 802.11ac and 802.11ax pair the modulation scheme with other technologies that enable even faster bit-rates.

QAM – (Quadrature Amplitude Modulation) – метод об'єднання сигналів в одному каналі для підвищення ефективності та підвищення пропускної спроможності.

У самій простій формі QAM – є метод QPSK (Quadrature Phase Shift Keying – квадратурно-фазова модуляція), де використовується дві несучі однакові частоти, зсунуті на 90º ($\pi/2$) і два можливих рівня амплітуди. Один рівень амплітуди відповідає – 0, інший – 1.

Основне застосування в безпроводових локальних Wi-Fi мережах QPSK отримав в стандартах IEEE 802.11b і IEEE 802.11g. Модуляцію QPSK замінила 16-позиційна квадратурна модуляція 16-QAM, що отримала застосування в стандарті IEEE 802.11a.

Зміна модулюючого сигналу по фазі при 16-QAM відбувається в 2 рази рідше, ніж при QPSK-модуляції при однаковій швидкості передачі інформації. За рахунок цього забезпечується підвищення спектральної ефективності у $k = log_2M$ разів, де M – число позицій для багатопозиційних видів модуляції. Тобто, спектральна ефективність модуляції 16-QAM у 2 рази вище, ніж спектральна ефективність QPSK-модуляції.

Аналіз спектральної ефективності найбільш часто використовуємих модуляцій M-QAM і M-PSK дозволяє зробити висновок, що з підвищенням щільності модуляції спектральна ефективність зростає у $k = log_2M$.

У стандарті IEEE 802.11n було запроваджено модуцію 64-QAM. Пропускна здатність підвищилася, як мінімум, в 4 рази в порівнянні з попередніми стандартами.

Перевага високих значень порядку QAM не тільки у спектральній ефффктівності, але і в підвищенні швидкості передачі даних, оскільки таким чином більшу кількість бітів інформації може бути передано в протязі одного циклу передачі.

Стандарт 802.11ac використовує квадратурну модуляцію 256-QAM. У стандарті 802.11ax, специфікація якого була опублікована у 2019 році,

підтримується квадратурна модуляція QAM-1024. Високий рівень модуляції підвищує пропускну здатність за рахунок більш щільного заповнення кожного пакету даних. У 1024-QAM кожен символ містить 10 біт даних – проти 8 біт у 256-QAM та 6 біт у 64-QAM . Таким чином, в порівнянні зі стандартом Wi-Fi 5 (802.11ac), ємність пакета у стандарті 802.11ax, який використовує модуляцію QAM-1024, збільшилася на 25%.

Оскільки передається більша кількість бітів на символ, швидкість передачі даних збільшується. В результаті, теоретична швидкість передачі одного потоку даних в каналі шириною 80 МГц при використанні модуляції QAM-1024 зросла до 600 Мбіт/с, що на 25% більше аналогічного параметра у попередньому стандарті 802.11ac (480 Мбит/с), лише завдяки зміні щильності модуляції QAM. Розрахунок проводився відповідно до формули Найквіста.

У разі підвищення щільності модуляції, рівні амплітуди сигналу розташовуються близько один до одного, підвищуючи тим самим вірогідність нерозрізненості двох рівнів, і як наслідок – підвищуючи чутливість системи до шуму.

У загальному випадку в системах передачі ЦРМ ознакою несправності є зникнення сигналу або перевищення критично допустимої величини коефіцієнта помилок BER. У багатьох системах ЦРМ це значення $BER \geq 10^{-3}$.

При недостатній завадостійкості каналу зв'язку доводиться знижувати кратність модуляції і підвищувати надмірність, при цьому, відповідно, знижується пропускна здатність і, як наслідок, падає спектральна ефективність. Для стабільної роботи безпроводового локального зв'язку Wi-Fi, при використанні найвищої модуляції 1024-QAM, рівень SNR повинен бути ≥ 36 дБ.

Таким чином, резюмуючи вищесказане, підвищення щільності модуляції, у кожному новому поколінні Wi-Fi, позначається на роботі безпроводової мережі лише позитивним чином, особливо ураховуючи той факт, що стандарти Wi-Fi підтримують адаптивну модуляцію сигналу, яка дозволяє змінювати щільність модуляції, ураховуючи рівень завад.

Перелік джерел:

1. Е.А. Шелковина, О.Г. Лебедев. Сравнительный анализ методов цифровой модуляции в стандартах цифрового радиовещания. 2014. – 58 с.

2. R. Wagner, M. Reil. Modulation and signal generation. Modulation Methods. August 2016. – 88 с.

3. Д.Н. Ивлев. Цифровые каналы передачи данных. 2013. – 21-22 с.

АНАЛІЗ АЛГОРИТМУ РОЗПОДІЛУ ЧАСТОТНО-ЧАСОВОГО РЕСУРСУ У МЕРЕЖІ КОГНІТИВНОГО РАДІО

Білик В. О.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії
ім. В.В. Поповського, тел. (057) 702-13-20)
e-mail: vitalii.bilyk@nure.ua

One of the problems that arise when allocating a frequency resource may be the lack of clear decision rules. In such cases, as a rule, nonparametric algorithms and methods are used, such as, for example, algorithms based on the mathematical apparatus of neural networks, or algorithms built on the mathematical apparatus of fuzzy logic.

Для призначення частотно-часових блоків всім АС в багатокористувацьких системах зв'язку широке поширення отримав алгоритм пропорційного справедливого розподілу фізичних ресурсів (Proportional Fair, PF) [1,2]. Відповідно до цього алгоритмому доступ до частотно-часового блоку отримує АС з максимальним значенням метрики , яка визначається виразом:

$$PF_i = \frac{I_i^{'}}{C_i}, \qquad (1)$$

де $I_i^{'}$ - миттєва швидкість передачі даних i-ї АС, - середня пропускна здатність i-ї АС, яка розрахована для деякого часового інтервалу.

У разі встановлення зв'язку відповідна АС повідомляє на БС миттєву швидкість передачі даних $I_i^{'}$ і середню пропускну здатність C_i, розраховану для деякого часового інтервалу. Модуль Fuzzy Logic в середовищі Matlab дозволяє будувати нечіткі системи двох типів - Мамдані та Сугено. Основна відмінність між цими системами полягає в різних способах завдання значень вихідних змінних в правилах, що утворюють базу знань. Для вирішення цієї задачі використаємо алгоритм виведення Мамдані. Для входу ВСЗШ задані три ФП гаусового типу, кожна з яких характеризує вхід, відповідно, як «низьке», «середнє» і «високе» в діапазоні від -10 до 40 дБ.

Для входу PF задані також три ФП гаусового типу, кожна з яких характеризує вхід, відповідно, як «низьке», «середнє» і «високе» в діапазоні від 0 до 1. При цьому PF = 0 при $I_i^{'}$ = 0 і PF = 1 при = $I_i^{'}$ = C_i.

За допомогою розробленої імітаційної моделі проведено аналіз алгоритму розподілу частотно-часового ресурсу в мережі когнітивного радіо.

На рис.7 надано графіки залежності запитуваних ресурсів від ВСЗШ.

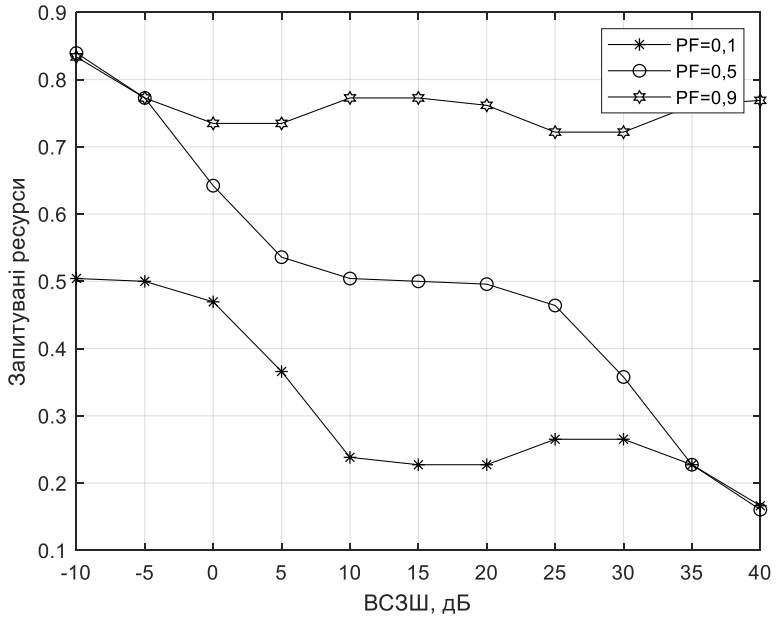


Рис.7. Залежності запитуваних ресурсів від ВСЗШ

Аналіз рис.7 показав, що дуже високу ймовірність надання ресурсу мають АС при повністю доступних ресурсах та запрошуваних ресурсах, які лежать у межах від 0,1 до 0,5. Високу ймовірність надання ресурсу мають АС: при повністю доступних ресурсах та запрошуваних ресурсах, які лежать у межах від 0,56 до 0,69; або при середніх доступних ресурсах та запрошуваних ресурсах, які лежать у межах від 0,1 до 0,19. Середню ймовірність надання ресурсу мають АС: при повністю доступних ресурсах та запрошуваних ресурсах, які лежать у межах від 0,69 до 1; або середніх доступних ресурсах та запрошуваних ресурсах, які лежать у межах від 0,19 до 0,8; або при низьких доступних ресурсах та запрошуваних ресурсах, які лежать у межах від 0,1 до 0,32. Малу ймовірність надання ресурсу мають АС: при середніх доступних ресурсах та запрошуваних ресурсах, які лежать у межах від 0,8 до 1; та при низьких доступних ресурсах та запрошуваних ресурсах, які лежать у межах від 0,32 до 1.

Список літератури:

4. Электромагнитная совместимость радиоэлектронных средств и систем / В.И.Владимиров, А.Л.Докторов и др.; Под ред. Н.М.Царькова – М.: Радио и связь, 1985 – 272 с.

5. Бородич С.В. Защитные отношения для сигналов, используемых в спутниковых системах связи. Труды НИИР № 4, 1990, с. 7 – 11.

3. Управление радиочастотным спектром и электромагнитная совместимость радиосистем. Учебн. пособие / Под ред. д.т.н., проф. М.А. Быховского. — М.: Эко-Трендз, 2006. — 376 с.

ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ЯКОСТІ КАНАЛІВ ВОСП ОПТИЧНОЇ ТРАНСПОРТНОЇ ІЄРАХІЇ

Федоренко А.С., Шамшур І.В.
Науковий керівник – к.т.н., доц. Педяш В.В.
Державний університет інтелектуальних технологій і зв'язку
65029, Одеса, вул. Кузнечна, 1, каф. Телекомунікаційних систем,
тел. (048) 705-03-53
e-mail: andrey.fedorenko@outlook.com

The paper presents the results of a study of quality indicators for channels of fiber-optic transmission systems (FOTS) of the optical transport hierarchy (OTH). For the transmission of digital signals of the OTU2-OTU4 type, it is advisable to use coherent reception methods. Therefore, a study of the qualitative characteristics of channels with QAM-4 modulation was performed. According to the block diagrams of the system, mathematical and simulation models of FOTS were developed. The influence of the power of the transmitter signal and the length of the fiber-optic linear path on the Q-factor of the signal in the receiver is calculated.

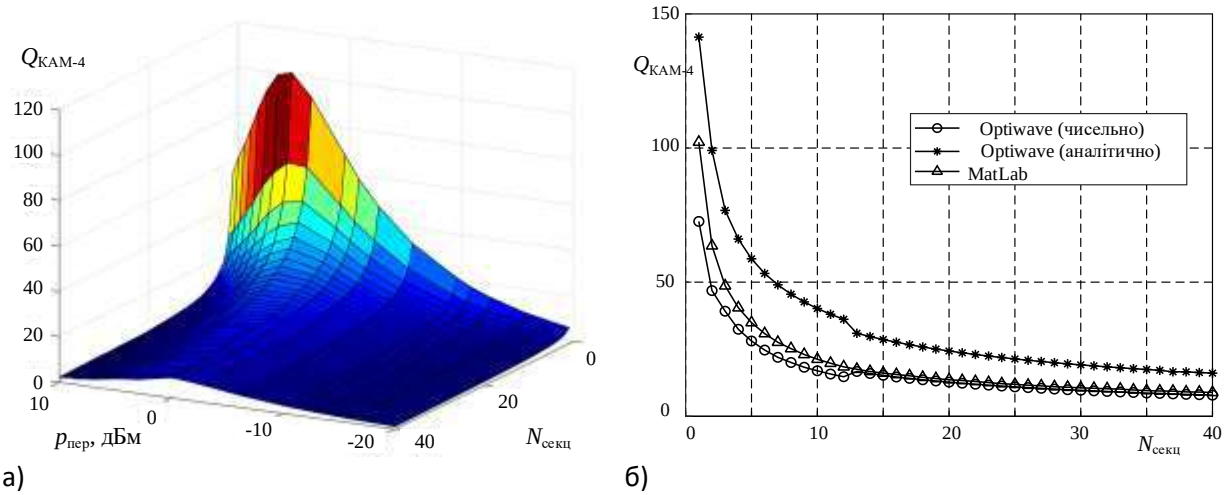
Високошвидкісна передача трафіку в сучасних телекомунікаційних мережах NGN і IMS виконується за допомогою волоконно-оптичних систем передавання. Цифрові системи передавання оптичної транспортної ієрархії (ОТН) дозволяють створювати канали із пропускною здатністю від 2,5 до 100 Гбіт/с, тому дослідження їх характеристик є актуальним завданням. Для збільшення довжини ділянки 3R регенерації доцільно використовувати методи когерентного прийому оптичних сигналів, наприклад, квадратурну амплітудну модуляцію невеликою кількістю позицій (КАМ-М) [1].

Тому метою даної роботи є дослідження параметрів якості (*Q*-фактора) каналу когерентної ВОСП ОТН з модуляцією КАМ-4.

Для вирішення даного завдання в програмі MatLab була розроблена імітаційна модель оптичної системи передачі з квадратурною амплітудною модуляцією (КАМ-4), яка містить передавач, середовище поширення та приймач оптичного сигналу. Модель лінійного тракту ВОСП побудована на базі Фур'є методу розщеплення на фізичні фактори і дозволяє вносити в сигнал лінійні та нелінійні спотворення середовища розповсюдження сигналу [2]. З метою зменшення обчислювальної складності моделі, формування шуму оптичного підсилювача виконувалося шляхом використання зворотного дискретного перетворення Фур'є. Перевірка достовірності розробленої імітаційної моделі виконувалася шляхом порівняння з результатами аналітичних розрахунків та моделювання в програмі Optiwave Optisystem.

Отримано залежності *Q*-фактора (рис. 1, а) від рівня потужності сигналу передавача $p_{\text{пер}}$ та кількості оптичних секцій лінійного тракту $N_{\text{секц}}$. Для збільшення довжини ділянки 3R регенерації запропоновано виконувати

оптимізацію потужності сигналу передавача за критерієм максимізації відношення сигнал/шум у приймачі.



а) б)

Рисунок 1 – Параметри якості каналу ВОСП СРК OTU2 з КАМ-4:
а) залежність Q-фактору від $N_{секц}$ та $P_{пер}$;
б) максимальне значення Q-фактора

Порівняння отриманих результатів показало, що для ВОЛТ з однією секцією похибка моделювання складає 40,7%. Збільшення кількості секцій ВОЛТ з 10 до 20 призводить до зменшення похибки з 25,4% до 7%. Метою дослідження моделі каналу ВОСП СРК є визначення довжини ділянки 3R регенерації, тому встановлений залежності $Q_{КАМ-4}(N_{секц})$ цілком задовольняє поставлену мету з визначення максимальної довжини лінії.

Підводячи підсумки можна вказати, що поставлена мета з дослідження параметрів якості каналу когерентної ВОСП ОТН виконана повністю. Запропоновано методи аналітичного та імітаційного моделювання ВОСП, які доцільно використовувати на етапі проектування системи передавання з метою оптимізації її параметрів та покращення її технічних характеристик.

Список використаних джерел

1. Педяш В.В. Влияние фазовой самомодуляции оптического сигнала на качество каналов ВОСП СРК / В.В. Педяш, О.С. Решетникова // Наукові праці ОНАЗ ім. О. С. Попова. – 2010. – № 1. – С. 109-114.

2. Агравал Г.П. Нелинейная волоконная оптика / Пер. с англ. С.В. Черникова и др. Под ред. П.В. Мамышева. — М.: Мир, 1996. — 323 с.

МОНІТОРИНГ ПОСЛУГ NB IoT (LTE)

Кухарчук М.М.
Науковий керівник – доц. Сабурова С.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14,
Кафедра Інфокомунікаційної інженерії ім. В.В. Поповського,
тел. (057) 702-13-20) e-mail: mark.kukharchuk@nure.ua,
факс (057) 702-13-20

Abstract. Methods of quality control of NB-IoT (LTE) services presented. One way to improve the performance and quality of IoT services is the NB-IoT protocol, which uses the potential of modern mobile networks. Methods of monitoring and testing the quality of NB-IoT deployment are considered. The method of calculation and estimation of parameters of quality of access to NB IoT LTE services is presented. NB-IoT is a technology of mobile communication based on LTE, designed for stationary outbuildings with low fees transferred to energy services. The NB-IoT standard is shown to companies that specialize in telecom services, a wide range of new features.

Інноваційною технологією Інтернету речей є рішення вузько-смугового IoT (Narrow-Band Internet of Things або NB-IoT). Це безпроводовий вузько-смуговий різновид глобальних мереж з низьким енергоспоживанням (Low Power Wide Area, LPWA), який в першу чергу призначен для додатків між-машинної взаємодії (M2M).

Стандартом для NB-IoT виділяються ресурси всередині існуючої LTE несучої, але NB-IoT несуча має підвищену потужність на 6дБ в порівнянні з ресурсними блоками LTE. Цей варіант добре підходить для моніторингу економії частотного ресурсу, але при цьому є проблема взаємного впливу з LTE-мережею (рис.1).

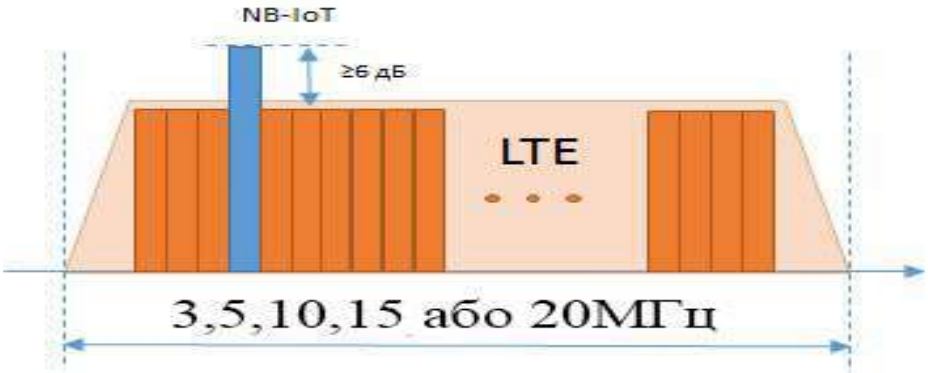


Рисунок 1 – Розміщення NB-IoT в режимі in-band на LTE мережі

Компанія Київстар спільно з Microsoft першою серед мобільних операторів в Україні запропонувала українським бізнес-клієнтам хмарну платформу Microsoft Azure. Тепер клієнти зможуть розміщувати дані в

межах України при розробці та адмініструванні програм і розгортанні LTE-інфраструктури компанії (рис. 2).

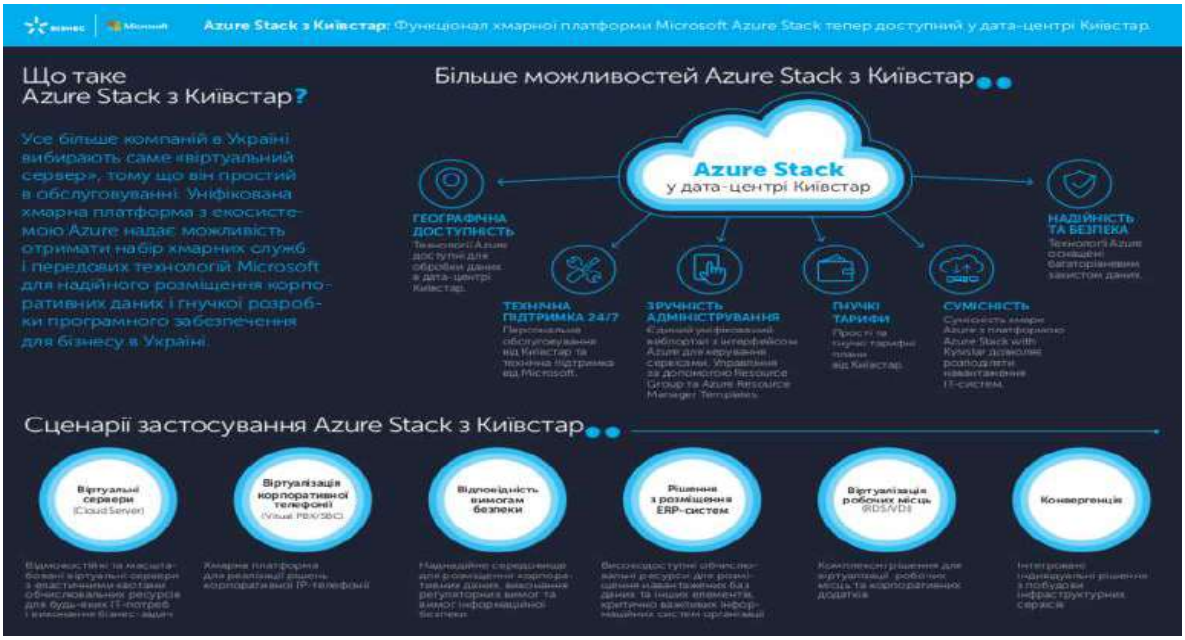


Рисунок 2 - Сценарій застосування Azure Stack на мережі NB-IoT LTE

Завдяки доступу до хмари Microsoft Azure, який пропонує Київстар, клієнти зможуть розробляти і впроваджувати гібридні хмарні додатки для бізнесу, застосовувати методики DevOps. Бізнес-клієнти Київстар можуть замовити як підключення до NB-IoT LTE, так і «розумні» пристрої і програмне забезпечення для моніторингу та управління.

Звісно, що в 2018 році компанія Київстар запустив ряд IoT-продуктів, зокрема, IoT-автосигналізацію «автотрекінг» і систему безпеки для будинку SafeHome, якими користувачі можуть керувати за власних смартфонів.

Висновки:

1. Київстар стратегічно розвиває і продовжить інвестувати в перспективний IoT-напрямок та інноваційні рішення для бізнесу. Йдеться не лише про гроші, а про проблеми, щоб навчити клієнта, показати вигоду і зручність у використанні мережі NB-IoT LTE.

2. У мобільного оператора lifecell пілотний проект мережі NB-IoT LTE розгорнут з системними інтеграторами Odine Solutions і Affirmed Networks на базі віртуалізованої пакетної мережі Affirmed Networks і радіообладнання Ericsson.

3. В свою чергу мобільний оператор Vodafone Україна мають стратегічні перспективи у впровадженні на розвиток IoT в Україні, а також готові інвестувати в ці проекти та будувати мережі NB-IoT LTE там, де є клієнти.

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ РОБОТИ CALL CENTRY

Корнейцова Н.В.
Науковий керівник – Сабурова С.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії
ім. В.В. Поповського, тел. (057) 702-13-20)
e-mail: natalia.kornieitsova.cpe@nure.ua,
факс (057) 702-13-20

New technologies are expanding in the world market and make it possible to create a single information society where geographical boundaries are losing their relevance as an economic factor. The work includes problem solving effective management of enterprises and business processes, which is impossible without electronic document management and database management systems (DBMS). The implementation of services by enterprises of any field is a success of the effectiveness of the functioning of business structures and organizations based on the CALL CENTRY.

Для функціонування сучасного підприємства та бізнес-процесів необхідні розгалужені інформаційні системи та мережі.

Без Internet технологій функціонування підприємств та бізнес-процесів неможливо, і без обміну даними головних офісів з філіями та партнерами в корпоративних та локальних мережах інфокомунікацій.

Ефективність управління підприємств та бізнес-процесами неможливе без електронного документообігу та систем управління базами даних (СУБД). Здійснення послуг підприємствами любої сфери є успіхом результативності функціонування Бізнес-структур та організацій на базі CALL CENTRY.

CALL CENTRY - це, як правило, автоматизовані сучасні системи обслуговування. Однак послуг існуючих телефонних центрів телефонної мережі з комутацією громадських послуг недостатньо для задоволення потреб клієнтів в Інтернеті. Більшість із них розроблені без урахування взаємодії, пов’язаної з покупками в Інтернеті. У своєму дослідженні в роботі розроблено CALL CENTRY під назвою IMC (Інтернет-мультимедійний центр викликів), який може бути інтегрований з Інтернет-торговим центром.

Послуги CALL CENTRY можна класифікувати на вхідні та вихідні послуги. Вхідні послуги відповідають на дзвінки клієнтів, включаючи прийняття замовлень, бронювання, придбання квитків, піклування про післяпродажне обслуговування або запити на претензії та надання інформації про товари та послуги. Вихідна послуга - це ініційована дія CALL CENTRY для зв’язку з клієнтами. Завдання включають підтримку продажів, прямі продажі, управління територією, опитування ринку, зв’язки

з громадськістю, рекламу тощо. Більшість сучасних центрів викликів використовують технологію інтеграції комп'ютерної телефонії (CTI).

Оскільки Інтернет-база електронної торгівлі розвивається і запити замовників стають більш складними, ніж у щойно згаданому сценарії, Інтернет-торгові центри повинні бути обладнані більш досконалими телефонними центрами. Найближчим часом ширина мережі Інтернету буде модернізована достатньо для повнодуплексного голосового зв'язку через TCP/IP (Transmission Control Protocol / Internetworking Protocol).

Особливості IMC, порівняно з телефонними центрами на базі CTI, можна узагальнити наступним чином: IMC забезпечує не лише інтелектуальну маршрутизацію дзвінків та спливаючий екран інформації про клієнтів - як на даний момент це можливо в центрах обробки викликів на базі CTI, - але також Інтернет-телефон, спливаючу веб-сторінку та контроль виконная послуг.

Таким чином, клієнти CALL CENTRY можуть почути голосову відповідь через Інтернет-телефон, дивлячись на відображення відповідних веб-сторінок (рис. 1).

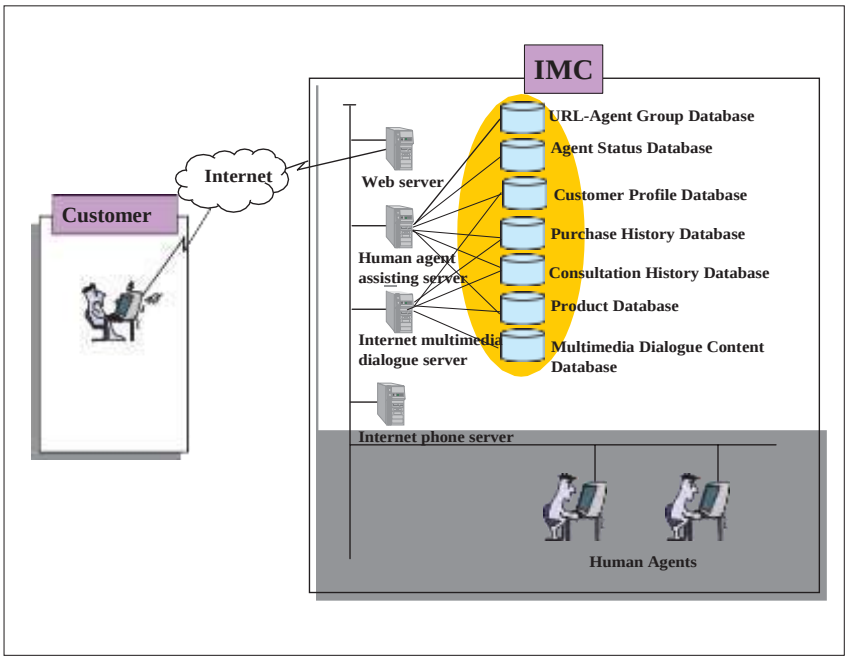


Рисунок 1 – Модель контролю функціонування мультімедійного CALL CENTRY

Висновки:

1. Модель контролю функціонування мультімедійного CALL CENTRY дасть можливість забезпечити якісний менеджмент послуг.

2. Відмінною рисою є те, що кожен алгоритмічний елемент процесу обробки первинних і повторних викликів виділено в окремий стан, що фіксується системою моніторингу CALL CENTRY.

АДАПТИВНИЙ АЛГОРИТМ ПСЕВДОВИПАДКОВОГО ПЕРЕМИКАННЯ РОБОЧИХ ЧАСТОТ РАДІОЛІНІЇ В УМОВАХ ПЕРЕШКОД

Муляр Б.П.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії им. В.В. Поповського,
тел. (057) 702-13-20) e-mail: bohdan.muliar@nure.ua

The principles of construction and evaluation of the efficiency of the adaptive algorithm of the radio line with pseudo-random switching of operating frequencies (PSOF), which operates in the conditions of interference, are considered. In the game-theoretic formulation, optimization problems are formulated and an example of an iterative procedure is given, which ensures the convergence of radio line strategies and sources of interference to the optimal ones.

Розглянуто принципи побудови та оцінки ефективності адаптивного алгоритму радіолінії з псевдовипадковим перемиканням робочих частот (ППРЧ), що функціонує в умовах перешкод. У теоретико-ігровий постановці сформульовані оптимізаційні завдання і наведено приклад ітеративної процедури, що забезпечує збіжність стратегій радіолінії і джерела перешкоди до оптимальних.

Одним із способів захисту радіоліній (РЛ) від перешкод є псевдовипадкове перемикання робочих частот (ППРЧ).

При відсутності перешкод так званим адаптивним алгоритмом управління радіоліній передбачається визначення найкращої з позиції передачі інформації частоти і використання її в якості робочої на уже згадуваному часовому інтервалі. При зміні перешкодової ситуації приймальна сторона радіолінії посилає передавачу сигнал про необхідність переходу на іншу (оптимальну) робочу частоту.

На відміну від ліній з простої програмної ППРЧ, далі розглядається адаптивна радіолінія, алгоритм вибору робочої частоти якої може ґрунтуватися на інформації про стан сукупності виділених частот з позиції можливості їх використання для ефективної передачі інформації. По суті справи при побудові адаптивного алгоритму РЛ покладається, що в процесі взаємодії РЛ з ДП умови, що визначають вихідні дані ігрового завдання, можуть змінюватися, що обумовлює доцільність відповідної зміни стратегій РЛ та ДП.

При адаптивному алгоритмі ППРЧ після входження в синхронізм і початку процесу передачі повідомлень за заздалегідь визначеною процедурою ППРЧ (тобто в заздалегідь визначеному режимі) робота радіолінії здійснюється наступним чином:

- на приймальній стороні радіолінії протягом певного часу проводиться аналіз стану сукупності виділених частот;

- за результатами аналізу здійснюється розрахунок оптимальної (рівноважної в теоретико-ігровому сенсі) сукупності параметрів, що визначають доцільний режим ППРЧ в даному стані середовища поширення сигналів;

- дані про доцільний режимі по зворотному каналу передаються на передавальну сторону радіолінії;

- в певний момент часу передавач і приймач РЛ переходять в новий режим ППРЧ.

Ітераційні процедури пошуку рівноважних ситуацій, з одного боку, забезпечують можливість аналізу ефективності адаптивних алгоритмів, з іншого, можуть безпосередньо використовуватися для управління режимами роботи радіолінії в процесі її функціонування. Моделювання процесу функціонування РЛ з адаптивним алгоритмом ППРЧ, побудованим на основі ітераційних процедур оптимізації, показало можливість його ефективного використання на практиці. Слід зазначити наступні дві важливі гідності подібних алгоритмів: 1) перш за все, це універсальність, обумовлена сходимістью до оптимального в теоретико-ігровому сенсі при наявності перешкод і до адаптивного вибору оптимальної частоти - при їх відсутності і 2) використання в процесі функціонування лише даних про послідовності номерів найкращих з виділених частот без необхідності ідентифікації присутніх в частотному діапазоні перешкод.

Список використаних джерел:

1. Жодзішскій А.І., Жодзішскій М.І. Потенційні можливості командних радіоліній з дискретно змінюваною частотою. Ракетно-космічна техніка, 1973, сер. VI, вип. 2 (11), С. 15-26.

2. Cook D.B. Interleaving frequency hopping and spread spectrum for finite messages under jamming // Proc / IEEE Nat / Aerosp. and Electron. Conf.- NAECON'77.- Dayton, N.Y., 1977.- P.1300-1306. Kullstam P. A. Spread Spectrum Performance Analysis in Arbitrary Interference. - IEEE Trans. Commun, 1977, v. 25, №8. P. 848-853.

3. Чуднов А.М. Перешкодозахищеність системи передачі інформації з псевдовипадковим перемиканням частот в умовах найгірших перешкод // Изв. вузів. Радіоелектроніка, 1984, т. 27, №9. С. 3-8.

РОЗРОБКА ТА ПРОСУВАННЯ ІНТЕРНЕТ-МАГАЗИНУ НА БАЗІ ОНЛАЙН-КАТАЛОГУ TECDOC

Дікаленко Д. Д.
Науковий керівник – к.т.н., с.н.с Калюжний М.М.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14,
Кафедра Інформаційно-мережної інженерії)
тел. 0731310763 e-mail: danylo.dikalenko@nure.ua

The paper considers the problem of branching queries to the multimillion database of automotive products. Ways to develop, optimize and promote the site in the market of competitive services are given. The main provisions of the online catalog TECDOC and Allzap.CMS are given.

Розробка високонавантажених web-систем для роботи з даними є одним з найбільш актуальних напрямків розвитку інформаційних технологій.

Найбільші компанії працюють над створенням нових інструментальних засобів для роботи з дуже великими обсягами даних, призначеними для роботи в подібних масштабах.

Продуктивність високонавантажених систем є необхідною складової їх успішного функціонування. Технічна складність і специфічні особливості програмування зробили створення сайтів запчастин окремим напрямком в IT-сфері.

Головною метою роботи є *розробка багатофункціонального інтернет-магазину на базі онлайн-каталогу TecDoc*, що дозволяє працювати в умовах багатомільйонної номенклатури та його просування на ринку конкурентних послуг.

Для виконання поставленої мети вкрай важливо правильно обрати CMS і Базу даних. Щоб забезпечити продуктивність *«АВТОСАЙТу»*, необхідно подбати не тільки про функціональність магазину, а й про наявність потужного сервера - місця для фізичного розміщення інформації.

Від технічних можливостей і правильного налаштування сервера залежить коректність і швидкість роботи інтернет-магазину, що розробляється для виходу на ринок.

Основна проблема полягає в тому, що Інтернет магазин по автозапчастинах - це мільйони товарних позицій. Щоб на сайті відображалася ціна, а клієнти мали змогу обрати ціну і терміни поставки, потрібен алгоритм націнок. Для правильного підбору запчастин по марці, моделі , двигуну необхідно розробити алгоритм оптимального підбору.

Для якісної роботи використовується база Tec Doc. Вона дозволяє підбирати запчастини на всі авто Європейського ринку та включає в себе більш 50000000 запчастин.

Складність проекту заключається в інтеграції такої великої бази даних на сайт. Для просування в подальшому важлива швидкість роботи і та правильна структура. Для цього найважливішим моментом є вибір CMS.

В Роботі було проведено аналіз відкритих CMS. Використання готових, безкоштовних CMS піднімає ряд складних завдань, ключові з яких - позбутися від непотрібного і додати необхідні складові.

Вибираючи *«движок»* з готових рішень, разом з універсальністю ми отримуємо масу зайвих функцій, які неодмінно будуть заважати не тільки роботі сайту, але і процесу просування, управління асортиментом і замовленнями. Виходячи з цього було прийнято рішення для даного проекту Allzap.CMS.

Allzap.CMS відрізняється високою продуктивністю і простотою адміністрування. Підтримує п'ять варіантів пошуку автозапчастин. Дозволяє легко керувати асортиментом і замовленнями, завантажувати і генерувати необмежену кількість прайс-листів, підключати оригінальні каталоги і додавати крос-зв'язку. Вона забезпечує продуктивну роботу інтернет-магазину запчастин при будь-яких навантаженнях та є адаптованою під мобільні пристрої.

Додатково передбачено ефективну SEO-оптимізацію та можлива інтеграція з платіжними сервісами, програмами обліку, CRM.

Використання в роботі Allzap.CMS вирішило проблему розгалуженості запитів та спростити навантаження на серверні потужності. Вона повністю підходить для наших завдань і сприяє подальшому економічно-вигідному просування на ринку інтернет-послуг.

Список літератури

1. Блог Allzap CMS - Готовый интернет-магазин автозапчастей [Електронний ресурс], Режим доступу: https://allzap.pro/blog/ 26.02.2021 – заголовок з екрану.

2. Каталог tecdoc - система пошуку авто запчастин [Електронний ресурс], Режим доступу: https://jak.koshachek.com/articles/katalog-tecdoc-sistema-poshuku-avto-zapchastin.html 26.02.2021 – заголовок з екрану.

МЕТОД УПРАВЛІННЯ ШВИДКІСТЮ БЕЗДРОТОВОГО ЗВ'ЯЗКУ НА ОСНОВІ ПРОТОКОЛУ ACCEL-BRAKE CONTROL

Бєлєнцов А.С.
Науковий керівник – д.т.н., проф. Шостко І.С.
Харьківський національній університет радіоелектроніки
(61166, Харьків, пр. Науки,14, каф. Інфокомунікаційної інженерії
ім. В.В. Поповського)
e-mail: anton.bielientsov@nure.ua,

Method Accel-Brake Control (ABC), a simple and deployable explicit congestion control protocol for network paths with time-varying wireless links. ABC routers mark each packet with an “accelerate” or “brake”, which causes senders to slightly increase or decrease their congestion windows. ABC achieves 30-40% higher throughput than Cubic+Codel for similar delays, and 2.2 lower delays than BBR on a Wi-Fi path. On cellular network paths, ABC achieves 50% higher through put than Cubic+Codel.

Швидкість зв'язку в бездротових мережах може швидко змінюватися з часом; наприклад, протягом однієї секунди швидкість бездротового зв'язку може як удвічі збільшитись, так і вдвічі зменшитись[1]. Це ускладнює роботу транспортних протоколів для досягнення як високої пропускної здатності, так і низької затримки. Для вирішення цієї проблеми вченими з Массачусетського технологічного інституту було розроблено та представлено протокол, який забезпечує зворотний зв'язок з передавачами, щодо збільшення і зменшення навантаження на основі безпосереднього знання про швидкість бездротового зв'язку. Простий новий протокол контролю черг для змінних у часі бездротових мереж, що називається Accel-Brake Control (ABC).

ABC маршрутизатори використовують один біт, щоб позначити кожен пакет значком зворотного зв’язку “accelerate” або “brake”, що змушує передавачів дещо збільшитись або зменшити швидкість відправки пакетів на основі поточної швидкості зв'язку. Отримавши цей відгук через ACK від приймача, передавач збільшує кількість пакетів на одиницю, у відповідь на “accelerate” (посилає два пакети у відповідь на ACK), чи зменшує на один у відповідь на “brake”, (не посилає жодного пакета). Це просто Механізм дозволяє маршрутизатору сигналізувати про великий динамічний діапазон змін розміру вікна в межах одного RTT: від регулювання вікна до 0, до подвоєння вікна. Головним у роботі ABC є новий алгоритм управління що допомагає маршрутизаторам надавати дуже точні відгуки про посилання відправленні у різний час.

ABC перевершує найкращі існуючі засоби управління потоком такі як XCP[3], але на відміну від XCP, ABC не вимагає модифікацій форматів пакетів або користувацьких пристроїв, що робить його простішим. Традиційні протоколи контролю черг, які часто використовуються такі, як Cubic та NewReno покладаються на відкидання пакетів, щоб зробити

висновок про перевантаження та відрегулювати швидкість. Такі протоколи, як правило, заповнюють буфер, викликаючи великі затримки в черзі, особливо в стільникових мережах, які використовують глибокі буфери, щоб уникнути втрати пакетів.

Основні властивості протоколу ABC:

1. Швидка обробка змін пропускної здатності в бездротових мережах зв'язку.
2. Немає змін у заголовках пакетів. ABC перепризначує існуючі біти ECN[4] що сигналізують про збільшення чи зменшення вікна перенавантаження.
3. Сумісність з маршрутизаторами що не підтримують протокол.
4. Сумісність з транспортними протоколами що не підтримують ABC протокол.

Протокол було перевірено експериментально за допомогою практичної реалізації на Wi-Fi маршрутизаторах до котрих було підключено передавачі Ethernet. Кожен передавач передає дані через WiFi-маршрутизатор на один приймач. Всі пакети мають однакову чергу FIFO на маршрутизаторі. У ході експерименту сценарію з одним користувачем протокол ABC було порівняно з протоколами Cubic + Codel, Copa, Vegas, PCC-Vivace та BBR. Незважаючи на те що PCC-Vivace, Cubic та BBR досягли трохи більшої пропускної здатності (4%), ніж ABC їх значення затримки було значно вище (67%). Багатокористувацький сценарій показав подібні результати, наприклад ABC досягає на 38%, 41% і 31% вище середньої пропускною здатності ніж Cubic + Codel, Copa і Vegas. Усе це вказує на те, що протокол ABC є перспективним протоколом.

Список використаної літератури

[1] K. Winstein, A. Sivaraman, and H. Balakrishnan.Stochastic forecasts achieve high throughput and low delay over cellular networks. Proceedings of the 10th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2013, Lombard, IL, USA, April 2-5, 2013, pages 459–471. USENIX Association, 2013

[2] "ABC: A Simple Explicit Congestion Controller for Wireless Networks," 15 Feb 2020. [Online]. Available: https://arxiv.org/abs/1905.03429. [Accessed 21 02 2021]

[3] F. Abrantes and M. Ricardo. XCP for shared-access multi-rate media. Computer Communication Review, 36(3):27–38, 2006.

[4] J. C. Hoe. Improving the start-up behavior of a congestion control scheme for TCP. In D. Estrin, S. Floyd, C. Partridge, and M. Steenstrup, editors, Proceedings of the ACM SIGCOMM 1996 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Stanford, CA, USA, August 26-30, 1996, pages 270–280. ACM, 1996.

МОДЕЛЬ ТРАКТУ ОБРОБКИ СИГНАЛУ ДОППЛЕРІВСЬКОГО ПЕЛЕНГАТОРА

Білокурова А.О.
Науковий керівник – к.т.н, доц. Філіппенко О.І.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ІКІ, тел. (057) 702-13-20)
e-mail: anastasiia.bilokurova@nure.ua

The article attempts to develop a model of the signal processing path of the Doppler direction finder, which allows to obtain at the output of the demodulator signal not in the form of pulses, but in the form as close as possible to a sinusoid. The method of smoothly changing the position of the virtual antenna by synchronously multipolar change of signal levels coming from two pairs of adjacent antennas was used. To assess the adequacy of the solutions, the system operation was simulated using the Matlab / Simulink package.

Вступ. Доплерівський пеленгатор відноситься до фазових пеленгаторів, які витягають інформацію про направлення поширення електромагнітної хвилі (ЕМХ) з просторового розташування ліній або поверхонь з однаковою фазою. Його дія ґрунтована на ефекті Доплера. Суть ефекту Доплера полягає в тому, що відносне (взаємне) переміщення приймача і передавача призводить до зміни частоти (а отже, і фази) коливань, що приймаються. Частота коливань, що приймаються, стає відмінною від частоти випромінюваних. Обумовлене обертанням антени приріст частоти, що наводиться в ній, ЕРС негативна в проміжки часу, коли антена віддаляється від передавача, і позитивна, коли антена наближається, і дорівнює нулю, коли антена рухається перпендикулярно напряму поширення ЕМХ.

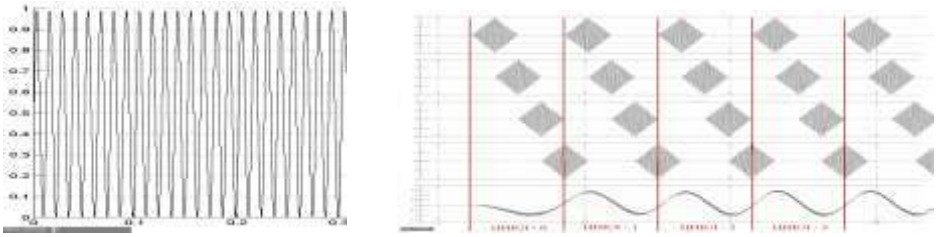
Зміст дослідження. Метою роботи була розробка моделі тракту обробки сигналу доплеровського пеленгатора, що дозволяє отримати ні виході демодулятора сигнал не в формі загострених імпульсів, а у формі максимально наближеної до синусоїди. Для цього було застосовано метод плавної зміни положення віртуальної антени шляхом синхронної різнополярної зміни рівнів сигналів, що надходять з двох попарно сусідніх антен.

Для оцінки адекватності рішень було здійснено моделювання функціонування системи за допомогою пакету Matlab/Simulink. Для оцінки залежності точності функціонування системи від типу вхідного сигналу було здійснено оцінку характеру змінення вихідного сигналу каналу обробки сигналів від чистого гармонічного сигналу до шумового сигналу при різних рівнях вхідного сигналу.

1. Джерело випромінювання випромінює гармонійний сигнал. Вхідний сигнал не містить шумів. Видно присутність та фазове співвідношення сигналів комутації антен та сигналу на виході каналу обробки.

Мета моделювання полягає в аналізі виду реконструйованого сигналу, який дає можливість визначити фазове зміщення у вхідному сигналі в

залежності від руху вібраторів антенної решітки, що комутується та аналізі залежності формі цього сигналу від співвідношення сигналу до шуму, що надходить з антени.

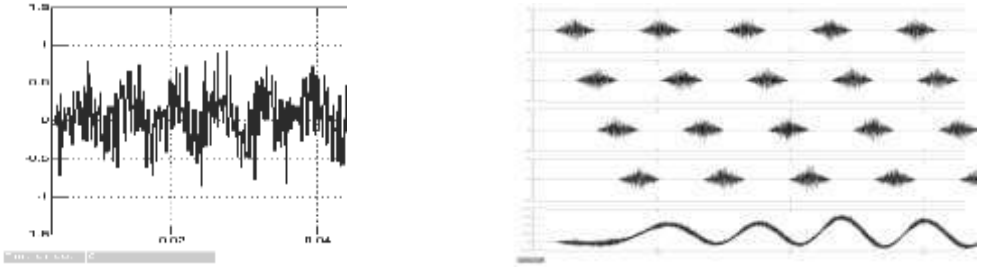


а) б)

Рисунок 1 – Робота на чистому сигналі: а) сигнал на вході, б) сигнали на виході комутатора та вихідний

З графіку видно, що для впевненого визначення кута надходження сигналу треба три повних циклу комутації антенної решітки.

2. До антенної решітки надходить сильно спотворений шумами сигнал. Відповідно на моделі видно присутність та фазове співвідношення сигналів комутації антен та сигналу на виході каналу обробки.



а) б)

Рисунок 2 – Робота на шумовому сигналі а) сигнал на вході, б) сигнали на виході комутатора та вихідний

З графіку видно, що для впевненого визначення кута надходження сигналу треба чотири повних циклу комутації антенної решітки.

Висновок. Розроблено модель системи та проведено моделювання та порівняльна оцінка ефективності запропонованої реалізації побудови системи для сигналів з різним співвідношенням сигнал/шум. З графіку видно, що для впевненого визначення кута надходження сигналу треба чотири повних циклу комутації антенної решітки.

Список джерел:

1. N. Cianos, .Low-Cost, High-Performance DF and Intercept Systems., Proc. of 1993WESCON Conference, pp. 372-376, September 1993.

2 David Adamy, “EW 101 A First Course in Electronic Warfare” Artech House Boston London.

ANALYSIS OF POLARIZATION IN MIMO ANTENNAS AND ADVANTAGES ON THE EVOLUTION OF 5G WITH MASSIVE MIMO

Tresor M.A.
Scientific adviser: candidate of technical science Martynchuk A.A.
Kharkiv National University of Radio Electronics,
Infocommunications Department,
Nauky Ave. 14, Kharkiv, 61166, Ukraine,
e-mail:mtumbeabitresor560@gmail.com

This article is about the MIMO (Multiple Input Multiple Output) technology which consists of simultaneously transmitting N information streams on N transmission antennas and each stream is received by M reception antennas. MIMO (Multiple Input Multiple Output) technology in 5G NR (New Radio) will be the specified and the main keys to unlocking 5G users but with an improvement, we call it Massive MIMO. Network and mobile devices must have close coordination with each other for MIMO to work. The design of new networks 5G NR MIMO is "massive" and crucial for deployments 5G NR.

This is all to say that these advancements are all aimed at improving the performance. Spatial multiplexing is not only the various experiences of the air channel that are used to improve performance, but multiple messages can be transmitted simultaneously without interfering with each other as they are separated in space. Massive MIMO grants fast 5G data rates:

- Increase in network capacity;
- Improved coverage.

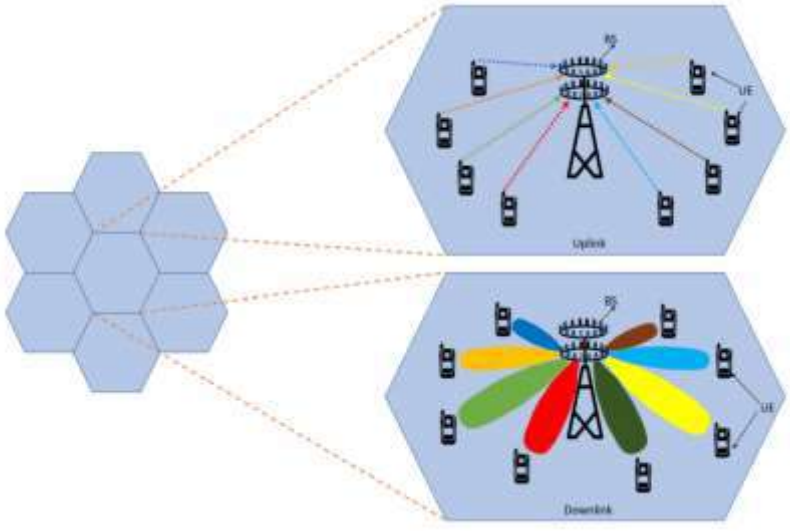


Figure1 - Massive MIMO uplink and downlink

As the number of antennas increases MIMO system, the radiated beams become narrower and spatially focused towards the user.

Table 1 - Comparison Table of MIMO and Massive MIMO using 5G

	MIMO	Massive MIMO
Number of antennas	≤ 8	≥ 16
Pilot Contamination	Low	High
Throughput	Low	High
Antenna Coupling	Low	High
Bit Error Rate	High	Low
Energy Efficiency	Low	High
Link Stability	Low	High
Antenna Correlation	Low	High

As mentioned, MIMO has been used in wireless communications for many years. But now, in the context of 5G NR, massive MIMO is changing dramatically. We no longer have to worry about whether we are in a good area to download or transfer large files. Massive MIMO technology bundles the antennas at the transmitter and receiver level to provide high spectral and energy efficiency using relatively simple processing. While massive MIMO offers immense benefits for 5G and 6G networks, there are still various deployment challenges such as pilots, channel estimation, precoding, user scheduling, hardware degradation, efficiency. Energy and the detection of signals that must be resolved before the goal can be achieved.

References:

1. M’TUMBE A.T.Localization in vehicle networks using radio frequency identification technology. XIV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2020. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2020. p. 381.

2. Tresor, M.A.,A.A.Martynchuk, 2019. Mobile info-communication systems and wireless 5G and 6G technologies. Третя міжнародна науково-технічна конференція «Комп’ютерні та інформаційні системи і технології». Збірник наукових праць. Харків: ХНУРЕ. 2019. С. 135.

3. Martynchuk O.O. Study of the effect of antenna polarization decoupling of the quality indicators of the MIMO channel with dual polarization // Ikeza Obasi Anyaso Destiny, Ajadi Ayodele Tega, M’TUMBE ABI Tresor // Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС-2020): Збірник наукових праць шостої міжнародної науково-технічної конференції / М-во освіти і науки України, Харківський національний університет радіоелектроніки. - Харків: ХНУРЕ, 2020.

IMPROVING THE WIFI MIMO COMMUNICATION CHANNEL BASED ON DUAL POLARIZATION ANTENNAS

Ikeza Obasi A. D.
Scientific Supervisor – Prof. Martynchuk A.A.
Kharkov National University of Radio Electronics,
Infocommunications Department,
Nauky Ave. 14, Kharkiv, 61166, Ukraine, e-mail: pastordee245@gmail.com

This paper work provides the basics of MIMO technology, standard of configuration, antenna polarization choices, benefits of communication channel. Types of channels and the dual polarization antenna for MIMO and how the dual polarization signal improves the communication quality.

In recent years, the use of MIMO technology with polarization-orthogonal channels has been intensively investigated. However, the resulting bandwidth limitations due to the final isolation by polarization have not been sufficiently studied. In works **Ошибка! Источник ссылки не найден.** attention is paid to the polarization decoupling, however, only if there is a 2x2 configuration using the MIMO. Studies of the possibility of using an increase in the number of antennas of MIMO systems with polarization-orthogonal antennas have not been sufficiently conducted.

An important characteristic of the radio wave is its purity of polarization. For a radio wave transmitted with a given polarization, the ratio of the power received with the expected polarization to the power received with the orthogonal polarization is called cross-polarization discrimination (XPD), which is given by

$$XPD=10\left(d_{xp}\right)=10\log\frac{P}{P_{+}}, \tag{1}$$

where P+ is the power of the orthogonal interference component caused by the XPD. When the XPD of the receiving antenna is considered, the receiving SNR of the signal should be replaced by the signal to noise and interference ratio (SNIR). The SNIR can be expressed as

$$r_{sni}=\frac{P}{n_0 B+P_{+}}=\frac{1}{\frac{1}{r_{sn}}+\frac{1}{d_{xp}}}=\frac{r_{sn}d_{xp}}{r_{sn}+d_{xp}}. \tag{2}$$

Fig.1 shows the relationship between the SNIR and the XPD when the SNR is constant (10, 20 and 30 dB). As can be seen, due to the existing of the XPD, the performance of the system will be deteriorated, and the SNIR will be less than the receiving SNR. When the XPD increases, the SNIR will be firstly increased and then keeps unchanged after approaching the SNR value. Fig. also shows that, if the antenna has a large SNR, then a high XPD should be provided to guarantee the receiving SNR. For example, when the SNR is 10 dB, the performance can be preserved when the XPD is 20 dB, however, when the SNR is larger than 20 dB, to guarantee the performance, the XPD need to be larger than 30 dB.

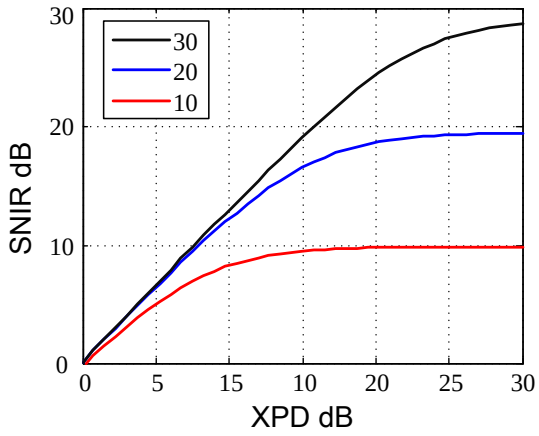


Figure 1 - Relationship between XPD and SNIR

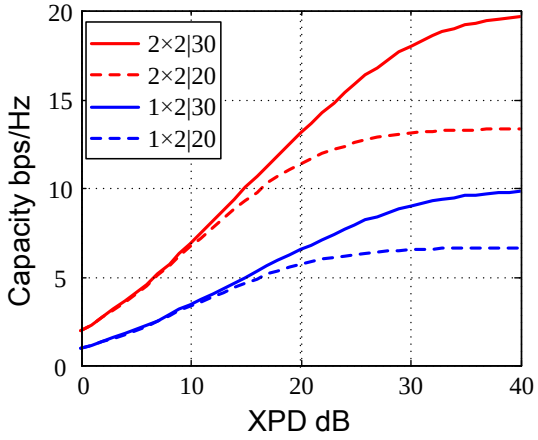


Figure 2 - Channel capacity with different configurations when the XPD changes

Fig. 2 shows the capacity of 1×2 and 2×2 channels when the XPD changes while the SNR keeps constant (20 and 30 dB). As can be seen, when the XPD increases, the capacity is firstly increased and then keeps constant. This is caused by the relationship between the XPD and the SNIR, as shown in Fig. 1. Furthermore, we compare the two results of the 2×2 or 1×2 channels, it can be seen that, when the SNR is larger, to obtain maximum capacity, a larger XPD should be provided, which is consistent with the analysis results in Fig 2.

So, the proposed method to increase system capacity includes the following: business division of the transmitted information flow; transmitting of each of the sub-streams on orthogonal polarizations compensated polarization distortion of antennas; organization receiving the full polarization orthogonal polarization antennas with the ability to compensate for polarization distortion; estimate of the time taken by the correlation of radio waves; adaptive assessment matrix received vector signal; finding the spectrum and eigenvectors of matrix and their analysis; preparation of the transformation matrix of the first two eigenvectors of matrix; converting the received vector signal into its major components; restore the flow of information through the use of principal component vector signal received.

Reference: [1] Martynchuk A.A. Some limitations of evaluating dual-polarized MIMO channel capacity / A.A. Martynchuk, Xuan Li // Новітні технології – для захисту повітряного простору: тези доповідей XVI міжнародна наукова конференція Харківського національного університету Повітряних Сил імені Івана Кожедуба 15 – 16 квітня 2020 р. – Х.: ХНУПС ім. І. Кожедуба, 2020. С. 367-368.

[2] Martynchuk O.O. Study of the effect of antenna polarization decoupling of the quality indicators of the MIMO channel with dual polarization // Ikeza Obasi Anyaso Destiny, Ajadi Ayodele Tega, M'TUMBE ABI Tresor // Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (EMC-2020): Збірник наукових праць шостої міжнародної науково-технічної конференції / М-во освіти і науки України, Харківський національний університет радіоелектроніки. - Харків: ХНУРЕ, 2020.

INVESTIGATION OF THE EFFICIENCY OF ORTHOGONAL POLARIZATION-FREQUENCY CODING OF SIGNALS TO IMPROVE THE PERFORMANCE OF COMMUNICATION CHANNELS WITH MIMO

Ayodele Tega Ajadi
Scientific Supervisor – Prof. Martynchuk A.A.
Kharkov National University of Radio Electronics,
Infocommunications Department,
Nauky Ave. 14, Kharkiv, 61166, Ukraine, e-mail: pastordee245@gmail.com

This paper presents the results of studying the efficiency of orthogonal polarization-frequency coding of signals to improve the quality parameters of communication channels with MIMO. The dependences of the channel capacity and the error probability for various design variations of antennas with MIMO are shown. MIMO technology can be used to efficiently improve the channel capacity of the communication system. Note that, this improvement of capacity is achieved by increasing the complexity of signal processing.

Shannon-Hartley's channel capacity theorem is applied to provide the upper bound of the data rate given a certain bandwidth and signal to noise ratio (SNR). It demonstrates that the effect of a transmitter power constraint, a bandwidth constraint, and additive noise can be associated with the channel and incorporated into a single parameter, called the channel capacity. For a single-input and single-output (SISO) channel, in the case of an additive white (spectrally flat) Gaussian noise interference, an ideal band limited channel of bandwidth B has a capacity C given by

$$C_s = B \cdot \log_2\left(1 + \frac{P_s}{n_0 B}\right) = B \log_2\left(1 + r_{sn}\right), \quad (1)$$

where P is the average transmitted power and n_0 is the power-spectral density of the additive noise, and r_{sn} is the receive SNR. The significance of the channel capacity is as follows: if the information rate R from the source is less than C, then it is theoretically possible to achieve reliable transmission through the channel by appropriate coding. On the other hand if R>C, reliable transmission is not possible.

For a MIMO channel with m transmitting antennas and n receiving antennas, when the users transmitting at equal power over the channel and the users are uncorrelated. Then, the channel capacity is given by

$$C_{mn} = B \cdot \log_2\left[\det\left(I_n + \frac{r_{sn}}{m} HH^H\right)\right] = B \log_2\left(1 + r_{sn}\right), \quad (2)$$

where I is an n×n identity matrix, H is the n×m channel matrix, HH is transpose conjugate.

As a result, when the SNR of the receiving antenna is certain, compared to the capacity of a SISO channel, the capacity of a MISO channel is slightly improved when the channel has a gain of hi≈1, the channel capacity of a SIMO

system will be improved logarithmically as the number of receiving antennas increases, while for the MIMO channel, its capacity can be linearly improved as the minimum number of receiving and transmitting antennas increases, as shown in Fig. 1. In the simulation, the receiving SNR is set as 20 dB, and the channel gain is set as hi=1.

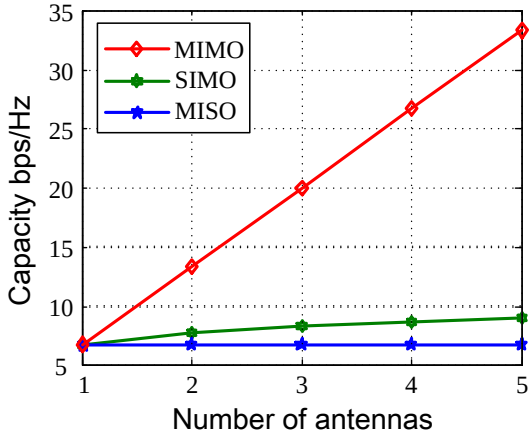


Figure 1 - Channel capacity of SISO, SIMO and MIMO systems

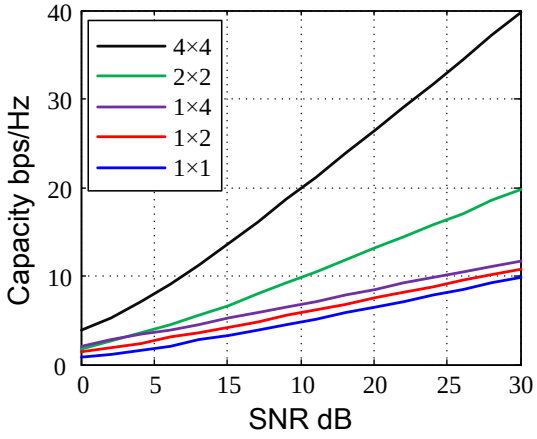


Figure 2 - Channel capacity with different MIMO configurations

Fig. 2 shows the simulation results of the channel capacity with different configurations when the receiving SNR changes. As can be seen, the capacity will be improved when the SNR increases. For the SIMO systems, the capacity will be increased by 1 bps/Hz when the number of the receiving antennas increases twice, as the results of 1×2 and 1×4 channels shown in the figure. While for the MIMO system, when the minimum number of receiving and transmitting antennas increases twice, the channel capacity will be also increased two times, as the results of 2×2 and 4×4 channels shown in the figure.

Therefore, MIMO technology can be used to efficiently improve the channel capacity of the communication system. Note that, this improvement of capacity is achieved by increasing the complexity of signal processing.

Reference:

[1] Martynchuk A.A. Some limitations of evaluating dual-polarized MIMO channel capacity / A.A. Martynchuk, Xuan Li // Новітні технології – для захисту повітряного простору: тези доповідей XVI міжнародна наукова конференція Харківського національного університету Повітряних Сил імені Івана Кожедуба 15 – 16 квітня 2020 р. – Х.: ХНУПС ім. І. Кожедуба, 2020. С. 367-368.

[2] Martynchuk O.O. Study of the effect of antenna polarization decoupling of the quality indicators of the MIMO channel with dual polarization // Ikeza Obasi Anyaso Destiny, Ajadi Ayodele Tega, M'TUMBE ABI Tresor // Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (EMC-2020): Збірник наукових праць шостої міжнародної науково-технічної конференції / М-во освіти і науки України, Харківський національний університет радіоелектроніки. - Харків: ХНУРЕ, 2020.

УДК 004:621.391

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

OPENSAMM – МОДЕЛЬ БЕЗПЕЧНОЇ РОЗРОБКИ ПЗ

Назаренко К.А.
Науковий керівник – д.т.н., проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, Кафедра інфокомунікаційної інженерії ім. В.В. Поповського (ІКІ), тел. (057) 702-13-20
e-mail: kseniia.nazarenko@nure.ua.

Standards, models, frameworks and guidelines have been developed for secure software development such as OpenSAMM. Current standard and model provide guidance for particular areas such as threat modelling, risk management, secure coding, security testing, verification, patch management, configuration management etc. But there is not a generally accepted model for a secure software development lifecycle.

Програмне забезпечення стає все більш поширеним, критично важливим і вразливим для інцидентів, пов'язаних з безпекою, тому вкрай важливо, щоб інформаційні системи були належним чином захищені з самого початку.

Найбільш важливою з цих проблем є уразливість програмного забезпечення, використовуваного хакерами і неусвідомлені користувачі. Уразливості – це слабкі місця в програмному забезпеченні, які дозволяють хакерам скомпрометувати цілісність, доступність або конфіденційність даних, що обробляються програмним забезпечення.

Уразливості програмного забезпечення є виникаючими властивостями, які з'являються під час проектування та циклів реалізації. Таким чином, підхід «до, під час і після» повинен бути розглянутий на рівні розробки програмного забезпечення.

Для розробки програмного забезпечення використовуються безпечні моделі, каркаси і керівництва. Поточні моделі забезпечують керівництво в певних областях наприклад, моделювання загроз, управління ризиками, безпечне кодування, тестування безпеки, перевірка управління, управління конфігурацією і т.ін.

Open Software Assurance Maturity Model (SAMM) – це відкрита модель, що дозволяє організаціям формулювати і реалізовувати стратегію забезпечення безпеки програмного забезпечення. Ця модель намагається вирішити конкретні ризики безпеки програмного забезпечення, з якими стикається організація. У цьому можуть допомогти ресурси, що надаються SAMM:

– оцінка існуючих в організації методів забезпечення безпеки програмного забезпечення;

– побудова збалансованої програми забезпечення безпеки ПЗ в чітко визначених ітераціях:

– демонстрація конкретних поліпшень в програмі забезпечення безпеки;

– визначення та вимірювання діяльності, пов'язаної з безпекою у всій організації.

Крім того, ця модель може бути застосована в масштабах всієї організації, для всього бізнесу або окремого проекту. OpenSAMM, пропонує карту і чітко визначену модель зрілості для безпечної розробки та впровадження програмного забезпечення.

Кожна бізнес-функція визначає три практики безпеки. Кожна практика безпеки будує гарантію для відповідної бізнес-функції. Отже, в цілому, є дванадцять практик безпеки.

Модель OpenSAMM показана на рис.2.

Рисунок 2 – Схема OpenSAMM

OpenSAMM модель типу CoBIT (Control Objective for Information and Related Technology) для кількісного виміру безпеки кожного продукту. У даній моделі рівень зрілості операції безпеки приймає значення між 0 і 3.

– 0 означає, що операція не застосовується;

– 1 означає, що немає системного підходу, але є базовий рівень застосування в організації;

– 2 означає, що операція застосовується на достатньому рівні зрілості на рівні організації;

– 3 означає, що операція застосовується в організації бездоганно.

Отже, програмні продукти мають слабкі і вразливі місця через недостатню безпеку процесів та інструментів розробки програмного забезпечення. Існують методи усунення проблем безпеки під час проектування, впровадження та терміну служби продукту. У цій роботі розглянуто OpenSAMM модель розробки ПЗ, яка може використовуватися в якості безпечного керівництва по життєвому циклу розробки програмного забезпечення для розробників додатків.

Перелік джерел

1. Инжиниринг безопасности системы. Модель зрелости потенциала [Електронний ресурс]. – 2003. – Режим доступу до ресурсу: http://www.ssecmm.org/docs/ssecmmv3final.pdf.

ДО ПИТАННЯ ПРОБЛЕМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ТЕРИТОРІЇ УКРАЇНИ У ПОРІВНЯННІ ІЗ GDPR

Товкун Ю.І.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки
61000, Харків, просп. Науки,14, каф. ІКІ ім. В.В. Поповського,
тел. (057) 702-13-20, e-mail: yuliia.tovkun@nure.ua

Since the General Data Protection Regulation (GDPR) came into force in the EU, it has become a flagship in personal data protection. Due to a short privacy history in Ukraine, our nation has yet to develop a strong privacy culture. However, forming this culture is no easy task and requires the involvement of many stakeholders. Ukraine, in turn, has made a commitment to improve the level of personal data protection and move toward GDPR compliant country. In the fall of 2018, working groups and public discussions were actively held on the future draft law, which was supposed to be an analogue of GDPR in Ukraine.

У сучасному цифровому світі, особливо з розвитком Big Data та таргетованої реклами, інформація стає одним з головних ресурсів, а її обсяги, які зберігаються компаніями, є просто колосальними. Актуальність даної теми пов’язана з серією гучних скандалів світового масштабу, пов’язаних з витоком приватної інформації (наприклад, Uber, SoftServe, Facebook та інші).

Пройшов певний час з моменту набуття чинності Загального регламенту про Захист Даних (GDPR) в ЄС. Україна, також рухаючись у сторону GDPR compliant країни, взяла на себе зобов’язання вдосконалити рівень захисту персональних даних. Ця робота зупинилась на стадії законопроєкту і у грудні 2019 року відбулося його чергове обговорення. На даний час існує Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 року [1]. Він був прийнятий з метою певної уніфікації національного та європейського законодавства в умовах розвитку нових видів правовідносин, які не врегульовані національним законодавством. Але здається, що цей Закон приймався поспіхом, без повного розуміння специфіки відносин, а тому у ньому відсутні багато важливих положень (наприклад, з приводу обробки персональних даних неповнолітніх осіб). Якщо порівняти положення GDPR і Закону України «Про захист персональних даних» можна зрозуміти, що ці два акти приймалися для різних цілей, а тому містять досить значні розбіжності. Так, GDPR приймався як загальноєвропейський законодавчий акт обов'язкової сили, який повинен регулювати питання обробки персональних даних. GDPR регулює максимально можливе коло відносин і питань щодо захисту персональних даних, а, як механізм додаткового перестрахування, він надав повноваження спочатку Working Party 29, а потім European Data Protection Board надавати додаткові роз'яснення положень GDPR, тим самим створив

можливість в майбутньому усувати недоліки законодавчого регулювання. В українському ж законодавстві проблемою є відсутність чіткого визначення згоди на обробку персональних даних і особливостей, пов'язаних з наданням такої згоди; відсутність законодавства з приводу обробки файлів cookies та інше. Все це виступає певною припоною на шляху розвитку України.

Було зроблено висновок, що важливим є скоріша імплементація GDPR у законодавство України і отримання нею статусу країни, яка забезпечує належний рівень захисту персональних даних. Так, згідно зі статтею 45 Регламенту, особисті дані можна передавати країнам з адекватним рівнем захисту персональної інформації без додаткових погоджень з контролюючими органами [2]. При цьому, зараз зміст таких повідомлень показує Україну з не найпривабливішою сторони: «Ваші дані будуть передані для обробки в Україну, в країну, де немає адекватного рівня захисту персональних даних». А якщо до цього всього додати передбачені Регламентом штрафи в розмірі десятків мільйонів євро, то шансів на співпрацю залишається мало. Адже зараз, якщо компанія працює з даними громадян ЄС – вона автоматично потрапляє під дію Регламенту і змушена трансформувати свої процеси, щоб відповідати європейським вимогам.

Тому, у першу чергу, Україні пропонується отримати статус GDPR compliant, аби простіше було зацікавити клієнтів з ЄС працювати з нашими компаніями, так само, як і переконати інвесторів у відкритті офісів або R&D в Україні. Підготовка до таких змін вимагає від компаній інвестицій і зміни всіх процесів, які хоч якимось чином пов'язані з даними, а саме, можна пропонувати такі дії: введення адекватної системи захисту інформації; протидіяти можливим витокам даних; сформувати відділ, який буде займатися забезпеченням безпеки інформаційного простору або ж наймати аутсорс-підрядників. Усі ці аспекти повинні бути обов'язково відображені у законодавстві України для того, щоб український бізнес повністю відповідав вимогам безпеки даних ЄС і не потрібно було додатково підтверджувати, той факт, що рівень захисту даних в компаніях знаходиться на належному рівні.

Список літератури

1. Закон України "Про захист персональних даних" [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

2. GDPR [Електронний ресурс] – Режим доступу до ресурсу: https://gdpr-info.eu/.

МОДЕЛЮВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

Семеренська В.В.
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікацій, тел. (057) 702-00-00
e-mail: viktoriia.semerenska@nure.ua.

Using three-dimensional modeling, it is possible to solve problems arising in the design process in the best way, taking into account complex influencing factors. For example, it is difficult to take into account obstacles covering part of the view area and the peculiarities of displaying three-dimensional objects in two dimensions. Three-dimensional modeling allows to see the final information of the system already in the process of designing – images on the monitors. This information will save you from expensive mistakes and allow you to choose the placement and parameters of the equipment with great accuracy, as well as to find new non-standard solutions of the set tasks.

У процесі проектування телевізійних систем відеоспостереження інженерам доводиться витрачати багато часу для розрахунку фокусних відстаней об'єктивів і правильних місць розміщення відеокамер для отримання необхідного зображення на екранах моніторів. Додаткові складності викликає розрахунок зон упізнавання людини і читання автомобільного номера. Завдання ускладняється багаторазово, коли потрібно вибрати оптимальне взаємне положення декількох камер або однією відеокамерою вирішувати одночасно кілька завдань (наприклад, розпізнавання осіб і спостереження за периметром).

У перших десятиліттях цього століття вже була доступна більшість функцій систем відеоспостереження, які активно використовуються в наші дні. Серед них – розпізнавання облич, передача кольору і багато інших. Відмінність систем відеоспостереження минулих років і наших днів полягає в тому, що ще 10 років тому технології, доступні сьогодні, були дорожчими і складнішими в реалізації. Зараз же моделювання системи відеоспостереження можна організувати дешевше і на більш високому рівні за рахунок використання більш доступних матеріалів і великого вибору програмних і апаратних допоміжних засобів.

У представленій роботі проводиться аналіз програми для тривимірного моделювання VideoCAD, у якій можна створити проект системи відеоспостереження будь-якої складності за короткий проміжок часу. Спеціалізовані розрахунки відеоспостереження (зони огляду, зони виявлення і впізнання людини, зони читання автомобільного номера, подробиці відображення об'єктів в різних ділянках зони огляду, глибина різкості, розрахунки довжини і електричних параметрів кабелів) тісно інтегровані з традиційним CAD інтерфейсом.

Хоча загальні принципи проектування систем охоронного телебачення (СОТ) при "ручному" і комп'ютерному моделюванні однакові, але особливості людського сприйняття графічних зображень і моделювання об'ємних об'єктів програмними засобами математичного моделювання обумовлюють різні підходи до засобів і об'єктів проектування. Далі розглядаються деякі особливості проектування систем охоронного телебачення стосовно до використання програми VideoCAD.

1. Паперовий план об'єкта може бути відсканований і використаний в VideoCAD в якості підкладки для розміщення камер.
2. Прямо на підкладці в VideoCAD створюється попереднє розміщення камер.
3. За допомогою VideoCAD розраховується довжина і необхідні параметри коаксіальних і силових кабелів. Генерується текстовий файл з повним описом всіх відеокамер і кабелів.
4. У проекті буде відзначено все, що необхідно: об'єктив, місце і висота установки кожної камери, зона огляду і навіть модель зображення від відеокамери.
5. Існує можливість вибору найбільш підходящих об'єктивів, висоти і місця установки відеокамер для забезпечення необхідних параметрів зон огляду, виявлення людини і впізнання людини, читання автомобільного номера і отримання на екрані монітора необхідного розміру зображень об'єкта з відомими розмірами і місцем знаходження.
6. Можна виміряти спотворення зони огляду, що виникають через перешкоди.
7. Отримання креслення, що включає 2 проекції контрольованої території із зображеннями зон огляду відеокамер з координатної сіткою і титрами.
8. Можна вивчити закономірності відображення об'єктів в різних ділянках зони огляду за допомогою тестового об'єкта і графічного вікна.
9. Всі розрахунки відбуваються в реальному часі, що дозволяє бачити вплив кожного параметра на кінцевий результат.
10. VideoCAD – недорога і масова програма, яка доступна за ціною навіть приватним користувачам.

Список літератури:

3. Тявловський К.Л. Владимирова Т.Л. Воробей Р.І. Системи відеоспостереження, основи проектування – 2012

4. Уточкін С. VideoCAD – программа для профессионального проектирования телевизионных систем – 2005

СТВОРЕННЯ HIGH AVAILABILITY / DISASTER RECOVERY ІНФРАСТРУКТУРИ ВЕБ-ДОДАТКУ У AMAZON WEB SERVICES

Добринін К.І.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (057) 702-13-20)
e-mail: kyrylo.dobrynin@nure.ua

The report focuses on the problem of web application accessibility under high load using Amazon Web Services. The report shows a way to improve the accessibility of a web application in Amazon Web Services.

Останнім часом все більше бізнесів компаній, продукти яких пов'язані з інформаційними технологіями, постають перед питанням вибору надійного, простого і безпечного хостингу для своїх веб-додатків. Все більше DevOps інженерів та архітекторів IT-рішень прагнуть створити просту і недорогу, але в той же час відмовостійку систему, яка дозволить безпечно зберігати і обробляти дані, а також обмінюватися ними між сервісами за допомогою шифрованих з'єднань.

Базуючись на оцінках експертів і рейтингів публічних хмарних провайдерів [1], одним з лідерів надання послуг хмарних технологій є Amazon Web Services (AWS). Даний провайдер дозволяє організаціям і їх бізнес-партнерам використовувати безпечне середовище AWS для обробки, обслуговування та зберігання інформації з обмеженим доступом [2], а також створювати і управляти великим спектром різних сервісів.

На сьогоднішній день все більше компаній намагаються ефективно управляти даними і забезпечувати їх захист, незалежно від області дії організації. Припустимо, що деяка компанія з назвою "ABCompany" планує розгорнути свій веб-додаток за допомогою хмарного провайдера AWS. У доповіді наведено рекомендації щодо створення відмовостійкого кластеру та впровадження систем аналізу метрик. За допомогою великого вибору сервісів AWS дані цілі можуть бути досягнуті швидко і ефективно.

Показано, що для досягнення High Availability / Disaster Recovery (HA/DR) рекомендується:

1. Створити власну віртуальну мережу та підмережі (Virtual Private Cloud - VPC), які дозволять серверам бути ізольованими і взаємодіяти між собою в рамках однієї віртуальної локальної мережі;
2. Створити групу безпеки (Security Group) в ізольованій мережі VPC. З точки зору безпеки рекомендується відкривати порти в світ тільки
3. 80 (HTTP) і 443 (HTTPS), а порти для підключення до бази даних (наприклад, 3306 - для MySQL) відкрити в межах поточної Security Group;
4. Створити групу автоматичного масштабування (Autoscaling Group)

з необхідними параметрами перевірки працездатності (Health Check)

5. для підтримки робочих серверів. Це дозволить завжди мати необхідну кількість працюючих серверів і створювати аналогічні нові, якщо, припустимо, деякий сервер став недоступним;

6. Створити, як мінімум, два сервера EC-2 (Elastic Compute Cloud) в різних зонах доступності (Availability Zones) у власній мережі VPC і Security Group з використанням Autoscaling Group. Включити шифрування дисків EBS (Elastic Block Store) та обрати оновлений дистрибутив операційної системи. Це дозволить завжди мати працюючий веб-додаток, навіть якщо одна зона доступності або сервер стануть тимчасово недоступними;

7. Створити балансувальник навантаження (Load Balancer) і додати його до Autoscaling Group, що дозволить розподіляти трафік, отриманий від запитів клієнтів, між серверами, а додавання його в групу масштабування дозволить автоматично підключати до нього нові сервера;

8. Впровадити і задіяти власні SSL сертифікати для шифрованого з'єднання (HTTPS) між сайтом і клієнтами. Рекомендується використовувати лише останні версії TLS - 1.2 і 1.3;

9. Створити інстанси бази даних в різних зонах доступності за допомогою сервісу RDS (Relational Database Service) та включити шифрування даних. Розгортання Amazon RDS в декількох зонах доступності забезпечує підвищену доступність та у разі відмови RDS виконує автоматичне перемикання на резервну репліку, що дозволить відновити роботу, як тільки обробка відмови буде завершена [3];

10. Впровадити на серверах pem ключ, який належить AWS для забезпечення шифрованого з'єднання між інстансами та базою даних [4].

Таким чином, раціональне виконання вищезгаданих рекомендацій дозволить забезпечити доступність веб-додатку, шифровані з'єднання і безпечне зберігання конфіденційних даних.

Список використаних джерел:

1. Top cloud providers in 2021. [Електронний ресурс] - Режим доступу: https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/

2. HIPAA in AWS - Overview. [Електронний ресурс] - Режим доступу: https://aws.amazon.com/compliance/hipaa-compliance/?nc1=h_ls

3. Amazon RDS Multi-AZ Deployments. [Електронний ресурс] - Режим доступу: https://aws.amazon.com/rds/features/multi-az/

4. Using SSL/TLS to encrypt a connection to an Amazon RDS Database instance. [Електронний ресурс] - Режим доступу: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html

СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Румянцева О.В.
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (057) 702-00-00
e-mail: olha.rumiantseva@nure.ua

The problem of information security of enterprises and organizations is undoubtedly relevant, and if viewed in the context of protecting critical information infrastructure, it is extremely acute. This report is devoted to modeling the security system of the organization's information system based on the use of information security audit systems. The report discusses the methodological position of the system for modeling the protection of information circulating in information objects in an organization, as well as issues related to the use of these systems. Feasibility and results of the systems application. Specific examples of systems of work.

20 років тому завдання забезпечення безпеки інформації вирішувалася за допомогою засобів криптографічного захисту, встановлення міжмережевих екранів, розмежування доступу. Зараз цих технологій недостатньо, будь-яка інформація, що має фінансову, конкурентну, військову чи політичну цінність, опиняється під загрозою. Додатковим ризиком стає можливість перехоплення управління критичними об'єктами інформаційної інфраструктури. У цій доповіді проводиться аналіз переваг SIEM-систем, які в режимі реального часу оброблюють події безпеки, що надходять від мережевих пристроїв і додатків.

SIEM (Security Information and Event Management) Системи - це програмно-апаратні засоби, що призначені для управління інформаційною безпекою в організаціях в цілому і управління подіями, отриманими з різних джерел. SIEM-системи здатні в режимі реального часу аналізувати події, що надходять від мережевих пристроїв і різних додатків.

Використання SIEM-систем найбільш актуально для організацій, які працюють з конфіденційною інформацією, і яким необхідно регулярно проводити аудити відповідності. Також використання SIEM-систем актуально для компаній, в яких щодня генерується безліч подій різного роду. SIEM використовує велику кількість джерел даних, забезпечуючи максимально повне охоплення подій, що реєструються в ІБ-інфраструктурі і додатках підприємства.

Основними джерелами SIEM систем є [1]:

1. Контроль доступу, аутентифікація (привілеї користувачів, контроль доступу до інформаційних систем, моніторинг).

2. Журнали подій серверів і АРМ (відмовостійкість, контроль доступу, дотримання норм ІБ компанії).

3. Активне мережеве обладнання (мережевий трафік, контроль змін, аварійні Log-повідомлення).

4. IDS \ IPS. (Зміна конфігурацій, мережеві атаки, доступ до пристроїв).

5. Антивірусний захист (працездатність ПО і баз даних, зміна політик і конфігурацій, виявлення шкідливого ПО).

6. Сканери вразливостей (інформація про слабкі місця ПО або мережевих пристроїв).

7. GRC-системи (виявлення ризиків і найбільш критичних загроз, підвищення пріоритету інциденту).

8. Інші системи ІБ і контролю, наприклад, DLP.

9. Системи інвентаризації (контроль активів компанії).

10. Системи обліку трафіку.

SIEM система складається з кілька компонентів [2]:

1. Клієнтські агенти - вони встановлюються на інформаційну систему, що інспектується (агент - це резидентна програма (демон або сервіс), яка збирає журнали подій на локальній машині і передає їх на сервер).

2. Колектори на агентах, вони представляють собою модулі або бібліотеки для розуміння того чи іншого журналу подій або системи.

3. Сервери-колектори - служать для попереднього збору подій від безлічі різних джерел.

4. Сервер-корелятор - збирає інформацію від колекторів і агентів і обробляє її за правилами і алгоритмами, що задані в системі.

5. Сервер сховища і баз даних, необхідний для зберігання всієї корисної інформації.

За допомогою SIEM можна домогтися майже абсолютної автоматизації процесу виявлення загроз. При коректному впровадженні такої системи підрозділ ІБ переходить на абсолютно новий рівень надання сервісу. SIEM дозволяє акцентувати увагу тільки на критичних і дійсно важливих загрозах, працювати не з подіями, а з інцидентами, своєчасно виявляти аномалії і ризики, запобігати фінансовим втратам і підвищувати ефективність і безпеку роботи компанії в цілому.

Список джерел:

5. SIEM как центр системы информационной безопасности [Електронний ресурс] – Режим доступу до ресурсу: https://channel4it.com/publications/SIEM-kak-centr-sistemy-informacionnoy-bezopasnosti-kompanii-14716.html.

6. SIEM: ответы на часто задаваемые вопросы [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/172389/.

БЕЗПЕЧНА АВТЕНТИФІКАЦІЯ ДО ВЕБ ДОДАТКУ З ВИКОРИСТАННЯМ JWT ТА BROWSER FINGERPRINTING

Мазепа А.Д., Тарасов А.С.
Науковий керівник – к.т.н., доцент Радівілова Т.А.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (057) 702-00-00
e-mail: artem.mazepa@nure.ua.

At present, the contemporary methods of authentication have become even more complex than they were 10 years ago. However, the most noticeable changes can be seen in the ever-changing world of the web development. Firstly, this article will discuss one of the many approaches for web authentication implementation with the usage of such concepts like sessions, JWT and browser fingerprinting. Secondly, it will analyze the efficiency of the above-mentioned technics from the security point of view in comparison to other authentication solutions and approaches. Finally, it will discuss some possible drawbacks and vector of improvement for that specific method of implementation.

В наші дні облікові записи від соціальних мереж, банків і різних платформ значать для нас дуже багато і повинні бути надійно захищені. Відповідно до звіту про розслідування порушень даних Verizon, у 2020 році було понад 150 000 підтверджених порушень даних, причому 81% цих інцидентів був пов’язаний із викраденими або слабкими паролями. Тому, підприємства повинні вдруге поглянути на безпеку своїх веб-додатків, починаючи з вивчення більш безпечних методів автентифікації.

Мабуть найбільш розповсюдженим методом автентифікації є JWT (JSON Web Token). JWT – це структура даних у вигляді довгої строки, яка поділяється точками на 3 менші строки. Ці три строки це заголовок, корисна інформація та підпис.

Заголовок зазвичай містить дві речі: тип токену, та назву алгоритму, що використовується для підпису (наприклад, {typ: ‘JWT’, alg: ‘HS256’}). Це кодується в base64.

Корисна інформація – це об’єкт даних JSON. Туди можна помістити все, що завгодно (наприклад, {userId: 2} або, можливо, навіть {userId: 2, admin: true}). Це також кодується в base64.

Підпис – це хеш кодованого заголовка, закодованого корисного навантаження та "секретний" ключ, який безпечно зберігається на сервері, використовуючи алгоритм, визначений у заголовку.

Алгоритм застосування подібний до cookie session, але замість використання session id, використовується JWT, який був підписаний на сервері за допомогою секретного ключа. Підпис дозволяє перевіряти, чи був токен змінений у процесі передачі, що робить його достатньо надійним. Наприклад, звичайний користувач не зможе змінити свій id, який було

прикріплено до його токену на сервері, або не зможе поставити флаг isAdmin: true у об’єкті з корисною інформацією. Інша особливість цього методу це те, що токен не потрібно зберігати на сервері у сховищі для сесій. Після створення, токен повністю автономний. Більш того, на токен не розповсюджуються обмеження з різними серверами, тому його можна використовувати як на різних серверах, так и на різних доменах.

Основний недолік JWT – це вразливість до XSS та інших атак які можуть потенційно отримати доступ до токену користувача, який практично надає повний доступ до облікового запису користувача.

Тому було вибрано механізм browser fingerprinting, який у комбінації з алгоритмом роботи JWT дозволить убезпечити обліковий запис користувача при крадіжки токена.

Browser fingerprints – це строка символів, сформована на основі комбінації даних з комп’ютера (процесор, версія ОС и т.д) та браузера (назва браузеру, версія). У даному випадку, буде використовуватися метод збору відбитків через HTML тег canvas з анімацією, яку кожен комп’ютер буде відображати по різному. Таким чином, при логіні юзера до серверу, він буде відправляти свої данні та відбитки браузера, які будуть слугувати додатковим ідентифікатором. Далі буде створено новий токен, з яким будуть асоціюватися відбитки браузера користувача у базі даних. Тепер, при кожному запиті на сервер, з токеном будуть надсилатися відбитки браузера. Таким чином, коли зловмисник, який вкрав токен, буде намагатися отримати доступу до інформації користувача, йому буде відмовлено тому, що його відбитки браузера будуть відрізнятися від відбитків користувача.

Цей метод достатньо надійний, але потрібно відмітити, що відбитки браузера однозначно ідентифікують користувача, тому зловмисник при отримані їх може прикинутись цим користувачем, та за допомогою вкраденого токена отримати доступ до облікового запису.

З цього можна зробити висновок, що у цьому методі ще є простір для вдосконалення, наприклад реалізація хешування відбитків у базі даних, або відстеження підозрілої активності за допомогою AI, що буде аналізувати підозрілі спроби автентифікації. Але навіть це не зможе гарантувати, що зловмисники не знайдуть інших прийомів для обходження сучасних систем автентифікації. Саме тому у сфері безпеки потрібно завжди бути напоготові.

Перелік використаної літератури:

1. Canvas fingerprinting [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Canvas_fingerprinting

РОЗУМІННЯ ТА ЗАХИСТ ВІД АТАКИ DNS REBINDING

Мазепа А.Д., Тарасов А.С.
Науковий керівник – к.т.н., доцент Радівілова Т.А.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії
ім. В.В. Поповського, тел. (057) 702-00-00
e-mail: artem.mazepa@nure.ua.

Over the past 10 years the market of IoT devices has grew substantially. Most of the families already own one or two of these devices in their homes, which are connected to the local network. Thus, it is essential to apply a proper security measures against possible attackers, who want to gain control over the IoT device for their benefit. Most of the companies do care about the security and apply some basic measures against common attacks. However, most of these measures are not covering the DNS rebinding attack, which is a substantial thread to the end users of IoT devices. This article will cover the general algorithm of the DNS rebinding attack and will explain how to defend your IoT devices from it.

Домашня мережа WiFi – це безпечне місце, наш власний, маленький район кіберпростору. У домашній мережі, ми зазвичай підключаємо наші розумні пристрої, які значно покращують наше життя. Як показує останнє дослідження, проведене британським університетом імені Варвіка, до кінця 2030 року сучасні будинки будуть складатися майже на 80% з IoT девайсів, які можна буде контролювати віддалено. Але навіть зараз вже було розроблено величезну кількість таких девайсів. Від розумних телевізорів та медіаплеєрів до домашніх помічників, камер безпеки, холодильників, замків, дверей та терморегуляторів. Тому на компанії, які виробляють IoT девайси покладена велика відповідальність, щодо захисту їх від різного роду атак. Однак, незважаючи на всі старання компаній закрити усі потенційні вразливі місця, половина з них забуває про дуже стару, але в наш час ефективну атаку DNS rebinding.

DNS rebinding дозволяє віддаленому зловмиснику обходити мережевий брандмауер жертви та використовувати її веб-браузер, як проксі-сервер для безпосереднього зв'язку з пристроями в приватній домашній мережі жертви.

Вперше DNS rebinding була згадана в 2007 році, але не була сприйнята всерйоз через малий спектр застосування, та незначні шанси на вдале проведення цієї атаки. Однак, не так давно, ця атака набула нової сили з розвитком IoT девайсів, та комп’ютерних програм, які застосовують локальний сервер на машинах користувачів.

Головною особливістю цієї атаки є факт того, що вона може подолати границі CORS політик браузера. Наприклад, якщо користувач переходить по зловмисному посиланню в Інтернеті, то веб-сторінка не зможе робити запроси на сайти інших доменів. Браузер обмежує цю поведінку, і дозволяє

робити HTTP запити на ресурси в рамках цього же домену, або іншого домену, який явно дозволяє спільне використання ресурсів.

Стандартний алгоритм цієї атаки виглядає наступним чином. Зловмисник контролює DNS-сервер, який відповідає на запити щодо домену website1. Зловмисник обманює користувача завантажити http://website1 у своєму браузері. Наприклад, за допомогою фішингу. Як тільки жертва переходить за посиланням, їх веб-браузер робить запит DNS, шукаючи IP-адресу website1. Отримавши запит DNS жертви, контрольований зловмисником DNS-сервер відповідає реальною IP-адресою http://website1, 9.9.9.9. Він також встановлює значення TTL для відповіді на 1 секунду, щоб браузер жертви не кешував відповідь від DNS на дуже довго. Жертва завантажує веб-сторінку з http://website1, яка містить шкідливий код JavaScript, який починає виконуватися у веб-браузері жертви. Сторінка починає неодноразово робити запити POST на http://website1/thermostat з корисним навантаженням JSON, наприклад {“tmode”: 1, “a_heat”: 100}. Спочатку ці запити надсилаються на веб-сервер зловмисника, що працює на 9.9.9.9, але через деякий час браузер зазначає, що запис DNS для website1 застарілий, і тому він робить ще один пошук DNS. Шкідливий DNS-сервер зловмисника отримує другий запит DNS жертви, але цього разу він відповідає IP-адресою 192.168.1.77, яка, як виявляється, є IP-адресою розумного термостата в локальній мережі жертви. Машина жертви отримує цю відповідь DNS і починає робити запити HTTP, на http://website1/thermostat, але з Ip 192.168.1.77. Цього разу цей запит POST надсилається на невеликий незахищений веб-сервер, що працює на термостаті, підключеному до Wi-Fi. Термостат обробляє запит, і температура в будинку жертви встановлюється на 100 градусів.

Захист від цієї атаки достатньо простий. У багатьох випадках, розробникам IoT девайсів потрібно перевіряти поле хост у HTTP запиті. Якщо поле хост відповідає сторонньому сайту, а не локальній мережі, то просто відхиляти запит на IoT девайси. Однак, проблема у тому, що у багатьох випадках користувачі IoT девайсів просто не оновлюють програмне забезпечення, та девайс залишається вразливим до атак, навіть коли патч вже було випущено.

Підводячи підсумки можна сказати, що ця атака ще буде актуальною якийсь час, доки усі розробники не будуть адресувати цю вразливість, та усі користувачі не оновлять свої смарт пристрої.

Перелік використаної літератури:

2. DNS Rebinding [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/DNS_rebinding

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ «STEALER»

Тарасов А.С., Мазепа А.Д.
Науковий керівник – к.т.н., доцент Добринін І.С.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (057) 702-00-00
e-mail: andrii.tarasov@nure.ua.

The transition from the classical method of storing and transmitting information in the form of paper data to the digital method entailed problems associated with information security. Cybersecurity is an activity aimed at protecting systems, networks and programs from digital attacks. One of the threats to cybersecurity is malware. The relevance is due to the fact that ignorance by users of personal computers and other devices that work over the Internet about the presence of malicious software «Stealer» and ways to protect against it, can lead to serious consequences, such as disclosure of confidential information, withdrawal of funds from bank accounts and more.

Нині більшість інцидентів інформаційної безпеки у світі пов'язані з крадіжкою персональних даних. Значні ризики становить шкідливе програмне забезпечення (ПЗ). Шкідливе ПЗ «Stealer» є одним з найбільш поширених типів шкідливих програм, виявлених в даний час. Предметом полювання зловмисників є крадіжка якомога більше персональних даних, від базової системної інформації до локально збережених імен користувачів й паролів.

Фундамент будь-якої системи становить модель загроз. Міжнародним стандартом з інформаційної безпеки ISO/IEC 27001 передбачається обов'язкове використання моделі загроз, на основі якою здійснюється вибір захисних методів та заходів з метою запобігання несанкціонованому доступу до персональних даних та передачі їх особам, які не мають права доступу до такої інформації. При виявленні загрози безпеки персональних даних пов'язаної з шкідливим ПЗ типу «Stealer» необхідно враховувати її при доповненні чи розробці моделі загроз.

Основними засобами протидії шкідливим ПЗ були та залишаються антивірусні програми, але використовуючи такі процедури та засоби як обфускація, криптори, обхід засобів віртуалізації, що здатні обійти методи статичного, динамічного та евристичного аналізу, використовуваних в новітніх антивірусних продуктах, отже необхідно застосовувати додаткові заходи безпеки.

Алгоритм дій даного типу шкідливого ПЗ як правило націлений на дані браузера, а саме на збережені паролі, облікові дані банківських послуг та файлів cookie, які зазвичай встановлені шляхом за замовчуванням.

Для уникнення проблем з доступом шкідливе ПЗ робить копію файлу зі збереженими паролями. Після чого робиться запит до бази даних цього фалу на такі поля як пароль, ім’я користувача та URL-адрес сайту. Всі поля зберігаються у відкритому вигляді, окрім пароля. З зашифрованого поля пароля вилучаються такі дані як одноразовий код, пароль та заголовок, необхідні для алгоритму дешифрування AES-256.

На сьогоднішній момент сучасні версії браузерів на основі Chromium використовують алгоритм AES-256, в той час, як криптографічний інтерфейс програмування додатків (DPAPI) використовується тільки для захисту ключа шифрування від вбудованого сховища. Секретний ключ зберігається у файлі шлях якого за замовчуванням визначено браузером, доступ до файлу є відкритим, тому шкідливе ПЗ вилучає зашифрований ключ. Для шифрування та дешифрування даних браузер використовує два виклики Windows API: CryptProtectData й CryptUnprotectData [1]. За викликом функції CryptUnprotectData на основі логіну та паролю користувача системи зашифрований ключ дешифрується. Таким чином за допомогою отриманих даних та ключа шифрування дешифрується пароль.

Додатковими функціями «Stealer» можуть слугувати файли сесії месенджерів. Орієнтуючись на встановлені шляхи за замовчуванням шкідливе ПЗ отримує доступ до акаунту без перешкод. Крім того, можливе вилучення логіну та паролю облікового запису користувача з використанням дампу пам’яті системного процесу перевірки автентичності локальної системи безпеки.

З метою забезпечити захист рекомендовано використовувати наступні заходи: використання майстра пароля зі зберіганням на довіреному сервері для захисту ключа шифрування; зміна шляхів файлів браузерів та месенджерів; припинити використання облікових записів адміністратора за замовчуванням та встановити рівень контроль облікових записів на «Завжди повідомляти»; відключити командну оболонку cmd та PowerShell й заборонити редагування реєстру; оновити бази сигнатур антивірусів.

Рекомендовані заходи значно знизять ризик атак від даного типу шкідливих програм.

Перелік використаної літератури:

3. Info Stealers | How Malware Hacks Private User Data [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://labs.sentinelone.com/info-stealers-how-malware-hacks-private-user-data/.

DIGITAL FORENSICS CHALLENGES PRESENTED BY IOT DEVICES

Joel Kashaija
Scientific Adviser – Assoc. Prof. Alexander Adamov
KNURE«Kharkiv National University of Radio Electronics»,
Faculty of Info Communication, 14, Nauka Ave., Kharkov, Tel (057)702-00-00
e-mail: joel.kashsija@nure.ua

The latest developments in the sensing capabilities and connectivity of the electronics devices led to the apparition of a very complex and challenging domain of Internet of Things – IoT. In this concept all the devices are interconnected between each another and also are connected to the Internet by using various standardized communication protocols. The recent DDOS attacks (October 2016) showed how vulnerable these tiny devices can be [5]. Below picture shows the IoT device architecture.

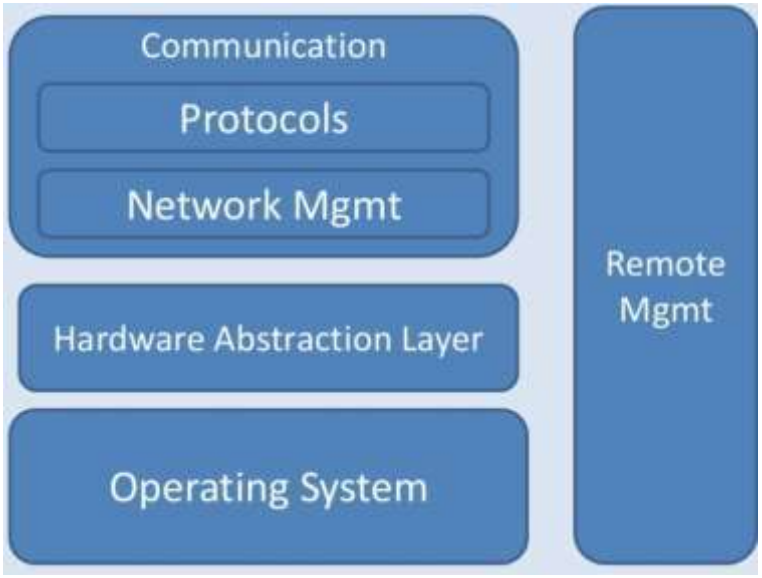


Fig 1 – IoT Device Architecture.

Some of These Challenges IoT devices present to forensics investigators are due to their nature of technologies such as RFID,Sensors and Cloud computing, used in IoT environments together with their small Capacity that presents mores issues when it comes to logging[2]. Although these challeges discussed are more sounding like technical IoT also present callenges such as determining what are IoT devices, How to forensically acquire data and Secure the Chain of Custody etc [2]. More Tools are Needed That should help Forensics investigators Tackle these Hurdles[3]. Eyhab in his Conference he proposed Fog Based IoT forensic Framework that solves critical functions such as data filtering and aggregation.[4]. In this framework frog computing is a network model in which computing and storage resources are place in the network. It offers numerous advantages to IoT systems, such as improved scability, reduced

network latency, faster responsiveness, and potential improvement for security and privacy. Its useful to filter traffic and data going to IoT devices. This Information can be used as digital evidence in case there is a cyber attack or threat. By deploying this framework it also helps in troubleshooting which Devices are not fucntioning properly or have been compromised.

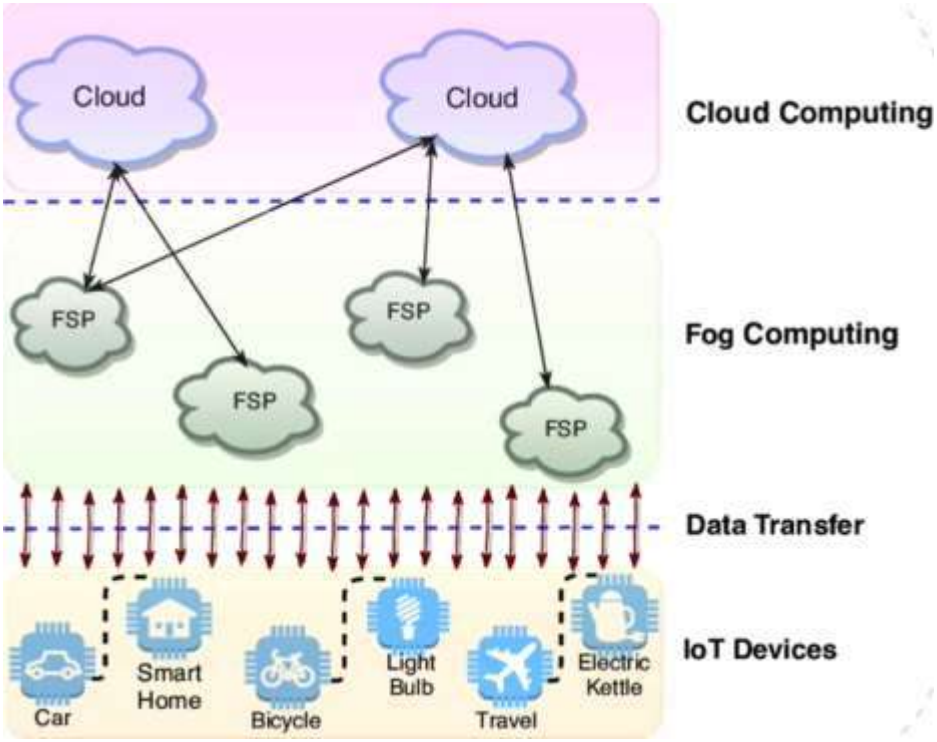


Fig 2 – General Framework of internet of things

In this article i illustrated some challenges presented by IoT devices mostly due to their nature. Lastly i illustrated how Fog can be utilised to identify and mitigate cyber attacks on IoT systems at early stages.

1. M. Dlamini, to M.Eloff, " Internet of things: Emerging and Future Scenarios from information security perspective",
2. Thamini Janarthan, "IoT forensics: An Overview of the Current Issues"
3. M. Stoyanova, Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues," IEEE Communications Surveys & Tutorials, 2020. doi: 10.1109/COMST.2019.2962586. [Online]. Available:
4. EyhabAl-masriYan Bai "Digital Forensic Investigation Framework for IoT Systems"
5. Hiitu garg, Dave" Securing IoT devices using Rest Api and Middleware"

КЛАСИФІКАЦІЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ ТА АТАК НА БЕЗПРОВОДОВІ МЕРЕЖІ

Герус М.А.
Науковий керівник – к.т.н., доц. Куля Ю.Е.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії імені В.В. Поповського, тел. (057) 702-13-20
e-mail: mariia.herus@nure.ua

Analysis of the current situation shows that the main reason for the indecision of the transition to wireless networks is the problem of information security, the level of which for both individual lines and for the system as a whole has not yet been determined. Wireless networks use air and space to transmit and receive information. Ensuring that the confidentiality and integrity of information is properly protected when it is transmitted between workstations and access points is a very important aspect of the security of the system as a whole. Due to the wide availability of wireless devices and their low cost, security breaches occur. The specifics of wireless networks provide that data can be intercepted and changed at any time.

Бездротові мережі використовують повітря і простір для передачі та прийому інформації. Тобто сигнали є відкритими для будь-якої особи, що знаходиться в зоні дії. Забезпечення належного захисту конфіденційності та цілісності інформації при її передачі між робочими станціями і точками доступу є дуже важливим аспектом безпеки всієї системи в цілому. Велика популярність безпровідних пристроїв та їх доступна вартість призводять до того, що в периметрі мережної безпеки виникають проломи.

Специфіка безпровідних мереж (БМ) має на увазі, що дані можуть бути перехоплені та змінені у будь-який момент. Для одних технологій досить стандартного бездротового адаптера, для інших потрібне спеціалізоване обладнання. Але в будь-якому випадку, ці загрози реалізуються достатньо просто, і для протистояння їм потрібні ефективні криптографічні механізми захисту даних.

Спочатку визначимо основні терміни, які будуть використовуватися в подальшому: «вразливість», «загроза» та «атака». Під вразливістю системи захисту розуміється така її властивість, яка може бути використана зловмисником для здійснення несанкціонованого доступу (НСД) до інформації. При цьому будь-яка вразливість системи захисту несе в собі загрозу здійснення зловмисником НСД до інформації, за допомогою реалізації атаки (або атак, які в загальному випадку можуть принципово відрізнятися) на вразливість в системі захисту. Таким чином, саме уразливість системи захисту – це ознака системи, а наявність (відсутність) вразливостей є характеристикою захищеності системи.

Вочевидь, що в загальному випадку причиною вразливості може бути або некоректність реалізації механізму захисту, або недостатність набору механізмів для умов використання об'єкта інформатизації, що захищається. Взагалі кажучи, властивості коректності реалізації і повноти (достатності для умов використання) є основними властивостями будь-якої технічної системи, в тому числі, і властивостями системи захисту інформації. Аналіз існуючого стану показує, що основною причиною нерішучості переходу на бездротові мережі є проблеми інформаційної безпеки, рівень якої як для окремих ліній, так і для системи в цілому, поки не визначений. Готуючись до забезпечення безпеки безпровідних мереж, перш за все, необхідно встановити, що може їм загрожувати.

Відразу слід зазначити, що бездротові мережі відрізняються від дротових тільки на перших двох – фізичному і частково канальному рівнях семирівневої моделі взаємодії відкритих систем. Більш високі рівні реалізуються відповідно до тих самих принципів, що і в дротових мережах, а реальна безпека мереж забезпечується саме на цих нижчих рівнях.

Прийнято вважати, що безпеці безпровідних мереж загрожують:

- порушення фізичної цілісності мережі;
- підслуховування трафіку;
- вторгнення в мережу.

Загрозу мережній безпеці можуть представляти природні явища і технічні пристрої, проте тільки люди впроваджуються в мережу для навмисного отримання або знищення інформації і саме вони становлять найбільшу загрозу. При розгляді вразливостей мереж стандарту 802.11 можна виділити дві групи загроз: загрози на сигнальному рівні і загрози на інформаційному рівні.

Наявність вразливостей на сигнальному рівні робить проблематичним захист інформаційного рівня, на якому вони повинні бути попереджені:

- цілеспрямоване спотворення переданих та отриманих даних;
- перехоплення управління системою зв'язку або інформаційною системою.

Крім того, до цих пір не розроблена детальна модель загроз, які існують в області цифрових мереж бездротового доступу, і методів боротьби з ними. Потрібно відзначити, що високий ступінь захищеності каналу на сигнальному рівні не є гарантією забезпечення настільки ж високої інформаційної захищеності всієї системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Буров Є.В. Комп'ютерні мережі. — Львів : БаК, 2003. — 584 с.

2. Климаш М.М., Пелішок В.О. Проектування ефективних систем безпровідного зв'язку. — Львів: «Львівська політехніка, 2010. — 224 с.

АКТУАЛЬНІСТЬ ТА ПРОБЛЕМАТИКА КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ

Красюкова В.В.
Науковий керівник – доц. Куля Ю. Е.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії імені В.В. Поповського)
e-mail: valeriia.krasiukova@nure.ua

With the prolific usage of electronic devices such as smartphones and computers, the amount of data generated from these devices is vast. As such, there can be an expectation within almost any investigation for the need to identify digital evidence. If identified, collected and analysed in a forensically sound manner, electronic evidence can prove crucial to the outcome of criminal, civil and corporate investigations. Evidence uncovered through computer forensics is subject to the same legal guidelines as all other criminal evidence. It must be legally obtained to be admissible in court.

З розвитком комп'ютерних технологій з'явилися нові види злочинів, об'єктом злочинного посягання яких є інформація і права на неї. Виникає гостра необхідність захисту такого роду інформації, що послугувало приводом для розгляду нових засобів по виявленню, розслідуванню і попередженню злочинів, які здійснюються з використанням комп'ютерної техніки.

Цифрова криміналістика – це підрозділ криміналістики, прикладна наука про розслідування злочинів (інцидентів) та збір цифрових доказів, які перебувають на комп'ютерах, системах зберігання даних, в комп'ютерних мережах, на мобільних і інших цифрових пристроях. Основним завданням комп'ютерної криміналістики є ідентифікація фактів, які дозволяють довести або спростувати звинувачення в шахрайстві або існування інциденту в сфері інформаційної безпеки, підготовка всебічного і аргументованого підходу до виявлення, збереження, аналізу, відтворення і перевірка електронних доказів.

Проблеми комп'ютерної криміналістики можна поділити на три сфери: технічні, правові та підготовка фахівців (експертів з комп'ютерної криміналістики).

Щодо технічних, то можна виділити такі як вилучення даних з цифрових носіїв, відновлення інформації, пошук, аналіз і інтерпретація даних та забезпечення збереження цифрових доказів.

Кожний пункт з цього списку має свій вплив на розслідування інцидентів.

Неправильне вилучення даних з жорсткого диску або флеш-накопичувачів, може зруйнувати всі докази, які могли зберегтися на них.

Треба дотримуватися таких правил: неруйнівне копіювання даних, відповідність копії до оригіналу, повнота копії (якщо є приховані файли, то вони обов'язково повинні бути перенесені, щоб надалі їх можна було розшифрувати), швидкість копіювання (висока ємність накопичувачів), збереження копій у відповідному стані, захист даних та запобігання витоку інформації.

Правові проблемі стосуються тих самих доказів (файли добуті із накопичувачів та ін.), адже не всі докази можуть в достатній мірі підтверджувати злочин. Також через неправильне відновлення інформації, частина доказів може буди знищена або змінена, тому їх можуть вважати недостовірними.

Проблематика хмарної криміналістики:

— більшість провайдерів хмарних послуг підтримують надмірну кількість центрів обробки даних, розташованих в декількох місцях по всьому світу;

— стрімке зростання кількості стільникових пристроїв, які отримують доступ/завантажують/створюють/змінюють і переміщують дані в хмарі, тобто дані можуть бути в декількох місцях в один і той же момент часу;

— користувач не володіє сховищем даних, він просто орендує його;

— відсутність контролю за доступом - дані, аналізовані в ході судової експертизи, повинні були б відділятися від інших даних;

— відсутність фізичної інфраструктури для фіксації або визначення часу створення/модифікації даних і ведення журналу подій;

— умови договору між організацією і провайдером хмарних послуг можуть не допускати судової експертизи, яку необхідно провести;

— отримати докази без їх модифікації надзвичайно складно;

— різні хмарні сервіси управляють своїми сховищами даних і умовами роботи по-різному.

Цифрова криміналістика – це кропітка праця, яка вимагає деталізації кожного кроку. Всі деталі повинні бути враховані, необхідно документувати все підозріле, що піддається розгляду, вміти думати як зловмисник (моделювати схему злочину) і мати великий запас терпіння для пошуку всіх доказів. У цифровій криміналістиці є багато областей, які вимагають глибоких експертних знань.

Список літератури:

1. Маркусь В. О. Криміналістика. Навчальний посібник – К.: Кондор, 2007.

2. Яблоков, Н. П. Криміналістика в 5 т. Том 1. Історія криміналістики: підручник для магістратури. — Москва: Юрайт, 2020.

ЗАБЕСПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕРЕЖ ІНТЕРНЕТА РЕЧЕЙ

Ларіонов В.В.
Науковий керівник – д.т.н., проф. Агеєв Д.В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (057) 702-13-20
e-mail: vitalii.larionov@nure.ua.

The Internet of Things (IoT) is a relatively new technology, but there are difficulties in its development that are characteristic of advanced developments. Among these problems, the most serious is the problem of information security. Given conference paper analyzes the main factors and threats to the information security of the Internet of Things. Factors that affect the security of the Internet of Things include: heterogeneity of devices, or fragmentation and security issues of obsolete devices. It is proposed to build the security of the Internet on the basis of: communication security; device protection; control of devices; control of network interactions.

Вступ

Інтернет речей (IoT - Internet of Things) - відносно нова технологія, яка об'єднує безліч «розумних» пристроїв в мережу, що дозволяє їм збирати, аналізувати, обробляти і передавати один одному дані. Ця галузь стрімко розвивається, проте на шляху її розвитку зустрічаються труднощі, характерні для передових розробок. Як і будь-яка технологія, що швидко розвивається, вона відчуває ряд «хвороб зростання», серед яких найбільш серйозною є проблема інформаційної безпеки. Чим більше «розумних» пристроїв підключається до мережі, тим вище ризики, пов'язані з несанкціонованим доступом в IoT-систему і використанням її можливостей зловмисниками.

Проблеми безпеки, пов'язані з Інтернетом речей.

Незважаючи на невелику кількість функцій і обмежені можливості пристроїв, існує ризик, що зловмисники отримають контроль над підключеними до мережі комп'ютерами загального призначення, можуть почати шпигувати за допомогою відеомоніторів для контролю за дітьми, а можуть і перервати роботу служб на обладнанні, призначеному для систем життєзабезпечення. Після отримання контролю зловмисники можуть вкрасти дані, припинити роботу служб або здійснити будь-які інші кіберзлочини. Атаки зі зломом інфраструктури Інтернету речей призводять не тільки злому даних і ненадійній роботі, а й фізичного пошкодження

обладнання або, що ще гірше, травм людей, які на ньому працюють або від нього залежать.

До факторів, що впливає на безпеку Інтернету речей можна віднести наступні.

Гетерогенність пристроїв, або фрагментація. У багатьох компаніях використовується величезна кількість всіляких пристроїв з різними програмами, мікросхемами і навіть методами підключення. Через нього виникають складності з відновленням всіх різноманітних підключених пристроїв і управлінням ними.

Проблеми безпеки застарілих пристроїв. Частина пристроїв впроваджені ще до Інтернету речей, і по відношенню до таких пристроїв ніколи не застосовувалася додатковий захист, тобто ідентифікація і усунення або зменшення вразливостей. Інша частина застарілих пристроїв розроблені без урахування питання безпеки в Інтернеті речей.

Атаки в Інтернеті речей можна в цілому розбити на п'ять категорій: спуфинг, незаконна зміна, розкриття інформації, відмова в обслуговуванні і підвищення прав.

Підхід для забезпечення безпеки Інтернету Речей.

Безпека інтернету речей можна побудувати на фундаменті з чотирьох наріжних каменів:

- безпека зв'язку;
- захист пристроїв;
- контроль пристроїв;
- контроль взаємодій в мережі.

На цьому фундаменті можна створити потужну і просту в розгортанні систему безпеки, яка здатна послабити негативний вплив більшості загроз безпеки для інтернету речей, включаючи цілеспрямовані атаки.

Висновок

Системи IoT бувають дуже складними і вимагають комплексних заходів захисту. Сьогодні IoT тільки розвивається, і, як і будь-яка нова технологія, все ще стикається з численними проблемами і перешкодами.

Однак у швидкому розвитку зацікавлені як користувачі, так і великі компанії, готові вкладати великі гроші в розвиток і дослідження безпеки. Простого і універсального рішення не існує, проте роблячи кроки в правильному напрямку, реально усунути будь-які уразливості. Можна з упевненістю сказати, що IoT чекає велике майбутнє.

ШЛЯХИ МІНІМІЗАЦІЇ ІНФОРМАЦІЙНИХ РИЗИКІВ ПРИ РОБОТІ З ВІРТУАЛЬНИМИ МАШИНАМИ

Шульга М.Д.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки
61000, Харків, просп. Науки,14, каф. ІКІ ім. В.В. Поповського,
тел. (057) 702-13-20, e-mail: mykyta.shulha@nure.ua

The level of penetration of virtualization technologies continues to grow, respectively, the number of information security threats increases and the attention to security tools increases. Modern virtualization platforms are becoming more reliable, and their implementation allows you to solve a wide range of security problems that are typical for traditional IT - for example, a cable break, a failure of the physical board of a particular server. At the same time, the main problems in the field of security of virtualization platforms are related to the design of end solutions based on them. Obviously, when implementing a virtualization platform, you need to evaluate different parameters: the criticality and volume of data, the risks, the cost of deploying and owning a virtual infrastructure-compared to traditional IT systems.

Завданням управління ризиками IT-проектів є своєчасне визначення факторів, пов'язаних з впровадженням інформаційної системи або системи автоматизації, які можуть негативно вплинути на реалізацію проекту впровадження, а також оптимальне планування дій з мінімізації цих факторів.

Зараз багато організацій використовують віртуальні машини в якості необхідного програмного забезпечення для тестування рішень. Актуальність захисту даних віртуальної машини є невід’ємною частиною інформаційної безпеки підприємства у роки впровадження віртуальної інфраструктури. Існує багато ризиків при роботі з віртуальними машинами. Наприклад: деякі організації використовують порт 445 або 139. Залишаючи дані порти незахищеними, компанія дає доступ на свій жорсткий диск вірусам, троянам, черв'якам. Але за деяких обставин, компанія не може закрити ці порти, тому цей момент треба враховувати при аналізі ризиків. Ринок віртуальних систем зараз пропонує безліч продуктів, які дозволяють вирішити всі ці проблеми, однак схема їх впровадження та обслуговування завжди індивідуальна для кожної організації і вимагає чималих витрат.

Віртуалізація породжує не тільки переваги, а й ризики для IT-інфраструктури, тому необхідні спеціальні засоби, які захищають віртуалізацію. Одним із перших свої рекомендації щодо захисту технологій віртуалізації видав Національний інститут стандартів і технологій США (NIST). Нижче наведено механізми захисту даних віртуальної машини запропоновані NIST:

– ізоляція операційних систем (поділ ресурсів);
– аудит гостьових операційних систем;
– контроль і перевірка копій образів і знімків гостьових машин;
– міграція операційних систем [2].

Засоби захисту віртуального середовища спрямовані на створення інструментів контролю і протидії зловмисникам або зловживанням. Таким чином, формуються умови щодо визначення дій, які необхідно виконати для зниження інформаційних ризиків і забезпечення безпеки застосування технологій віртуалізації IT-інфраструктури [2].

Взявши за основу механізми захисту запропоновані NIST можна додати ще деякі рішення, які знизять ймовірність форс-мажорів при роботі з віртуальними машинами:

– використовувати багатофакторну аутентифікацію та шифрування;
– використання SaaS-рішення (Software as a service) Crowdstrike;
– використовувати принцип найменших привілеїв;
– аналізувати файли журналів системи;
– побудова системи розгортання оновлень безпеки операційних систем і додатків;
– використовувати DLP-рішення (Data Loss Prevention).

Застосування всіх рекомендацій створює комплексне рішення захисту віртуальної інфраструктури на всіх рівнях. Впровадження технологій віртуалізації на різних рівнях в організації являє собою досить складний і трудомісткий процес, який вимагає дуже грамотного планування і кваліфікованого персоналу. Оцінити, як саме в грошовому еквіваленті віртуалізація принесе ефект, завжди дуже складно. Необхідно провести повну інвентаризацію та аналіз існуючого парку програмного і апаратного забезпечення, врахувати специфіку платформ віртуалізації, їх вимоги та обмеження, спланувати стратегії резервного копіювання і відновлення після збоїв, налагодити управління віртуальними системами і підготувати фахівців.

Список літератури:

7. Guide to Security for Full Virtualization Technologies [Електронний ресурс] – Режим доступу до ресурс https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf/

8. Аналіз ризиків застосування технологій віртуалізації і контейнеризації в хмарних сервісах [Електронний ресурс] – Режим доступу до ресурсу: https://con.dut.edu.ua/

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ, ПОБУДОВАНИХ ПО ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Сердюк А.Ю.
Науковий керівник – к.т.н., доц. Снігуров А.В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (068)194-31-69
e-mail: alona.serdiuk@nure.ua.

The report presents the results of threats and vulnerabilities analysis identified for systems built on IoT technology. The paper analyzes the possibility of using for risk analysis of information security systems built on IoT technology, such risk assessment techniques as CRAMM, GRIF, COBRA, OCTAVE, presents the results of information security risk analysis for medical systems built on IoT technology, which provide monitoring of vital human parameters.

Концепція Інтернету речей (IoT) на даний час охоплює усі сфери нашого життя. По даним Juniper Research [1] загальна кількість підключень IoT досягне до 2024 року 83 мільярди. Це більше порівняно з оцінками щодо 35 мільярдів підключень у 2020 році, і це означає зростання кількості пристроїв IoT на 130% протягом наступних чотирьох років.

Згідно з The American Society of Mechanical Engineers [2] деякими найпоширенішими прикладами використання технології IoT у 2020 році були наступні.

1. Пристрої для забезпечення home security. IoT використовує датчики, сигнали тривоги, камери, світло та мікрофони для забезпечення цілодобової та безперервної безпеки, - всіма якими можна керувати за допомогою смартфона.

2. Трекери активності. Ці сенсорні пристрої призначені для носіння протягом дня для моніторингу та передачі основних показників здоров’я в режимі реального часу, таких як втома, апетит, фізичні рухи, рівень кисню, кров’яний тиск, виявлення падіння та дотримання ліків.

3. AR-окуляри. Google Glass - це невеликий, легкий комп’ютер, який носять як окуляри для роботи в режимі “вільні руки”. Інформація представлена в “лінзах” окулярів, які можуть отримати доступ до різноманітних Інтернет-програм, включаючи Карти Google та Gmail.

Наразі технології IoT функціонують не тільки на рівні взаємодії з людиною, а й на підприємствах, та у масштабі міст. Прикладами приладів з таких розгорнутих IoT систем наразі є: IoT Сенсори (прилади, які зчитують, передають і зберігають таку інформацію, як температура, тиск, вібрації, тощо), система відстеження та моніторингу IoT (за допомогою GPS пристроїв відстежують об’єкти на великих відстанях), система управління фабрикою, система зв’язку багатьох інших систем, які використовуються на рівні

забезпечення життєдіяльності (генератори електроенергії, дроти передачі сигналів, системи їх використання та інші).

IoT охоплює багато сфер життя, тому може бути дуже різноманітним список технологій, які використовуються в IoT: Bluetooth, RFID, Wi-Fi, Thread, ZigBee, NB-IoT, LoRaWAN, LTE-Cat m1, Sigfox тощо.

Різноманіття пристроїв та сфер застосування технології IoT призвело до наявності значної кількості загроз та вразливостей. У 2018 році команда проекту OWASP визначила найнебезпечніші загрози для IoT [3]:

- слабкі, вгадувані паролі;
- небезпечні послуги мережі;
- небезпечні інтерфейси екосистеми;
- відсутність механізму безпечного оновлення;
- використання незахищених або застарілих компонентів;
- недостатній захист конфіденційності;
- небезпечна передача та зберігання даних;
- відсутність менеджменту та інші.

В роботі предметом дослідження є підходи до аналізу ризиків інформаційних систем, побудованих по технології IoT. В доповіді приводяться результати аналізу загроз та вразливостей, які виявлені різними дослідниками для таких систем. Враховуючі, що різні методики оцінки ризиків інформаційної безпеки мають певні особливості для їх використання, в роботі проведений аналіз можливості застосування для аналізу ризиків систем, побудованих по технології IoT, таких методик як CRAMM (CCTA Risk Analysis and Management Method), ГРИФ, COBRA (Consultative Objective and Bi-Functional Risk Analysis), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

В доповіді приведений приклад оцінки ризику інформаційної безпеки медичним системам, побудованим по технології IoT, які забезпечують моніторинг життєвих параметрів людини.

Список використаних джерел:

1. IoT Connections to Reach 83 Billion by 2024, Driven by Maturing Industrial Use Cases [Електронний ресурс]. – Режим доступу: https://www.juniperresearch.com/press/press-releases/iot-connections-to-reach-83-billion-by-2024-driven.

2. Best IoT Examples in 2020 [Електронний ресурс]. – Режим доступу: https://www.asme.org/topics-resources/content/10-best-iot-examples-in-2020.

3. OWASP IoT Top 10 List of IoT Vulnerabilities [Електронний ресурс]. – Режим доступу: https://sectigostore.com/blog/owasp-iot-top-10-iot-vulnerabilities/.

МЕТОДИКА ПРОВЕДЕННЯ DOS-АТАКИ НА МЕРЕЖІ СТАНДАРТУ 802.11 ЗА ДОПОМОГОЮ ПАКЕТІВ KALI LINUX ТА AIRCRACK-NG З МЕТОЮ АНАЛІЗУ ЇХ ВРАЗЛИВОСТЕЙ

Гонтарь І. А.
Науковий керівник – доц. Снігуров А. В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії
ім. В.В.Поповського, тел. (057) 702-10-67
e-mail: ivan.hontar@nure.ua.

The report presents a method of a DoS-attack on an end-user, using the Kali Linux and Aircrack-ng packages. Also, it includes a bash-based script creation and actions, which can be realized on a wireless network, and existing simple attacks on it. The results of the experiment on the DoS-attack are attacks on the experimental 802.11 network.

A denial-of-service (DoS) attack is an attack designed to shut down machines or networks, making it inaccessible to scheduled users. DoS attacks achieve this by flooding targeted traffic or sending information that fails.

Одним з основних процесів побудови та експлуатації систем менеджменту інформаційної безпеки організацій (установ) є аудит, основне призначення якого є визначення вразливостей інформаційних систем (етап планування), оцінка якості системи захисту (етап функціонування та моніторингу). Методи проведення аудиту залежать від того, які інформаційні системи перевіряються. Для перевірки технічних систем дуже ефективним є тест на проникнення (Penetration test, пентест), який є методом проведення аудиту. Такий тест проводиться фахівцем з інформаційної безпеки (білим хакером), який шляхом злому системи захисту інформаційної системи намагається виявити вразливості для кібератак для подальшої їх ліквідації.

У роботі було розглянуто використання пакету Kali Linux та його інструменту Aircrack-ng для розробки скрипта для DoS атаки на мережі стандарту 802.11. Дані програмні пакети створені спеціально для тестування та знаходження вразливостей у системі фахівцями з інформаційної безпеки для зменшення ризику несанкціонованого доступу. Ці системи є у відкритому доступі та мають великі можливості, завдяки значній кількості інструментів та утиліт, які допомагають виявляти вразливості в системі. Aircrack-ng – це повний набір інструментів для оцінки безпеки мережі WiFi. Він фокусується на різних областях безпеки WiFi [1]:

– моніторинг: захоплення пакетів та експорт даних у текстові файли для подальшої обробки сторонніми інструментами;

– атаки: повторні атаки, деаутентифікація, створення підроблених точок доступу тощо за допомогою пакетної ін'єкції;

– тестування: перевірка карт WiFi та драйверів (захват і введення);
– злом: WEP і WPA PSK (WPA 1 і 2).

Методика проведення DDOS-атаки на безпроводові мережі стандарту 802.11 має наступну послідовність дій.

1. Сканування за допомогою airodump-ng усіх доступних бездротових точок доступу для знаходження цілі.

2. Запам'ятовування MAC адреси цілі (bssid).

3. Використовуючи airodump-ng та відому MAC адресу точки доступу – з'ясування MAC адреси клієнта.

4. Застосування скрипта у вічному циклі:

– ! # / bin / bash
– while true
– do
– aireplay-ng –0 [x] -a [y] -c [z] wlan0
– ifconfig wlan0 down
– iwconfig wlan0 mode monitor
– ifconfig wlan0 up
– iwconfig wlan0 | grep Mode
– sleep [k]
– echo pause
– done,

де [x] – кількість пакетів на деаутентифікацію, [y] – MAC адреса точки доступу, [z] – MAC адреса кінцевого клієнта, [k] – кількість секунд на затримку роботи скрипта.

Після запуску скрипта, клієнт не зможе підключатися до бездротової точки доступу, а інші – зможуть.

В доповіді розглядається методика проведення DoS атаки на кінцевого клієнта за допомогою пакетів Kali Linux та Aircrack-ng. Також в доповіді розглянуто створення скриптів на основі bash та дії, які можна здійснити при підключенні до мережі, та які прості атаки існують на бездротові мережі. Приведені результати експерименту по проведенні DoS – атаки на експериментальну точку доступу мережі 802.11.

Список використаних джерел:

1. Aircrack-ng [Електронний ресурс]. – Режим доступу: https://www.aircrack-ng.org/documentation.html.

УДК 004:621.391

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

СИНТАКСИЧНИЙ АНАЛІЗ ВИХІДНОГО КОДА ПРОГРАМ З МЕТОЮ ВИЯВЛЕННЯ ЗБІГІВ

Чапарин І.М.
Науковий керівник – ас. Дух Я.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ЕОМ, тел. (057)-702-13-54)
e-mail: illia.chaparyn@nure.ua

Plagiarism has been a serious problem at all times.

However, in the era of rapid technological development, it takes on new and new forms, which require new solutions. Completely different solutions. Source code analyzing is not an easy job for a human brain, since it is just adapted for text in natural languages. While the computer deals with this task many times better and more accurately. Parsing is a key concept to help us manage this.

Одним з центральних понять в обробці інформації є формалізуюча операція, яка називається синтаксичним аналізом (або парсингом).

Вхідною послідовністю є певний текст. Це може бути текст іншою мовою (або на іншому рівні мови), або недостатньо або зовсім не формалізований текст, непридатний для простої автоматичної обробки.

Парсинг – це процес зіставлення лінійної послідовності лексем мови з його формальної граматикою[1].

Тобто для виконання такого роду аналізу необхідно визначити граматику мови, а також мати необхідний набір різних граматик для ймовірних мов.

Результатом зазвичай є дерево розбору (синтаксичне дерево). Зазвичай застосовується спільно з лексичним аналізом[1].

Синтаксичний аналізатор (парсер) – це програма або частина програми, що виконує синтаксичний аналіз, тобто розпізнавання вхідної інформації. При цьому вхідні дані перетворюються до вигляду, придатного для подальшої обробки. Цей вид зазвичай являє собою формальну модель вхідної інформації на мові подальшого процесу обробки інформації[2].

Використання аналізаторів залежить від вхідних даних. У випадку мов програмування аналізатор є компонентом компілятора або інтерпретатора, який аналізує вихідний код мови комп'ютерного програмування для створення певної форми внутрішнього представлення; аналізатор є ключовим кроком в інтерфейсі компілятора. Мови програмування, як правило, вказуються в термінах детерміністичної контекстно-вільної граматики, оскільки для них можуть бути написані швидкі та ефективні аналізатори. Для компіляторів сам аналіз може бути виконаний за один прохід або кілька проходів.

Як правило, результатом синтаксичного аналізу є синтаксична структура, представлена або у вигляді дерева залежностей, або у вигляді

дерева складових, або у вигляді деякої комбінації першого і другого способів подання.

Розглянемо, яким же чином можна використовувати синтаксичний аналіз для пошуку збігів. Побудова повного дерева – досить ресурсномістка операція, крім того по відношенню до поставленої задачі вона є також надмірною.

Компромісним рішенням в даному випадку є побудова якоїсь спрощеної структури, яка б дозволила зберігати рівно стільки інформації про фрагмент коду, скільки потрібно для того щоб визначити, чи є цей фрагмент схожим з іншими фрагментами чи ні.

Перед виконанням аналізу текст розділяється на лексеми (токени) відповідно до певних правил. Також на цьому етапі може статися відсікання зайвих частин. Наприклад, коментарі не повинні сприйматися як частина коду і не повинні брати участь в синтаксичному розборі. У нашому випадку слід також позбутися від строкових констант, так як вони не впливають на сутність написаного програмного коду.

Після етапу поділу на токени важливо визначити до якої граматики належить вихідний текст. Це можна зробити порівнявши деякі з токенів із ключовими словами мови. При наявності збігів можна зробити висновок, що вихідний текст належить до тієї чи іншої граматики, або ж не належить ні до однієї з існуючих. В останньому випадку синтаксичний аналіз неможливий і слід застосувати інші методи аналізу.

Запропонований метод порівняння полягає в тому, щоб провести аналіз коду і формалізувати інформацію про нього певним чином.

Формалізований опис буде зберігати в собі інформацію про:

- кількість змінних в блоці коду;
- кількість операторів в блоці коду;
- кількість ключових слів в блоці коду.

З одного боку, такий об’єм інформації не дуже великий і не характеризує вихідний код з усіх боків.

Однак дає необхідну для аналізу інформацію і при цьому такий опис не займає багато місця, в разі якщо його необхідно зберегти. Підхід є ефективним і досить простим в реалізації.

Список використаної літератури:

1. Ахо А., Сети Р., Ульман Д. Компиляторы. Принципы, технологии, инструменты. – М.: Вильямс. – 2001.

2. Свердлов С. З. Языки программирования и методы трансляции. – М.: Питер. – 2007.

ОСОБЛИВОСТІ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ БЕЗДРОТОВИХ МЕРЕЖ ВИСОКОЇ ЩІЛЬНОСТІ

Шевченко К. Л.
Науковий керівник – д.т.н., проф. Рапін В. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інформаційно-мережна інженерія,
тел. (057) 702-13-06)
e-mail: kostiantyn.shevchenko@nure.ua

The paper presents requirements for high-density Wi-Fi networks, as well as features of such devices construction and operation. It was shown also their differences from conventional office networks. The main problem of network implementation, its specific characteristics and peculiarity of its use are shown. The technique that should be implemented in the design of high-density wireless networks to ensure high throughput are listed. The fundamental differences in approaches to the design of networks with a high user density in comparison with traditional architectures are demonstrated.

Мережі Wi-Fi високої щільності безсумнівно набувають все більшої важливості серед технологій радіодоступу, тому в останні роки і до існуючих бездротових мереж почали пред'являтися вимоги підтримки якнайбільшої кількості користувачів.

У подібній ситуації навіть надзвичайно грамотно спроектована мережа Wi-Fi, що має хороші рівні сигналу і ставлення сигнал/шум на цільової площі виявляється не в змозі забезпечити необхідну продуктивність, тому що розстановка точок доступу зазвичай походила з забезпечення 10 – 20 м^2 на одного користувача. А під мережами Wi-Fi високої щільності (далі МВЩ) розуміється бездротове середовище не тільки з великою кількістю користувачів, а й з високою концентрацією користувачів, до 1 користувача на м^2, які інтенсивно працюють з мережевими сервісами. Ця обставина вимагає більшого числа точок доступу, що в свою чергу, веде до високої інтерференції.

Таким чином основна проблема МВЩ полягає в необхідності забезпечити працездатність бездротової мережі в умовах високої інтерференції, коли радіопокриття всій цільової площі тільки виходячи з вимоги достатнього рівня прийому сигналу не відповідає вимогам мережевих сервісів. Для таких мереж введена спеціальна характеристика, це ставлення сигнал/интерференция+шум, яка враховує вплив інших точок доступу.

Основним завданням проектування мереж МВЩ є збільшення можливого числа обслуговуваних клієнтів мережі, розміщених на можливо меншій площі осередку мережі. Сукупна доступна пропускна здатність мережі, тобто швидкість передачі корисних даних, виміряна на дротовому інтерфейсі точки доступу, відноситься до осередку мережі, тому кількість користувачів, а також характеристики їх з'єднань для даного осередку мережі визначають питому пропускну здатність.

В інженерній практиці існує кілька підходів, комбінування яких дозволяє мінімізувати ефект інтерференції, це:

- зниження розміру осередків мережі до мінімально можливого.;
- збільшення числа точок доступу, але не більше ніж необхідно для досягнень цільової ємності (більше - не означає краще);
- високе повторне використання частот;
- використання спрямованих антен;
- використання конструкцій будівлі для загасання сигналу і поділу осередків мережі;
- використання спеціалізованого ПЗ для моделювання радіопокриття;
- оптимізації налаштувань обладнання.

Для більшості організацій помітна стійка тенденція мереж Wi-Fi для підтримки щільного розміщення користувачів. Однак, такий підхід повинен застосовуватися з обережністю, оскільки обмеження існуючих архітектур можуть негативно вплинути на проектні рішення і зробити неможливим досягнення цільової продуктивності і ємності бездротових мереж.

Література:

1. Florwick J., Whiteaker J., Amrod A. C., Woodhams J. Wireless LAN Design Guide for High Density Environments in Higher Education. Cisco Systems. 2017.

2. Родичев Ю. А. Компьютерные сети: архитектура, технологии, защита. Самара: Универсгрупп. 2006. 468 с.

3. Викулов А. С., Парамонов А. И. Исследование нагрузки в сети стандарта IEEE 802.11 // Информационные технологии и телекоммуникации. 2017. Т. 5. № 4.

4. Викулов А. С., Парамонов А. И. Анализ эффективности использования канала сети беспроводного доступа стандарта IEEE 802.11 по результатам наблюдений // Интернет вещей и 5G. 2017.

СИСТЕМА ЗБОРУ ТА ОБРОБКИ ВІДГУКІВ ВІД КОРИСТУВАЧІВ

Шатунова М.С.
Науковий керівник – ас. Дух Я.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ЕОМ, тел. (057)-702-13-54)
e-mail: marharyta.shatunova@nure.ua

Feedback is a one of forms of social approval. Both the quantity and quality of feedback are important. Customer impressions are important for any business. The article discusses one of the possible ways to solve this problem by creating a system for collecting and processing feedback from users, which allows a person to conveniently and quickly share their impressions of the service, as well as to track and share the impressions of other users.

Більшості людей психологічно важливо прочитати враження інших людей про яку-небудь послугу. Відгуки - це одна з форм прояву соціального схвалення. При цьому значення має як кількість, так і якість відгуків. Враження клієнтів важливі для будь-якого бізнесу. Люди схильні довіряти рекомендаціям та враженням інших споживачів більше, ніж заявам співробітників компаній, тому необхідно розуміти і отримувати максимальну користь із відгуків.

У статті розглядається один із можливих шляхів вирішення цієї проблеми шляхом створення системи збору та обробки відгуків від користувачів, яка дозволяє людині зручно та швидко поділитися своїми враженнями від отриманої послуги, а також відстежити та ознайомитися з враженнями інших користувачів. Було вирішено створити веб-застосунок для відгуків про кав'ярні Харкова.

Для створення застосунку пропонується використовувати фреймворк Django та мову програмування Python, а також HTML&CSS для створення веб-сторінок і Sqlite для зберігання усіх необхідних даних.

Django[2] - це веб-фреймворк Python високого рівня, який дозволяє швидко розробляти безпечні і підтримувані веб-сайти. Створений досвідченими розробниками, Django бере на себе більшу частину турбот веб-розробки, тому можна зосередитися на написанні свого застосування, не вигадуючи велосипед. Він безкоштовний і з відкритим вихідним кодом, має процвітаючу і активна спільноту, відмінну документацію і безліч варіантів безоплатної та платної підтримки. Архітектура Django нагадує шаблон «Модель-Вид-Контролер» (MVC), однак в якості «контролеру» в Django фактично виступає «вид», а в якості «виду» - «шаблон». Таким чином, розробники Django модель MVC назвали MVT («МодельВид-Шаблон»)

Робота веб-застосунку досить проста та зрозуміла. Користувачу пропонується увійти до аккаунту за допомогою логіну та паролю або ж за допомогою свого аккаунту Google. Якщо користувач не має аккаунту, він може зареєструватися та увійти у систему. Оскільки було враховано

схильність людей довіряти відгукам справжніх та перевірених користувачів, то було вирішено не дозволяти можливість залишити анонімний відгук, тому процедура авторизації є необхідною. Після входу в аккаунт користувач потрапляє у персональний кабінет, де може відстежувати свої коментарі, а також деяку інформацію про аккаунт.

Користувач може перейти на сторінку зі списком кав'ярень та відстежувати їх рейтинг, місце розташування, середні оцінки за визначеними критеріями (кава, сервіс, загальне враження), а також сортувати кав'ярні за потрібним критерієм. Після натискання на обрану кав'ярню користувач потрапляє на її персональну сторінку, де може залишити відгук та оцінки, якщо він цього не зробив раніше, а також переглянути відгуки та оцінки інших користувачів системи. Відгуки можна відсортувати за датою створення або ж у зворотньому порядку. Також є можливість додавання коментарю до свого відгуку, що дає змогу вільно висловити свою думку про відвідане місце.

Зберігання даних про кав'ярні та відгуки організовано за допомогою системи керування базами даних Sqlite [1]. Ця система надає можливість зберігання своїх даних у звичайних файлах, що дає змогу використовувати програму портативно і швидко, не вирішуючи при цьому питання встановлення і налаштування серверу для бази даних. Вона визначається наступними особливостями: висока надійність, продуктивність, відсутність сервера, а також відсутність необхідності конфігурації та установки СКБД, відповідно інтеграція ядра СКБД виконується в сам файл бази даних. Такий підхід зменшує накладні витрати, час відгуку та істотно спрощує програму. SQLite зберігає всю базу даних (включаючи визначення, таблиці, індекси і дані) в єдиному стандартному файлі на тому комп'ютері, на якому виконується застосунок.

Для реалізації проекту використовується PyCharm. Це інтегроване середовище розробки для мови програмування Python, що надає засоби для аналізу коду, графічний відладчик, інструмент для запуску юніт-тестів і підтримує веб-розробку на Django. PyCharm розроблена компанією JetBrains на основі IntelliJ IDEA.

Список використаної літератури:

1. Учебник по SQLite [Електронний ресурс] – Режим доступа: www/ URL: https://coderlessons.com/tutorials/bazy-dannykh/vyuchit-sqlite/uchebnik-posqlite – 06.03.2019 р. – Загл. з екрану

2. Головатый А., Каплан-Мосс Дж. Django. Подробное руководство, 2-е издание. – Пер. с англ. – СПб.: Символ- Плюс, 2010р

ДОСЛІДЖЕННЯ АЛГОРИТМІВ РОЗПІЗНАВАННЯ ГЕНДЕРНОЇ ПРИНАЛЕЖНОСТІ ЛЮДИНИ ЗА ЇЇ ГОЛОСОМ

Єрмолаєв А.А.
Науковий керівник к.т.н., доц. Омельченко С.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. IMI, тел. (057) 702-14-29)
e-mail: artem.yermolaiev@nure.ua

Object of research – methods of gender recognition using speech signals.

The purpose of this work is a research and implementation of methods for automatic gender identification by voice.

The main methods of gender recognition using speech signals are: method of support vector machines, method of gaussian mixture model. A comparative analysis of methods has been made. Voice features and a method of their extraction on a basis of mel-frequency cepstral coefficients were reviewed. Also algorithms of gender recognition through speech were reviewed. In the practical part the algorithm of gender recognition was implemented based on the frequency of the main tone of voice.

Мета роботи: дослідити ефективність запропонованих методів автоматичної ідентифікації статі людини за голосом. У ході роботи були розглянуті основні методи розпізнавання статі людини за голосом: метод опорних векторів, метод гаусових сумішей. Були розглянуті голосові ознаки та метод їх вилучення на основі мел-частотних кепстральних коефіцієнтів. В практичній частині було реалізовано алгоритм розпізнавання статі на основі частоти основного тону голосу та 2-ої формантної частоти.

Експериментальні дослідження алгоритму розпізнавання статі диктора з одноетапним визначенням кількості нулів в смугах формант проводилися методом статистичного випробування на вибірках 5-ти сигналів для кожного з 5-х різних дикторів чоловічої та жіночої статі. За вибірками оцінювалися параметри вирішального правила, а також контрольні вибірки реальних сигналів використовувалися для оцінювання якості розпізнавання сигналів.

Дослідження показали, що найбільший внесок в розпізнавання вносить друга форманта і показник її ексцесу, де можливе лінійне розділення класів. На рис. 1 показано отримане експериментальне зосередження пар вимірювань середнього значення другої формантної частоти основного тону та коефіцієнту ексцесу для п'яти жіночих голосів (трикутники) і п'яти чоловічих голосів (квадрати). Це дозволяє використовувати для другої форманти лінійні розділяючі межі між ними.

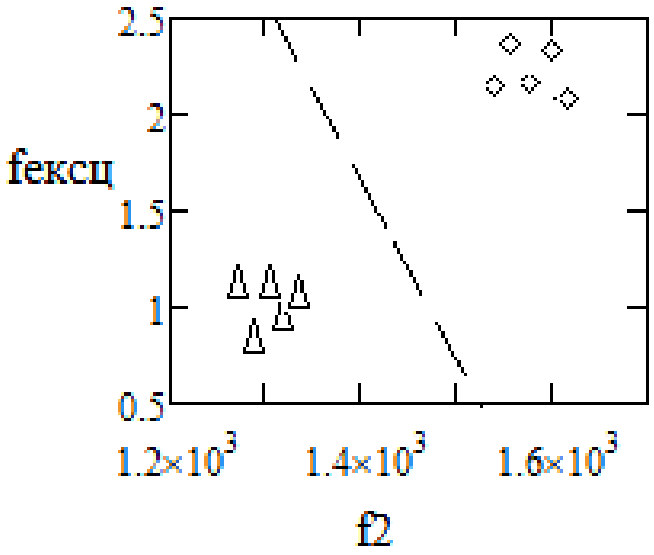


Рисунок 1 – Зосередження пар вимірювань середнього значення другої формантної частоти основного тону і коефіцієнта ексцесу для жіночих голосів (трикутники) і чоловічих голосів (квадрати)

Експериментальне дослідження показало помилку ймовірності розпізнавання, що дорівнює 0. При додатковій дії адитивної завади типу гаусів білий шум, отримана оцінка середньої ймовірності правильного розпізнавання при відношенні сигнал/шум $q = 20$, для алгоритму розпізнавання по частоті основного тону та 2-ої формантної частоти – 0.8.

Проведене дослідження підтверджує можливість використання запропонованого алгоритму розпізнавання за оцінками моментів частоти основного тону та 2-ої формантної частоти.

ПЕРЕЛІК ПОСИЛАНЬ

1. Пресняков И. Н. Автоматическое распознавание раздельных слов и фонем речи / И. Н. Пресняков, С. В. Омельченко. // Радиоэлектроника и информатика научно-технический журнал. – 2003. – №2. – С. 41–47.
2. Пресняков И. Н. Автоматическое распознавание речи в каналах передачи / И. Н. Пресняков, А. В. Омельченко, С. В. Омельченко. // Радиоэлектроника и информатика научно-технический журнал. – 2002. – №1. – С. 26–31.

АНАЛІЗ МЕТОДІВ КОМПРЕСІЇ ЗОБРАЖЕНЬ ФОРМАТУ JPEG ДЛЯ ПІДВИЩЕННЯ РІВНЯ СТИСНЕННЯ

Курлан О.О.
Науковий керівник – к.т.н., доц. Омельченко С.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. IMI, тел. (057) 702-14-29)
e-mail: oleksandr.kurlan@nure.ua.

The object of research – improving JPEG image compression level.

The purpose of this work is analysis approaches to improve JPEG image compression level.

The fundamental theoretical techniques of image compression are considered. Their comparative analysis was performed. Approaches of images compression level increasing presented in JPEG format will be investigated. In the practical part, there will be a software implementation of the investigated approaches and a comparative characteristic.

Данна робота має на меті аналіз шляхів підвищення рівню стиснення зображень формату JPEG.

У процесі дослідження було розглянуто такі основні теоретичні підходи до підвищення рівню компресії зображень, представлених у форматі JPEG, як метод теоретичного вибору порогового значення та метод вибору порогового значення з використанням cross-validation.

У ході експерименту було проаналізовано 31 зображення в напівтоновому діапазоні кольору. Були отримані перші низькочастотні ДКП коефіцієнти (для кожного з зображень), значення яких близькі до нуля, отже вони були прийняті за нуль без втрати якості зображення.

Було побудовано зображення PSNR (коефіцієнт пікового сигналу до шуму) у порівнянні зі розміром для цих зображень, стиснених з використанням наших порогових методів, з RD-OPT квантуванням. Крім того, зображені графіки PSNR-розміру для цих зображень, стиснених з використанням таблиць квантування «за замовчуванням JPEG». Також, графіки частот PSNR також показані у випадку RD-OPT без порогу, тобто просто оптимізації таблиці квантування.

Оцінки, показані на цих ділянках, є фактичними показниками, що виникають в результаті стиснення JPEG з кодуванням Хаффмана, а не оцінок ентропії. Для кожного зображення метод теоретичного порогового значення з таблицею квантування в відношенні розміру-спотворення призводить до збільшення PSNR до 2 дБ (децибел), порівняно з алгоритмом RD-OPT без порогової обробки і 4 дБ порівняно з JPEG з таблицею квантування за замовчуванням. У випадку порогового значення за допомогою Інформаційного Критерію, наш алгоритм досягає майже тієї ж PSNR, як схема безграничного кодування RD-OPT в

низьких бітових швидкостях. Однак існує момент для обох тестових зображень, за якими продуктивність починає знижуватися.

Ефективність наших глобальних порогових методів, що застосовуються до базової лінії JPEG з використанням результатів стиснення, наведено для двох зображень «Lena» і «Boat» (рис. 1 і рис. 2).

Рисунок 1 – 512x512 зображення у градаціях сірого «Lena»

Рис 2 – 256x256 зображення у градаціях сірого «Boat»

За результатами проведеного дослідження можна зробити висновок, що метод вибору порогового значення з використанням cross-validation, дозволяє вибрати набагато більше порогове значення, ніж методу теоретичного вибору порогового значення.

Теоретичний метод з використанням Інформаційного Критерію не задовольнив умов по стисненню зображення і не дав суттєвого підвищення ефективності.

Проведене дослідження дозволяє зробити висновок, що підвищення ефективності стиснення зображень, представлених у форматі JPEG можливо. Також слід зазначити, що завдяки реалізованим методам – можна ще більше знизити розмір файлу (посилити компресію файлу) без помітного зниження якості зображення.

ЕВОЛЮЦІЯ І РОЗВИТОК ПОКОЛІНЬ МОБІЛЬНИХ СИСТЕМ ВІД 3G ДО 5G

Пушкарьов В. В.
Наукові керівники: - д.т.н., проф. Безрук В.М., ст. викл. – Малінін О. П.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. інформаційно-мережної інженерії, (057) 702-14-29)
e-mail: slavik5320xm@gmail.com, тел. 097-357-81-89

5G - (5th generation mobile networks or 5th generation wireless systems) a name used in scientific papers and projects for designations of the following main phases of mobile telecommunications standards after 4G standards. Currently, 5G is not official term, use for any particular specifications or in any official documents prior to publication telecommunications companies or standards bodies, such as 3GPP, WiMAX Forum and ITU-R. 5G telecommunication networks should solve the problems that are present in 4G networks. The 5G standard is a new stage in the development of technologies that will provide unlimited access to the network of users and devices.

5G - (5-е покоління мобільних мереж або 5-е покоління бездротових систем) назва, яку використовують в наукових роботах і проектах для позначення таких основних фаз мобільних телекомунікаційних стандартів після стандартів 4G. В даний час, 5G не є офіційним терміном, використання для будь-якої конкретної специфікації або в будь-яких офіційних документах до опублікування телекомунікаційними компаніями або органами по стандартизації, такими як 3GPP, WiMAX Forum і MCE-R. Телекомунікаційні мережі 5G повинні вирішити проблеми, які присутні в мережах 4G.

Стандарт 5G - новий етап розвитку технологій, який забезпечить необмежений доступ до мережі користувачів і пристроїв. З моменту появи і до сьогоднішнього дня мережі мобільного зв'язку пройшли великий шлях розвитку; з'явилися нові типи абонентських пристроїв - смартфони і планшети. Можливості, які відкривають мобільні технології сьогодні, вже давно вийшли за рамки голосових послуг, створюючи нові способи спілкування, обміну даними. Поширення пристроїв привело до експоненціального зростання трафіку в мережах по всьому світу. Однак це тільки початок тієї революції, якій сприяє активний розвиток технологій.

Технології продовжать свій розвиток в напрямку до більш високої продуктивності і все більшій кількості можливостей. На додаток існуючим технологіям радіодоступу, з'являться також нові технології, які дозволять вирішувати ті завдання, які вирішити за допомогою 3G / 4G неможливо. Інтеграція існуючих і нових технологій буде сприяти підвищенню якості існуючих абонентських послуг і появи нових.

Системи другого покоління засновані на методі множинного доступу з тимчасовим поділом каналів (Time Division Multiple Access - TDMA).

Однак уже в 1992-1993 рр. в США був розроблений стандарт системи стільникового зв'язку на основі методу множинного доступу з кодовим поділом каналів (Code Division Multiple Access - CDMA) - стандарт IS-95 (Діапазон 800 МГц). Він почав застосовуватися з 1995-1996 рр. в Гонконзі, США, Південній Кореї, причому в Південній Кореї найбільш широко, а в США почала використовуватися і версія цього стандарту для діапазону 1900 МГц. Напрямок персонального зв'язку знайшло своє поширення і в Японії, де в 1991 -1992 рр. була розроблена і з 1995 року почала широко використовуватися система PHS діапазону 1800 МГц (Personal Handyphone System - буквально «система персонального ручного телефону»).

3.5G - HSDPA (англ. High-Speed Downlink Packet Access високошвидкісна пакетна передача даних від базової станції до мобільному телефону) - стандарт мобільного зв'язку, розглядається фахівцями як один з перехідних етапів міграції до технологій мобільного зв'язку четвертого покоління (4G). Максимальна теоретична швидкість передачі даних за стандартом становить 14,4 Мбіт / сек., практична досяжна в існуючих мережах - близько 8 Мбіт / сек. 4G - Технології, які претендують на роль 4G:

- LTE;
- TD-LT;
- Mobile WiMAX;
- UMB;
- HSPA+.

В даний час запущені мережі WiMAX і LTE. Першу в світі мережу LTE в Стокгольмі і Осло запустив альянс TeliaSonera / Ericsson – розрахункове значення максимальної швидкості передачі даних до абонента становить 382 Мбіт / с і 86 Мбіт / с - від абонента. Щодо UMB плани застосування не відомі, так як жоден оператор (в світовому масштабі) не уклав контракт на його тестування. Варто відзначити, що стандарт WiMAX не всі відносять до 4G, так як він не інтегрований з мережами попередніх поколінь таких як 3G і 2G, а також через те, що в мережі WiMAX самі оператори не надають традиційні послуги зв'язку, такі як голосові дзвінки і SMS, хоча і користування ними можливо при використанні різних VoIP сервісів. Також, IMT дозволив мережам HSPA+ називатися 4G, тому що вони забезпечують відповідні швидкості.

Перелік джерел

1. Мережі п’ятого покоління [Електроний ресурс]: https://www.itu.int/ru/mediacentre/backgrounders/Pages/5G-fifth
2. Структура мережі 5G [Електроний ресурс]: https://www.viavisolutions.com/ru-ru/5g-architecture

РОЗРОБКА ADS-B ПУНКТУ СПОСТЕРЕЖЕННЯ ЗА ПОВІТРЯНИМ ПРОСТОРОМ ІЗ ВИКОРИСТАННЯМ SDR ТЕХНОЛОГІЇ

Сердюк К.М.
Науковий керівник – к.т.н. Іваненко С.А.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки 14, каф. Інформаційно-мережної інженерії, тел. +38 (057) 702-14-29
e-mail: kostiantyn.serdiuk1@nure.ua

With the development of technology and microelectronics, it has become possible to create an ADS-B airspace surveillance point with available to everyone equipment such as PCs, laptops, single-board computers, and free software. Also currently available are many models of different SDR receivers that have the ability to receive radio waves in this range and are suitable for this purpose, and antenna designs designed for this range, which can be created by the presence of a drawing that is also available and open source equipment, or buy ready-made.

21 вересня 2014 року міжнародне партнерське об'єднання в складі ПАНО з Ірландії, Італії, Данії та Канади оголосило про створення служби визначення місцеположення повітряних суден та стеження за ними в нештатних ситуаціях (ALERT) - рішення, передбачають глобальне стеження в позаштатних ситуаціях, яке дозволить координаційним центрам пошуку і рятування (RCC), ПАНО і уповноваженим користувачам, а також відповідним сторонам запитувати розташування і останню лінію шляху будь-якого оснащеного засобами ADS-B в режимі радіомовлення (out) на частоті 1090 МГц повітряного судна, що виконує політ в будь-якому повітряному просторі.

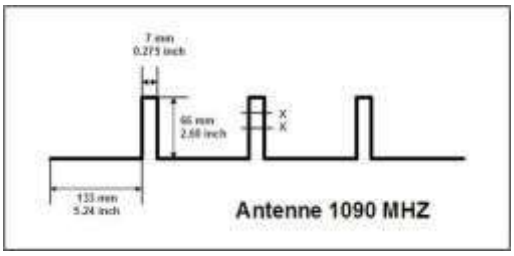


Рис. 1 – Антена для прийому ADS-B Рис.2 – Інтерфейс прийому «rtl1090»

ADS-B – нова технологія спостереження за повітряним рухом, яка впроваджується зараз на території Європи, США та інших країн. Саме тому актуальним є ознайомлення з цією новою технологією спостереження та використання в навчальному процесі засобів отримання ADS-B сигналів і дослідження за їх допомогою повітряного трафіку.

Пропонується дослідницька робота з питання більш широкого використання даних автоматичного залежного спостереження в режимі радіомовлення ADS-B. Таким чином, було виявлено, що технологію SDR можна використовувати в моніторингу цифрових сигналів радіосистем ADS-B повітряних об'єктів різного класу. Для цих цілей добре підходить тюнер для прийому сигналів DVB-T.

Обладнане ADS-B передавачем повітряне судно протягом усього польоту передає в реальному часі свої точні координати, швидкість, висоту, курс та іншу інформацію. Доступ до ADS-B інформації безкоштовний і вільний для всіх. ADS-B сигнал може прийматися на землі для цілей спостереження (ADS-B-out) або іншими повітряними судами для отримання інформації щодо навколишнього трафіку (ADS-B-in) і запобігання зіткнень. ADS-B-out система почала функціонувати в 2008 році, ADS-B-in - в 2011 році. Система ADS-B-out може використовуватися для цілей спостереження самостійно, а також разом з радарами і системами MLAT (multilateration). Для передачі ADS-B повідомлень використовується режим транспондера Mode S Extended Squitter.

ADS-B пункт спостереження на базі SDR приймача потрібен для того, щоб додатково прийнятими і розшифрованими повідомленнями з іншого місця розташування прийому, допомогти авіадиспетчерам, експертам або другим службам зв’язаним с повітряним рухом на наземному пункті спостереження руху повітряних суден, побачити з більшою точністю, ніж це було доступно раніше радарними аналоговими системами, і отримувати аеронавігаційну інформацію: координати місця розташування протягом усього польоту, разом з іншими даними, такими як курс, висота, горизонтальна і вертикальна швидкість.

На сьогоднішній день технології дозволяють фіксувати сигнали літаків автономна практично будь де, що дозволяє дублювати прийом телеметрії того або іншого повітряного об’єкта, і це дозволяє охопити більшу територію спостереження, з метою підвищення безпеки повітряного руху.

Список літератури:

1. ДРУГА КОНФЕРЕНЦІЯ ВИСОКОГО РІВНЯ З БЕЗПЕКИ ПОЛЬОТІВ 2015 року (HLSC 2015) [Електронний ресурс] / Режим доступу: www/ URL: https://www.icao.int/Meetings/HLSC2015/Documents/WP/wp048_rev1_ru.pdf – Назв. з екрана.
2. SOFTWARE FOR ADS-B DONGLES [Електронний ресурс] / Режим доступу: www/ URL: https://rtl1090.com/ – Назв. з екрана.
3. RTL-SDR DONGLES (RTL2832U) [Електронний ресурс] / Режим доступу: www/ URL: https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/ – Назв. з екрана.

ВПРОВАДЖЕННЯ ХМАРНОЇ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ НА ПРИКЛАДІ ОРКЕСТРАТОРА KUBERNETES

Ходаківський М.А.
Науковий керівник: - д.т.н., проф. Безрук В. М., ст. викл. – Малінін О. П.
Харківський національний університет радіоелектроніки (61166, Харків, просп. Науки, 14, каф. інформаційно-мережної інженерії, (057) 702-14-29)
e-mail: mykola.khodakivskyi@nure.ua, тел. 098-88-61-265

Today there is a problem with speed, complexity and efficiency of development of the final software product, for many years the developers have written large web applications with the so-called monolithic method, this is when developing a large application that stores all the modules and pieces of code, it was and is quite convenient in writing, but this method has significant disadvantages, first of all, if an application fails one module or another, the whole application ceases to function, which is a critical aspect when looking from a business standpoint, a difficult process debugging and application updates.

Microservice architecture is the architecture of the current lion's fate of all the most popular resources, or projects that use this particular application building system. The principle of microservice architecture is that the whole application is broken down into services, for example, the application is authorized, in the service architecture it can be made a separate module, etc. The advantages of this principle are the stability of the application, if one service fails it will be easy to repair, easy to update the version of the application, also a disadvantage is the difficult process of debugging and updating the application.

На сьогоднішній день існує проблема зі швидкістю, складністю та ефективністю розробки кінцевого програмного продукта, багато років розробники писали великі веб-додатки так названим монолітним методом, це коли розробляється великий додаток який в собі зберігає всі модулі та частинки коду, це було і є досить зручно в написанні, але такий метод має певні недоліки, перш за все якщо в додатку вийде з ладу тий чи інший модуль тоді працездатність всього додатка стане під загрозою, що є критичним аспектом, якщо дивитись з позиції бізнесу то як недолік варто віднести досить важкий процес відлатки та оновлення додатку.

Мікросервісна архітектура – це архітекура сьогодення львина доля всіх найпопулярнійших ресурсів, або проектів використовує саме цю систему методику побудови додатків. Принцип мікросервісної архітектури в тому, що весь додаток розподіляється на мікросервіси, наприклад додаток має авторизацію, в сервісній архітектурі його можливо зробити окремим мікросервісом. Переваги такого принципу є стабільність додатку, якщо один мікросервісом вийде з ладу його буде легко полагодити, також легко

оновлювати версію додатку. Як недолік можна віднести досить важке налаштування і в цілому міжсервісна взаємодія.

Kubernetes – потрібен для управління мікросервісною архітектурою,. На рис 1. Зображена основна концепція побудови мікросервісної архітектури на основі kubernetes. Основним елементом системи є “Master-Node” окрема фізична машина, або віртуальна машина, яка контролює всі процеси що проходять в нашій системі, базовим елементом виступає “Node” – це фізична машина, або віртуальная машина, на якій може виконуватися робота так само як і на “Master-Node”. В середені “Node” є “Pod” – це область в якому можуть зберігатися наші ізольовані контейнери з нашими мікросервісами, за допомогою kubernetes ми створюєму логічну мережну архітектуру в середені “Node” за допомогою сущності “Service”, таким чином створювати бізнес логіку та міжсервісну архітектуру також за допомогою kubernetes можливо зручно дублювати наші сервіси для більш відмовостійкості.

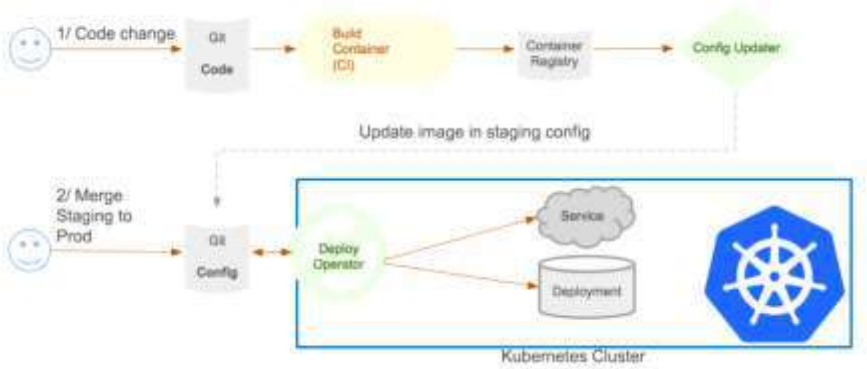


Рисунок1. Концепція мікросервісної архітектури Kubernetes

Процес роботи буде виглядати таким чином, розробник працює над певним мікросервісом, він робить так званий “patch-set” тобто зміну в своєму коді, код попадає до блоку “ci” що на малюнку там він компілюється, тестується, і на виході він попадає в блок “container-regestry” , далі в ручному, або в автоматичному режимі потрібно оновити окремий мікросервіс вказавши йому в налаштуваннях шлях до “артефакта” таким чином можна дуже зручно та безпечно поступово оновлювати та розробляти додаток.

Перелік джерел

1. Ознайомлення з Kubernetes [Електроний ресурс]: https://kubernetes.io/ru/docs/concepts/overview/what-is-kubernetes/
2. Основи Kubernetes [Електроний ресурс]: https://habr.com/ru/post/258443/

БЛОКУВАННЯ САЙТІВ З ВИКОРИСТАННЯМ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Семенченко О. А.
Науковий керівник – к.т.н. доцент Омельченко А. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інформаційно-мережна інженерія,
тел. (057) 702-13-06)
e-mail: oleksandr.semenchenko@nure.ua, +380507683086

The rapid development of information technology is gradually transforming the world. Open and free cyberspace expands the freedom and opportunities of people, enriches society. But unfortunately, not all information is beneficial fo person. Therefore, it is necessary to monitor such resources and block. In this we will help data mining, namely Data Mining.

With the help of Data Mining technologies it becomes possible to solve many problems the analyst faces. The main ones are: classification, regression, search for associative rules and clustering.

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство. Але не вся інформація може нести користь людині.

Тому необхідно відстежувати шкідливі ресурси і блокувати їх. Широкі можливості з автоматизації цих процесів з'являються внаслідок використання засобів інтелектуального аналізу даних (Data Mining) [1-5], зокрема Text Mining та Web Mining.

Маючи на руках засоби Text Mining та Web Mining можна проаналізувати матеріал на наявність шкідливого або небезпечного матеріалу.

До шкідливого матеріалу можна віднести [1]: ненормативну лексику; заклики до суїциду; утиску прав віруючих; екстремістські матеріали; використання образ та матеріали, що сіють ворожнечу за расовою, національною, релігійною або статевою ознакою.

Метою роботи є розвиток методів і засобів виявлення шкідливого контенту (ненормативної лексики та спроб торгівлі органами) у текстових даних, для подальшого блокування пов'язаних з ними ресурсів.

Для розв'язання задач Text Mining існують програмні засоби на таких мовах програмування як: Python, R, MatLab, SQL, Java, Scala, Julia, C++, JavaScript, Ruby, Perl.

У даній роботі для розв'язання задач виявлення шкідливої інформації у текстах використано мову програмування R, яка є широко розповсюдженою, має у своєму розпорядженні прикладні пакети практично для будь-якого застосування, зокрема стосовно задач Text Mining.

Додаткова зручність програмування мовою R забезпечується завдяки використанню середовища розробки програмного забезпечення RStudio.

У практичній частині роботи проводиться аналіз декількох текстів на наявність ненормативної лексики з попереднім пошуком сленгових слів. Пошук проводиться в створеній програмі, яка за заданими параметрами знаходить слова чи частину слів, що викликають підозру.

Спочатку програма присвоює кожному слову порядковий номер і після чого вказує, де саме у тексті знаходиться це слово або його частина, яка може бути замаскованою (додаванням зайвих літер або написанням слів разом).

Отримавши результат, аналітик може визначити, наскільки слово несе загрозу. Відносно тексту з небезпечним контентом можна поступити наступним чином: винести попередження, при якому власник сайту повинен знищити шкідливий матеріал або блокувати ресурс.

Розглянуто методи блокування ресурсів: блокування по IP-адресу, за допомогою технології DPI, блокування по URL-адресу, блокування за допомогою платформи та DNS блокування.

Виконано багатокритеріальний вибір найкращого методу блокування ресурсу за сукупністю показників якості, що враховують складність програмного забезпечення, затрати на апаратуру, умови блокування. Встановлено, що блокування за допомогою DNS є найкращим методом блокування.

Література:

5. Закон України «Про основні засади забезпечення кібербезпеки України» // (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403
6. Конвенція Ради Європи «Конвенція про кіберзлочинність» // http://zakon.rada.gov.ua/laws/show/994_575
7. А. А. Барсегян, М. С. Купріянов, І. І. Холод, М. Д. Тесс, С. І. Єлізаров. «Аналіз даних і процесів: навч. Посібник» - 3-е вид., Перераб. і доп. - СПб .: БХВ-Петербург, 2009. - 512 с .
8. Tony Ojeda, Sean Patrick Murphy, Benjamin Bengfort, Abhijit Dasgupta «Practical Data Science Cookbook»
9. Ingo Feinerer «Introduction to the tm Package Text Mining in R» // https://cran.r-project.org/web/packages/tm/vignettes/tm.pdf

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПОСЛУГ МУЛЬТИСЕРВІСНИХ МЕРЕЖ

Бураківська А. О.
Науковий керівник – к.т.н. доцент Омельченко А. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інформаційно-мережна інженерія,
тел. (057)702-13-06)
e-mail: anastasiia.burakivska@nure.ua, +380666562668

The concept of Next Generation Network NGN (Next Generation Network), which uses TCP / IP technology as a basis for building multiservice networks, gives the operator great opportunities to organize a virtually unlimited number of services. But at the same time it sets new challenges in terms of creating and implementing new methods of traffic service.

The struggle for resources affects the quality of service for all types of traffic, including IPTV traffic. The modern model of differentiated service provides for the division of traffic into classes with giving them different priorities in service.

The problem of establishing priorities for different types of traffic was solved by the method of reducing individual quality indicators to a generalized value function of the additive type using weights.

Концепція мереж зв'язку наступного покоління NGN (Next Generation Network), яка використовує технологію TCP/IP як основу для побудови мультисервісних мереж, дає оператору великі можливості по організації практично необмеженої кількості послуг. Але водночас вона ставить нові завдання з точки зору створення та впровадження нових методів обслуговування трафіку. Переважну частину трафіку мультисервісної мережі займає мультимедійний трафік, при цьому істотна його частина представлена відеотрафіком IPTV.

Боротьба за ресурси впливає на показники якості обслуговування для всіх видів трафіку, в тому числі й трафіку IPTV. Це пов'язано із тим, що множина потоків даних передається мережею, ресурси якої необхідно розподілити між цими потоками за певною пропорцією. Таким чином, виникає проблема управління трафіком в мультисервісній мережі в умовах наявності великої кількості різноманітних додатків, які істотно відрізняються вимогами до показників обслуговування [1-3].

На сьогодні визначені основні сервісні моделі QoS, а саме, модель кращої можливості Best Effort, модель інтегрованих сервісів Integrated service і диференційованого обслуговування Differentiated service. Модель диференційованого обслуговування передбачає поділ трафіку на класи з наданням їм різних пріоритетів в обслуговуванні. Вона забезпечує «розумне» управління трафіком [4].

Метою даної роботи є розробка процедури встановлення пріоритетів для різних видів трафіку у мультисервісних мережах з використанням методів багатокритеріальної оптимізації.

Основними показниками якості QoS, що використовуються при управлінні трафіком є імовірності втрати пакетів, середні мережні затримки, джитер та потрібна смуга пропускання [1, 2]. Значення часу доставляння та джитеру є важливими мережними характеристиками для послуг, що надаються у реальному масштабі часу.

Задача встановлення пріоритетів для різних видів трафіку була вирішена методом зведення окремих показників якості до узагальненої функції цінності адитивного виду з використанням вагових коефіцієнтів [3]. При цьому виконувалося попереднє нормування показників якості, а вагові коефіцієнти для різних показників якості QoS обиралися як: «1» - не особо важливо; «2» - важливо; «3» - дуже важливо.

Наведено приклад багатокритеріальної оптимізації призначення класів пріоритетності. У ньому використані значення затримки, джитеру, імовірності втрати пакета та смуги пропускання, що визначені як припустимі для основних типів мультимедійних послуг Європейським дослідницьким центром в області телекомунікацій (RACE – Research on Advanced Communication in Europe) [5]. Наведено отримані значення функції цінності різних видів трафіку, що визначають їх клас пріоритетності.

Реалізація розрахованих пріоритетів повинна бути прописана в граничних маршрутизаторах для класової обробки мультисервісного трафіку. Значення пріоритету можуть бути прописані значеннями трьох бітів в полі ToS моделі обслуговування DiffServ.

Література:

1. Степанов С.Н. Основы телетрафика мультисервисных сетей. - М.: Эко-Трендз, 2010. -392 с.

2. Usman Ahmad, "QoS architectures: a detailed review", International Journal of Reviews in Computing, Sep. 2012, pp. 32-47 20.

3. Безрук В.М., Бідний Ю.М., Омельченко А.В. Інформаційні мережі зв’язку. Ч.1. Математичні основи інформаційних мереж зв’язку: навч. посібник. – Харків: ХНУРЕ, 2011. –292 с.

4. Крылов В.В., Самохвалова С.С. Теория телетрафика и ее приложения. – СПб.: BHV. –2005. –288 с.

5. A. Danthine, O. Bonaventure, "From Best Effort to Enhanced QoS", Deliverable R2060/ULg/CIO/DS/P/004/b1 of the RACE CIO project, 51 p. (SART 93/15/15).

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ОПТИМІЗАЦІЇ ТА НАДІЙНОСТІ ВЗАЄМОДІЇ СЕРВЕРНОЇ І КЛІЄНТСЬКОЇ ЧАСТИН МЕРЕЖНИХ WEB-ДОДАТКІВ

Лялічев В. Д.
Науковий керівник – к.т.н. доцент Бондар Д. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інформаційно-мережна інженерія,
тел. (057) 702-13-06)
e-mail: vladyslav.lialichev@nure.ua , +380669148523

The spread of information systems is constantly increasing, but they are becoming more complex. Over time, computer resources began to evolve rapidly into ideas and mechanisms that began to grow and evolve. It was to ensure the maximum benefit and performance of information systems that the client-server architecture was invented, which helped solve many problems at the time.

As the number of these systems continues to grow, so do their requirements. The complexity of designing and developing such systems requires a lot of time and effort, and the methods and tools used to implement such projects differ from the development of standard systems.

Поширення інформаційних систем постійно збільшується, але вони стають дедалі складнішими. З часом комп’ютерні ресурси почали швидко еволюціонувати в ідеї та механізми, які почали рости та розвиватися.[1]

Саме для забезпечення максимальної вигоди та продуктивності інформаційних систем була винайдена архітектура клієнт-сервер, яка допомогла вирішити багато проблем на той час.

Термін "клієнт-сервер" відноситься до такого архітектурного програмного комплексу, в якому його функціональні частини взаємодіють з найпростішою схемою, клієнт дає попит, сервер дає відповідь.

Якщо ми розглянемо кожну частину взаємодії з цього комплексу, один з них, конкретний клієнт, робить активну роботу, тобто вони утворюють певні вимоги, а інший, сервер, відповідає.

Як розвиток інформаційних систем, ці завдання можуть відрізнятися, наприклад, розробка блоків одночасно для виконання функцій сервера та функцій клієнтів у порівнянні з іншими блоками.

Щоб стати сучасною архітектурою, взаємодія клієнт-сервер пройшло довгий шлях, починаючи з централізованої системи архітектурних додатків, які були популярні в 70-х роках минулого століття. Згодом такі системи перейшли на новий рівень, рівень персональних комп'ютерів і локальних задач на цих машинах.

З розвитком персональних машин на новий етап перейшли локальні мережі з розвиненою файлово-серверної архітектурою. Так з'явилися перші однорангові мережі, і з розвитком цих мереж почалося перше поділ комп'ютерів на клієнтів і сервери.[3] А з розвитком технологій і їх

вдосконаленням була створена архітектура клієнт-сервер, яка сьогодні займає високі позиції.

Але в наш час такі системи зростають і стають настільки складними, що набувають глобального характеру, і діяльність великої кількості людей почала залежати від їх правильної та надійної роботи. Такі системи часто мають дуже складну архітектуру, що складається з великого набору компонентів, кожен з яких працює на окремому пристрої. [4]

Клієнт-сервер є класична архітектура, що має розподіляти три основні частини програми на двох фізичних модулях. Зазвичай дані зберігання знаходяться на інформаційному сервері, таких як певний сервер баз даних, користувальницький інтерфейс - на стороні клієнта та обробка даних розподіляється між частинами клієнта та сервером.

Оскільки кількість цих систем продовжує зростати, зростають і їх вимоги.[2] Складність проектування та розробки таких систем вимагає багато часу та зусиль, а методи та засоби, що використовуються для реалізації таких проектів, відрізняються від розробки стандартних систем.

Література:

10. Многоуровневые системы клиент-сервер Валерий Коржов. [Текст]. Режим доступу : https://www.osp.ru/nets/1997/06/142618. /. –Дата доступу: березень 2021.
11. Компоненты сетевого приложения. [Електронний ресурс]. Режим доступу : http://www.4stud.info/networking. –Дата доступу: березень 2021
12. Архитектура клиент-сервер [Електронний ресурс]. Режим доступу : https://sergeygavaga.gitbooks.io/–Дата доступу: травень 2020.
13. Клиент-сервер. [Електронний ресурс]. Режим доступу : https://developer.mozilla.org/ Дата доступу: березень 2021.
14. What is a Thin Client [Електронний ресурс]. Режим доступу : https://www.clearcube.com/posts/what-is-a-thin. –Дата доступу: березень 2021.

МЕТОДИКА ПРОЕКТИРОВАНИЯ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ

Аль-Вандави Саиф Ахмед Искандар Исмаель, Хвостик И.О.,
Безрученко О.Ю., Рязанцева Л.Н.,
Научный руководитель – д.т.н, профессор Москалец Н.В.
Харьковский национальный университет радиоелектроники
61166, Харьков, пр. Науки,14, каф. ИКИ им. В.В. Поповского,
тел. (057) 702-13-20.
e-mail: mykola.moskalets@nure.ua

A methodology for designing multiservice networks based on a mathematical model of a network, which is based on set theory and matrix data representation, has been developed. This mathematical model takes into account the sets: network nodes, access nodes, network subscribers, tariff plans of the operator, as well as the speed of access to the Internet according to the tariff plan, the adjacency matrix describing the network topology, routing matrix, distribution matrix of subscribers consuming Internet access services, between access nodes and tariff plans, distribution matrix of subscribers who consume digital television services.

Современные мультисервисные сети имеют иерархическую структуру и состоят из транспортной сети и сети доступа. Транспортная сеть состоит из узлов доступа (УД), узлов предоставления услуг, узлов управления, шлюзов с другими сетями и каналов связи (КС), соединяющих данные узлы. К УД по средствам сети доступа подключены абоненты сети, являющиеся потребителями предоставляемых на сети услуг.

В настоящее время мультисервисные сети в основном проектируются для последующего предоставления на них услуг входящих в состав «Triple Play». Данные услуги является базовыми, и все остальные услуги могут быть представлены в виде их комбинаций.

К одним из важнейших задач, решаемых на этапе проектирования мультисервисных сетей, относятся задачи выбора сетевого оборудования и пропускных способностей каналов связи сети. Данные элементы отвечают за передачу и коммутацию информационных потоков генерируемых при предоставлении услуг абонентам мультисервисной сети. Следовательно, для обеспечения требуемого качества предоставления услуг их выбор должен осуществляться на основании значений группового трафика в КС мультисервисной сети при предоставлении услуг «Triple Play». Причем в качестве исходных данных должны быть использованы данные технического задания на проектирование, к которым относятся:

– количество абонентов каждой из услуг и их распределение между УД;

– скорости доступа абонентов к сети Интернет для различных тарифных планов;

– количество ретранслируемых телеканалов для каждого тарифного плана;

– структура абонентской базы услуги телефонии.

Таким образом, вначале необходимо рассчитать значения группового трафика в КС мультисервисной сети при предоставлении услуг «Triple Play» в соответствии с данными технического задание на проектирование.

Для решения поставленной задачи используется математическая модель сети, базирующеюся на теории множеств и матричном представлении данных. Данная модель учитывает топологию сети, структуру абонентской базы, параметры планируемых к внедрению на сети услуг.

Принципы предоставления услуг «Triple Play» на сети сильно отличаются друг от друга. Основные отличия в предоставлении услуг «Triple Play»:

– при предоставлении услуг телевидения информационные потоки передаются от узла «Headend» к УД, величина которых зависит от топологии сети, маршрутов передачи потоков, количества абонентов получающих доступ к услуге через УД, количества ретранслируемых телеканалов и их рейтинга;

– при предоставлении услуг доступа к сети Интернет информационные потоки передаются между узлом «Gateway» и УД, величина которых зависит от количества абонентов подключенных к УД и тарифных планов, по которым они работают;

– при предоставлении услуг телефонной связи потоки передаются между УД, шлюзами с другими сетями телефонии, узлом «Softswitch», величина которых зависит от количества абонентов подключенных к УД, структуры абонентской базы, количества абонентов сетей: ТФОП и мобильной связи в данном населенном пункте;

– при предоставлении услуг доступа к сети Интернет и услуг телефонной связи применяется технология unicast, а при предоставлении услуг телевидения технология multicast.

Таким образом, определение значений и характеристик информационных потоков, передаваемых по каналам связи, необходимо производить для каждой услуги отдельно, а затем производить их объединение.

Список использованных источников:

1. Бакланов, И. Г. NGN: принципы построения и организации / под ред. Ю. Н. Чернышова // М. : Эко-Трендз. – 2008. – 400 с.
2. ITU-T Recommendation Y.1541 (02/2006) - Network performance objectives for IP based services.
3. Гольдштейн Б. С, Пинчук А. В., Суховицкий А. JI. IP-телефония. – М.: Радио и связь. – 2003. – 312 с.

ОРГАНІЗАЦІЙНІ МЕТОДИ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ОСНОВІ ЕФЕКТИВНОГО ВИКОРИСТАННЯ РАДІОЧАСТОТНОГО РЕСУРСУ

Хачіров Е.Ф., Селіванов К.О., Москалець М.В.
Науковий керівник – д.т.н, професор Лошаков В.А.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки,14, каф. ІКІ ім. В.В. Поповського,
тел. (057) 702-13-20.
e-mail: mykola.moskalets@nure.ua

It is proposed to solve the problem of increasing the productivity of mobile networks and efficient use of radio frequency resources, through the optimal use of unused physical resources, which are respectively determined by the parameters of signal energy, time, time, space, polarization. The analysis carried out at the macro- and micro-level against the background of trends in the development of mobile communications formulates a set of tasks to improve the efficiency of radio frequency resources, taking into account the introduction of new radio technologies.

У системах мобільного зв'язку на етапах планування, функціонування, використання, забезпечення електромагнітної сумісності (ЕМС) та ін. доводиться розглядати багатовимірний векторний простір параметрів, що характеризують безліч сигналів, завад, засобів і технологій. Всі безліч параметрів складаються з таких підмножин: $\{F\}$ - часотних, $\{T\}$ - часових, $\{G\}$ - просторових, $\{p\}$ - поляризаційних, $\{P\}$ - енергетичних [48]:

$$\{PЭС\} = \{F^R, T^R, G^R, p^R, P^R\} + \{F^T, T^T, G^T, p^T, P^T\}, \qquad (1)$$

де індекси R і T - відносяться відповідно до параметрів приймальної і передавальної апаратури.

З множини параметрів (1) для рішення конкретних практичних задач доводиться вибирати групу (допустима підмножина станів даної системи $\{D\}$), найбільш придатних, що задовольняють критерії якості на інтервалі часу функціонування $\Phi(x(t)) \to extr$. Множина (1) можна розглядати як вектор-функцію параметрів динамічної системи. Для динамічних систем, що розвиваються на інтервалі часу $t \in T = [t_0, t_N]$, вектор (1), що визначає стан параметрів системи $x(t)$, необхідно доповнити ще вектором параметрів управління $u(t)$, $u \in U$, U – множина допустимих значень керування, що забезпечує стан даної системи на необхідному рівні або переведення системи в потрібні фазові стани у відповідності з критерієм $\Phi(x,u,t) \to extr$. Незважаючи на великий перелік завдань, число позитивних ефектів, що досягаються з просторово-поляризаційними характеристиками, обмежується, в основному, поліпшенням енергетики в лінії зв'язку, що забезпечується вибором коефіцієнтів підсилення антени

$G = (S_{эфф} \times 4\pi)/\lambda^2$, де $S_{эфф} = S \times K_{вп}$ – ефективна площа антени, $K_{вп}$ – коефіцієнт використання площі, λ – довжина хвилі несучої сигналу зв'язку. Що стосується поляризації, то при організації зв'язку досягаються узгодження поляризації антени з повністю поляризованою компонентою корисного сигналу. Таке пасивне використання просторових параметрів не є раціональним. При цьому, чим більше місць розміщення елементів зв'язку, тим економніше витрачається просторовий спектр, чим динамічніше управління просторово-поляризаційними параметрами, тим вища продуктивність і стійкість систем.

Продуктивність мережі мобільного зв'язку багато в чому залежить від ефективності використання фізичних ресурсів, які визначаються відповідними параметрами [25,27,49,50]:

– енергетикою радіолінії, що визначається рівнем корисного сигналу на вході приймача $P_{пр} = P_{пер} G_{пер} G_{пр} \left(\frac{\lambda}{4\pi R} \right)^2$ і значенням рівня шуму в смузі частот прийому $P_ш = N_ш \times \Delta F$;

– часовими параметрами: тривалістю імпульсів $\tau_u = \Delta t$, переносять інформацію в багатопроменевих каналах зв'язку;

– частотою: номіналом несівній f_0 і смугою частот корисних сигналів і ділянкою смуги ΔF – виділеній для передачі;

– просторовими параметрами G_i, обумовленими як місцем розташування АС і БС, так і напрямками, на яких поширюється і відповідно – радіосигнал приймається;

– поляризаційними параметрами p_c, що визначаються як ступенем поляризації m, так і елліптичністю годографа напруженості електричної складової поля.

Очевидно, кожен із цих ресурсів здатний робити свій внесок у досягнення високої ефективності використання фізичного рівня і відповідно формування необхідного рівня обслуговування споживачів.

Список використаних джерел:

1. Поповский В. В. Эффективное использование всего физического пространства сигналов в мобильных телекоммуникационных системах / В. В. Поповский, Ю. А. Василенко // Межрегиональный форум МСЭ. Национальная комиссия, осуществляющая государственное регулирование в сфере связи и информатизации (НКРСИ) (г. Киев, 11-13 сентября 2012 г.). Киев, 2012. С.42–45.

2. Про затвердження Плану використання радіочастотного ресурсу України : Постанова Кабінету міністрів України від 9 червня 2006 р. № 815 із змінами і доповненнями, внесеними постановами від 5 вересня 2012 року № 838.

ДОСЛІДЖЕННЯ НЕПАРАМЕТРИЧНИХ АЛГОРИТМІВ ВИЯВЛЕННЯ НЕЗАЙНЯТИХ ЧАСТОТНИХ КАНАЛІВ В МЕРЕЖАХ КОГНІТИВНОГО РАДІО

Пономарьов А.К.
Науковий керівник – проф. Безрук Валерій Михайлович
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інформаційно-мережна інженерія,
тел. (057) 702-13-06)
e-mail: andrii.ponomarov@nure.ua, +380976501381

Currently, there is a rapid development of radio data transmission systems. The ever-growing requirements for the speed and volume of transmitted information induce the developers of such systems to use broadband communication channels. At the same time, there is a growing need for more efficient use of the radio frequency spectrum to provide access to information resources for new users.

В даний час відбувається бурхливий розвиток систем радіопередачі даних. Постійно зростаючі вимоги до швидкості і обсягу інформації, що передається спонукають розробників таких систем використовувати широкосмугові канали зв'язку. У той же час зростає потреба в більш ефективному використанні радіочастотного спектру для забезпечення доступу до інформаційних ресурсів для нових користувачів [1].

На даний момент розподіл спектра грунтується на виділенні конкретного діапазону частот для конкретної послуги. Однак, велика частина виділеного діапазону радіочастот використовується час від часу, що призводить до неефективного використання частотного ресурсу [2].

Виявлення сигналу з невідомими параметрами є одним з основних завдань мереж когнітивного радіо для підвищення ефективності використання радіоспектру, який є найціннішим ресурсом. Вирішення даної задачі необхідне при визначенні приналежності виявленого сигналу до класу вторинних чи первинних користувачів або визначенні появи нових сигналів для раніше невідомих радіовипромінювань. При цьому слід враховувати існування сигналів, яких немає в базі даних КР, і які можуть потрапляти на розпізнавання, що призводить до помилок віднесення таких сигналів до класу відомих. [3].

Метою роботи є дослідження непараметричних алгоритмів виявлення сигналів, їх порівняльний аналіз та реалізація непараметричного алгоритму на базі тесту Вілкоксона.

Найчастіше для виявлення сигналів використовують двохвибірковій тест Вілкоксона (або Манна - Уїтні, або суми рангів) і вельми простий в практичній реалізації знаковий тест [4]. Більш потужними виявляються рангові тести, які на відміну від знакового враховують не тільки факт,

але і ступінь відхилення елементів досліджуваної вибірки від деякого рівня або елементів опорної вибірки. також.

Двохвибіркові тести охоплюють більш загальні випадки виявлення сигналів, ніж одновиборочніе, оскільки потребують меншої кількості апріорних відомостей [4]. Обумовлено це використанням опорної (або перешкодою) вибірки, яка є фактично «навчальної». Безумовно, застосування рангових алгоритмів призводить до неминучої втрати частини інформації, однак при збільшенні обсягу спостережень ці втрати зменшуються [5].

Для вирішення задач виявлення сигналів існують програмні засоби на таких мовах програмування як: Python, MatLab, R. У даній роботі для вирішення задачі виявлення сигналу в умовах шуму використано мову програмування MatLab. Вона надає зручні засоби для розробки алгоритмів, включаючи високорівневі, з використанням концепцій об'єктно-орієнтованого програмування. У ньому є всі необхідні засоби інтегрованого середовища розробки, включаючи відладчик і профайлер. Функції для роботи з цілими типами даних полегшують створення алгоритмів для мікроконтролерів і інших додатків, де це необхідно. використовується в задачах моделювання процесів та має багато внутрішніх функцій для роботи з сигналами.

У практичній частині роботи проводиться реалізація алгоритму виявлення сигналу на тлі шуму за допомогою знако-рангового тесту Вілкоксона. Алгоритм навчається на вибірках сигналу, шо виступає шумом, де виконується базове налаштування, а потім на корисному сигналі з додаванням шуму задля перевірки виявлення сигналу в каналі з шумом. Отримавши результат, система зможе визначити чи повинен її стан змінитися, для надання вільного каналу користувачу, чи ні.

Література:

1. Д. Д. Стоянов, «Розробка і дослідження алгоритмів виявлення сигналів в когнітивних радіомережах», Ярославль, 2014. - 6 с.
2. Н.Є. Мірошнікова. «Огляд систем когнітивного радіо», 2013. - 1с
3. С. А. Іваненко, «Визначення незайнятих частотних каналів у когнітивних радіомережах методами виявлення та розпізнавання сигналів в умовах апріорної невизначеності», Харків, 2019. - 1-2 с
4. Тарасенко Ф. П. Непараметрична статистика. Томськ: ТГУ, 1976.
5. Нікітенок, В. І. Швидкі непараметричні алгоритми виявлення сигналів / В. І. Нікітенок. - Мінськ: БДУ, 2010. - 131 с.

АНАЛІЗ ВИДІВ ЗАХИСТУ ОСОБИСТИХ ДАНИХ ВИКОРИСТОВУЮЧИ АНТИВІРУСНІ ПРОГРАМИ

Вервейко В.В.
Науковий керівник – доц., к.т.н. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інформаційно-мережна інженерія,
тел. (057) 702-13-06)
e-mail: vladyslav.verveiko@nure.ua, +380952174439

The rapid development of information technology is gradually transforming the world. Open and free cyberspace expands the freedom and opportunities of people, enriches society. But there is a downside, which is the theft of personal data, extortion or valuable information.

Having anti-virus programs on your personal computer can, if not prevent, severely prevent a fraudster from accessing information that is personal.

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство. Але є і зворотня сторона, яка являє собою крадіжку особистих даних, виманювання коштів чи цінної інформації.

Маючи на своєму персональному комп'ютері антивірусні програми можна якщо не запобігти, то доволі сильно завадити шахраю дістатися до інформації яка є особистою.

Метою роботи є аналіз видів захисту своїх персональних данних, аби вони не потрапили до рук шахраїв та не були продані на тіньових ресурсах. Тільки у 2020 році у даркнеті було опубліковано більш ніж 386 мільйонів записів користувачів.

Для вирішення задач захисту особистої інформації існують такі антивірусні програми як : BullGuard Internet Security, Kaspersky Internet Security, NortonLifeLock, AhnLab V3 Internet Security, Avast Free AntiVirus, AVG Internet Security, Avira Antivirus Pro, Microsoft Windows Defender.

Для знаходження кращіх антивірусів ми будемо перевіряти їх на вміння знаходити вірусні програми та захищати користувача, ефективність – темп роботи та оновлення баз даних і відсутність сбоїв у роботі системи, а також зручність у використанні. В ході виконання роботи було взято 8 антивірусних програм та взявши параметри зазначені вище присвоїв кожному бали. Результат представлений у таблиці.

Таблиця 1 - Порівняльна характеристика антивірусних програм.

Антивірус	Захист	Ефективність	Зручність використання
BullGuard Internet Security	5.9	6	6
Kaspersky Internet Security	6	6	6
NortonLifeLock	5.6	5.8	6
AhnLab V3 Internet Security	6	6	5.5
Avast Free AntiVirus	5.9	6	6
AVG Internet Security	6	6	5.7
Avira Antivirus Pro	6	5.6	6
Microsoft Windows Defender	5.8	5.9	5.9

Підрахунок балів виконано за допомогою формули :

$$V_i = \frac{\sqrt[n]{\prod_{j=1}^{N} W_{ij}}}{\sum_{i=1}^{N} \sqrt[n]{\prod_{j=1}^{N} kj}} \quad (1)$$

де $\prod_{j=1}^{N} W_{ij}$ – добуток всіх елементів строк;

$\sum_{i=1}^{N} \sqrt[n]{\prod_{j=1}^{N} kj}$ – загальна сума всіх добудків кожної строки матриці.

В результаті було знайдено кращу антивірусну програму яка впевнено впоралась із поставленими задачами і може захистити наш комп’ютер від вірусних програм. Kaspersky Internet Security надає найкращій захист і здатний запобігти втрату ваших даних або зараженню комп’ютера.

Відносно цього результату ми можемо прийти до висновку що усі антивіруси спрямовані на протидію шахраям та їх програм, і яким би ви антивірусом не користувались він буде виконувати свою функцію та захищати ваші дані.

Література:

1. К.Є. Клімєнтьєв «Комп’ютерні віруси і антивіруси» ДМК Прес,2013р.
2. С.В. Гошко «Технології боротьби з комп’ютерними вірусами» СОЛОН Прес,2010р.
3. С. Мазаник «Безпека Комп’ютерів» ЕКСМО, 2014р.

ДОСЛІДЖЕННЯ МЕТЕОРНИХ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ ПАСИВНОЇ РАДІОЛОКАЦІЇ

Давиденко Н.В.
Науковий керівник – к.т.н.,ст.викл. каф. ІМІ Іваненко С.А.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інформаційно-мережна інженерія, тел. (057) 702-00-00
e-mail: nataliia.davydenko@nure.ua .

The purpose of the work is to predict the possible collision of the Earth with potentially dangerous objects, which include some asteroids, by studying the associated meteoric flows with the help of radio-surveillance; forecasting the conditions for the propagation of radio waves during the design and operation of meteorological communication systems and synchronization of the time and frequency standards of the study of dynamic processes in the Earth's atmosphere.

Кожного місяця протиракетними службами великих країн світу реєструються десятки, космічних тіл, які потрапляють в атмосферу Землі і можуть досягнути її поверхні і спричинити руйнівні наслідки. Змінити орбіту астероїда, який вже знаходиться досить близько досить важко. Проте більшість з них належать певним метеорним потокам. Тому, якщо приділити достатню увагу їх вивченню, завдяки тим з них, що потрапляють в атмосферу, можна зібрати певні дані, які допоможуть вивченню та запобіганню цієї проблеми.

Радіолокаційні дослідження навколоземних астероїдів дозволили різко збільшити надійність багаторічних прогнозів їхнього руху, що найбільше актуально для, так званих, потенційно небезпечних астероїдів. В роботі пропонується метод дослідження метеорних слідів за допомогою SDR устаткування та методів пасивної радіолокації.

У якості передавача у такій системі дослжідення пропонується використання сигналу від телевізійної станції. Максимальна відстань для використання передавальної телевізійної вежі для виявлення метеорного розсіювання становить 2070 – 2300 км. Розглянемо радіус в 2000 км навколо вежі, розташованої в місті Харків. Для приймачів прямого виявлення метеорного розсіювання можна використовувати пілот-сигнал ATSC, специфічний для кожного каналу DTV, трохи нижче за частотою, ніж аналогова несуча відео. Щоб оцінити максимальний діапазон (40 – 70 МГц) сигналу, відбитого метеорною стежкою, можна вирішити задачу геометрії. Максимальна відстань:

$$D_{max} = 2R\arccos(R/(R+H)) \quad (1)$$

R: Радіус Землі (6371 км), H: Висота точки відбиття (85… 105 км)

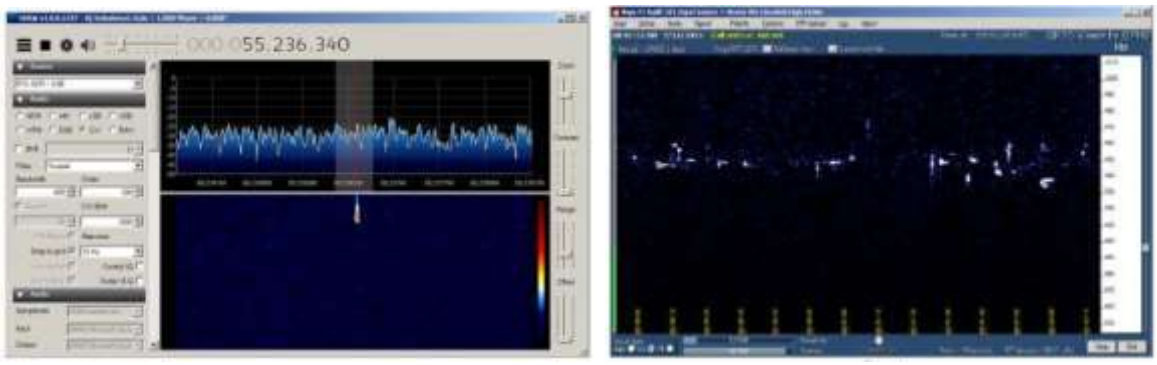
Програмне забезпечення, що працює на комп'ютері, складається з программи SDR# таі ARGO.

Приймач використовує чіп Realtek RTL2832U, який використовується для демодуляції DVB-T. Оригінальний USB-ключ, який продається як DVB-T-приймач, здатний надавати хосту необроблені зразки I/Q, і він створив програмне забезпечення Open Broadcaster Software (OBS) для захоплення відповідної області екрану, яка охоплює SDR і ARGO. на Linux для демодуляції FM на цьому приймачі.

RTL2832U виводить 8-бітові I/Q-семпли, теоретично максимальна можлива швидкість становить 3,2 мс/с, проте максимальна швидкість без втрати даних, яка була отримана на практиці склала 2,8 мс/с.

Аудіосигнал, модульований за допомогою SDR, направляється внутрішньо до ARGO через стереомікшер Windows.

Результати роботи такої установки на ведені на рис.1.



а) б)

Рисунок 1 – а) модульований аудіо сигнал, б) аудіосигнал який направляється внутрішньо до ARGO.

В роботі проаналізовано недоліки традиційного підходу до моніторингу метеорної активності та запропонований варіант їх вирішення за допомогою розробленої установки з устаткуванням SDR, а саме вирішена задача зменшення витрат на радіометеорні дослідження завдяки використанню існуючих теле/радіопередавачів ефірного мовлення як джерела зондуючого сигналу.

Література

1. Томпсон Р., Моран Дж., Свенсон Дж. Інтерферометрія і синтез в радіоастрономії / Пер. з англ. - М .: Мир, 1989.

2. Дулевич В.Е. «Теоретические основы радиолокации.» М., Сов.радио, 1978г. – 608с.

3. Белоцерковський Г.Б. «Основы радиолокации и радиолокационные устройства». – М.: Советское радио, 1975. 336с.

УДК 004:621.391

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ, МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ, СТАНДАРТИЗАЦІЯ І СЕРТИФІКАЦІЯ

ИССЛЕДОВАНИЕ МЕТОДОВ И СРЕДСТВ ПРЕЦИЗИОННОГО ИЗМЕРЕНИЯ ТЕМПЕРАТУРЫ

Бельков Е.А.
Научный руководитель – к.т.н., доцент Крушев В.Т.
Белорусский государственный университет информатики и радиоэлектроники
(220013, Минск, ул. П. Бровки, 6, каф. ИРТ, тел. (8017) 293-89-11)
e-mail: zenya.belkov@mail.ru.

Today, precision temperature measurement is a very relevant task in many high-tech areas. This article discusses the main methods and means of precision temperature measurement. The purpose of this work is to analyze and select the most accurate and stable method of temperature measurement. The article describes the principles of work of each of the methods and provides examples of their implementation. The advantages and disadvantages of each method are listed. As a result, it was found that the nuclear quadrupole resonance method is the most promising for further research due to its high accuracy and good stability in time.

На сегодняшний день, существует несколько способов прецизионного измерения температуры, и каждому из них присущи свои уникальные преимущества и недостатки.

Для точного измерения температуры с помощью терморезистивного метода в качестве датчика используют металлические и полупроводниковые резисторы, которые обладают достаточно стабильным температурным коэффициентом сопротивления (ТКС) и линейной зависимостью сопротивления от температуры. В качестве материалов для таких резисторов применяют платину, медь, никель и т.д. Использование платины позволяет измерять температуру с абсолютной погрешностью в $0,001\ ^{\circ}\mathrm{C}$.

К достоинствам металлических терморезисторов относятся: высокая точность измерений, простота и надёжность, удобство в эксплуатации. К недостаткам относятся маленький ТКС, резкое уменьшение чувствительности в области сверхнизких температур (для платиновых термометров), и достаточно большие габариты по сравнению с полупроводниковыми термометрами сопротивлений [1].

Полупроводниковые терморезисторы (ПТР) имеют меньшие габариты и большие значения ТКС. Для сравнения ПТР и медного терморезистора построена температурная зависимость [2], представленная на рисунке 1. В данном случае ТКС ПТР имеет отрицательное значение и уменьшается обратно пропорционально квадрату абсолютной температуры, что является недостатком, который существенно снижает качество измерения.

Достоинствами ПТР являются: большое удельное электрическое сопротивление и ТКС, высокая чувствительность, широкий температурный диапазон, малые погрешности, простота и надёжность. Недостатками ПТР

являются: нелинейность температурной характеристики и значительный разброс номинального сопротивления *R*. Из-за этого возникают проблемы с получением линейных шкал термометров, с взаимозаменяемостью терморезисторов, а также построением многоканальных приборов.

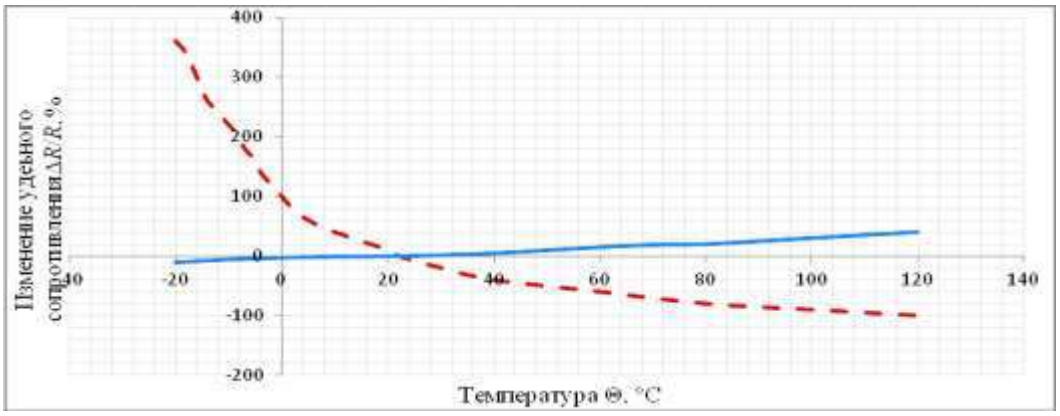


Рисунок 1 – Температурная зависимость ПТР (пунктирная линия) и медного терморезистора (сплошная линия)

Для измерения температуры с помощью термоэлектрического метода используют два проводника из разных сплавов, соединённых на одном конце и образующих часть устройства. В результате разных температур между точкой соединения (горячим спаем) и другими точками (холодным спаем) возникает ЭДС, которую можно измерить с помощью соответствующей цепи.

К основным преимуществам термопары относятся её прочность, широкий диапазон рабочей температуры от -270 до $3000\ °C$, быстрое срабатывание, и низкая стоимость. К числу недостатков можно отнести невысокую точность $\pm 0,01\ °C$ и большой шум. Однако повысить точность термопары можно методом компенсации холодного спая. В этом случае система оснащается ещё одним термодатчиком (термистор), который устанавливается на точку холодного спая [3].

Одним из термочастотных методов является метод ядерного квадрупольного резонанса (ЯКР). Данный метод основан на взаимодействии градиента электрического поля кристаллической решётки и квадрупольного электрического момента ядра, вызванного отклонением распределения заряда ядра от сферической симметрии.

Для измерения температур в диапазоне $1 - 600\ K$ в качестве термометрического вещества используют соль $KClO_3$, в которой определяется частота ЯКР ядер ${}^{35}_{0}Cl$. При температурах до $870\ K$ используется ЯКР ядер ${}^{63}_{0}Cu$ в Cu_2O или ядер *Re* в соли $NaReO_4$. На рисунке 2 представлены зависимости ЯКР от температуры перечисленных выше ядер.

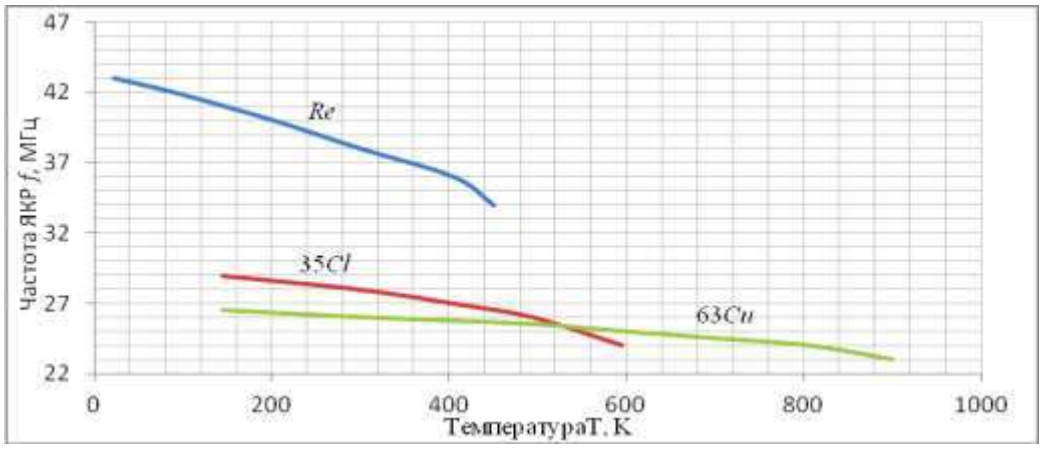


Рисунок 2 – Зависимость частоты ЯКР от температуры для ядер $^{35}_{0}Cl$ в $KClO_3$, для ядер $^{63}_{0}Cu$ в Cu_2O и для ядер *Re* в $NaReO_4$.

Достоинством ЯКР-термометра является его неограниченная во времени стабильность, т.к. зависимость частоты от температуры определяется только молекулярными свойствами вещества, а также высокая точность, позволяющая использовать такие термометры для создания вторичных эталонов температуры. Из графика видно, что недостатком является резкая нелинейность их характеристики, исключающая возможность прямого цифрового отсчёта температуры [2], а также сложность технической реализации в заводских условиях.

Заключение. Проведённое исследование показывает, что применение ЯКР для прецизионного измерения температуры более целесообразно, т.к. данный метод использует свойства кристаллической решётки вещества (состояние решётки строго зависит от температуры). Это позволяет повысить стабильность характеристик во времени и точность измерения температуры по сравнению с другими прецизионными методами.

Список использованных источников:

1. Мирошников, В.В. Обзор существующих методов и средств измерения температуры / В.В. Мирошников, А.И. Котуза. – Луганск : ВНУ, 2008. – С. 118 – 127.

2. Электрические измерения неэлектрических величин: учеб. пособие / А.М. Турчин [и др.]. Л. : Энергия, 1975. – 576 с.

3. С. Гупта. Прецизионное измерение температуры в промышленных системах контроля / С. Гупта, У. Камат // Конференция «Цифровая электроника». – М. : электроника медиагруппа, 2011. – С. 32–34.

КОНЦЕПЦІЇ НЕВИЗНАЧЕНОСТІ ТА ПОХИБКИ ВИМІРІВ

Ащепков В.О.
Науковий керівник — д.т.н. проф. Неєжмаков П.І.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Радіотехніки, тел. (057) 702-00-00
e-mail:valerii.ashchepkov@nure.ua

It is believed that the term "uncertainty of measurements" has replaced the term "error of measurement". However, this is not entirely a correct statement. In fact, the notion of "error" also has the right to exist. The terms "error" and "uncertainty" are different expressions of the same notion - "accuracy of measurements". There are two approaches to the evaluation of measurement accuracy parameters - the concept of uncertainty and the concept of unambiguity of measurements. The concept of uncertainty is aimed at obtaining the most accurate result, while the concept of unambiguity is aimed at obtaining the most realistic result.

Невизначеність вимірів розуміють як неповне знання значення вимірюваної величини і для кількісного вираження цієї неповноти розглядають розподіл вірогідності можливих значень цієї величини. Таким чином, параметр цього розподілу кількісно характеризує точність результату вимірів. Зазвичай основою для введення невизначеності вважають непізнаваність істинного значення фізичної величини. Тому дуже важливо встановити спільність і відмінність в поняттях невизначеності і похибки. Концепція невизначености почала формулюватись в 1978 р., коли теорія похибки вже досягла піку свого розвитку. Очевидною перевагою нової концепції стало підвищення надійності і якості реезультатів вимірів. Абсолютно невипадково країни з розвиненою економікою прийняли саме невизначеність як найкращу оцінку точності результату вимірів.

Чому ж теорія похибки не прижилася у світовому просторі? Самим очевидним її недоліком було те, що вона базується на понятті “ Істинного значення фізичної величини", визначити яке просто неможливо через недосконаліть методів і засобів вимірів. На практиці за істинним зазвичай приймають дійсне значення. Концепція ж невизначеності заснована на "оцінці середнього значення деякої величини", яку цілком реально розрахувати, тобто міра довіри до якості результату зростає.

Ще однією недосконалістю концепції похибки є класифікація її на систематичну і випадкову, тобто за характером виникнення. Тоді як класифікація невизначеності здійснюється за способом оцінювання. Виділяють невизначеність типу А - дані, що отримуються методом статистичного аналізу ряду спостережень, і невизначеність типу В, - дані, отримані способоми, відмінними від статистичного аналізу ряду спостережень. Розподіл невизначеностей за способом оцінювання виглядає більш розумним, ніж розподіл похибок на систематичні і випадкові.

Метод оцінювання невизначеності єдиний у всьому світі. Невизначеність вимірів оцінюється при заяві відповідності міжнародним вимогам, при взаємному визнанні результатів калібрувань, звірень і випробувань, при заяві про якість продукції. Також він використовується як міра довіри в області охорони здоров'я, безпеки і охорони довкілля, при проведенні фундаментальних наукових досліджень.

Україна на сьогодні знаходиться на перехідному етапі, який затягнувся на невизначений час. Але паралельне існування двох систем оцінки якості вимірів ускладнює методи оцінки характеристик точності і суперечить базовим принципам стандартизації. Не можна визнати правильною компіляцію цих двох систем. Кожна з них є самодостатньою, але з'єднання їх частин не може бути успішним. У Україні діє нормативна документація, яка базується на понятті "похибка". Проте в окремих видах метрологічної діяльності, таких як: робота по міжнародних проектах, міжнародні звірення національних еталонів, публікація матеріалів в зарубіжному друці, випуск продукції і надання послуг відповідно до вимог зарубіжного замовника, акредитація систем менеджменту якості національних метрологічних інститутів, акредитація вимірювальних лабораторій та ін., ми вже вимушені результат вимір представити тільки в термінах невизначеність.

Для метрологічної взаємодії з іншими країнами перехід до невизначеності стає неминучим. Єдність підходів з питання оцінювання точності відсутня. Повністю перейти до концепції невизначеності доки не вдається. .

Список використаних джерел:

Испытания, измерения, анализ “ Погрешность или неопределенность? Вот в чем вопрос... “ Ю.В. Грачёва, инженер-метролог отдела контроля качества ЗАО «РОСА»

ГОСТ 34100.3-2017/ISO/IEC Guide 98-3:2008 Неопределенность измерения. Часть 3. Руководство по выражению неопределенности измерения.

Захаров И.П. “Неопределенность измерений. Для чайников и ... начальников”.

В.П. Чалый “Неопределенность и погрешность, их сходство, различие и употребление в разных метрологических процедурах”// Невизначеність вимірювання: наукові, нормативні та прикладні аспекти.

Захаров И.П. Составление бюджета неопределенности совместных измерений // Український метрологічний журнал. – 2005. – No 3. – С. 15-18.

СИНТЕЗ ВИПРОБУВАЛЬНИХ СИГНАЛІВ СПЕЦІАЛЬНОЇ ФОРМИ ЕКСПОНЕНЦІАЛЬНИМИ СПЛАЙНАМИ

Куліченко В.В.
Науковий керівник – к.т.н., доц. Шумков Ю.С.
Національний технічний університет України КПІ ім. Ігоря Сікорського,
03056, м. Київ, пр-т Перемоги, 37,
каф. Інформаційно-вимірювальних технологій, тел. (044) 204-99-38
e-mail: vladkulichenko@gmail.com

Analog filtering is used to obtain smooth dependences during discrete synthesis. If the conditions of Kotelnikov's theorem are not satisfied, then the exact reproduction of a continuous signal by its discrete samples is not possible. Filtration results in some smoothed functions. The synthesis problem becomes approximation, is solved in the time domain in the class of piecewise exponential functions. In the discrete synthesis of test signals, which belong to the class of exponential signals and are described by the same functions as the approximating functions, exponential splines are optimal. The high efficiency of the synthesis method with a small number of approximation sites from the point of view of reducing the measurement error of the parameters of electric circuits in comparison with other systems of approximating functions is shown.

Для одержання гладких залежностей під час дискретного синтезу застосовується аналогова фільтрація. Найчастіше це фільтрація деякого кусково-ступінчастого сигналу, який сформовано ЦАП. Якщо умови теореми Котельникова не виконуються, то точне відтворення неперервного сигналу за його дискретними відліками не можливо [1]. Фільтрація призводить до деяких згладжених функцій. Задача синтезу стає апроксимаційною та розв’язується у часовій області у класі кусково-експоненціальних функцій. При цьому для одержання гладких залежностей доцільним є використання математичного апарату сплайн-функцій [2]. Експоненціальні сплайни є оптимальними для формування випробувальних сигналів (ВС) спеціальної форми, які теж описуються експонентами, та використовуються під час вимірів та контролю параметрів багатоелементних електричних кіл за методом нулів та полюсів [3]. Сутність дискретного синтезу полягає в подані сигналів, що формуються, у вигляді суми зміщених у часі фінітних базисних експоненціальних сплайнів зі своїми ваговими коефіцієнтами.

$$sf_{\mathrm{Gm}}(\bar{t}) = \sum_{i=-\infty}^{\infty} f[n+1-i]\cdot G_{\mathrm{m}}(i+\varepsilon) =$$

$$= A^{\bullet}(\boldsymbol{a})\left[0 + f[n+1]\cdot b_0(\varepsilon) + f[n]\cdot b_1(\varepsilon) + f[n-1]\cdot b_2(\varepsilon) + \ldots + f[1]\cdot b_{\mathrm{m\text{-}1}}(\varepsilon) + 0\right]$$

Сплайн-функція $sf_{\mathrm{Gm}}(\bar{t})$ порядку m є дискретною згорткою решітчастої функції $f[n]$ з експоненціальним сплайном $G_{\mathrm{m}}(\bar{t}) = G_{\mathrm{m}}(n+\varepsilon)$, який є імпульсної перехідної характеристикою деякого сплайн-

апроксимуючого фільтру, $\bar{t} = n + \varepsilon$ – відносний час, пов'язаний з дійсним часом $\bar{t} = t/h$; h – рівномірний інтервал дискретизації; $n = 0, 1, 2, \ldots$; $\varepsilon \in [0,1]$; $\{b_i(\varepsilon)\}_{i=0}^{m-1}$ – кускові функції, що на кожній дільниці утворюють сплайн; складаються з розв'язків деякого лінійного диференціального рівняння електричного кола, з розв'язків якого формується сплайн; m – порядок диференціального рівняння, $A^{\bullet}(\boldsymbol{a})$ – нормуючий множник.

Нижче наведено приклад фінітного базисного сплайну $G_{3,1}(\bar{t})$ та експоненціальної сплайн-функції $sf_{G3,1}(\bar{t})$ третього порядку.

$$G_{3,1}(\bar{t}) = \begin{cases} \left(-1+\alpha+e^{-\alpha}\right)^{-1}\left[-1+\alpha\varepsilon+e^{-\alpha\varepsilon}\right], \ \bar{t} \in [0,1]; \\ \left(-1+\alpha+e^{-\alpha}\right)^{-1}\left[1+\alpha+e^{-\alpha}-(1+e^{-\alpha})\cdot\alpha\varepsilon-2e^{-\alpha\varepsilon}\right], \bar{t} \in [1,2]; \\ \left(-1+\alpha+e^{-\alpha}\right)^{-1} e^{-\alpha}\left[-1+\alpha(\varepsilon-1)+e^{-\alpha(\varepsilon-1)}\right], \ \bar{t} \in [2,3]; \\ \quad 0, \ \bar{t} < 0, \ \bar{t} > 3. \end{cases}$$

$$sf_{G3,1}(\bar{t}) = \left(-1+\alpha+e^{-\alpha}\right)^{-1}\Big\{ f[n+1]\cdot(-1+\alpha\varepsilon+e^{-\alpha\varepsilon}) +$$

$$+ f[n]\cdot\left[1+\alpha+e^{-\alpha}-(1+e^{-\alpha})\cdot\alpha\varepsilon-2e^{-\alpha\varepsilon}\right] + f[n-1]e^{-\alpha}\left[\alpha(\varepsilon-1)-1+e^{-\alpha(\varepsilon-1)}\right]\Big\},$$

де відліки $f[n]$ – коефіцієнти сплайн-функції.

У роботі наведено аналіз математичної моделі формування ВС сплайнами, умови синтезу сплайнів, приклади одержання різноманітних моделей експоненціальних сплайнів другого та третього порядків за моделями передатної функції лінійних електричних кіл. Наведено вимоги до передатної функції. Приклади апаратної реалізації методу синтезу. Наведено використання ВС спеціальної форми, які сформовано сплайнами, під час вимірів та контролю параметрів електричних кіл. Показано високу ефективність методу синтезу при невеликої кількості ділянок апроксимації з точці зору зменшення похибки вимірів у порівняння з іншими системами апроксимуючих функцій.

Я.З. Цыпкин, *Теория линейных импульсных систем*, М.: Физматгиз, 1963, 968 с.

Brian J. McCartin, «Theory of Exponential Splines», *Journal of Approximation Theory*, vol. 66, pp. 1-23, 1991.

Yu. Shumkov, «Exponential splines in electric circuits' parameters measuring», *in Proc. of the International Conf. Actual problems of Measuring Technique "Measurement-98"*, Kyiv, Ukraine, 1998, pp. 250-253.

В.В. Куліченко, та Ю.С. Шумков, «Аналіз математичної моделі формування сигналів експоненціальними сплайнами», на *XV Всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених "Ефективність інженерних рішень у приладобудуванні"*, Київ, 10-11 грудня 2019, с. 506-509.

РОЗРОБКА ЕЛЕМЕНТІВ СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ МАШИНОБУДІВНОГО ПІДПРИЄМСТВА

Варченко М.А., Запотроєв Д.І.
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. МТЕ, тел. (057) 702-13-31),
E-mail: d_mme@nure.ua

The system objects for quality management at machine-building enterprise. Developed activities for development, metrology expertise, quality assessment developed technical documentation for the wheel - shaft, it is estimated the impact of technological process on the quality of finished products, proposed statistical methods for quality control of manufactured production, developed a quality manual. Object of study – the elements of quality management system the machine enterprise. Purpose – to improve the quality of products.

У центр економічної політики держави на сучасному етапі поставлено завдання всебічного підвищення технічного рівня і якості продукції, яка повинна втілювати новітні технології, задовольняти найвищі техніко-економічні, естетичні та інші вимоги споживачів. Питання стандартизації, взаємозамінності і технічних вимірювань безпосередньо пов'язані з якістю машин, надійністю і їх довговічністю. Взаємозамінність вимагає високого рівня вимірювальної техніки та метрологічного забезпечення.

Всі види діяльності людини підпорядковані одному: підвищення якості життя. А в сфері матеріального виробництва: поліпшення якості продукції, що виробляється [1]. Якість – головна мета і основна рушійна сила розвитку суспільства. Згідно ISO 9000:2015 [2] якість – ступінь відповідності сукупності при-сущих характеристик об'єкта вимогам.

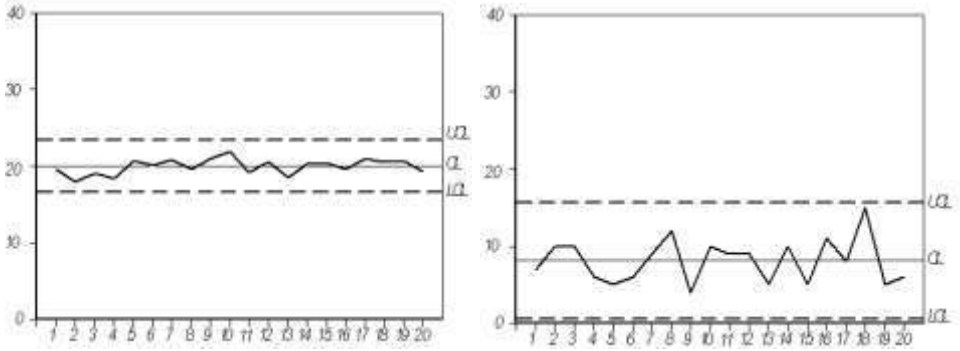
Особливе місце якість займає у виробництві продукції машинобудування – головної галузі економіки будь-якої держави. Продукція, що випускається машинобудівною промисловістю це машини, верстати, прилади, інструменти і пристосування, які складаються з деталей різноманітних форм і розмірів. Для машинобудування найефективнішими показниками якості є експлуатаційні характеристики машин. Експлуатаційні показники механізмів і машин (довговічність, надійність, точність і т. д.) в значній мірі залежать від правильності вибору посадок, допусків форми і розташування, шорсткості поверхні.

Система управління якістю підприємства – інтегрований механізм управління, призначений для реалізації цілей в області якості і орієнтований як на мінімізацію всіх видів втрат, так і на узгоджене функціонування всіх елементів. Одним з головних елементів управління якістю є управління контрольним, вимірювальним та випробувальним обладнання відповідно до міжнародного стандарту ISO 10012 "Measurement management systems - Requirements for measurement processes and measuring equipment". При проектуванні деталей машин їх геометричні параметри задаються розмірами

елементів, а також формою і взаємним розташуванням їх поверхонь. При виготовленні виникають відхилення геометричних параметрів реальних деталей від запроектованих значень. Ці відхилення називаються похибками. Вимірювання є головним джерелом відомостей про відповідність продукції встановленим вимогам. Для контролю відповідності встановленим вимогам використовують контрольно-вимірювальні інструменти. Тому для забезпечення належної якості проектування, виготовлення деталей, вузлів і машин важливим є питання метрологічного забезпечення контролю та вимірювань параметрів якості виробів.

Для того щоб визначити придатність деталі необхідно визначити її дійсні розміри. Відхилення дійсного розміру деталі від номінального для заданого квалітету не повинно виходити за межі допуску, встановленого стандартами ISO 286: 2010 [3].

У дослідженні застосовано статистичні методи управління якістю машинобудівної продукції. Статистичне регулювання технологічного процесу ґрунтується на застосуванні контрольних карт. Щоб в найбільш повною мірою відобразити технологічний процес і в подальшому вживати заходів щодо його регулювання виберемо два типи контрольних карт: карта, яка відображає відхилення від номінального радіального биття (тобто математичного очікування) – карта середніх значень; і карта, що характеризується розсіювання (розмах) окремих значень і їх зміна в часі – карта розмахів «R» (рис.1).



а) б)

Рисунок 1 - Контрольна карта середніх значень (а), карта розмахів «R» (б).

Список використаних джерел:

1. ДСТУ ISO 9001:2015 Системи управління якістю. Вимоги (ISO 9001:2015, IDT). – Введ. 2016-07-01. – Київ: УкрНДНЦ, 2016. – 31 с.

2. ДСТУ ISO 9000:2015 Системи управління якістю. Основні положення та словник термінів (ISO 9000:2015, IDT) [Текст]. – Введ. 2017–01–01. – Київ: УкрНДНЦ, 2016, 50 с.

3. ISO 286-1 : 2010 ISO system of limits and fits – Part 1: Bases of tolerances, deviation and fits.4.

АЛГОРИТМ ВИБОРУ ПОРЯДКУ ІНТЕРПОЛЯЦІЙНОГО ПОЛІНОМА ПРИ ПОБУДОВІ НЕЛІНІЙНОЇ ФУНКЦІЇ ПЕРЕТВОРЕННЯ ЗАСОБУ ВИМІРЮВАНЬ

Русанова Є.В.
Науковий керівник – к.т.н., доц. Запорожець О. В.
Харківський національний університет радіоелектроніки
61166, м. Харків, пр. Науки,14, каф. метрології і
технічної експертизи, тел. (057) 702-13-31
e-mail: yelyzaveta.rusanova@nure.ua

The problem of choosing the order of the interpolation polynomial for constructing the transformation function of measuring devices is considered. Increasing this parameter increases the accuracy of the approximation, but significantly increases the number of required calculations. A heuristic algorithm is proposed that provides a compromise between accuracy and computational complexity of the model. Modeling was performed using the system of engineering and scientific calculations MATLAB to study the proposed algorithm.

У метрологічній практиці досить часто доводиться мати справу з вимірювальними пристроями, що мають нелінійні характеристики. Для ідентифікації функції перетворення таких засобів вимірювань зазвичай здійснюють лінеаризацію математичної моделі шляхом заміни змінних з наступним визначенням її параметрів за допомогою методу найменших квадратів. Але при цьому необхідно мати апріорну інформацію про вид цієї нелінійної функції, тобто знати структуру математичної моделі засобу вимірювань. Обґрунтований вибір загального виду нелінійної залежності є досить складною задачею, що погано піддається формалізації.

У сучасній математиці розроблено численні методи вирішення завдань побудови функціональних залежностей за експериментальними даними, перш за все – статистичні методи, засновані на імовірнісних моделях для похибок вимірювань. Найбільш поширеним з них є метод найменших квадратів. У цьому методі оцінки параметрів залежності визначають з умови, що сума квадратів відхилень розрахункових значень від експериментальних мінімальна. Метод найменших квадратів було розроблено для оцінок параметрів лінійної моделі. У випадку суттєво нелінійних функціональних залежностей для апроксимації використовуються нелінійні функції, які зводяться до лінійного вигляду шляхом заміни змінних.

Одним із ефективних підходів до вирішення задачі відшукання нелінійної функції перетворення є застосування математичних моделей на базі алгебраїчних поліномів або многочленів. Обґрунтуванням доцільності такого вибору служить той факт, що поліноміальні функції мають добрі апроксимуючі властивості і придатні для відтворення широкого класу нелінійностей, їх можна вважати універсальними апроксиматорами.

Оптимальні коефіцієнти поліноміальної функції визначаються методом найменших квадратів.

Проте є певні труднощі, пов'язані з обґрунтованим вибором порядку поліноміальної моделі. Зрозуміло, що чим вище порядок інтерполяційного полінома, тим точніше модель буде відтворювати нелінійну залежність. Однак, метод найменших квадратів передбачає розв'язання системи лінійних алгебраїчних рівнянь, порядок якої на одиницю більше порядку інтерполяційного полінома. З одного боку, це призводить до суттєвого зростання обсягу обчислень, а з іншого системи рівнянь високих порядків в методі найменших квадратів часто бувають погано обумовленими.

Таким чином, порядок інтерполяційного полінома є компромісом між точністю апроксимації і обчислювальною складністю задачі. Пропонується евристичний алгоритм вибору порядку поліноміальної моделі, який дозволяє автоматизувати цю процедуру. Ідея полягає у тому, що спочатку за допомогою методу найменших квадратів будується лінійна функція (поліном першого порядку) і оцінюється середньоквадратична похибка апроксимації. Далі послідовно в циклі порядок полінома збільшується на одиницю, оцінюються коефіцієнти нової моделі і середньоквадратична похибка апроксимації. Перехід до наступної ітерації циклу здійснюється у випадку, якщо середньоквадратична похибка моделі порядку n зменшується в 1,5…2 рази порівняно з похибкою моделі порядку $n-1$ (значення цього коефіцієнта задається на початку роботи програми). Алгоритм зупиняється, коли збільшення порядку поліноміальної моделі дає несуттєвий приріст точності, не співрозмірний із збільшенням обчислювальної складності.

Для дослідження запропонованого алгоритму було проведене моделювання з використанням системи інженерних та наукових розрахунків MATLAB. Результати моделювання підтвердили ефективність розробленої процедури вибору порядку інтерполяційного полінома.

Література:

1. Грановский В. А. Методы обработки экспериментальных данных при измерениях [Текст] / В. А. Грановский, Т. Н. Сирая. – Л. : Энергоатомиздат, 1990. – 288 с.

2. Лященко М. Я. Чисельні методи : Підручник [Текст] / М. Я. Лященко, М. С. Голованъ. – К. : Либідь, 1996. – 288 с.

3. Нікітенко О. М. Maple : навч. посібн. [Текст] / О. М. Нікітенко. – Харків : ХНУРЕ, 2011. – 288 с.

4. Дьяконов В. П. MATLAB. Полный самоучитель. [Текст] / В. П. Дьяконов. – М. : ДМК Пресс, 2012. – 768 с.

АНАЛИЗ РЕЗУЛЬТАТОВ ПИЛОТНЫХ И КЛЮЧЕВЫХ СЛИЧЕНИЙ КИЛОГРАММА. НАЧАЛО НОВОЙ ФАЗЫ ПЕРЕДАЧИ КИЛОГРАММА

Паценко А. Н.
Научный руководитель – д.т.н., проф. Захаров И. П.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Науки, 14, каф. Метрологии и технической экспертизы,
тел. (057) 702-13-31
e-mail: sashapatsenko@ukr.net

The new definition of the kilogram, based on the fixed numerical value of the Planck constant, came into force on May 20, 2019. The paper analyzes the results of pilot and key comparisons of kilogram realizations based on the new definition. Shows the consistency of the results obtained with those expected according to the roadmap of a complete transition within 10-20 years.

После переопределения килограмма неопределенность международного прототипа килограмма (IPK) $u_{m_{IPK}}$ составляет 0,010 мг.

В табл. 1 представлены результаты пилотных и ключевых сличений, влияющие на согласованное значение IPK и его неопределенность [1-3] через прослеживаемость к постоянной Планка.

Цели ключевого сличения состояли в том, чтобы определить уровень согласия между реализациями килограммов от различных национальных метрологических институтов (NMI) и предоставить информацию для расчета первого согласованного значения (CV).

Таблица 1 – Результаты пилотных [1] и ключевых [2] сличений

№	NMI	2017			2020		
		Отклонение от эталонного значения $\Delta m_i'$/мг	Стандартное отклонение $u(\Delta m_i')$/мг	Расширенная неопределенность отклонения (k = 2) $U(\Delta m_i')$ /мг	Отклонение от контрольного значения ключевого сравнения (KCRV) $\Delta m_i'$/мг	Стандартное отклонение $u(\Delta m_i')$ /мг	Расширенная неопределенность отклонения (k = 2) $U(\Delta m_i')$ /мг
	BIPM *(IPK)*[1]	0,0006	0,0113	0,0226	-	-	-
1	BIPM	-	-	-	0,0252	0,0485	0,0970
2	LNE	-0,2038	0,1396	0,2792	-	-	-
3	NIST	0,0296	0,0274	0,0548	0,0003	0,0259	0,0519
4	NMIJ	-0,0012	0,0218	0,0436	0,0022	0,0201	0,0401
5	NRC	-0,0015	0,0119	0,0238	0,0154	0,0091	0,0181
6	PTB	-0,0061	0,0165	0,0330	-0,0210	0,0104	0,0209
7	KRISS	-	-	-	0,0724	0,1070	0,2140
8	NIM	-	-	-	-0,0117	0,0449	0,0899
	BIPM *(h(IPK)*[2]	-	-	-	0,0188	0,0138	0,0276

Примечание 1. Средневзвешенное значение результатов пяти NMI. Результат: $\overline{\Delta m} = -0.0006$ мг; стандартная неопределенность: 0,0102 мг.

Это означает, что средневзвешенное значение результатов калибровки для эталонов 1 кг участников всего на 0,0006 мг отличается от калибровки, основанной на IPK.

После завершения первого ключевого сличения экспериментов по реализации принято согласованное значение килограмма, которое составляет 1 кг - 0,002 мг. Стандартная неопределенность 0,020 мг [4].

Значение будет физически поддерживаться BIPM, который обеспечит прослеживаемость национальных эталонов массы. Прослеживаемость единицы массы в системе СИ будет взята из согласованного значения килограмма, начиная с 1 февраля 2021 года. Первоначальное согласованное значение рассчитано на основе среднего арифметического трех наборов данных:

- данные, напрямую отслеживаемые до IPK (последний раз использовались в 2014 году и поддерживаются рабочими эталонами BIPM);
- данные пилотного сличения экспериментов по реализации CCM, проведенного в 2016 г. (в соответствии с рабочими эталонами BIPM), с поправкой на сдвиг, введенный корректировкой CODATA 2017, в отношении значения CODATA 2014, которое использовалось в качестве эталона в пилотном сличении;
- контрольное значение ключевого сравнения (KCRV) ключевого сличения (отклонение $\overline{\Delta m} = -0.0188$ мг по отношению к единице массы, поддерживаемой рабочими эталонами BIPM, со стандартной неопределенностью 0,0075 мг).

Литература:

1. Результаты пилотных сличений CCM.R-kg-P1. Report on CCM Pilot Study CCM.R-kg-P1. Comparison of future realizations of the kilogram. Final Report. https://www.bipm.org/cc/CCM/Allowed/16/03-7B2_CCM-PilotStudy-FinalReport.pdf

2. Результаты ключевых сличений CCM.M-K8.2019. Report on the CCM key comparison of kilogram realizations CCM.M-K8.2019 Final Report.

3. CCM detailed note on the dissemination process after the redefinition of the kilogram https://www.bipm.org/cc/CCM/Allowed/17/06B_CCM-DetailedNote_Dissemination-after-redefinition.pdf

4. CCM Task Group on the Phases for the Dissemination of the kilogram following redefinition, “Calculation of the Consensus Value for the Kilogram 2020”, available from the BIPM web site.

СИСТЕМА ВІДДАЛЕНОГО ЗБОРУ ЕКСПЕРИМЕНТАЛЬНИХ ДАНИХ З ВИКОРИСТАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ

Мальцев Д.В., Богомазов С.А.
Науковий керівник – к.т.н., доц. Богомазов С.А.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна
03056, Київ, просп. Перемоги, 37, каф. Інформаційно-вимірювальних технологій, тел. (044) 204-98-93, e-mail: malcevdimitriy@gmail.com

The article presents an analysis of the peculiarities of the organization of experimental data collection systems. Determining the main advantages of using this concept in modern IoT systems. The system is implemented using the Electric Imp platform. The Electric Imp connects sensors, devices, or systems to services and IoT applications quickly. It securely scales to large volumes. On the basis of this platform the model of system of collecting and processing of temperature parameters of diesel engines was developed.

На сьогоднішній день Інтернет речей – один із головних світових трендів в сфері інформаційних технологій. Звичні нам прилади стають частиною системи Інтернету речей і можуть виконувати нові функції. Важливу роль в таких системах відіграють засоби віддаленого збору вимірювальної інформації. Складні обчислення в таких системах в багатьох випадках виконуються в хмарному середовищі. При цьому виникає необхідність розробки систем автоматизації віддаленого збору експериментальних даних. Тому було проведено аналіз особливостей реалізації таких систем на базі платформи Electric Imp[1].

На базі цієї платформи була розроблена модель системи збору і обробки температурних параметрів дизельних двигунів. Вона складається з модуля imp001 (мережевого вузла бездротового зв’язку)[2], плати-носія impExplorer, хмарного середовища Electric Imp Cloud і блоку вимірювання температур. Плата impExplorer включає в себе датчик температури і вологості, акселерометр, датчик атмосферного тиску та надає можливість розширення своїх функцій за допомогою чотирьох роз’ємів GroveSystem (два роз’єми для підключення пристроїв за допомогою інтерфейсу I2C, інші – для підключення цифрових і аналогових пристроїв)[3].

Платформа Electric Imp складається з трьох рівнів. На рівні пристроїв (Device Tier) авторизований модуль imp дозволяє підключити кінцевий пристрій до хмари Electric Imp Cloud. Наступний рівень платформи – рівень хмари Electric Imp Cloud Tier. Хмарне середовище Electric Imp Cloud є кінцевою точкою для всіх пристроїв і надає необхідні послуги для:

- управління пристроєм;
- оновлення “на льоту” (Over-the-Air – OTA);
- аутентифікації пристрою в системі;

- безпечного збереження даних;
- можливості легкого масштабування системи.

Electric Imp Cloud надає віртуальне представлення пристрою в хмарі та виконує логіку додатку і інтеграції від імені пристрою[4]. Кожний пристрій системи Electric Imp пов'язаний зі своїм програмним агентом, який розташований в хмарному середовищі і відповідає за безпеку і обробку вхідних даних. Третій рівень платформи (Customer Cloud Tier) – це користувацький хмарний додаток, що отримує надійні та оброблені дані від хмари Electric Imp.

Розроблена модель системи реалізує п’ять вимірювальних каналів (температура води на вході дизеля, температура води на виході правого і лівого блоків дизеля, температури масла на вході і температури масла на виході дизеля). В якості датчиків температури було використано платинові термометри опору. Мікропроцесорний блок вимірювання температури виконує вимірювання опору та розраховує температуру за відповідною залежністю. Отримані значення температури передаються по інтерфейсу I2C на модуль Electric Imp. Пристрій imp001 зчитує інформацію від блоку вимірювання температури і надсилає її агенту в хмарне середовище для подальшої обробки і передачі на інший пристрій або сервер.

Використання хмарних технологій для збору експериментальних даних забезпечило можливість проведення випробувань дизельних двигунів із обробкою результатів вимірювань в реальному часі і збереженням даних в хмарному середовищі.

Таким чином, розроблена система для отримання експериментальних даних з використанням хмарних технологій надає можливість швидко підключати будь-який сенсор, пристрій або систему до додатків Інтернету речей. Використання хмарних технологій та платформи Electric Imp спрощує організацію систем віддаленого збору даних, підвищує їх надійність і надає великі можливості для розширення свого функціоналу.

Список використаних джерел

1. Мальцев Д.В., Богомазов С.А. Організація системи Інтернету речей на базі платформи ElectricImp// Збірник праць XVI Всеукраїнської науково-практичної конференції “Ефективність та автоматизація інженерних рішень у приладобудуванні”. – К.: ПБФ, КПІ ім. Ігоря Сікорського. – 2020. – С. 419 - 421
2. Imp001.[Online]. Available: https://store.electricimp.com/products/imp001?variant=31635697938. Accessed on: November 22, 2020.
3. Electric Imp impExplorer Kit [Online]. Available: https://developer.electricimp.com/hardware/resources/reference-designs/explorerkit. Accessed on: November 22, 2020.
4. Electric Imp Cloud. [Online]. Available: https://www.electricimp.com/platform/cloud/. Accessed on: November 22, 2020.

ОСОБЕННОСТИ СОСТАВЛЕНИЯ БЮДЖЕТА НЕОПРЕДЕЛЕННОСТИ РЕЗУЛЬТАТА ИЗМЕРЕНИЙ В ОБЛАСТИ ИОНИЗИРУЮЩИХ ИЗЛУЧЕНИЙ

Тищенко М.В.
Научный руководитель – д.т.н., с.н.с. Скляров В.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, просп. Науки, 14, каф. Метрологии и технической экспертизы, тел. (057) 702-13-31
e-mail: vladimir.skliarov@gmail.com

The report discusses the features of budgeting the uncertainty of the measurement result in the field of ionizing radiation. As an example, the issue of compiling the uncertainty budget for the national standard of radon-222 volumetric activity was studied. The budget of the measurement uncertainty has been calculated and presented, taking into account the half-life and the emanation coefficient of the mass of the radon generator based on a standard sample of uranium ore UR-768C. The calculations of the uncertainty of the measurement result for the reference points of the volumetric activity of radon-222 for several laboratories for radon monitors have been performed.

Особенностью ссотавления бюджета неопределенности в области ионизирующих излучений, на примере национального эталона объемной активности радона-222 есть невозможность представления в виде коэффициентов чувствительности [1]. В данном случае, имеет место представление бюджета неопределенности в виде бюджета погрешностей, пересчитанных в терминах теории неопределенности (см. табл.1).

Таблица 1

Составляющие неопределенности	u_i, % значение	
	A	B
Фактор эманации радона-222 из стандартного образца	-	0,393
Фактор массы стандартного образца	-	0,027
Фактор распада радона-222	-	0,003
Фактор геометрии еталонной установки	-	0,076
Фактор температуры	-	0,041
Фактор давления	-	0,032
Фактор откалиброваного эталона-переносчика	1,743	-
Фактор геометрии эталона переносчика	-	0,165
Суммарная стандартная неопределеность, u_c	1,797	
Росширенная неопределенность, U_P	4,629	

При этом, среднеквадратическое отклонение, которое характеризует случайную погрешность, соответствует стандартной неопределенности типа А. Среднеквадратическое отклонение, которое характеризует неисключенную систематическую погрешность, соответствует стандартной неопределенности типа В и пересчитывается по формуле [2]:

$$u_B = \frac{\Theta(p)}{k\sqrt{3}},$$

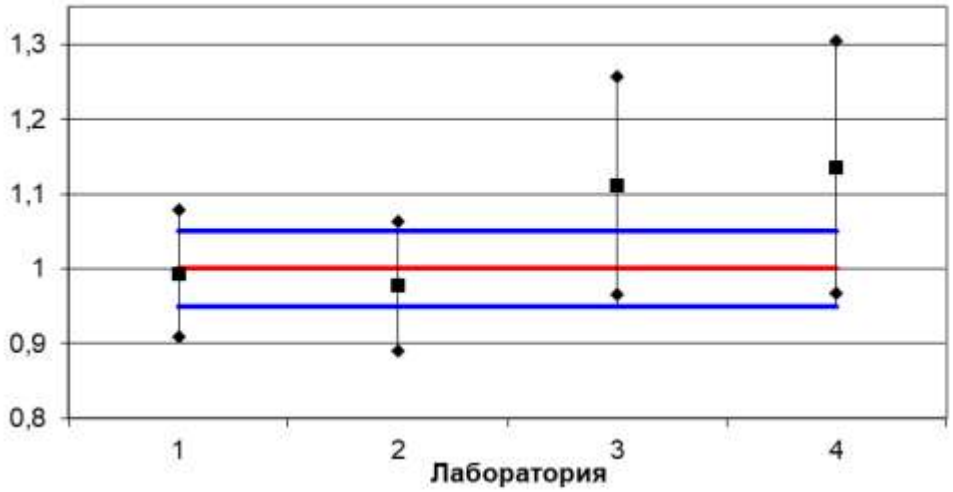
где $\Theta(p)$ - доверительные границы неисключенной систематической погрешности результата измерения, k =1,4 при p=0,95.

Результаты расчета опорного значения измерений [3] для точки 1500 Бк/м^3 для четырех различных лабораторий, с учетом расширенной неопределенности, представлены в таблице 2.

Таблица 2

Лаборатория	x_{ref}, Бк/м^3	$U(x_{ref})$, Бк/м^3	x_i, Бк/м^3	$U(x_i)$, Бк/м^3
1	1500	75	1474,70	68,26
2			1579,53	143,91
3			1666,41	212,60
4			1736,74	286,22

Нормированные значения результатов представления измеренных значений активности 1500 Бк/м^3 относительно опорного значения и с учетом неопределенности представлено на рисинке.



Результаты измеренных значений с учетом расширенной неопределенности.

Список источников

1. Применение «Руководства по выражению неопределенности измерений». Государственное предприятие „Всероссийский научно-исследовательский институт метрологи им. Д.И. Менделеева // Санкт-Петербург, 2001. - 20 с.

2. I.A. Kharitonov, A.G. Chunovkina. The estimation of the data of the regional key comparisons//Izmeritelnaya tekhnika.- 2005.- No. 5.-P. 11-17.

3. M.G. Cox. The evaluation of key comparison data // Metrologia, 2002, 39, 589-595.

ИЗУЧЕНИЕ ЭЛЕМЕНТОВ СИСТЕМЫ КАЧЕСТВА АДДИТИВНОГГО ПРОИЗВОДСТВА

Твердохлеб Л.А.
Научный руководитель – к.т.н., с.н.с. Буденный М.М.
Харьковский национальный университет радиоэлектроники
61166, Харьков, просп. Науки, 14, каф. Метрологии и технической экспертизы, тел. (057) 702-13-31,
mmb@mtl.kharkov.ua

An integral area of additive technologies is the regulatory framework. The existing volume of regulations can be divided into three areas: general purpose standards defining process requirements and applications; standards for materials that apply; standards that define the requirements for the additive manufacturing process for various consumers from aerospace to medicine. Harmonization of regulatory documents of additive manufacturing is a significant task for Ukrainian scientists in the field of metrology. Because of the metal Additive Manufacturing (AM) industry moves towards industrial production, the need for qualification standards covering all aspects of the technology becomes ever more prevalent.

Перспективы аддитивного производства (АМ) привлекли внимание промышленности в таких отраслях, как аэрокосмическая, медицинская и оборонная. Использование технологий аддитивного производства прменительно для выпуска металлических элементов изделия, позволит сократить время изготовления изделия без ухудшения качества выпускаемой продукции. Помимо значительного сокращения времени изготовления, существуют другие бизнес-факторы, в том числе снижение веса, сокращение количества составных элементов изделия, высокий уровень геометрической сложности [1]. Раскрывающиеся перспективы и явные преимущества аддитивного производства не снижают, а повышают требования к качеству и надежности выпускаемой продукции. Разработка отраслевых стандартов и нормативовм особенно важны в быстро меняющейся среде производства, должны способствовать надежной квалификация выпускаемой продукции.

Для выполнения возрастающих требований к аддитивному производству и стандартизации аддитивного производства, в США создан межотраслевой координирующий орган Additive Manufacturing Standardization Collaborative (AMSC). AMSC координирует совместную деятельность по стандартизации аддитивного производства, является межотраслевым органом, целью которого – ускорение разработки стандартов с спецификаций аддитивного производства в соотвествтии с потребностыми заинтересованных сторон [2].

Стандарты аддитивного производства охватывают весь жизненный цикл аддитивной печати детали, от входных данных трехмерного дизайна до выбора исходных материалов; контроль качества в процессе печати;

постобработку; оценку свойств готового материала; тестирование, квалификация и сертификация; обслуживание и ремонт.

Дорожная карта, разработанная AMSC, описывает 9 областей (технических направлений), в которых, в настоящее время, не существует опубликованных стандартов или спецификаций, которые могли бы удовлетворить потребности конкретной отрасли. На рисунке представлены основные направления для стандартизации и обеспечения качества аддитивного производства [3].

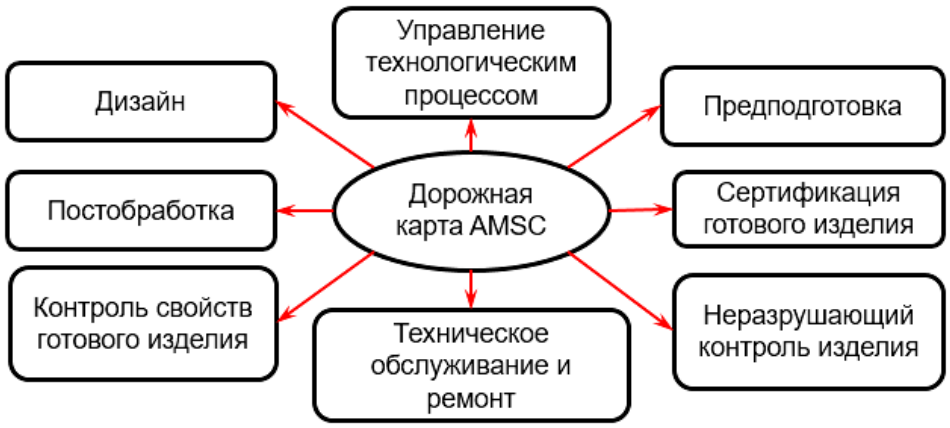


Рисунок – Направления система качества аддитивного производства

Каждое из направлений содержит ряд поднаправлений для стандартизации, сертификации, обеспечения качества и надежности аддитивного производства. В частности, раздел “неразрушающего контроля” (NDE) содержит 8 подразделов регламентирующих: терминологию для идентификации дефектов АМ, обнаруживаемых методами NDE; стандарты проектирования и изготовления артефактов или фантомов, подходящих для демонстрации возможности неразрушающего контроля; руководства по применению NDE к объектам, производимым процессами АМ; размерная метрология внутренних элементов; объединение данных; NDE полимеров и других неметаллических материалов; NDE контрафактных деталей АМ; критерии приемки неразрушающего контроля для критических для разрушения частей АМ.

Список источников

1. GE Additive (www.geadditive.com), “GE Additive.” [Online]. Available: www.geadditive.com. [Accessed: 20-Dec-2016].
2. America Makes & ANSI Additive Manufacturing Standardization Collaborative (AMSC), “Standardization Roadmap for Additive Manufacturing.” ANSI, p. Public Draft, 2017.
3. Электронный ресурс: https://www.ansi.org/portal/amsc/america-makes-and-ansi-amsc-overview

МОНІТОРИНГ ТА ВИМІРЮВАННЯ У ISO 14001

Юношев Д.Є.
Науковий керівник – доц. каф. МТЕ Штефан Н.В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки, 14, каф. МТЕ, тел. (057) 702 13 31
e-mail: dmytro.yunoshev@nure.ua

After the introduction of the new version of ISO 14001, it became necessary to change the rules for use of the standard. The version of ISO 14001:2015 removes the mandatory requirement for full monitoring of locations where significant environmental impacts exist or may exist. To do so, consider what the standard itself proposes and the need to documenting monitoring and measurement in ISO 14001.

У версії стандарту ISO 14001:2015 не має обов'язкової вимоги до повного моніторингу тих областей, де існує або може існувати значний вплив на навколишнє середовище.

Проте переглянутий стандарт вимагає, щоб екологічні показники та наступні поліпшення вимірювалися та відстежувалися. Є необхідність розглянути, що необхідно визначати, які методи необхідно використовувати та коли необхідно аналізувати данні та повідомляти про них. У якості загальної рекомендації організаціям, що вводять ISO 14001, необхідно визначити, яка інформація їх необхідна для оцінки екологічної результативності та ефективності.

Після введення СЕМ (системи екологічного менеджменту), стандарт вимагає постійного моніторингу системи, а також періодичних перевірок.

– оцінки ефективності, впровадженої СЕМ;
– об'єктивної оцінки, наскільки добре виконуються мінімальні вимоги стандарту;
– перевірки, наскільки були задоволені вимоги, що пред'являються до організації, зацікавленим сторонам та законодавству;
– аналіз придатності, адекватності, ефективності та дієвості СЕМ;
– демонстрації, що планування було успішно виконано;
– оцінки ефективності процесів СЕМ;
– визначення необхідності або можливості для постійного поліпшення СЕМ.

Впровадження СЕМ в організаціях без ефективного моніторингу та вимірювань не може показати кінцевого результату системи.

Моніторинг у розумінні ISO 14001 означає, що організація повинна перевіряти, контролювати, інспектувати та стежити за запланованими заходам, щоб переконатися, що вони проводяться так, як це планувалося. Отже, якщо операційний контроль вказує, що внутрішній аудит повинен проводитися двічі на тиждень, то це вважається процесом моніторингу.

Моніторинг та вимірювання допомагають у наступних процесах СЕМ:

- оцінювання екологічних характеристики;
- аналізування кореневих проблем;
- оцінки відповідності законодавчих вимог;
- визначення області, де необхідно прийняти коригуючі міри;
- покращення продуктивності та підвищення ефективності системи.

Для працездатної СЕМ необхідно визначити критерії вимірювання (показники ефективності) програми, що допоможе оцінювати успіхи програми СЕМ у цілому.

ISO 14001:2015 не вимагає використання ключових показників ефективності (KPI). Однак, пункт 9.1.1 висуває вимогу визначити, за якими критеріями буде оцінюватися екологічна діяльність та за якими саме показниками необхідно відстежувати деякі екологічні показники, але сам термін KPI перестав використовуватися.

Однак, якщо організація спеціалізується в галузі, яка вже використовує термін KPI, то у системі менеджменту організації або де-небудь ще, можливо, буде легше використовувати цей термін, коли мова йде про моніторинг і контроль процесів, що мають значні екологічні аспекти.

Необхідність документування у моніторингу та вимірюваннях

ISO 14001:2015 не висуває вимоги про ведення документації на кожний процес та процедуру, але необхідно переконатися, що всі вимоги до моніторингу та вимірюванням задокументовані, і включає необхідну документацію, для проведення вимірювання, таку як: очікувані значення та перелік обладнання, що використовується. Таким чином, з’являється впевненість у тому, що вимірювання проводяться послідовно між всіма співробітниками, які залучені до цих процесів, та це гарантує, що важливі екологічні аспекти не перетворяться в надзвичайні екологічні події. А записи о калібруванні або верифікації необхідні для підтвердження виконаної роботи та можуть використовуватися при розслідуванні, у випадку виникнення проблем у процесах організації.

Під кінець необхідно підсумувати те, що моніторинг та вимірювання, які вказані у редакції ISO 14001:2015, мають істотне значення в процесах СЕМ організацій.

ПРОЦЕДУРА ОЦЕНИВАНИЯ НЕОПРЕДЕЛЕННОСТИ ИЗМЕРЕНИЙ ПРИ КАЛИБРОВКЕ МАГАЗИНА СОПРОТИВЛЕНИЯ

Семенихин В.С., Фоменко В. Д.
Научный руководитель – профессор Захаров И. П.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, кафедра МТЭ, тел. +38 066-175-1092)
E-mail: valeriia.fomenko@nure.ua

Using the example of resistance calibration on a direct current, the features of taking into account the distribution of input valuess in the procedure for estimating uncertainty when using the method of excesses and propagation of expanded uncertainty are shown. The procedure for estimating the measurement uncertainty is described, and the uncertainty budget is given. An example of uncertainty estimation of measurements when calibrating a resistance box P33 class 0.2 using a Fluke 8508A digital multimeter is described.

Оценивание неопределенности измерений в аккредитованных испытательных и калибровочных лабораториях регламентировано международным стандартом ISO 17025:2017 [1]. При этом [1] предписывает использовать в качестве нормативного документа Руководство по выражению неопределенности измерений (GUM) [2]. Однако использование GUM сопряжено с рядом недостатков, основным из которых является независимость получаемых оценок расширенной неопределенности от законов распределения (PDF) входных величин и наличие смещения числовых значений измеряемой величины и ее стандартной и расширенной неопределенностей при нелинейных модельных уравнениях.

Именно поэтому Рабочей группой 1 (WG-1) Объединенного комитета по руководствам в метрологии (JCGM) разработано Дополнение 1 к GUM основанное на методе Монте-Карло [3], устраняющем указанные недостатки. Однако следует отметить, что даже при линейных модельных уравнениях и гауссовских распределениях входных величин оценки неопределенности, получаемые с помощью [1] и [2] отличаются друг от друга [4].

Причиной этому являются разные подходы к оцениванию характеристик неопределенности типа А в обоих документах [4]. Поэтому при разработке процедур оценивания неопределенности целесообразно опираться на подходы, приводящие к результатам, совместимым с результатами, получаемыми методом Монте-Карло. Такие подходы описаны в разработанной в ННЦ «Институт метрологии» процедуре оценки неопределенности измерений, однако этот документ не содержит примеров использования предлагаемых подходов. Восполняя этот пробел, в статье [5], на которой основываются данные тезисы, рассмотрены особенности учета законов распределений входных величин

при оценивании неопределенности измерений на примере калибровки магазина сопротивления.

Выводы

1. При оценивании неопределенности в калибровочных лабораториях используют Руководство по выражению неопределенности измерений и Дополнение к нему, основанное на методе Монте-Карло, дающие различные значения неопределенности при линейных модельных уравнениях и гауссовских распределениях входных величин.

2. Для устранения расхождений в оценках неопределенности предлагается использование метода эксцессов и закона распространения расширенной неопределенности, описанные в разработанной в ННЦ «Институт метрологии» процедуре оценивания неопределенности измерений.

3. Рассмотрены процедуры оценивания неопределенности при калибровке магазина сопротивления на постоянном токе, составлены бюджеты неопределенности, которые могут служить основой для создания программных средства для автоматизации оценивания неопределенности измерений при калибровке.

4. Исследование неопределенности измерений, проводимых при поверке магазина сопротивлений Р33 с помощью цифрового мультиметра Fluke 8508A показало хорошее совпадение полученных результатов с оценками расширенной неопределенности, получаемыми методом Монте-Карло.

Перечень ссылок:

1. ISO/IEC 17025:2017 General requirement for the competence of testing and calibrating laboratories, 2017, 30 p.

2. Guide to the Expression of Uncertainty in Measurement. ISO, Geneva, First Edition. – 1995 – 101 p.

3. Zakharov I.P., Vodotyka S.V. Application of Monte Carlo simulation for the evaluation of measurements uncertainty // Metrology and Measurement Systems, 2008, Vol. XV, № 1. – pp. 118-123.

4. Боцюра О.А., Захаров И.П. Особенности оценивания неопределенности измерений типа А на основе Байесовского подхода// Системи обробки інформації, 2015, вип. 6(131), с. 17 – 20.

5. I. Zakharov, O. Botsiura, V. Semenikhin, V.Fomenko. Considering of the input quantities distributions in the procedure for measurement uncertainty evaluating on the example of resistance box calibration. *Ukrainian Metrological Journal*, 2020, no. 4, pp. 3–8. doi: 10.24027/2306-7039.4.2020.224189

РОЗРОБЛЕННЯ АВТОМАТИЗОВАНОГО РОБОЧОГО МІСЦЯ ЕНЕРГОМЕНЕДЖЕРА НА ОСНОВІ ВИМОГ МІЖНАРОДНИХ СТАНДАРТІВ

Хіхло В.Ю., Мірошников П.П.
Науковий керівник – д.і.н., проф. О.Є. Тверитникова
Національний технічний університет
«Харківський політехнічний інститут»
61002, Харків, вулиця Кирпичова, 2, кафедра «Інформаційно-вимірювальні технології і системи», тел. (057) 707-61-15
e-mail: vadym.khikhlo@gmail.com, pashamiroshnikov99@gmail.com

Energy saving is a priority of the state policy of Ukraine. Implementation of energy management allows to get a detailed picture of energy consumption, to determine the optimal required amount of their consumption at the appropriate quality, to determine the most affordable types of energy, to obtain maximum economic, environmental and social effects. It also allows you to plan energy consumption for future periods, monitor targets and optimize limited financial resources for energy efficiency projects.

Економічна і політична ситуація в Україні, призводить до різкого зниження державної дотації енергопостачальним компаніям та субсидій їх споживачам, що тягне за собою підвищення тарифів на енергоносії. В цих умовах необхідність в розробленні й реалізації цілеспрямованої політики енергозбереження особливо актуальна.

Енергетичний менеджмент (ЕМ) – система управління процесом енергоспоживання, спрямована на досягнення максимального рівня енергоефективності споживання енергоресурсів при мінімумі витрат на них. Автоматизоване робоче місце (АРМ) енергоменеджера (рисунок 1) складається з персонального комп'ютера (ПК), який підключено до інтернету. ПК періодично зв'язується з віддаленим сервером, на якому розміщена програма збору даних з «інтелектуальних» приладів обліку, підключених до відповідних каналів зв'язку, які потім обробляються базовою програмою. Згодом оброблені дані формуються в графіки або цифрові показники, зручні для перегляду та аналізу. Дана система дозволяє контролювати споживання енергоресурсів в оперативному режимі, виключити наднормативне споживання і планувати ефективне витрачання коштів. Програмне забезпечення налаштовується індивідуально для кожної локальної мережі і адаптується для конкретного споживача.

Збір інформації для АРМ енергоменеджера можна розділити на два рівня. Перший рівень: збір інформації про споживання енергоресурсів в цілому по об'єкту: електроенергія; теплова енергія; споживання палива (газу); споживання холодної та гарячої води; зовнішня температура повітря; природна освітленість; кількість відвідувачів об'єкта. Другий рівень

доповнюється поглибленим дослідженням структури споживання електроенергії.

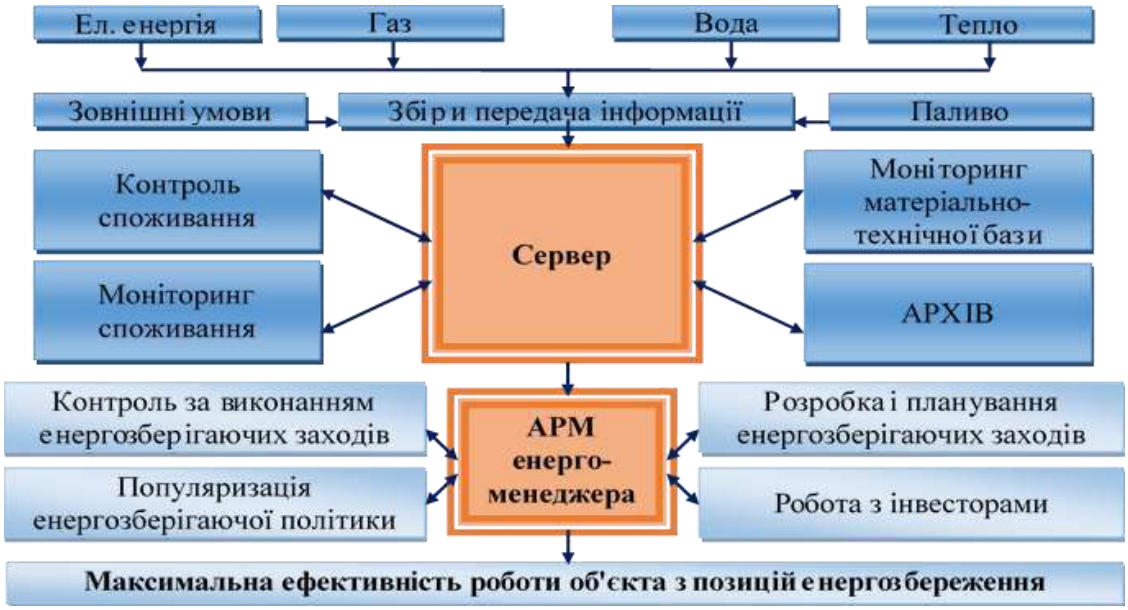


Рисунок 1. Автоматизоване робоче місце (АРМ) енергоменеджера

Спожита електроенергія розбивається на групи: освітлення; кліматична техніка; оргтехніка; спеціальне обладнання (печі, верстати, медичне обладнання, тощо). Також на другому рівні проводяться виміри освітленості, вологості і температури кожного приміщення в будівлі. Також рекомендується установка сенсорів задимлення і CO_2. На третьому рівні додаються дані з енергопостачальних компаній (обленерго, теплові мережі, водоканал, тощо): обсяги відпущеної електроенергії, тепла, води; споживання паливно-енергетичних ресурсів [1].

Євроінтеграційні процеси економічної політики сучасної України, поширення зовнішньоекономічних зав'язків з країнами Європи та світу безумовно вплинули на створення нових підходів до впровадження системи ЕМ та інтеграції нормативних документів України до міжнародного та європейського рівня. Зокрема міжнародного стандарту ISO 5001, який регламентує на законодавчій основі впровадження системи ЕМ в адміністративних одиницях і на промислових підприємствах. Згідно міжнародного та вітчизняного досвіду впровадження системи ЕМ дозволяє знизити витрати на енергоносії від 10 до 20%.

Список використаних джерел

1. Концепція організації служби енергетичного менеджменту в житлово-комунальному господарстві на рівні територіально-адміністративної одиниці. Методичне керівництво. Поточне діловодство кафедри ІВТС НТУ «ХПІ». 18 с.

ОЦІНЮВАННЯ НЕВИЗНАЧЕНОСТІ ВІДТВОРЕННЯ ОДИНИЦІ ОБ'ЄМНОЇ ВИТРАТИ ГАЗУ ІЗ ЗАСТОСУВАННЯМ УДОСКОНАЛЕНОЇ ПОРШНЕВОЇ УСТАНОВКИ

Кепещук Д. Т.
Науковий керівник – доц., к.т.н. Витвицька Л.А.
Івано-Франківський національний технічний університет нафти і газу
76000 м. Івано-Франківськ, вул. Карпатська, 15, кафедра метрології та інформаційно-вимірювальної техніки, тел. 0988527814
e-mail: denkepe@gmail.com

The metrological analysis of the developed reference piston installation of the improved design for reproduction and measurement of a gas expense is carried out. Factors influencing the accuracy of reproduction and transmission of the volume and volume flow of gas are analyzed. Based on experimental data, the values of the components of the total uncertainty, which are associated with design deviations of the cylinder dimensions and additional effects of changes in temperature and pressure of the internal environment, are calculated. The expediency of improving the design of the reference piston installation is substantiated, as the expanded uncertainty reduced to the control reproducible volume was 0.025%.

Для забезпечення єдності вимірювань, в першу чергу, ставиться задача створення еталонів одиниць вимірюваних величин. Однією з основних і дуже важливих з економічної точки зору фізичних величин є об'єм і об'ємна витрата газу, оскільки це пов'язано з проблемами обліку газу, особливо в комунально-побутовій сфері. Тому створення високоточних засобів для відтворення, передачі і зберігання одиниць об'єму і витрати газу є актуальною задачею, яка на даний час вирішується багатьма різними методами, серед яких одним з основних є поршневий метод [1]. Принцип дії поршневих еталонних установок базується на вимірюванні переміщення поршня, що рухається в мірній ділянці трубопроводу. Було встановлено, що основним недоліком поршневих еталонних установок є наявність незгладжуваних пульсацій тиску та значні його втрати на поршнях, що впливає на стабільність відтворення витрати. Тому запропонована удосконалена конструкція поршневої установки зі спеціальними ущільнювачами та точним приводом руху поршнів, яка забезпечує відсутність перетоків газу за рахунок створення надмірного тиску мастила для переміщення поршнів.

Для встановлення доцільності розроблення удосконаленої конструкції поршневої еталонної установки здійснено її метрологічний аналіз на основі концепції невизначеності. Процедуру менеджменту невизначеності проведено на основі аналізу факторів впливу на процес відтворення та передавання одиниці витрати. Складові невизначеності визначені на основі експериментально отриманих даних при випробуваннях поршневої

установки на базі державного підприємства Івано-Франківськстандартметрологія [2].

Відтворення одиниці об'єму газу забезпечується незмінністю та стабільністю геометричних розмірів циліндрів поршневих секцій. Об'ємна витрата газу є умовною похідною об'єму відносно одиниці часу і формується тільки при передаванні одиниці об'єму газу. Тому сумарна невизначеність відтворення одиниці об'єму газу залежить від невизначеності задання об'єму газу і впливу додаткових факторів, основними з яких є температура і тиск внутрішнього середовища, що приводить до зміни геометричних розмірів циліндрів, в яких рухаються поршні. Оскільки загальний об'єм витісненого мастилом газу у поршневій установці визначається з врахуванням діаметра основи та висоти кожного циліндра і роздільної здатності оптичної лінійки,за якою визначається положення поршня, то саме неточність вимірювання цих величин і впливає на невизначеність задання об'єму. Виходячи з технологічних особливостей поршневої установки, яка може мати чотири паралельно працюючі поршневі секції необхідно звернути увагу на те, що така конструкція зменшує сумарну невизначеність установки, оскільки при паралельній роботі ідентичних засобів їхня випадкова невизначеність зменшується в $\sqrt{n}$ разів, де n – кількість одночасно працюючих паралельних одиниць. Тому розрахована сумарна невизначеність задання одиниці об'єму газу склала $1{,}836 \cdot 10^{-5}$ м^3. Невизначеність, спричинена температурним об'ємним розширенням металу, склала $5{,}9 \cdot 10^{-6}$ м^3. Невизначеність, спричинена впливом на розміри циліндрів надлишкового тиску до 1,6 МПа, рівна $8{,}9 \cdot 10^{-7}$ м^3.

Загальне значення сумарної невизначеності відтворення одиниці об'єму газу при тиску до 1,6 МПа склало $1{,}93 \cdot 10^{-5}$ м^3. Розширена невизначеність (при коефіцієнті охоплення, рівному 2 і при довірчій ймовірності, рівній $P = 0{,}95$) з приведенням до контрольного відтворюваного об'єму газу, виражена у відсотках, склала 0,025%, що свідчить про високу точність відтворення одиниці витрати, а значить, і про доцільність розроблення і впровадження поршневої установки удосконаленої конструкції.

1. Петришин І.С. Технічні аспекти створення еталонної бази для метрологічного забезпечення лічильників газу в експлуатації / І.С. Петришин, П.Я. Джочко, Т.І. Присяжнюк, В.А. Бас // Український метрологічний журнал - 2013. - №1 - С. 50—55.

2. Про науково-дослідну та дослідно-конструкторську роботу створення державного первинного еталона одиниць об'єму та об'ємної витрати газу на газовому середовищі при тиску до 1,6 МПа / І.С. Петришин П.Я. Джочко, О.А. Бас, Я.В. Безгачнюк http://www.ifdcsms.com.ua/ - Сайт ДП «Івано-Франківськстандартметрологія».

МЕТОДИЧНИЙ ПІДХІД ДО ОБРОБЛЕННЯ ВИМІРЮВАЛЬНОЇ ІНФОРМАЦІЇ ПРО БАЛІСТИЧНІ ЕЛЕМЕНТИ ПОСТРІЛУ ПРИ ДІАГНОСТУВАННІ ТЕХНІЧНОГО СТАНУ КАНАЛІВ СТВОЛІВ ТА БОЄПРИПАСІВ

Мельніков Р.С.
Науковий керівник – д.т.н., проф. Крюков О.М.
Національна академія Національної гвардії України.
61001, Харків, м-н Захисників України, 3, докторантура та ад'юнктура,
тел. (067) 584-84-23 e-mail: melnikov85r@gmail.com.

Deviations of the internal geometric parameters of the barrel bore at its wear or blow-up, leads to irretrievable loss of energy of powder gases at the shot.

Known methods and means of diagnosing the technical condition of the channels of barrels and ammunition for barrel systems are ineffective, because they are based on outdated principles and provide for the use of measuring instruments of limited accuracy.

Proposes a promising method for diagnosing the technical condition of the channels of barrels and ammunition based on the analysis of ballistic elements of the shot.

Хід кривих балістичних елементів пострілу $p(t)$, $v(t)$ визначається параметрами перебігу процесу пострілу і, зокрема, геометричними характеристиками каналу ствола (КС), а також енергетичними характеристики порохового заряду та швидкістю його горіння. Між геометричними характеристиками КС та характеристиками порохового заряду і виглядом кривих для балістичних елементів пострілу (БЕП) існує певний зв'язок. При цьому певним дефектам КС та боєприпасів відповідають пов'язані з ними відхилення реальних кривих $p_{\partial}(t)$, $v_{\partial}(t)$. Наприклад, роздуття КС внаслідок прориву порохових газів і втрати частини їх енергії призводить до падіння тиску порохових газів («провалу» кривої $p_{\partial}(t)$ на ділянці, що відповідає місцю розташування такого дефекту.

Таким чином, за виглядом кривих $p(t)$, $v(t)$ можна встановити характер та місце знаходження дефекту КС або характер і ступінь деградації порохового заряду.

Для отримання об'єктивних даних про реальні БЕП $p_{\partial}(t)$, $v_{\partial}(t)$, які відповідають поточному технічному стану КС і боєприпасу, потрібна реалізація їх визначення шляхом вимірювань. Для цього можуть бути застосовані як засоби вимірювання миттєвих значень тиску порохових газів, так і засоби вимірювання миттєвих значень швидкості руху снаряду, принципи побудови і характеристики яких детально розглянуті в літературі, зокрема, [1-5].

Однак, у цих джерелах не отримали розвитку науково-методичні основи аналізу і інтерпретації результатів таких вимірювань для встановлення виду і ступеню прояву дефекту КС або боєприпасів. З огляду на це постає актуальне завдання, пов'язане з обґрунтуванням методичних

основ оброблення вимірювальної інформації про балістичні елементи пострілу при діагностуванні технічного стану каналів стволів та боєприпасів.

Ключовим питанням для практичної реалізації діагностування технічного стану КС та боєприпасів на основі аналізу характеристик БЕП залишається встановлення залежностей між видом дефекту КС (боєприпасу) і ступенем його прояву та виглядом кривих $p(t)$, $v(t)$. Такі залежності можуть бути встановлені на основі розв'язання системи рівнянь внутрішньої балістики за умов інтеграції до неї виразів, які моделюють відхилення відповідних геометричних параметрів КС та енергетичних параметрів порохового заряду. З огляду на можливості сучасних засобів обчислювальної техніки, доцільним є отримання рішення рівнянь внутрішньої балістики чисельним шляхом. Зокрема, із застосуванням чисельних методів можуть бути визначені номінальні криві $p_n(t)$, $v_n(t)$, які відповідають справному стану КС та боєприпасу.

Таким чином, запропонований методичний підхід до оброблення вимірювальної інформації про балістичні елементи пострілу полягає у отриманні кривих для БЕП $p_д(t)$ або $v_д(t)$ шляхом вимірювань та співставленні їх з відповідними номінальними кривими ($p_n(t)$ або $v_n(t)$), які відповідають технічно справному стану КС та боєприпасу. Визначається характер і обсяг відхилень цих кривих, і за показниками цих відхилень та на основі формалізованих правил (критеріїв) встановлюється вид дефекту та ступень його прояву.

Застосування запропонованого методичного підходу та відповідних засобів вимірювання відкриває шлях для реалізації експлуатаційного контролю зброї та боєприпасів в польових умовах, що виключатиме її транспортування до стаціонарних місць проведення контролю. Внаслідок цього може бути суттєво підвищена оперативність контролю.

Список використаних джерел:

1. Медведева Н.П. Эксперементальная баллистика. Часть 1 Методы измерения давления [Текст] : Н.П. Медведева, - Томск: ТГУ 2006.-148с.
2. Михайлов, К. В. Экспериментальная баллистика. Приборы и методы баллистических измерений [Текст] / К. В. Михайлов. – София : ВТС, 1976. – 388 с,
3. Шкворников П.Н. Эксперементальная баллистика [Текст] : П.Н. Шкворников, Н.М. Платонов, София ВТС 1976.- 392с,
4. Крюков А.М. Дифференциальная лазерная доплеровская анемометрия объектов со световозвращающей поверхностью [Текст] / Крюков А.М. , Доля Г.Н., Мудрик В.Г. Прикладная радиоэлектроника – 2013 –Т 12 № 3 ЖДТУ. – С. 436-441,
5. Крюков, О. М. Проблеми вимірювального контролю параметрів внутрішньобалістичних процесів [Текст] / О. М. Крюков, О. А. Александров // Збірник наукових праць Харківського національного університету Повітряних Сил. – Х. :, 2009. – Вип. 1 (19). – С. 150–152.

РОЗПОДІЛЕНА ІВС МОНІТОРИНГУ ПОЖЕЖНОЇ СИТУАЦІЇ НА ТОРФ'ЯНИХ РОДОВИЩАХ З ВИКОРИСТАННЯМ ІНТЕРНЕТ РЕЧЕЙ

Шестак О.А.
Науковий керівник – к.т.н., доц. Павлишин М.М.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, Київ, вул. Політехнічна 14, корпус 18, каф. Інформаційно – вимірювальних технологій, каб.334, тел. (044) 204-98-93
email: shashashestak@gmail.com (або soa-ivt-pbf22@lll.kpi.ua)

This work is devoted to the development of the distribution of IMS parameters of peat mass. Namely temperature and humidity at different depths. It simultaneously measures the temperature and humidity of atmospheric air. This IMS prevents the critical situation of spontaneous combustion of peatlands. And including the conservation of biosphere resources and natural biodiversity. Therefore, this system is very useful and necessary for our planet. The need for such IMS is about thousand a year. This system is very easy to implement.

Майже кожен рік ми стикаємося з проблемою горіння торф'яних родовищ, та з наслідками таких катастроф - гектарами вигорілої землі, задимлень, падінь дерев, а також провалу людей і техніки під землю. Причинами пожеж є суттєві зміни клімату, а саме підвищення температури та зменшення кількості опадів.

Для запобіганню займання запропонована система, яка складається з сукупності сенсорів з відповідним обладнанням (модуль інтернет – речей), розташованих на конкретній локальній території та на достатніх відстанях один від одного. На кожному модулі розміщаються по три датчики температури, які заглиблюються на 1.8м в землю, цей же модуль містить датчкички вологості ґрунту та датчики вимірювання температури та вологості атмосферного повітря.

Датчики які знаходяться у ґрунті розташовані вертикально в ґрунті через 60см і вимірюють температуру та вологість торфу, відповідно на поверхні ґрунту вимірюється температура та вологість повітря. Результати вимірювань вказаних параметрів передаються на мікроконтролер ІВС за допомогою GSM модулів. ІВС проводить обробку та оцінку результатів вимірювань, формує інтегральний висновок результатів вимірювання і по каналах радіо зв'язку і передає цю інформацію в службу ДСНС.

Для передачі інформації ми обрали модуль стандарту GSM, бо він має в порівнянні з іншими такі переваги: хороша якість зв'язку при певній щільності розташування, велика ємність мережі, низький рівень похибок в частотному діапазоні, а також ефективне кодування.

На рисунку 1 представлена схема електрична структурна даної ІВС. На рисунку 2 приведено алгоритм роботи даної ІВС. Робота даної ІВС

зводиться до почергового опитування модулю інтернет- речей, обробки та оцінювання результатів вимірювання та формуванню результату по кожній точці вимірювання. Модуль інтернет – речей представляє собою сукупність вище описаних датчиків, мікроконтролера, елементів пам'яті та засобів зв'язку. Живлення такого модуля комбіноване – акумулятор плюс сонячна батарея.

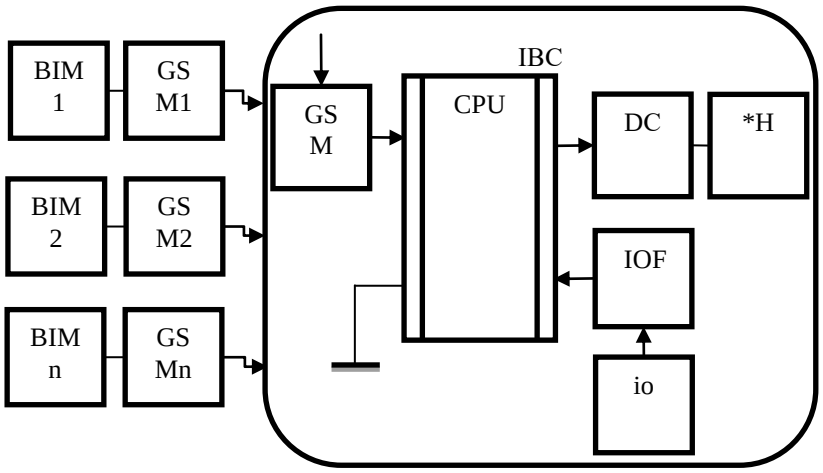


Рисунок 1

CPU – центральний процесор
GSM – модуль передачі даних
IOF — інтерфейс
DC –дешифратор
io – пристрій вводу/виводу

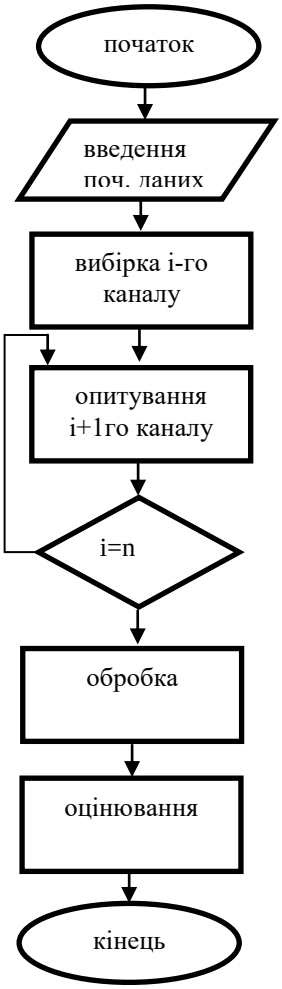


Рисунок 2

Висновок: використання запропонованої ІВС дозволить контролювати рівень пожежної безпеки торф'яників, вчасно реагувати на критичні ситуації та забезпечить збереження навколишнього середовища та природного різноманіття.

Література

1. https://uk.wikipedia.org/wiki/%D0%A2%D0%BE%D1%80%D1%84
2. https://fireman.club/inseklodepia/torfyanye-pozhary/
3. https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/industrial-internet-things-iiot/
4. https://wireless-e.ru/gsm/enfora/
5. http://edu-mns.org.ua/files/materials.pdf

ПРИМЕНЕНИЕ МЕТОДА ЭЛЕКТРОМАГНИТНОГО ПОИСКА ДЛЯ ОПТИМИЗАЦИИ ПЛАНОВ МНОГОФАКТОРНОГО ЭКСПЕРИМЕНТА

Малкова А.В.
Научный руководитель – д.т.н., проф. Кошевой Н.Д. Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»
61070, Харьков, ул. Чкалова, 17, каф. интеллектуальных измерительных систем и инженерии качества, тел. (057) 788-43-03 e-mail: amalkova158@gmail.com

The cost of the experiment is significantly influenced by the order of alternation of the levels of change in the factors of the planning matrix. Therefore, an urgent task is to study and apply methods that will allow alternating experiments in such a way that the cost of conducting an experiment becomes minimal. For this, a method has been developed for optimizing a multifactor experiment using electromagnetic search. This method is based on Coulomb's law and the idea of the attraction-repulsion mechanism of the theory of electromagnetism.

В науке и технике всё больше возрастает необходимость рационального использования труда ученых и инженеров, а также средств производства – технического оборудования и материалов. Одним из направлений повышения производительности научного труда является применение передовых математических методов и вычислительных средств. К таким методам относится планирование эксперимента. Его качественная и оптимальная реализация позволяет успешно решать научные, производственные и технологические проблемы.

Разработан метод оптимизации многофакторного эксперимента с использованием алгоритма электромагнитного поиска. Метод основан на аналогии с законом Кулона: агент – это электрически заряженная частица, заряд которой прямо пропорционален значению функции в той точке области поиска, где ее значение минимальное и обратно пропорционально расстоянию между этими частицами [1]. Реализация метода заключается в перестановке строк матрицы планирования эксперимента и нахождения минимального значения стоимости перестановки по отношению к первой строке матрицы. Одновременно с этим, на минимальное значение стоимости влияет расстояние между строками матрицы.

При исследовании фотоэлектрических преобразователей угловых перемещений [2] в качестве факторов, влияющих на процесс, целесообразно выбрать: x_1 – угол отклонения центральной оси излучающего элемента (ИЭ) от центральной оси принимающего элемента (ПЭ), x_2 – интервал между центральными осями ИЭ и ПЭ, x_3 – дистанция между ИЭ и ПЭ. Напряжение U, мВ является параметром оптимизации. Для построения математической модели в виде $U = f(x_1, x_2, x_3)$ достаточно применить полный факторный эксперимент 2^3. Стоимости изменений значений

факторов приведены в таблице 1.

Таблица 1 – Стоимости изменений значений факторов

Уровни	$S_{x1,}$ у.е.	$S_{x2,}$ у.е.	$S_{x3,}$ у.е.
-1 → +1	3,2	6,8	7
+1 → -1	3	5,5	6,4

План эксперимента, полученный с помощью метода электромагнитного поиска, представлен в таблице 2.

Таблица 2 – План эксперимента, полученный методом электромагнитного поиска

Номер опыта	Факторы		
	x_1	x_2	x_3
1	-1	-1	-1
2	-1	-1	+1
3	+1	-1	+1
4	+1	+1	+1
5	-1	+1	+1
6	-1	+1	-1
7	+1	+1	-1
8	+1	-1	-1

Стоимость проведения эксперимента составляет 35,1 у.е. По сравнению с начальным планом эксперимента [3], который имеет стоимость реализации 47,9 у.е., выигрыш составляет 1,3 раза.

Разработан метод, который реализует оптимизацию многофакторного эксперимента с использованием алгоритма электромагнитного поиска.

Выполнено построение оптимального плана эксперимента для исследования фотоэлектрических преобразователей угловых перемещений. Перспективы дальнейших разработок заключаются в создании и применении программного обеспечения для оптимизации данным методом планов многофакторных экспериментов с количеством факторов $k>3$.

Список литературы

1. Карпенко А.П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой: учебное пособие. М.: изд-во МГТУ им. Н. Э. Баумана, 2014. 446 с.
2. Кошевой Н. Д., Костенко Е.М. Оптимальное по стоимостным и временным затратам планирование эксперимента: монография. Полтава: изд. Шевченко Р.В., 2013. 317 с.
3. Адлер Ю.П., Маркова Е.В., Грановский Ю.В. Планирование эксперимента при поиске оптимальных условий. М.: Наука, 1971, 283 с.

ВИЗНАЧЕННЯ КІЛЬКІСНИХ КОНТРОЛЬНИХ МЕТОДІВ ОЦІНЮВАННЯ СТАНУ ЗРАЗКІВ ТЕХНІКИ

д.т.н., проф. Кононов В.Б., Кононова О.А.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба
61023, Харків, вул. Сумська 77/79, каф. метрології та стандартизації,
тел. 0673045784 e-mail: aveprofessor@gmail.com

In this report we will consider the quantintive evulation methods of vehicle samples condition, in basis of which there are operations of measurement control, accuracy properties of which are characterized by probability indicators. Existed measuring methods of complex devices workability control are based on individual predictive and diagnostic methods of controlling the vehicle condition. For evulation the probability of which we use the known errors probability for the first and second type, which are functionally related with vehicles parameters measurement errors.

В основі кількісних контрольних методів оцінювання стану зразків техніки лежать операції вимірювального контролю працездатності (ВКП), точнісні властивості яких характеризуються показниками ймовірності.

Кожна група методів ВКП відрізняється сукупністю засобів вимірювання, що використовується. У системі контролю працездатності складних виробів можуть бути передбачені методи індивідуального прогнозуючого контролю стану (ПКС) й діагностичного контролю стану (ДКС). ДКС, які використовують кількісні (параметричні) або якісні (функціональні) методи пошуку й локалізації відмов апаратури зразків техніки, завжди базуються на операціях контролю. Для оцінки ймовірності яких використовуються відомі ймовірності помилок першого й другого роду, що функціонально пов'язані з похибками вимірів параметрів зразків техніки. Визначимо існуючи ВКП.

При проведенні контролю - перевірки працездатності зразків техніки за ВКП 1 працездатність зразків техніки оцінюється за результатами ВКП його технічних параметрів (метод диференціального або поелементного контролю). Система контролю зразка техніки, що реалізує методи ВКП1, є сукупністю засобів вимірювання кожного контрольованого параметра зразків техніки й ланки контролю, що виробляє сигнали “придатний” або “непридатний” по параметрах, а також по зразку техніки в цілому.

При проведенні контролю - перевірки працездатності зразків техніки, за ВКП 2 працездатність зразків техніки оцінюється безпосередньо за результатами контролю вихідних (узагальнених) параметрів або характеристик зразків техніки, що отримуються розрахунковим шляхом, на основі вимірювання його технічних параметрів. Він має назву інтегрального або комплексного контролю. В якості узагальненого параметру виробу виступають показник потенціалу зразка техніки, його наробіток на відмову, коефіцієнт готовності, коефіцієнт збереження ефективності. Система контролю стану, яка здійснює реалізацію методу ВКП 2, є сукупністю засобів вимірювання параметрів зразків техніки, пристроїв обробки даних і

обчислення узагальнених параметрів зразків техніки й ланки контролю, що виробляє контрольну оцінку “придатний” або “непридатний” по зразку техніки в цілому.

При проведенні контролю - перевірки працездатності зразків техніки, за ВКП 3 працездатність зразків техніки оцінюється безпосередньо за результатами порівняння вихідних параметрів виробу з параметрами контрольного (“зразкового” або “еталонного”) зразка техніки, характеристики якого в 2 - 10 раз точніше відповідних характеристик контрольованого зразка техніки**.**

У систему контролю стану, що реалізує методи ВКП1-ВКП3, входить контрольний зразок, наприклад, оптичний або лазерний засіб для контролю, ланка контролю із пристроєм обробки й аналізу результатів порівняння вихідних параметрів, що виробляють сигнали “придатний” або “непридатний” по зразку техніки в цілому.

При проведенні контролю - перевірки працездатності зразків техніки, за ВКП 4 працездатність зразків ОВТ оцінюється за результатами аналізу відгуків виробу на контрольні (стимулюючі, іспитові) сигнали (тести) генераторів або імітаторів з нормованими метрологічними або точністними характеристиками. Система контролю стану, що реалізує методи ВКП 4, містить джерела каліброваних сигналів, індикатори або засоби вимірів параметрів відгуків на функціональних виходах зразка техніки, пристрою обробки й аналізу вимірювальної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кононов В.Б. Використання вимірювальних перетворювачів виїзними метрологічними групами в умовах проведення операції Об’єднаних сил: підручник / В.Б. Кононов, І.В. Толок, А.М. Науменко та ін.. – Х.:ХНУПС, 2019. – 428 с.

2. Кононов В.Б. Застосування електричних вимірювань засобами вимірювальної техніки в умовах проведення АТО: навч. посіб./ В.Б. Кононов, А.М. Науменко, О.В. Коваль та ін.. – Х.:ХНУПС, 2018. – 392 с.

3. Кононов В.Б. Основи експлуатації засобів вимірювальної техніки військового призначення в умовах проведення АТО: навч. посіб./ В.Б. Кононов, А.М. Науменко, О.В. Коваль та ін.. – Х.:ХНУПС, 2017. – 288 с.

4. Кононов В.Б. Instrumentation and general principles of sensors. Part 1: навч. посіб./ В.Б. Кононов, А.М. Науменко, О.В. Коваль та ін.. – Х.:ХНУПС, 2018.-64 с.

5. Mohammed A.S. Optimal Forecast Model for Erbil Traffic Road Date/ ZANCO Journal of Pure and Applied Sciences. 2017. Vol. 29. No 5. P/ 137 – 145, DOI: https://doi.org/10.21271/ZJPAS.29.5.15.

СТРУКТУРНА СХЕМА ЦИФРОВОГО ВИМІРЮВАЧА ТИСКУ

д.т.н., доц. Шевяков Ю.П., к.т.н., доц. Рафальський Ю.І.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба,
61023, Харків, вул. Сумська 77/79, каф. Метрології та стандартизації,
тел. 0673045784
e-mail: aveprofessor@gmail.com

In this report we consider the structural scheme of digital pressure meter. The following questions will be discussed: using the measuring pressure converters in the automatized system of parameters controlling of pressure measuring devices (ASPC); reasoning the structural scheme of digital pressure meter. For the purpose of developing the structural scheme of pressure meter, in this report were considered the conceptions about construction the chains of structural schemes of measuring devices. Based on this analysis the auothors proposed the structural scheme of digital pressure meter.

В доповіді розглядається структурна схема цифрового вимірювача тиску. Розглядаються наступні питання, як: використання вимірювальних перетворювачів тиску в автоматизовані системи контролю параметрів засобів вимірювання тиску (АСКП); обгрунтовунання структурної схеми цифрового вимірювача тиску.

Основою вдосконалення і розробки перспективних засобів вимірювання тиску є автоматизовані системи контролю параметрів АСКП та розробка нових приладів. Це дозволяє скоротити витрати часу з метою підтримання метрологічних характеристик засобів вимірювання тиску на необхідному (відповідному) рівні. Для прямого вимірювання тиску рідкої або газоподібної середи з відображенням його значення безпосередньо по шкалі, табло або на індикаторі у якості первинного вимірювального приладу використовуються манометри. Манометри класифікують за принципом дії та конструкції, по виду вимірюванного тиску, за застосуванням та призначенням, по типу відображення данних та іншими ознаками. За принципом дії манометри можно розділити на рідинні,деформаційні, вантажнопоршневі, електричні (тиск визначається на основі залежності електричних параметрів та інші (теплові, онізаційні, термопарові та інші). В промисловості при локальних вимірюваннях тиску енергоносіїв в більшості випадків використовуються деформаційні манометри на основі одновиткової трубчатої пружини-трубки Бурдона - для прямопоказуючих стрілкових приладів або з багатовитковими пружинами для самописних манометрів, але на зміну їм все частіше надходять електричні манометри з цифровим табло та розвиненою системою інтерфейсів.

На сьогоднішній день найпопулярніші в світі є тензорезисторні ВПТ. Тензорезисторні чутливі елементи ТРЧЕ зображують собою металеву та або діелектричну вимірювальну мембрану, на якій розміщуються тензорезистори з контактними площадками для провідного підключення до внутрішньої або зовнішньої схеми – електронному блоку обробки.

Тензорезистори (ТР) виконуються, як із металу так і з напівпровідників. Для ТРЧЕ, особливо напівпровідникових, існує вплив температури на пружні та електричні характеристики ТР, що потребує застосування спеціальних схем температурної компенсації.

З метою розробки структурної схеми вимірювача тиску в доповіді розглянуті поняття щодо побудови ланцюгів структурних схем ЗВТ.

В засобі вимірювання, сигнал, що переносить інформацію про значення вимірюваної величини, звичайно проходить ряд перетворень з метою отримання потрібного вихідного сигналу. Кожне перетворення сигналу можна уявити собі окремими частинами і дати їм назву “ланки”. З’єднання таких ланок у визначений ланцюг перетворювачів має назву структурної схеми. Структурна схема визначає основні функціональні частини виробу, їх призначення і взаємозв’язок. Основними ланками вимірювальних систем є: вимірювальний елемент; вимірювальний ланцюг; чутливий елемент; вимірювальний механізм; звітний пристрій. В залежності від з’єднання кіл розрізняють два основних виду структурних схем: прямого перетворення (дії) та врівноваженого (компенсаційного) перетворювання (дії). Структурна схема врівноваженої дії також має назву схеми з від’ємним зворотним зв’язком. На основі цього аналізу авторами була запронована структурна схема цифрового вимірювача тиску.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кононов В.Б. Використання вимірювальних перетворювачів виїзними метрологічними групами в умовах проведення операції Об’єднаних сил: підручник / В.Б. Кононов, І.В. Толок, А.М. Науменко та ін.. – Х.:ХНУПС, 2019. – 428 с.

2. Кононов В.Б. Застосування електричних вимірювань засобами вимірювальної техніки в умовах проведення АТО: навч. посіб./ В.Б. Кононов, А.М. Науменко, О.В. Коваль та ін.. – Х.:ХНУПС, 2018. – 392 с.

3. Кононов В.Б. Основи експлуатації засобів вимірювальної техніки військового призначення в умовах проведення АТО: навч. посіб./ В.Б. Кононов, А.М. Науменко, О.В. Коваль та ін.. – Х.:ХНУПС, 2017. – 288 с.

4. Кононов В.Б. Instrumentation and general principles of sensors. Part 1: навч. посіб./ В.Б. Кононов, А.М. Науменко, О.В. Коваль та ін.. – Х.:ХНУПС, 2018.-64 с.

5. Mohammed A.S. Optimal Forecast Model for Erbil Traffic Road Date/ ZANCO Journal of Pure and Applied Sciences. 2017. Vol. 29. No 5. P/ 137 – 145, DOI: https://doi.org/10.21271/ZJPAS.29.5.15.

АНАЛІЗ МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ЗАКОНОДАВЧО РЕГУЛЬОВАНИХ ЗАСОБІВ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ В СФЕРІ ЗАХИСТУ ЖИТТЯ ТА ОХОРОНИ ЗДОРОВ'Я ГРОМАДЯН

Інженер з метрології 2 категорії Дученко П.Ю.,
інженер з метрології Сафін В.Т.
Керівник – начальник науково-виробничого відділу прикладної метрології фізико-хімічних вимірювань (ВФХ) Пономарьов А.В.
ДП «Харківський регіональний науково-виробничий центр стандартизації, метрології та сертифікації» (ДП «Харківстандартметрологія»)
61002, Харків, вул. Мироносицька, 36, тел. 0680742511, 0958142162
e-mail: pasha-duchenko@ukr.net, safin31021@gmail.com

The purpose of this work is to analyze the impact of changes to the Technical Regulations of legally regulated measuring equipment № 94 from 13.01.2016, introduced by the Resolution of the Cabinet of Ministers № 598 from 10.07.2019 to ensure the unity of measurements in the field of life and health.

Keywords**:** measurement, metrology, maintenance, means of measuring equipment, means of medical equipment.

Метою цієї роботи є аналіз впливу зміни до Технічного регламенту законодавчо регульованих засобів вимірювальної техніки № 94 від 13.01.2016р., внесені Постановою КМУ № 598 від 10.07.2019р. на забезпечення єдності вимірювань в сфері захисту життя та охорони здоров'я громадян.

Урядом України у 2013 році медичні вироби з функцією вимірювання включено до сфери регулювання Технічного регламенту щодо медичних виробів, затвердженого постановою Кабінету Міністрів України від 02.10.2013р. № 753, та Технічного регламенту щодо медичних виробів для діагностики in vitro, затвердженого постановою Кабінету Міністрів України від 02.10.2013р. № 754 (далі – Технічний регламент № 753, Технічний регламент № 754), без відсильної норми на будь-які інші технічні регламенти щодо вимірювальної техніки.

З прийняттям Технічного регламенту законодавчо регульованих засобів вимірювальної техніки, затвердженого постановою Кабінету Міністрів України від 13.01.2016р. № 94 (далі – Технічний регламент № 94), під його регуляторну дію потрапили медичні вироби з функцією вимірювання, на які поширюється дія Технічного регламенту № 753 або Технічного регламенту № 754, чим створено проблему подвійної оцінки відповідності медичних виробів з функцією вимірювання вимогам технічних регламентів, що негативно вплинуло на нормальне функціонування операторів ринку.

На початку 2017 року наказом Міністерства економічного розвитку і торгівлі України від 02.02.2017р. № 129 створено Робочу групу з питань удосконалення оцінки відповідності законодавчо регульованих засобів вимірювальної техніки, що застосовуються для забезпечення захисту життя та охорони здоров'я громадян (далі – робоча група).

Робочою групою, сформованою для вирішення проблеми, прийнято рішення (протокол від 11.05.2017р. № 2) підготувати проекти змін до Технічного регламенту № 94, на ті засоби вимірювальної техніки, що є медичними виробами та на які поширюється дія Технічного регламенту № 753 та/або Технічного регламенту № 754. Постановою КМУ № 598 від 10.07.2019р., яка набрала чинність з 19.01.2020р. були внесені зміни до Технічного регламенту законодавчо регульованих засобів вимірювальної техніки № 94 від 13.01.2016р. з якого виключили медичні вироби з функцією вимірювання.

З одного боку, операторам ринку спростили вимоги для введення в обіг медичних виробів з функцією вимірювання, однак з іншого це негативно вплине на забезпечення єдності та точності вимірювань у сфері захисту життя та охорони здоров'я громадян, оскільки Технічний регламент № 753 не містить вимог щодо метрологічних характеристик засобів вимірювальної техніки.

З наведеної вище інформації можна зробити висновок, що для забезпечення єдності вимірювань та простежуваності в сфері забезпечення захисту життя та охорони здоров'я громадян, до Технічного регламенту №753 необхідно долучити вимоги щодо технічної документації на медичні вироби з функцією вимірювання, яка повинна бути достатньою мірою деталізованою для забезпечення додержання таких вимог:

1) визначення метрологічних характеристик;

2) відтворюваність метрологічних характеристик виготовлених засобів вимірювальної техніки за умови проведення належного регулювання з використанням призначених для цього засобів.

Наведені вище висновки є важливими, так як метрологічне забезпечення є важливою складовою якості надання медичних послуг, оскільки точність результатів вимірювань, яка використовується в медичних закладах безпосередньо впливають на точність діагнозу та правильність лікування, а отже – на здоров'я та життя пацієнтів.

Список використаних джерел:

1. Про метрологію та метрологічну діяльність: Закон України від 03.07.2020 № 1314-VII.

2. Про технічні регламенти та оцінку відповідності: Закон України від 03.07.2020 № 124-VIII.

3. Кушнір М. Проблеми метрологічного забезпечення діяльності закладів первинної медико-санітарної допомоги // Метрологія та прилади. – 2019. – № 3. – С. 67–71.

ВІДТВОРЕННЯ НАПРУГИ ЗМІННОГО СТРУМУ НА ЕФЕКТІ ДЖОЗЕФСОНА

Жирна Г.А.
Науковий керівник - д.т.н., проф. Павленко Ю.Ф.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14, каф. Метрології та технічної експертизи,
тел. (050) 619-92-83, e-mail: hanna.zhyrna@nure.ua

The reference base, which currently has 79 national standards, creates conditions for improving product quality and production efficiency, environmental control and protection of life and health of citizens, improving the country's defense capabilities, ensuring the requirements of technical regulations. Therefore, this article will consider methods for implementing AC voltage on the Josephson effect.

Створенні еталонів постійної напруги з використанням ефекту Джозефсона і багатоконтактних матриць стимулювали дослідження щодо можливості використання цього ефекту для відтворення напруги змінного струму. Формування напруги змінного струму з використанням ефекту Джозефсона може бути виконане:

1. Методом синтезу відліків або програмованої матриці (PJVS-метод);
2. Кодоімпульсним методом (JAWS-метод);
3. Методом з використанням частотної модуляції НВЧ-опромінення;

PJVS-метод полягає в отриманні серії дискретних відліків постійної напруги з виводів джозефсонівської матриці і у формуванні східчастого сигналу змінного струму. Для відтворення напруги змінного струму необхідна швидка і точна перекомутація опорних напруг Джозефсона. Перекомутація неможлива з переходами SIS (надпровідник-ізолятор-надпровідник). Таку можливість надають тільки лінійні матриці сильно загасаючих переходів – SINIS і SNS, однак при цьому збільшується необхідне число переходів.

Матриця з частотою опромінення 70 ГГц повинна мати близько 70 000 переходів для одержання напруги 10 В, що у 5 разів більше, ніж у стандартної матриці для одержання постійної напруги. Якщо з ряду причин потрібно використовувати більш низьку частоту опромінення (близько 20 ГГц), число переходів навіть збільшується пропорційно зменшенню частоти опромінення. Такі високотехнологічні матриці випускають тільки метрологічні інститути США і Німеччини.

Даний метод має як переваги, так і недоліки. Перевага - мала невизначеність рівня кожної сходинки, яка не перевищує $5\cdot 10^{-9}$ на частотах до 1 кГц, недолік - у спектрі такого сигналу міститься велика кількість

гармонік, що не дозволяє використовувати даний метод у деяких задачах метрології.

JAWS-метод. Недолік попереднього методу можна виправити, якщо використовувати як опромінюючий сигнал не синусоїдальний, а послідовність імпульсів. Залежно від тривалості окремих імпульсів по переходу буде проходити певне число квантів потоку на імпульс. Шляхом регулювання частоти імпульсів на матриці генерується точно визначена напруга змінного струму. Для цього в найпростішому випадку можна використовувати промисловий високошвидкісний генератор імпульсів.

Метод з використанням програмованої джозефсонівської матриці (PJVS-метод) забезпечує високу вихідну напругу (до 10 В), однак її спектр містить чималу кількість гармонік (тобто має значні спотворення). Кодоімпульсний метод (JAWS-метод) забезпечує чистий спектр, але рівень вихідного сигналу не перевищує 1 В.

Метод з використанням частотної модуляції НВЧ-опромінення .Цей метод базується на прямій залежності напруги на виході джозефсонівської матриці від частоти опромінення. Метод запропоновано в ННЦ «Інститут метрології», на цей час він знаходиться в стадії дослідження.

Можлива **комбінація двох методів**, яка поєднує у собі позитивні якості першого та другого методу, тобто (PJVS+JAWS) метод, , який дозволяє одержати рівень напруги до 10 В з високою спектральною чистотою. Поетапно синтезують сигнал методом PJVS і на нього накладають сигнал JAWS (метод суперпозиції). Експеримент показує, що при коректній реалізації і синхронізації сигнал JAWS здатний суттєво зменшити стрибки напруги, які виникають у сигналі PJVS.

Еталони змінної напруги на ефекті Джозефсона мають своє особливе значення для метрології, воно полягає в можливості відтворення напруги змінного струму з невизначеністю, на 1-2 порядки меншою, ніж існуючі еталони, які працюють на методі теплового компарування.

Список використаної літератури:

1. Вступ до квантової метрології. Підручник. Ю.Ф. Павленко, С.І. Кондрашов, П.І. Неєжмаков та ін.; за ред. Ю.Ф. Павленка. – Харків : ФОП Мезіна В.В., 2017.

ОСОБЕННОСТИ ПРОФЕССИИ QUALITY ASSURANCE ИНЖЕНЕР

Луценко М.И.
Научный руководитель - к.т.н., проф. Егоров А.Б.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки,14, каф. Метрологии и технической экспертизы, тел. (057) 702-13-31)
e-mail: milana.lutsenko@nure.ua

Quality assurance (QA) is any systematic process of determining whether a product or service meets specified requirements.QA establishes and maintains set requirements for developing or manufacturing reliable products. A quality assurance system is meant to increase customer confidence and a company's credibility, while also improving work processes and efficiency, and it enables a company to better compete with others.

Современное понимание обеспечения качества (Quality Assurance) продукции включает в себя прежде всего принцип отражения качества продукции в процессах, ее создающих, уменьшение вариативности процессов вследствие их статистического контроля (управления) и стандартизацию. Отцами современного менеджмента по обеспечению качества безусловно являются Такиши Тойлда, Генри Форд, Уолтер Шухаржд и Эдвард Дкминг.

Иногда ошибочно считают, что QA - инженер и тестировщик ПО – это одно и тоже. На самом деле тестировщик программного обеспечения занимается тестировкой уже готового ПО, QA - инженер работает над формированием процессов всего жизненного цикла ПО.

Quality Assurance engineer — это специалист по обеспечению качества, деятельность которого направлена на улучшение процесса разработки ПО, предотвращение дефектов и выявление ошибок в работе продукта.

Основная задача QA — обеспечение качества процессов. QA-инженер фокусирует внимание на процессах разработки ПО, улучшает их, предотвращает появление дефектов и проблем (Makes sure you are doing the right things, the right way).

Процесс обеспечения качества состоит из таких этапов:

- проверка требований к продукту;
- оценка рисков;
- планирование идей по улучшению качества продукта;
- планирование тестирования;
- анализ результатов тестирования.

Поскольку QA-инженер сотрудничает с большим количеством людей, он должен разговаривать с ними на одном языке и в какой-то мере обладать качествами этих специалистов:

- как девелопер - понимать код и иметь представление о технических рамках для реализации различных методологий;

- как бизнес-аналитик — знать рынок и целевую аудиторию, для которой создаётся ПО;

- как менеджер проекта — видеть общую картину, составленную из всех частей проекта;

- как конечный пользователь — понимать удобство пользования ПО.

К безусловным плюсам профессии можно отнести следующее:

- возможность (и необходимость!) постоянного повышения профессионального уровня в соответствии с прогрессом IT-отрасли и сферы бизнеса. Профессия не позволяет расслабиться и умственно деградировать, заставляет быть в курсе новых технологий;

- высокая оплата труда;

- престиж и всё возрастающая востребованность профессии в будущем.

Недостатками профессии являются:

- рутинная и монотонная работа при прохождении тест-кейсов в ручном тестировании и работе с документацией;

- постоянная сидячая работа за компьютером;

- большое количество заинтересованных лиц в каждом проекте, у которых свои пожелания и требования: заказчики, разработчики, пользователи.

По данным ДОУ, среднему украинскому QA-инженеру 26 лет. Он имеет опыт работы от полугода (джуниор) до 5 лет (сеньор) и получает зарплату $600-2700.

Литература:

1. ДСТУ ISO 13053-1:2011. Статистичні методи. Методологія поліпшення процессів «Шість сигма». Частина 1. Методологія DMAIC/

2. Статистическое управление процессами. Оптимизация бизнеса с использованием контрольных карт Шухарта / Дональд Уиллер, Девид Чамберс; Пер. с англ. – М.: Альпина Паблишер, 2019 – 409 с.

3. https://searchsoftwarequality.techtarget.com/definition/quality-assurance.

4. https://www.profguide.io/professions/qa_injeneer.html.

5. https://dou.ua/lenta/articles/qa-engineer-position/.

МЕТОДИ ТА ЗАСОБИ ВИМІРЮВАННЯ ШВИДКОСТІ ПОВІТРЯНОГО ПОТОКУ

Інженер з метрології 2 категорії Бондаренко С.В.
Керівник – начальник сектору прикладної метрології вимірювань механічних та акустичних величин (СМА) Юрченко В.М.
ДП Харківський регіональний науково-виробничий центр стандартизації, метрології та сертифікації (ДП «Харківстандартметрологія»)
61002, Харків, вул. Мироносицька, 36, тел. 0969787348
e-mail: sergey3bond@gmail.com,

The main purpose of the article is to reveal the reasons for measuring the air flow velocity and the processes it affects, to classify air flow velocity measuring instruments. Description of the main types of anemometers is presented. The article is of great help to choosing an anemometer to solve specific problems. From this work we can conclude that to choose an anemometer you need to clearly understand for what purposes it will be used.

Keywords**:** air flow velocity, anemometer, impeller, hot wire, pressure tube, ultrasound, laser.

Метою цієї роботи є розкриття цілей вимірювання швидкості повітряного потоку та процесів на які вона впливає, наведення класифікації вимірювальних приладів за їхніми конструктивними відмінностями, методом взаємодії з потоком та принципом дії.

Швидкість повітряного потоку – це дуже важливий параметр, який впливає на продуктивність людської праці, строк напрацювання на відмову механізмів, проведення будівельних робіт на висоті, метеорологічні умови оточуючого середовища та на багато інших процесів, які зустрічаються у нашому житті.

Для вимірювання швидкості повітряного потоку використовуються вимірювальні прилади, які називаються анемометрами. Анемометр **–** це прилад для вимірювання швидкості потоків та напрямку руху повітря, газів і рідин**.** Принцип роботи анемометра полягає у виявленні зміни деякої фізичної властивості потоку, або у дії потоку на механічний пристрій, розміщений в потоці.

В залежності від методу вимірювання та типу приймального пристрою анемометри поділяють на ряд типів [1]: механічні (крильчаті, чашкові), теплові (термоанемометри), динамометричні (з напірними трубками), ультразвукові (акустичні), оптичні (лазерні допплерівські).

У крильчатих та чашкових анемометрах рух повітря сприймається чотирма полими півкулями або пластинками, вигнутими у вигляді лопатей. Їхнє обертання передається стрілкам індикатору системою зубчатих коліс (анемометри АСО-3 та МС-13). Також механічні чутливі елементи можуть бути використані у поєднанні з електронним вторинним перетворювачем (анемометри Testo 417, АЦК-10). Механічні анемометри мають діапазон

вимірювань від 0,1 до 50 м/с. Переваги: порівняно невисока ціна, певна стійкість до турбулентних потоків, незалежність від температури потоку. Недоліки: недовговічність обертального механізму, невисока точність [2].

Принцип роботи теплового анемометра полягає у вимірюванні температури пластини чи нитки розжарювання, з якою взаємодіє потік. В залежності від швидкості потоку, необхідна різна енергія для того, щоб підтримувати температуру сталою. Тобто за температурою пластини можна визначити швидкість повітряного потоку (термоанемометри Testo 405, ТКА-ПКМ, МЕТЕОСКОП-М). Діапазон вимірювань від 0,01 до 20 м/с. Переваги: достатньо висока точність, невеликі розміри, висока чутливість. Недоліки: менший діапазон вимірювань, вища ціна.

Вимірювання швидкості потоку повітря можна проводити також методом визначення тиску повітря всередині напірної трубки (найчастіше конструкції Піто та НИИОГАЗ). Швидкість руху повітря обчислюється шляхом порівняння надлишкового тиску повітря всередині трубки та зовні. Це так звані динамометричні анемометри. Вимірювальний діапазон від 2 до 100 м/с. Переваги методу: визначення високих швидкостей повітряного потоку, широкий температурний діапазон, довгий строк служби напірної трубки. Недоліки: неможливість вимірювання низьких швидкостей, необхідність використання напірної трубки у взаємодії з диференційним манометром, необхідність проведення розрахунків [3].

Ультразвукові та лазерні анемометри використовуються для вирішення спеціальних завдань. Вони хоча і мають високу точність та широкий діапазон вимірювань, але коштують дуже багато, через це для контролю швидкості потоку у повсякденних задачах їх використовувати недоцільно та дорого.

З наведеної вище інформації можна зробити висновок, що найпоширенішими вимірювачами швидкості повітряних та газових потоків є механічні, теплові та динамометричні анемометри. Для того, щоб обрати потрібний вимірювальний прилад, треба знати у якому діапазоні та з якою динамікою змінюється швидкість повітряного потоку, з якою точністю її потрібно виміряти та розуміти скільки коштів ви готові заплатити за бажаний прилад.

Список використаних джерел:

1. Анемометр//https://simvolt.ua/anemometr-prilad-dlya-viznachennya-shvidkosti-ta-napryamku-rukhu-potoku/, 23.02.2021.

2. Голінько В.І. Основи охорони праці: підручник / В.І. Голінько – Харків : НГУ, 2014. – 271 с.

3. Посудін Ю.І. Методи вимірювання параметрів навколишнього середовища: підручник / Ю.І. Посудін — Київ: Світ, 2003. — 288 с.

ПРОВЕРКА ПРОФЕССИОНАЛЬНОГО УРОВНЯ КАЛИБРОВОЧНЫХ ЛАБОРАТОРИЙ МЕТРОЛОГИЧЕСКИМ ЦЕНТРОМ ГП «ХАРЬКОВСТАНДАРТМЕТРОЛОГИЯ»

Новомодный О.Н., PhD Коржов И.М.
Государственное предприятие «Харьковский региональный научно-производственный центр стандартизации, метрологии и сертификации»
Украина, 61002, г. Харьков, ул. Мироносицкая, 36,
тел. (057) 752-43-82, e-mail: 330@mtl.kharkov.ua, provayder330@gmail.com

Proficiency testing is the most objective tool for external quality assessment of calibration laboratories. Proficiency testing is performed by a proficiency testing provider. The Metrological Center of SE "Kharkovstandartmetrology" is the first in Ukraine accredited proficiency testing provider. The metrological center of SE "Kharkovstandartmetrology" has implemented about 100 rounds of proficiency testing schemes, in which 39 different calibration laboratories took part. SE "Kharkovstandartmetrology" implements European and world approach to recognition of proficiency testing.

Проверка профессионального уровня (проверка квалификации) (proficiency testing) – наиболее объективный и эффективный инструмент внешней оценки общего качества метрологических работ и деятельности, калибровочных лабораторий в частности [1].

Согласно ДСТУ EN ISO/IEC 17043:2017 [2] проверку профессионального уровня реализует провайдер проверки профессионального уровня. Для независимого подтверждения своей компетенции в проведении работ по проверке профессионального уровня провайдер профессионального уровня Метрологический центр ГП «Харьковстандартметрология» первый в Украине успешно прошёл аккредитацию в Национальном агентстве аккредитации Украины на соответствие ДСТУ EN ISO/IEC 17043:2017 [2] в 2018 году.

ГП «Харьковстандартметрология», в качестве провайдера проверки профессионального уровня и Отдел прикладной метрологии измерительных систем и процессов (ОСП), в качестве координатора, регулярно проводят раунды проверки профессиональной деятельности по таким направлениям как калибровка средств измерительной техники и испытание продукции. За 5-и летний период деятельности провайдер –Метрологический центр ГП «Харьковстандартметрология» реализовал около 100 раундов схем проверки профессионального уровня, в которых приняли участие 39 различных калибровочных лабораторий различных форм собственности. В тоже время, на момент написания статьи, согласно реестру Національного агентства з акредитації України (НААУ) [3], в Украине насчитывается 35 аккредитованных калибровочных лабораторий, для которых участие в подобных проверках является обязательным.

Заинтересованность к деятельности Метрологического центра ГП «Харьковстандартметрология» как провайдера проявляют лаборатории и организации не только в Украине, но и за рубежом (см. рис. 1):

Рис. 1 – Статистика посещаемости официального web-сайта провайдера

Метрологический центр ГП «Харьковстандартметрология» не останавливается на достигнутом и разрабатывает новые направления реализации раундов проверки профессиональной деятельности. Наши предложения открыты широкому кругу лабораторий благодаря освещению деятельности провайдера в глобальной сети Интернет по адресу http://khsms.com/primaryactivity/metrology/about/type/remont/id/23/lang/ua [4]

Деятельность ГП «Харьковстандартметрология» в этом направлении реализует европейский и мировой подход к признанию профессионального уровня не только в рамках Украины, но и позволяет поставщикам продукции и услуг выходить на международный уровень.

Список литературы:

1. Коржов І. М. Перспективи розвитку теорії і практики контролю та діагностування в розрізі перевірки кваліфікації лабораторій // Вісник Національного технічного університету ХПІ. Серія: Математичне моделювання в техніці та технологіях. – 2018. – №. 27. – С. 62-67

2. ДСТУ EN ISO/IEC 17043:2017 (EN ISO/IEC 17043:2010; ISO/IEC 17043:2010, IDT) Оцінка відповідності. Загальні вимоги до перевірки професійного рівня

3. Реєстр акредитованих ООВ Національне агентство з акредитації України URL: https://naau.org.ua/reyestr-akreditovanix-oov/ (дата звернення 23.02.2021)

4. Офіційна веб-сторінка провайдера перевірки професійного рівня Метрологічний центр ДП «Харківстандартметрологія» URL: http://khsms.com/primaryactivity/metrology/about/type/remont/id/23 (дата звернення 23.02.2021)

РЕАЛІЗАЦІЯ СТАТИСТИЧНИХ ІНСТРУМЕНТІВ ЦИКЛУ PDCA В СМК MAPLE

Пахомова А. О.
Науковий керівник –к.т.н., старший викладач Мощенко І.О.
Харківський національний університет радіоелектроніки,
61166, Харків, просп. Науки,14, каф. Метрології та інформаційно-вимірювальної техніки,
тел.: 0951613590, e-mail: anastasiia.pakhomova@nure.ua

Due to international standards, the quality of products of Ukrainian manufacturers meets the requirements of international and European standards. The methodological support of the guarantor of a certain level of product quality is the introduction of the PDCA cycle, which helps to achieve a certain level of product quality without the development and application of additional processes through the principle of feedback. Statistical methods of quality control are used for effective implementation of this cycle. Computer data processing methods can be used to increase the efficiency and reliability of statistical quality control methods.

Відповідність якості продукції українських виробників вимогам міжнародних та європейських нормативних документів забезпечується виконанням рекомендацій основоположного стандарту в галузі якості ДСТУ EN ISO 9001:2018 Системи управління якістю. Вимоги (EN ISO 9001:2015, IDT) [1]. Методологічною підтримкою гаранту визначеного рівня якості продукції виступає реалізація циклу PDCA («Plan» - «Do» - «Check» - «Act»), який допомагає завдяки виконанню послідовних ітераційних операцій з планування, контролю та корекції визначених параметрів продукції або технологічного процесу досягти певного рівня якості продукції без розробки та застосування додаткових процесів завдяки принципу зворотного зв'язку. Тому впровадження практичних інструментів, що забезпечують реалізацію циклу PDCA у вітчизняній промисловості, виступають сьогодні дуже важливим науковим і практичним завданням науки і техніки України.

Складність практичної реалізації циклу PDCA в умовах виробничого процесу полягає у першу чергу в тому, що його коректне та ефективне застосування передбачає обґрунтований вибір та використання статистичних методів контролю якості, перелік та загальні рекомендації щодо застосування яких наведено в ДСТУ ISO/TR 10017:2005 Настанови щодо застосування статистичних методів згідно з ISO 9001:2000 (ISO/TR 10017:2003, IDT) [2]. Переважна більшість цих методів передбачає оперування з масивами статистичних даних, отриманих під час застосування методів описової статистики, і вимагає досконалого розуміння і практичних навичок використання методів математичної статистики та теорії ймовірності для отримання достовірних результатів.

Для підвищення ефективності й достовірності при реалізації статистичних методів контролю якості, кращої візуалізації отриманих результатів в умовах виробничого процесу можуть використовуватися методи

комп'ютерної обробки даних, зокрема реалізовані за допомогою систем комп'ютерної математики (СМК). Дослідження застосування таких програмних середовищ, як, наприклад, СМК Matlab, Microsoft Office Excel, Statistica, SAP, SPSS, Microsoft Visual Studio, при реалізації окремих інструментів циклу PDCA, наведено в працях науковців [3]. Але відсутній системний підхід до комплексної реалізації інструментів контролю якості в рамках одного програмного середовища, яке є нескладним в застосуванні та вивчається студентами метрологічних та технічних спеціальностей вищих навчальних закладів України. Таким програмним засобом є СМК Maple, яка є однією з найбільш розповсюджених в застосуванні, значні можливості для здійснення символьних обчислень, велику базу команд для обчислення статистичних показників, можливості побудови та дослідження багатої кількості законів розподілу випадкових величин й генерування нових законів розподілу, наочної візуалізації отриманих статистичних результатів у вигляді дво- та тривимірної графіки.

Планується розробити модель комплексної реалізації базових інструментів контролю якості, що застосовуються в процесі застосування циклу PDCA на базі СМК Maple. Перелік статистичних методів, за якими будуть реалізовані програмні модулі на відповідних етапах циклу PDCA, наведено в таблиці:

Етап №	Сутність етапу	Інструмент контролю якості
1	Оцінка відхилення параметрів технологічного процесу або виробленої продукції від нормативних значень	Контрольні мапи, контрольні аркуші, гістограма якості
2	Оцінка факторів, які можуть викликати відхилення	Метод стратифікації, діаграма розкиду і причинно-наслідкова
3	Визначення найбільш значущих факторів	Діаграма Парето
4	Розробка та реалізація заходів щодо усунення або зменшення впливу цих факторів	-
5	Оцінка ефективності заходів	Контрольні мапи, гістограма якості, діаграма Парето

Список літератури

1. ДСТУ EN ISO 9001:2018 Системи управління якістю. Вимоги (EN ISO 9001:2015, IDT; ISO 9001:2015, IDT). Київ : ДП «УкрНДНЦ», 2018.

2. ДСТУ ISO/TR 10017:2005 Настанови щодо застосування статистичних методів згідно з ISO 9001:2000 (ISO/TR 10017:2003, IDT). Львів : ДП «НДІ «Система», 2005.

3. Власов А.И., Маркелов В.В., Сергеева Н.А., Зотьева Д.Е. Реализация визуальных инструментов контроля качества в среде Matlab. *Международный научно-исследовательский журнал*. № 4 (46). 2016. С. 59-70.

ВСТАНОВЛЕННЯ УЗГОДЖЕННОСТІ РЕЗУЛЬТАТІВ ЕКСПЕРТНОГО ОЦІНЮВАННЯ

Пономарьов А.В.
Науковий керівник – к.т.н., доцент Козлов Ю.В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки, 14, каф. Метрології та технічної експертизи,
тел. (096) 352-98-04, e-mail: yurii.kozlov83@nure.ua

The approach to solving the problem of checking the consistency of experts' opinions when considering the tasks of expert evaluation is considered. To do this, use different indicators. The most used of these is the concordance factor. But the results of calculations show some of its shortcomings. A modified concordance coefficient or Spearman's rank correlation coefficient is recommended. These coefficients are also suitable for use in algorithms for constructing ranked lists of any objects of comparison using a four-point scale, as well as in professional selection procedures and in pedagogical qualimetry.

При вирішення завдань експертного оцінювання з використанням різних шкал виникає потреба у виявлені зв’язку між кількісними та якісними показниками властивостей деяких об’єктів порівняння (ОП), поданими, наприклад, у вигляді ранжируваного списку. Зазвичай для цього використовують різні характеристики: коефіцієнт кореляції Пірсона або коефіцієнт кореляції знаків Фехнера (для шкал відношень, інтервалів та кількісної шкали), рангову кореляцію Спірмена або Кендалла (для шкал порядку), тобто для випадку використання даних нечислової природи [1]. В цьому разі недостатня узгодженість ОП і малий обсяг вибірки не дають змоги отримати очікуваний результат [2].

В практиці експертного оцінювання часто за міру узгодженості думок експертів використовують так званий коефіцієнт конкордації (КК), що розраховується в два кроки за відомими формулами [3]. Наявність у чисельнику першої з них постійного коефіцієнту 12 викликає «підозру» як натяк на емпіричність. Результати аналітичного моделювання із застосуванням табличного процесора MS Excel показують, що при рівності рангів деяких об’єктів значення КК перевищує одиницю (що потребує попередньої обробки ранжируваного списку), а при недостатній узгодженості об’єктів навіть по одному з вимірів різко зменшується. До речі, нульове значення КК є взагалі недосяжним при парній кількості експертів. Але головним недоліком коефіцієнта конкордації є необхідність підбору експертної групи і «тренування» експертів, що, на нашу думку, виключає будь-яку об’єктивність при вирішенні завдань експертного оцінювання.

Для порівняння вибірок X та Y, складених із оцінок y_i та x_i, отриманих за шкалою порядку запропоновано використовувати [4] модифікований коефіцієнт конкордації (МКК):

$$W_{м} = 1 - \frac{\sum_{i=1}^{m} |y_i - x_i|}{m(k-l)}, \quad (1)$$

де m – обсяг вибірки (фактично – кількість об'єктів експертизи, оцінюваних ознак тощо); k та l – відповідно максимально та мінімально можливі значення оцінок експертів, тому можна розглядати $(k – l) = L$ як довжину шкали, застосовувану для оцінювання.

Легко перевірити, що для будь-яких m, k, l при повному збігу оцінок числівник дробу дорівнює 0, так як $m \cdot \Delta_i = m \cdot 0 = 0$, значення $W_м = 1$, при повному незбігу числівник дробу дорівнює $m \cdot \Delta_i = m \cdot (k – l)$, значення $W_м = 0$.

Якщо одну із вибірок, наприклад Y, визначити як зразок ($y_1 = y_2 = ... = y_i = y_m = 5$ за чотирибальною шкалою), то МКК можна використати для ранжирування будь-яких об'єктів порівняння за деякими ознаками, відповідні оцінки x_i яких визначені експертним методом і приведені до чотирибальної шкали [5]; розрахункова формула приймає такий вигляд:

$$W_{м} = 1 - \frac{\sum_{i=1}^{m} |y_i - x_i|}{3m}. \quad (2)$$

Крім розглянутого МКК, для встановлення узгодженості експертних оцінок зі зразком, можна використовувати також коефіцієнт рангової кореляції Спірмена. Такий підхід може бути прийнятним також для вирішення завдань педагогічної кваліметрії і професійного відбору.

Список використаних джерел

1. Корреляция [Электронный ресурс] Режим доступа: ru.wikipedia.org. – Название с экрана.

2. Орлов, А.И. Нечисловая статистика. – М.: МЗ-Пресс, 2004. – 516 с.

3. Шишкин, И.Ф. Метрология, стандартизация и управление качеством/ И.Ф. Шишкин; под ред. акад. Н.С. Соломенко. – М.: Изд-во стандартов, 1990. – 342 с..

4. Кузнецов, А.В. Модифицированный коэффициент конкордации и его использование в нечисловой статистике/ А.В. Кузнецов [Электронный ресурс] Режим доступа: exponenta.ru›educat/referat/ XIkonkurs/ student32.

5. Дубровіна, В.В. Встановлення узгодженості результатів при вирішенні завдань експертного оцінювання/ В.В. Дубровіна, В.Є. Козлов, Ю.В. Козлов, ОО. Новикова// Зб. наук. праць Національної Академії Національної гвардії України. – Харків, 2014. – Вип. 2 (24). – С. 92- 94.

МЕТОДИКА БАГАТОКРЕТИРІАЛЬНОГО ОЦІНЮВАННЯ ЯКОСТІ ОБ'ЄКТІВ КВАЛІМЕТРІЇ РІЗНОЇ ПРИРОДИ

Черняк О.М., Сороколат Н.А., Каницька І.В.
Українська інженерно-педагогічна академія
61003, м. Харків, вул. Університетська, 16, каф. охорони праці,
стандартизації та сертифікації, тел. (057)733-78-38,
e-mail: cherniak@uipa.edu.ua

Having single quality indicators in a single (dimensionless) assessment scale, it is proposed to determine a single integrated quality indicator of a qualimetry object using integration methods. It is proposed to find the area under the broken curve, which is constructed as a result of combining the assessments of quality indicators on a dimensionless scale during a certain observation time. A method for determining a generalized quality indicator of a qualimetry object is proposed, which can be considered universal, since it can be used for multi-criteria assessment of the quality of qualimetry objects of various nature.

Виробництво якісних товарів - актуальне завдання національної економіки України, так як являється головною умовою для забезпечення конкурентоспроможності продукції національних виробників на європейських та міжнародних ринках. Для забезпечення якості продукції на виробництві існує ряд завдань, для вирішення яких необхідно застосовувати сучасні методи вимірювання, оцінювання, аналізування з метою управління технологічними процесами.

Продукція характеризується набором показників якості, які мають різні одиниці та діапазони вимірювання, тому необхідно володіти або великою кількістю інженерних методик оцінювання їх якості, або одну, універсальну, яка могла би застосовуватися для об'єктів кваліметрії різної природи. В даному випадку під об'єктом кваліметрії різної природи розуміємо різні види продукції, які мають різні показники якості зі своїми одиницями та діапазонами вимірювання.

Для розроблення такої методики необхідно вирішити декілька важливих задач, серед яких:

- визначити вид залежності між виміряним значення показника якості об'єкту кваліметрії та його оцінкою на безрозмірній шкалі;
- запропонувати метод об'єднання оцінок виміряних показників якості у єдину (комплексну) оцінку.

Пропонується методика визначення комплексного показника якості об'єкту кваліметрії, яка складається з ряду кроків:

Крок 1. Вимірюються дійсні показники якості об'єкту кваліметрії в одиницях його вимірювання.

Крок 2. Використовуючи одну із залежностей [1-3] визначають оцінки кожного показника якості на безрозмірній шкалі.

Крок 3. Будують часовий ряд зміни оцінки кожного показника якості з часом у вигляді, показаному на рисунку 1.

Рисунок 1 – Часовий ряд оцінок показників якості

Крок 4. Визначають площу під ламаною лінією, яка будується в результаті об'єднання оцінок протягом певного проміжку часу застосовуючи метод середніх прямокутників для інтегрування часового ряду з метою отримання комплексного показника якості об'єкту кваліметрії з часом:

$$S = h\sum_{i=1}^{n} x_i. \quad (1)$$

Крок 5. Використовуючи формулу (2) визначають об'єм під ламаною площиною, яка будується в результаті об'єднання усіх оцінок усіх показників якості протягом певного проміжку часу.

$$V = h \cdot k\sum_{i=1}^{n}\sum_{j=1}^{m} x_{i,j}, \quad (2)$$

де i = 1, 2,…n; j = 1, 2, …m.

Величина об'єму під ламаною площиною буде являтися комплексною оцінкою якості об'єкту кваліметрії з часом. Таку методику можна застосовувати для багатокритеріального оцінювання якості об'єктів кваліметрії різної природи.

Список використаних джерел

1. Ginevičius R., Trishch H. Petraškevičius V. "Quantitative assessment of quality management systems' processes". Economic Research-Ekonomska Istraživanja. 2015. №. 28:1, P. 1096-1110.

2. Cherniak O., Trishch R., Kim N., Ratajczak S. Quantitative assessment of working conditions in the workplace. Engineering Management in Production and Services. 2020. № 12(2). P. 99-106.

3. Trisch R., Gorbenko E., Dotsenko N., Kim N., Kiporenko A. Development of qualimetric approaches to the processes of quality management system at enterprises ac-cording to international standards of the ISO 9000 series. Eastern-European Journal of Enterprise Technologies. 2016. № 4/3 (82). P. 18-24.

ЗАСТОСУВАННЯ ВІДНОШЕННЯ НЕЧІТКОЇ ПЕРЕВАГИ ПРИ ПОРІВНЯННІ СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ

Босенко Д.В., Яремчук Н.А., Шведова В.В.
Науковий керівник – професор, к.т.н., Яремчук Н.А.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, м. Київ, проспект Перемоги, 37, кафедра інформаційно-вимірювальних технологій, тел. (044) 204-98-97
qwertyzs@bigmir.net, shvedova_viktoiya@ukr.net, yaremchukna@i.ua

The paper proposes the application of the relation of fuzzy advantage when comparing distance learning systems for quality using a linguistic evaluation scale and fuzzy expert evaluations that characterize the degree of belonging of system quality indicators to certain gradations or classes of equivalence of the linguistic scale.

На сьогоднішні день все більшого поширення набуває дистанційне навчання, і невід'ємним його елементом технічного забезпечення є система дистанційного навчання.

Вибір найкращої для реалізації поставлених завдань системи дистанційного навчання є процедурою не тривіальною і часто залежить від: а) якщо експерта, який приймає рішення, один - його досвіду, кваліфікації і ряду суб'єктивних чинників; б) якщо експертів декілька, що є суттєвою перевагою – від їх консолідованої позиції, або умовно кажучи «вирішального алгоритму прийняття рішення», який теж може бути недостатньо обґрунтованим.

Тому в публікації запропоновано застосувати підхід, який дозволяє проранжувати декілька варіантів систем дистанційного навчання із застосуванням експертного оцінювання та поєднання отриманих оцінок експертів за алгоритмом нечіткого оцінювання.

На експертизу подано декілька проектів систем дистанційного навчання. Експертизу проводять експерти за шкалою оцінок:

$$Y = (Y1, Y2, Y3),$$

де $Y1$ - «повністю відповідає вимогам», $Y2$ - «відповідає більшості вимог», $Y3$ - «відповідає меншій частині вимог».

Узагальнені нечіткі оцінки групи експертів характеризують ступінь приналежності до наведених вище категорій шкали, наприклад $Y1|0,7$; $Y2|0,3$; $Y3|0$. Для вибору найкращого проекту запропоновано використати відношення нечіткої переваги [1].

Між градаціями лінгвістичної шкали обрано чіткий лінійний порядок S, тобто:

	Y1	Y2	Y3
Y1	1	1	1
Y2	0	1	1
Y3	0	0	1

За оцінками групи експертів визначається наближеність оцінки якості проекту до градацій лінгвістичної шкали.

Наприклад, для трьох проектів $X1$, $X2$, $X3$ нечітке відношення $F1(XY)$ становить:

	Y1	Y2	Y3
X1	0,5	0,4	0,1
X2	0,4	0,6	0
X3	0,45	0,55	0

Після нормалізації отримуємо $FN(XY)$:

	Y1	Y2	Y3
X1	0,83	0,67	0,15
X2	0,67	1,0	0
X3	0,75	0,93	0

Для отримання відношення нечіткої переваги формуємо композицію нечітких відношень R:

$$R = FNT * S * FN,$$

де FNT - трансформована матриця відношення FN.

	X1	X2	X3
X1	0,83	0,83	0,83
X2	0,67	1,0	0,83
X3	0,75	0,93	0,93

Відношення суворої переваги P (за формулою з [1]):

	X1	X2	X3
X1	0	1	1
X2	0	0	0
X3	0	1	0

З відношення переваги витікає, що $X1$ краща за $X2$ та $X3$, а $X3$ краща за $X2$, тобто системи дистанційного навчання за результатами експертного оцінювання та застосування лінгвістичної шкали можна проранжувати з точки зору якості в такому порядку: $X1$, $X3$, $X2$.

Література

1. Нечеткие множества и теория возможностей. Последние достижения: Пер. с англ./Под ред. Р. Р. Ягера. – М.: Радио и связь, 1986. - 408 с.

АЛФАВІТНИЙ ПЕРЕЛІК

ЗМІСТ

ДЛЯ НОТАТКІВ

ДЛЯ НОТАТКІВ

«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

МАТЕРІАЛИ 25-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

Відповідальний за випуск: А.В. Снігуров

Комп'ютерна верстка О.І. Ільїна, В.Г. Чепела

Матеріали збірника публікуються в авторському варіанті без редагування

Підп. до друку 09.04.2021 Формат 60x84 1/16 Спосіб друку - ризографія
Умов. друк. арк. 10,23 Тираж 99 прим.
Зам. № __-____. Ціна договірна

ХНУРЕ. Україна. 61166, Харків, просп. Науки, 14

Віддруковано в редакційно-видавничому відділі ХНУРЕ
61166, Харків, просп. Науки, 14

NURE