

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ



90
РОКІВ

ХАРКІВСЬКОМУ НАЦІОНАЛЬНОМУ
УНІВЕРСИТЕТУ РАДІОЕЛЕКТРОНІКИ

1930-2020

МАТЕРІАЛИ

XXIV МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У ХХІ СТОЛІТТІ



Том 4

Харків 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ
XXIV МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

**«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ
У XXI СТОЛІТТІ»**

7 – 9 квітня 2020 р.

Том 4

**КОНФЕРЕНЦІЯ
«ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ
ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ
ТЕХНОЛОГІЙ»**

Харків 2020

XXIV Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т. 4. – Харків: ХНУРЕ. 2020. – 188 с. – pdf 3,6 Mb.

В збірник включені матеріали
XXIV Міжнародного молодіжного форуму
«Радіоелектроніка та молодь у XXI столітті»

Видання підготовлено факультетом інфокомунікацій
Харківського національного університету радіоелектроніки

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

E-mail: mref21@nure.ua

© Харківський національний університет
радіоелектроніки (ХНУРЕ), 2020

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
Сергієнко М.П.	к.т.н., зав. каф. МТЕ
Захаров І.П.	д.т.н., проф. каф. МТЕ
Павленко Ю.Ф.	д.т.н., проф. ННЦ «Інститут метрології»
Несжмаков П.І.	д.т.н., генеральний директор ННЦ «Інститут метрології»

ПРОБЛЕМИ ІНФОКОМУНІКАЦІЙ

КРИТЕРІЇ ОЦІНКИ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

Чурсанов М.О.

Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20)

e-mail: mykyta.chursanov@nure.ua факс (057) 702-13-20

It is shown that one of the rather simple and universal criteria for evaluating EMC is the protective ratio. Its disadvantages are that it does not take into account the degree of damage caused by interference with a particular frequency-time and statistical structure. A more accurate criterion is the convolution of the signal and interference spectra, which can be obtained if the analytical dependence of the power spectral density level on the frequency for the signal, interference, and noise is known. In practice, this relationship is often unknown. In conditions of such uncertainty, it is permissible to use the criterion of the ratio of the signal power to the sum of the interference and noise powers

При виборі критерію стану електромагнітної сумісності (ЕМС) виникають дві основні задачі:

- як зв'язати і як співвіднести параметри завади з параметрами корисного сигналу і шуму в смузі прийому цього сигналу з тим, щоб можна було судити про ступінь впливу завади на якість роботи радіоелектронного засобу (РЕЗ);
- як вибрати рівень відліку для оцінки впливу завади.

Складність вирішення цих завдань пов'язана з тим, що в багатьох системах значення корисних сигналів, шумів, а також завад є випадковими, а часто і нестаціонарними процесами з невідомими поточними параметрами [1-3]. Спектри частот корисних сигналів і завад зазвичай різні, з різним ступенем перекриття.

Одним з досить простих і універсальних методів оцінки стану ЕМС є використання захисного відношення, допустимого відношення сигнал / завада, при якому якість зв'язку не погіршується:

$$A = \min(P_c / P_z)_{\text{дон}}, \quad (1)$$

Недоліками цього критерію є те, що при цьому не враховується ступінь збитку, що завдала завада з тією чи іншою частотно-часовою і статистичною структурою.

Є декілька методів оцінки зазначених частотних відмінностей. Так в [2] рекомендується використовувати відповідний коефіцієнт, що враховує вибірковість приймача:

$$N(\Delta f) = 10 \lg \left(\frac{\Delta F}{\Delta F_{\text{РПД}}} \right), \quad (2)$$

де ΔF – перекриття смуги випромінювання радіопередавача (РПД) і радіоприймача (РПМ) на рівні -30 дБ; $\Delta F_{РПД}$ - робоча смуга частот передавача, Гц.

Більш точним є врахування особливостей структури спектрів, що приводить до відношення згорток спектрів сигналу і завади:

$$h_{cn}^2 = \frac{D_c(F, \delta f)}{D_z(F, \delta f)}, \quad (3)$$

де F – середня частота спектра сигналу (завади); δf - різниця несійних частот корисного сигналу і завади; $D_c(F, \delta f), D_z(F, \delta f)$ - згортки спектрів корисного сигналу з частотною смугою приймача та завади відповідно.

Кількість завад може бути декілька, а також з урахуванням наявності теплових шумів вираз (3) перетвориться до вигляду:

$$h_{\Sigma}^2 = \frac{D_C(F, \delta f)}{\sum_i D_{zi}(F, \delta f) + D_{ш}}, \quad (4)$$

де $D_{ш}$ – спектральна густина потужності (СГП) шуму в приймальному пристрої.

Значення згорток можна отримати, якщо відома аналітична залежність рівня СГП від частоти. На практиці така залежність часто невідома. В умовах такої невизначеності допустимо використовувати показник відношення рівня сигналу до суми завад і шуму (ВСЗШ).

$$h_{ВСЗШ}^2 = P_C / (\sum_i P_{zi} + P_{ш}). \quad (5)$$

Діючи таким чином (5), можна помилитися в один або в інший бік. Однак, з огляду на те, що ентропія білого гаусівського шуму більше ентропії будь-якого відмінного від шуму сигналу можна стверджувати, що розрахункове значення виявиться трохи менше реального. Таке зміщення, призведе до декілька завищених показників, тобто реальна обстановка виявиться дещо кращою.

Список літератури:

1. 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.
2. Бородин 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.

ОПТИМИЗАЦИОННАЯ МОДЕЛЬ ДЛЯ ПЛАНИРОВАНИЯ СЕТЕЙ 5-ГО ПОКОЛЕНИЯ

Бондаренко О.С.

Научный руководитель – д.т.н., проф. Агеев Д.В.

Харьковский национальный университет радиоэлектроники
(61166, г. Харьков, пр. Науки, 14, каф. ИКИ имени В.В. Поповского,
тел. (057) 702-55-92)

E-mail: oleg.kh.bondarenko@gmail.com, тел. (050) 911-51-02

The transition to 5th generation communication standards is not an instantaneous process. It requires careful preparation and preliminary planning. It is necessary to update both the data transmission network and the subscriber radio access network, and since the transition process will be carried out within the network serving subscribers, it is necessary to develop an approach allowing to make network resource updates invisible for customers and with minimal costs for mobile operators.

В этой статье рассматривается модель оптимизации планирования мобильных сетей 5-го поколения. Модель учитывает основные физические, радио-электрические параметры и параметры планирования.

В конечном итоге модель представляется как смешанная целочисленная задача линейного программирования. Основой модели стали исследования в отношении проектирования сетей WiMAX [1].

В связи с развитием систем беспроводной связи 4-го поколения переход на технологии 5G неизбежен. Системы мобильных технологий 5-го поколения улучшают и дополняют системы прошлых поколений и обратно совместимы с ними.

Комитет 3GPP предложил использовать поэтапный подход и представил архитектуры NSA (Non-Standalone) и SA (Standalone) для развития технологий 5G.

Архитектура SA гарантирует, что каналы управления и передачи данных используют сети 5G, NSA же будет использовать существующую радиосвязь LTE и базовую сеть в качестве основы для радио-покрытия.

Мобильные операторы, которые заинтересованы в использовании 5G для увеличения пропускной способности своих сетей, могут развернуть 5G gNB наряду с LTE eNB. В этом случае узлы LTE eNB отвечают за мобильность клиента и управления сетью. Они работают на более низких частотах и имеют более широкую зону покрытия, чем узлы gNB, работающие на более высоких частотах. eNB становится ответственным за объединение традиционных несущих LTE и несущих 5G, обрабатываемых gNB. Эта опция также упоминается как конфигурация NSA [2].

Предложенная модель рассматривает возможность плавного перехода от LTE к 5G с использованием как раз подхода NSA. Ядром сети

является EPC, а стандарты 5G NR используются в качестве технологий для организации сети доступа.

Функция максимизации, которая включена в работу модели, позволит сосредоточиться конкретно на прибыли оператора мобильной связи. Такой подход сведет к минимуму затраты на обновление элементов сети и сделает переход к технологии 5-го поколения практически незаметным.

Одним из нововведений 5G является возможность подключения одного абонента к нескольким БС одновременно [3]. Пока модель не детализирует структуру клетки и не делит ее на микро- и пикосоты, это задача дальнейших исследований. На данный момент она учитывает возможность подключения абонента только к нескольким базовым станциям.

Оценка эффективности и правильности предложенной модели оптимизации проводилась на основе исходных данных, которые были сгенерированы случайным образом. Эксперимент проводился много раз с использованием разного количества сетевых узлов 5G.

Анализ результатов показывает эффективность модели с практической точки зрения, рис. 1.

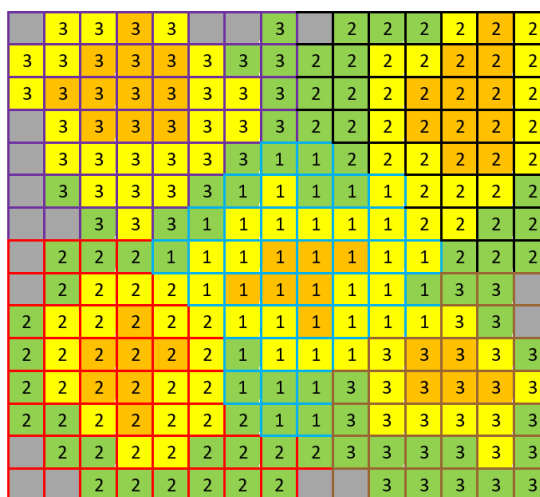


Рисунок 1 – Смоделированный участок сети 5G

Используя предложенную модель, можно получить набор переменных, необходимых для построения оптимизированной и сбалансированной сети.

Список источников:

1. Zhang Y. WiMAX Network Planning and Optimization / Y. Zhang / Auerbach Publications, Boston, MA, USA. - 2009 – 451p.
2. Prasad R. 5G: 2020 and beyond / R. Prasad / Aalborg: River Publishers. - 2015.
3. Sauter M. From gsm to lte-advanced pro and 5g / M. Sauter / Wiley. - 2017.

МЕТОД РАСПРЕДЕЛЕНИЯ ЧАСТОТНО-ВРЕМЕННОГО РЕСУРСА В КОГНИТИВНОЙ РАДИОСЕТИ, ОСНОВАННЫЙ НА АППАРАТЕ НЕЧЕТКОЙ ЛОГИКИ

Муляр Б.П.

Научный руководитель – д.т.н., проф. Коляденко Ю.Ю.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. Инфокоммуникационной инженерии
им. В.В. Поповского, тел. (057) 702-13-20)

e-mail: bohdan.muliar@nure.ua

Algorithm for the distribution of the time-frequency resource in a cognitive radio network.

An algorithm for the distribution of the time-frequency resource in the cognitive radio network is proposed. A distinctive feature of the developed algorithm is the use of both a parameter of the proportional fair distribution of physical resources PF and SINR. In addition, the decision in this algorithm is based on the mathematical apparatus of fuzzy logic. This algorithm is applicable at the stage of network operation in the presence of a large number of subscriber stations and centralized frequency management by the base station.

Концепция когнитивного радио может быть охарактеризована как радио с изучением возможностей. Свойство когнитивности подразумевает способность радиосистемы решать следующие задачи: переход от одного стандарта к другому; использование нескольких стандартов; перестройку частоты; возможность участия в динамическом распределении спектра; возможность к вторичному использованию спектра; динамическую оптимизацию емкости; регулировку антенн; реконфигурацию транспортной сети.

Применение нечеткой логики характерно для ситуаций, когда отсутствует не только детерминистская интерпретация решаемой задачи, но и стохастические вероятные методы не удастся применить в силу отсутствия данных о каких-либо распределениях.

Формальный аппарат нечеткой логики включает в себя определения: а) функции принадлежности (ФП), б) лингвистической переменной (ЛП), в) логических операторов MINIMUM, MAXIMUM, г) нечеткого правила «Если...То...» [3]. Нечеткое множество A задается упорядоченной парой: $A = \{(x, \mu_A(x)) | x \in X\}$, где x есть порождающий элемент, а $\mu_A(x)$ есть мера принадлежности к множеству A [3]. Функция принадлежности $\mu_A(x)$ принимает значения на отрезке $[0,1]$, $\mu_A : X \rightarrow [0,1]$, она является выпуклой, непрерывной и нормированной на единицу функцией. В общем случае ФП может иметь и симметричную, и асимметричную форму, поскольку условие выпуклости предопределяет наличие только одного «максимума».

«Компактное» нечетко-логическое описание физических параметров, имитирующее способность человека обозначать словами составные понятия, основывается на понятии лингвистической переменной (ЛП) [1]. Лингвистическую переменную T (также называемую терм-множеством) задают на области определения X как пары множеств $T = \{T^1, T^2, \dots, T^K\}$ и $\mu(x) = \{\mu^1(x), \mu^2(x), \dots, \mu^K(x)\}$, где $k = 1, \dots, K$ и $T^k \rightarrow \mu^k(x)$, т.е. каждый терм T^k для ЛП T имеет нечеткое имя и характеризуется своей ФП $\mu^k(x)$. Принципиально число термов ЛП не ограничено, но на практике оно редко превышает 5...6 [1], иначе возможное число нечетких правил «Если...То...» будет слишком большим. Таким образом, один и тот же физический параметр может быть охарактеризован сразу целым семейством ФП. Выбор конкретного профиля ФП осуществляется на основе экспертных знаний и последующей корректировки в процессе отладки системы [2].

Базовые логические операции в нечеткой логике могут быть определены различными способами (в рамках концепций Т-норм и Т-конорм) [2], но наиболее часто из них используются операторы MIN и MAX. Для двух произвольных множеств «1» и «2», заданных на x , где $x \in X$, и описываемых двумя функциями принадлежности (ФП) $\mu_1(x)$ и $\mu_2(x)$, эти операторы могут быть заданы так:

$$\begin{aligned} MIN\{\mu_1(x), \mu_2(x)\} &= \mu_1(x) \wedge \mu_2(x) = MINIMUM\{\mu_1(x), \mu_2(x)\}, \\ MAX\{\mu_1(x), \mu_2(x)\} &= \mu_1(x) \vee \mu_2(x) = MAXIMUM\{\mu_1(x), \mu_2(x)\}, \end{aligned} \quad (2)$$

где $\vee$ - дизъюнкция, $\wedge$ - конъюнкция.

Для практической реализации такого ограничителя следует перебрать все возможные значения x и для каждой пары значений $\mu_1(x)$ и $\mu_2(x)$ выбрать, соответственно, наименьшее или наибольшее значения сигналов из числа подаваемых на входы. В общем случае для выполнения операций MIN и MAX следует проводить аналоговые операции с непрерывными ФП, но на практике обычно применяют дискретные операции, выполняя их для достаточно большого числа градаций по x и μ [3]. С помощью символов логических операций $\wedge$ и $\vee$, а также символов $\mu(x)$ различных ФП могут быть записаны логические термы и проведены логические вычисления подобно тому, как это делается для традиционных двоичных вычислений с булевыми операторами и символами двоичных переменных.

Список использованных источников:

1. Tafazolli, R. (ed) (2006): Technologies for the Wireless Future, vol. 2, Wireless World Research Forum, (WWRF), John Wiley & Sons, Chichester, England.
2. Burns P. SDR For 3G. – Boston, Artech House, 2003 – 279 p.
3. Haykin S. Cognitiveradio: brain-empowereswirelesscommunications, IEEE JournalSelectedAreasinCommunication, vol. 23, no. 2, February 2005.

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА СТАНДАРТУ WI-FI 802.11AX

Греков І.

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)

A study was conducted of innovations in the new Wi-Fi standard 802.11ax, and a comparison was made of the main features and technologies with previous Wi-Fi standards 802.11n and 802.11ac. Practical application was carried out on terminal devices that support this standard in order to record the performance of the new standard and indicators of connection speed.

Новий стандарт Wi-Fi 802.11ax - наступний крок безперервних інновацій у безпроводових мережах. Його засновано на сильних сторонах 802.11ac, при цьому додаючи стабільність, гнучкість і масштабованість. Також, на відміну від 802.11ac, 802.11ax є двухдіапазонною технологією, що дає переваги в дальності зв'язку.

IEEE 802.11ax дозволяє точкам доступу забезпечувати підключенням до мережі більшу кількість пристроїв. Користуватися Wi-Fi в місцях великого скупчення людей стане зручніше. Це також забезпечує більшу продуктивність для таких функцій, як відео з роздільною здатністю 4K і 8K або реалізація бездротових офісів та Інтернет речей (IoT).

У новому стандарті 802.11ax підтримується модуляція QAM-1024. У 1024-QAM кожен символ містить 10 біт даних - проти 8 біт у 256QAM та 6 біт у 64-QAM. Таким чином, ємність пакета збільшилася на 25%. В результаті, теоретична швидкість передачі одного потоку даних в каналі шириною 80 МГц зросла до 600 Мбіт/с, що на 39% більше аналогічного параметра у Wi-Fi 5 (433 Мбіт/с) [1].

У стандарті 802.11ax з'явиться нова для Wi-Fi технологія мультиплексування великої кількості абонентів в загальній смузі пропускання: Orthogonal Frequency Division Multiple Access (OFDMA). OFDMA у 802.11ax дозволяє додатково "нарізати" стандартні канали шириною 20, 40, 80 і 160 МГц на більш дрібні. Таким чином, відбувається поділ каналів на більш дрібні підканали з визначеною кількістю піднесучих [2].

У завантажених середовищах багато користувачів неефективно використовують виділений канал, новий для Wi-Fi механізм OFDMA обслуговує їх одночасно з меншим, але виділеним спеціально для користувача підканалом, що покращує середню пропускну здатність для кожного окремого користувача.

Щоб ефективніше використовувати спектр, частотний канал в стандарті 802.11ax розділяється на піднесучі шириною близько 78 кГц [2]. У попередніх стандартах ширина спектра між піднесучими становила

312.5 кГц. Таким чином, канал з мінімальною шириною 20 МГц містить 256 піднесучих замість 64, як у 802.11ac.

У Wi-Fi 6 збільшений захисний інтервал (Guard Interval, GI) між символами, що дозволяє зменшити міжсимвольну інтерференцію. Таким чином, ефективність передачі виросла більш, ніж на 5% в порівнянні з 802.11ac.

Технологія явного формування променя до клієнта (explicit beamforming) вирішує ряд питань, пов'язаних із завмиранням і перевідбиттям сигналів та з їх не синфазністю. Приходячи в різних фазах, сигнал втрачає потужність, а це сильно впливає на дальність і швидкість передачі даних. Explicit beamforming вимагає від клієнта повернення діаграми спрямованості.

У Wi-Fi 6 закладено механізм маркування пакетів в частотних каналах, які використовуються різними пристроями – BSS coloring. Якщо декілька точок доступу працюють в одному і тому ж каналі, вони можуть передавати дані з унікальним "кольоровим" ідентифікатором і встановлювати паралельні бездротові підключення, не створюючи один одному перешкод.

Wi-Fi 6 зможе забезпечити MU-MIMO Downlink/Uplink, тобто одночасні передачу, і прийом. Це дозволить в чотири рази збільшити теоретичну максимальну пропускну здатність у порівнянні з Wi-Fi 5.

Порівнявши мережеві карти стандарту 802.11ac і вже сертифіковану мережеву карту стандарту 802.11ax можна зафіксувати, що максимальна можлива швидкість при використанні діапазону 2.4 ГГц зросла на 0,67 Гбіт/с.

За наявності адаптера і роутера з підтримкою Wi-Fi 6, операційна система Windows 10 в параметрі «Швидкість лінії» фіксує значення 1201 Мб/с на прийом і 907 Мб/с на передачу.

На смартфоні нового покоління з використанням стандарту Wi-Fi 6 показники швидкості вище на 20-25%, тобто близько 200 Мб/с.

Таким чином, застосування поновлених механізмів в комбінації, 802.11ax зможе вийти на фізичні швидкості - 10Gbps, гарантувати паралельне функціонування значної кількості абонентського обладнання і користуватися усім доступним «неліцензованим» діапазоном частот. Маючи такий рівень швидкості, стандарт зможе стати вагомим конкурентом для майбутніх мобільних мереж 5G.

Перелік джерел:

1. А.Г. Кірьянов, А.И. Ляхов, Д.А. Міхлина, Е.М. Хоров, И.А. Щолкіна. Проблеми створення IEEE 802.11ax — нового покоління мереж Wi-Fi. Інформаційні процеси. 2016, стр. 3.
2. S. Kittipiyakul and T. Javidi, “A Fresh Look at Optimal Subcarrier Allocation in OFDMA Systems”, UW Technical Report, University of Washington, 200

РОЗШИРЕННЯ МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ТЕРИТОРІЇ ЗАПОРІЗЬКОЇ ТЕС

Пушкарьов В. В.

Науковий керівник: - к.т.н., доц. Бондарь Д. В., 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

Today, there is a great need for extended mobile coverage in as many people's living or working areas as possible. This need is especially evident in industrial areas and large enterprises. The problem of low quality of mobile communication at such sites is connected with the complexity of the works on the design and placement of equipment in the industrial buildings of enterprises, the complexity of signal propagation through a large number of complex industrial metal structures in reinforced concrete structures. The purpose and task of the project is to develop project documentation for the construction of mobile base stations in the territory of TPP.

На сьогоднішній день існує велика потреба у розширенні зони покриття мобільним зв'язком якомога більшої території, де живуть або працюють люди. Особливо ця потреба проявляється на територіях промислових зон та великих підприємствах. Проблема низької якості мобільного зв'язку на подібних об'єктах пов'язана із складністю робіт по проектуванню та розміщенню обладнання на промислових спорудах підприємств, складністю розповсюдження сигналу через велику кількість складних промислових металевих та залізобетонних конструкцій. Метою та завданням проекту є розробка проектної документації для побудови базових станцій мобільного зв'язку на території ТЕС. Вибрати найбільш актуальне обладнання та способи його встановлення на спорудах підприємства.

Для встановлення на об'єктах ТЕС було вибрано обладнання мобільного зв'язку китайської фірми HUAWEI. Дане обладнання добре себе зарекомендувало на тисячах побудованих базових станцій мобільного зв'язку по всій території України. Головні переваги в порівнянні з раніше використованим та демонтуємим у теперішній час обладнанням фірми SIEMENS є:

- компактність, за рахунок модульної побудови обладнання HUAWEI;
- можливість використання стандартів UMTS та LTE;
- збільшення КПД базової станції у зв'язку з довжиною фідера від радіомодуля до антени в декілька метрів.

Встановлення обладнання відбувається на існуючих конструкціях споруд на території ТЕС. Секторні антени, що будуть встановлені на базових станціях вибрано від фірм-виробників, таких як Kathrein, APX, MOBI. Антени даних виробників відповідають виставленим вимогам. Зв'язок базових станцій між собою виконується через обладнання ВОЛЗ, а також в основному за допомогою релейного зв'язку з використанням

релейних станцій фірми OmniBAS. Секторні антени та радіомодулі кріпляться на споруди за допомогою спеціалізованих металоконструкцій, таких як трубо стійки та розвантажувальні рами. Системні модулі HUAWEI BBU3910 та блоки електроживлення розташовуються у доступних для обслуговування місцях в середині будівель. Підключення радіомодулів RRU від системного модуля відбувається за допомогою оптичного кабеля та кабеля живлення. Передача радіосигналу від радіомодулів до секторних антен виконується через фідер 1/2".

Приклад радіотехнічної схеми та план встановлення обладнання в будівлі берегової насосної станції №1 представлено на рис. 1.

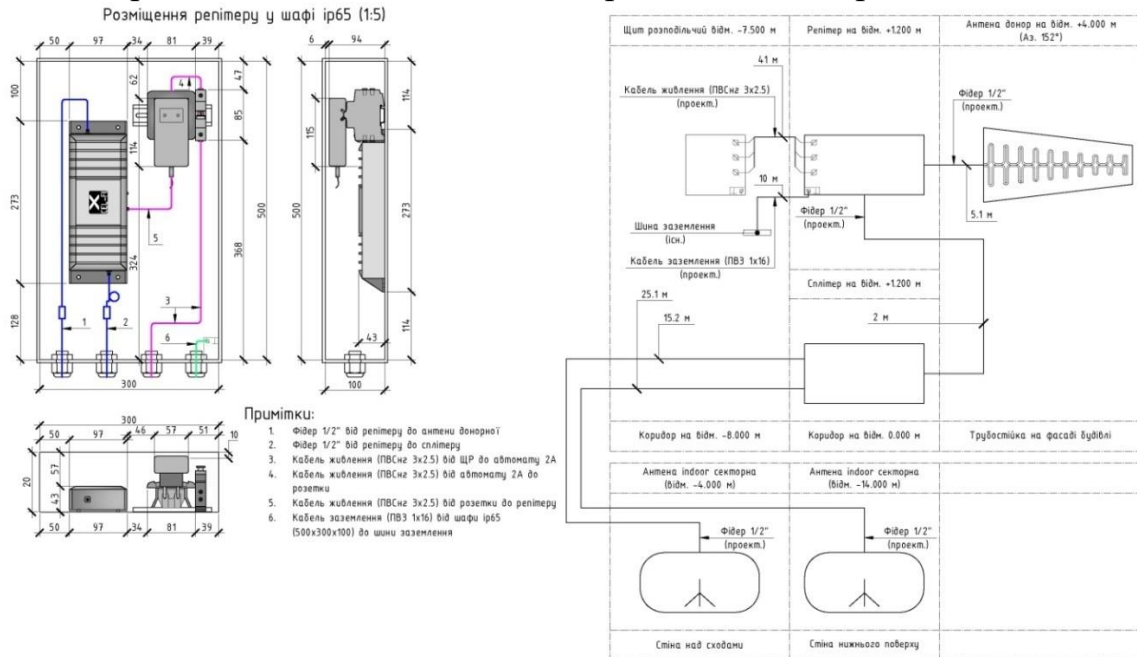


Рисунок 1. Встановлення обладнання

Для забезпечення розповсюдження сигналу мобільного зв'язку в середині невеликих будівель раціонально використовувати антенні репітери. Вони складаються з антени донора, що отримує сигнал ззовні будівлі, пристрою репітера та блоку живлення. Сигнал від антени донора до репітера і від нього до індор антени передається через фідер 1/2".

Розроблена мережа базових станцій стандартів GSM-900, DCS-1800, UMTS-2100 буде встановлена та підключена в ефір у найближчі декілька місяців.

Перелік джерел

1. Релейні станції [Електроний ресурс]: <http://www.intracom-svyaz.ru/products/omnibas.htm>
2. Базові станції HUAWEI [Електроний ресурс]: <https://e.huawei.com/en/material/wireless/elteindustry>

ВПРОВАДЖЕННЯ ХМАРНОЇ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ НА ПРИКЛАДІ КОНТЕЙНОРНОЇ ПРОГРАМИ OPENSIFT

Ходаківський М.М.

Науковий керівник: - к.т.н., доц. Бондарь Д. В., 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 продукту, 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 зберігає значні недоліки, перш за все якщо в додатку вийде з ладу тий чи інший модуль працездатність всього додатка стане під загрозою, що є критичним аспектом якщо дивитись з позиції бізнесу, також як недолік варто віднести досить важкий процес відлатки та оновлення додатку.

Мікросервісна архітектура – це архітектура сьогодення львина доля всіх найпопулярніших ресурсів, або проектів використовує саме цю систему побудову додатків. Принцип мікросервісної архітектури в тому, що весь додаток розбивається на сервіси, наприклад додаток має авторизацію, в сервісній архітектурі його можливо зробити окремим сервісом. Переваги такого принципу є стабільність додатку, якщо один сервіс вийде з ладу його буде легко полагодити, також легко оновлювати версію додатку. Як недолік можна віднести досить важке налаштування і в цілому міжсервісна взаємодія.

Openshift потрібен для створення мікросервісної архітектури, в основі кожного сервіса лежить контейнер – це ізольована операційна система в середині якої є певна програма, тобто це і є сервіс. На рис 1. Зображена основна концепція побудови мікросервісної архітектури на основі openshift. Основним елементом системи є “MASTER” так звана система яка контролює всі процеси що проходять в нашій системі, базовим елементом виступає “Node” – це фізичний комп’ютер в середині якої є “Pod” – це область в якому можуть зберігатися наші ізольовані контейнери з нашими сервісами, за допомогою openshift ми маємо змогу пов’язувати певні контейнери один з одним, таким чином створювати бізнес логіку та міжсервісну архітектуру також за допомогою openshift можливо зручно дублювати наші сервіси для більш відмовостійкості.

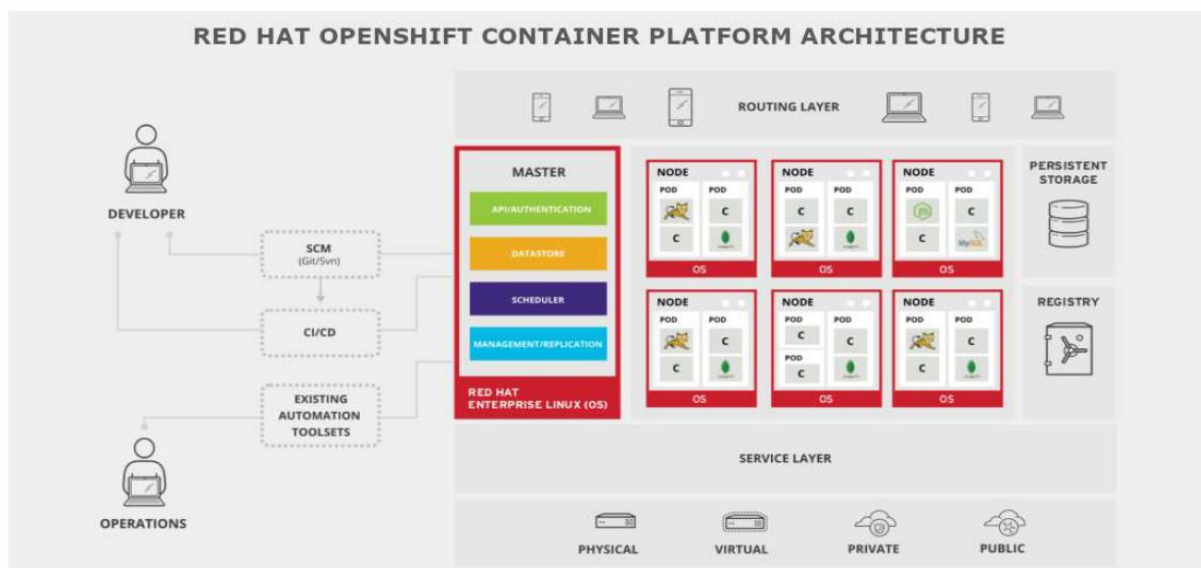


Рисунок1. Концепція мікросервісної архітектури Openshift

Процес роботи буде виглядати таким чином, розробник працює над певним сервісом, він робить так званий “patch-set” тобто зміну в своєму коді, код попадає до блоку ci/cd що на малюнку там він компілюється, тестується, і на виході він попадає в блок “Registry” це є кінцевий результат “артефакт” тобто ми маємо snap-shot версію сервіса, далі в ручному, або в автоматичному режимі потрібно оновити окремий сервіс вказавши йому в налаштуваннях шлях до “артефакта” таким чином можна дуже зручно та безпечно поступово оновлювати та розробляти додаток, це дуже зручно так як певна група розробників займаються тільки окремим сервісом.

Перелік джерел

1. Книга “Openshift in action” [Електронний ресурс]: <https://www.manning.com/books/openshift-in-action>
2. Ознайомлення з Openshift [Електронний ресурс]: <https://habr.com/ru/article/454624/>

ВИКОРИСТАННЯ ХМАРНИХ ОБЧИСЛЕНЬ ДЛЯ ОПРАЦЮВАННЯ СИГНАЛІВ

Галушка А.В.

Науковий керівник – к.т.н., доц. Костромицький А.І.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно-мережної інженерії,
тел. (057) 702-14-29)

e-mail: andreygshadow@gmail.com, тел. (099) 65-05-639

Use of signals delivery in various areas is presented. A new way to the organization of the calculation process is shown. Benefits of cloud computation of single- and multi-measurement signals in diverse areas of transformation is given. Proposed way for more efficient systems of data computation. Explained possibility of accomplishing signals efficiency in the process of simultaneous usage low-wave transformation and cloud computation technologies.

На сучасному етапі розвитку систем опрацювання даних широко застосовуються методи, які використовують різні області подання сигналів. Саме від них істотно залежать ефективність аналізу і оброблення самих сигналів, покращання ряду характеристик і отримання детальнішої інформації про сигнал. До таких областей належать: часова область, частотна область – Фур'є, область косинусного та синусного представлень, короткочасова область Фур'є (за Габором), область гільбертового представлення та ін. На їх основі будуються алгоритми кореляційного аналізу, фільтрації, кодування сигналів та зображень, а також алгоритми зворотних відтворень.

Характеристики низки сучасних систем суттєво погіршуються у випадку перетворення і опрацювання ними неперіодичних сигналів – як швидкоплинних, перехідних, так і повільних з високим вмістом різного типу завад. Крім того, використання існуючих методів подання стримується складністю математичних моделей та алгоритмів їх реалізації, зменшенням рівня чутливості інформативних параметрів, швидкодії та високою вартістю розробок. Радикальним шляхом підвищення ефективності і таких систем є розроблення нових методів подання та технологій для їх реалізації, які б повніше інтерпретували вхідні сигнали і базувалися на одночасній локалізації сигналів у різних областях. Моделі перетворень, які створюватимуться на їх основі, не повинні бути складними і мають враховувати особливості архітектури обчислювальних засобів. Тому на сучасному етапі розвитку теорії швидких алгоритмів перетворення і оброблення сигналів спостерігається велике зацікавлення різними новими типами подання інформації, методами її перетворень, технологіями реалізації, які ґрунтуються на їх основі. Зокрема як альтернативу до дискретного перетворення Фур'є використовують короткочасове перетворення Фур'є за Габором, різні спеціальні випадки швидкого

перетворення Фур'є, різні варіанти косинусного та синусного перетворень, алгоритми швидкого перетворення Хартлі та ін. Є підходи до побудови зазначених засобів опрацювання сигналів, які зменшують кількість обчислень, однак потребують більшої апіорної інформації про вхідні сигнали і значного збільшення кількості алгоритмів і часових затрат на апаратурну реалізацію, особливо за наявності широкого спектра завад.

Суттєвим недоліком відомих методів подання сигналів є те, що вони локалізують їх лише в одній із областей, що приводить, з одного боку, до їх надлишковості, а з іншого – до втрати інформативних даних про сигнал. Такий підхід ускладнює математичні моделі, структуру і реалізацію алгоритмів перетворення та оброблення сигналів на їх основі. Отже, існує наукова проблема, яка полягає в необхідності розроблення нових підходів до подання сигналів, створення на їх основі математичних моделей та алгоритмів перетворення і ефективних технологій цифрового оброблення даних, які можна практично застосовувати для розв'язання широкого кола прикладних задач.

Розроблення теорії і технології подання та опрацювання сигналів у часо-частотній області має особливе значення для розвитку науки і виробництва в Україні. Прикладом може бути розв'язання проблеми цифрового фільтрування та компресії зображень та аудіосигналів, які є обов'язковими елементами усіх існуючих систем збереження та передавання баз даних, зображень і аудіосигналів. Використання часо-частотного перетворення відкриває широкі можливості для фільтрування сигналів, нанесення цифрових підписів, захисту інформації у фінансовій та банківській справі. Однак необхідно зазначити, що ефективність подання і опрацювання неперіодичних, швидкоплинних, широкосмугових сигналів, зокрема сигналів зображень та відео у часо-частотній, вейвлет області вимагає великих обчислювальних затрат, а також швидкодії обчислень. Точність їх апроксимації у вейвлет області залежить від оптимального вибору базових функцій і кількості рівнів перетворення. З огляду на це використання хмарних обчислень для перетворення і опрацювання таких сигналів у реальному часі є особливо бажаним та своєчасним. Забезпечення ефективного фільтрування та компресії сигналів, представлених у вейвлет області є цілком реальною і вирішуваною задачею. Отже, комплексний підхід до розв'язання таких задач, а саме представлення та опрацювання неперіодичних, широкосмугових сигналів у часо-частотній області, з одного боку, і використання для їх реалізації сучасних хмарних технологій з іншого, може забезпечити найефективніше розв'язання задач, поставлених споживачем.

На основі наведеного аналізу показано новий підхід до організації обчислювального процесу, що передбачає розподілену віддалену обробку та зберігання даних, які відбуваються в процесі об'ємних наукових та прикладних досліджень у сучасних інформаційних системах.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КОМПЛЕКСА ПРОГРАММ ELK STACK

Лябах А.С. Хачиров Е.Ф.

Научный руководитель – доц., к.т.н. Токарь Л.А. Харьковский национальный университет радиоэлектроники (61166, Харьков, пр. Науки, 14, кафедра инфокоммуникационной инженерии им. В.В. Поповского, тел.

+380954176623, e-mail: artemliabakh@gmail.com

+380988345085, e-mail: ed.khachirov@gmail.com

The complex of ELK Stack software products has been analyzed. It is shown that this is an excellent solution for fast troubleshooting in the code, and a very convenient tool for developers, as well as for creating or implementing individual elements in large projects. It has been brought to the attention of ELK functionality that allows it to be used as a central repository of logs, an event aggregator with convenient navigation, as well as an analytical system with a machine learning algorithm.

Деятельность любой организации, предоставляющей определенные ресурсы, направлена на получение дохода. В связи с чем, при предоставлении любой услуги, например видео, аудио, хостинга, IP-телефонии, необходимо рассчитать их стоимость, а также провести расчеты с конечными пользователями. Таким образом, устанавливается своя мера, их характеризующая ресурсы: время, мегабайты и т.д. Поэтому возникает вопрос биллинга, что и определяет актуальность данной работы.

Основная проблема заключается в том, что для биллинга не так уж много готовых инструментов. Кроме того, они все являются платными.

Одним из решений данного вопроса предложено использовать комплекс программ ELK Stack, который является бесплатным, отвечает широким потребностям, предоставляет удобную и гибкую статистику, которая необходима для работы.

ELK расширяется как elasticsearch, logstash и kibana. Ранее это были три самостоятельных продукта, но позже стали принадлежать одной компании и развиваться в одном направлении. Каждый из этих инструментов (с небольшими примечаниями) является полноценным независимым open source продуктом, а вместе они составляют мощное решение для широкого спектра задач сбора, хранения и анализа данных.

Logstash – это утилита для сборки, фильтрации и последующего перенаправления в конечное хранилище данных. Ее другое название fluentd – logstash, но данная утилита решает ту же самую задачу и написана на ruby и более совместима с elasticsearch.

Elasticsearch – это решение для полнотекстового поиска, построенное поверх Apache Lucene, но с дополнительными удобствами в виде легкого масштабирования, репликации и прочих преимуществ, которые сделали elasticsearch очень удобным и хорошим решением для высоконагруженных проектов с большими объемами данных. Особенно привлекает в elasticsearch его простота и работоспособность сразу после установки. Конфигурация по-умолчанию работает для проектов средней и относительно высокой нагрузки. При этом вокруг ES сложилось отличное сообщество, которое всегда подскажет, как правильно настроить ваш ES-кластер для конкретной задачи.

Kibana, позволяет брать\искать данные по elasticsearch и строить множество интересных графиков. Это очень удобный интерфейс, позволяющий пользователю компании построить интерактивную панель для вывода аналитики того, что logstash отправил в elasticsearch.

ELK Stack позволяет проводить мониторинг большого количества данных, фильтровать их, и при необходимости производить быстрый поиск. Таким образом, это мощный инструмент, для сбора и фильтрации логов, что позволит использовать stack для биллинга во многих системах, а также значительно сократить расходы. Еще одним преимуществом является простота установки, однако для этого потребуются определенные навыки для настройки фильтров.

В результате адекватного выбора предложенного комплекса программ ELK Stack можно получить мощную CMS систему, которая способна обрабатывать огромное количество данных в секунду, предоставлять подробные отчеты, а также позволит сторонним разработчикам модифицировать систему.

Список источников:

1. Elastic Stack and Product Documentation [Электронный ресурс], Режим доступа: <https://www.elastic.co/guide/index.html>. - 2019.
2. Гольдштейн Б.С., Ехриель И.М., Перле Р.Д. Интеллектуальные сети. — М.: Радио и связь, 2000.

МОДЕЛЬ ДОСЛІДЖЕННЯ ОКРЕМИХ МЕТОДІВ КОНТРОЛЮ РЕСУРСІВ ДОСТУПУ ДО ПОСЛУГ MULTI PLAY

Волокітіна О.І.

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: lemur-97@mail.ru, факс (057) 702-13-20

New technologies spread in the world market and provide an opportunity to create united information society where the geographical boundaries lose its relevance as an economical factor. The work includes the program, developed using the Java programming language to illustrate the packet traffic movement in the network under investigation and to calculate its parameters. This research have shown that the method of using classes is more effective because the C-clients get the proper speed of Internet.

Основними факторами розвитку сучасної світової економіки виступають телекомунікаційні та інформаційні технології. Нові технології завойовують світовий ринок і дозволяють створити єдине інформаційне суспільство, де географічні кордони втрачають своє значення як економічний фактор.

Розглянемо два методи контролю параметрів доступу до послуг Multiplay: метод контролю параметрів доступу для абонентів, які розбиті на класи, і метод контролю параметрів доступу для абонентів згідно послуг. Що дало об'єднання абонентів за класами? Як змінилася кількість переданих пакетів у вузол доступу та смуга пропускання, і що конкретно викликало ці зміни. В результаті порівняння отримали підтвердження, що метод контролю параметрів доступу для абонентів, які розбиті на класи, кращий завдяки підвищенню швидкості абонентів, які використовують інтернет.

Вузол доступу обробляє сумарну кількість пакетів від усіх користувачів послуг Multiplay: телефонія, інтернет, відео. Кількість переданих пакетів від послуги телефонія і від послуги IPTV в обох розглянутих методах однакова. Різниця в кількості пакетів від послуги інтернет. В методі із класами кількість пакетів від послуги інтернет складається із двох частин. Перша залежить від швидкості передачі пакетів від класу В: абонентів, які використовують інтернет і телефонію, і вона співпадає із швидкістю передачі від послуги Інтернет в методі згідно послуг; Друга - від швидкості передачі від класу С: абонентів, які використовують телефонію, інтернет і відео, яка співпадає із швидкістю передачі пакетів від послуги IPTV, тобто більша, ніж в методі згідно послуг, яка дорівнює тільки швидкості інтернету. У підсумку у методі контролю параметрів доступу до послуг Multiplay для абонентів, які розбиті на класи передається: більша кількість пакетів від послуги інтернет

і в цілому загальна кількість пакетів, ніж у методі контролю параметрів доступу згідно послуг. Так і смуга пропускання більша, бо напряму залежить від середнього числа пакетів в секунду, ніж при методі, коли абоненти об'єднані згідно послуг.

За допомогою мови програмування Java розроблено програму математичної моделі із розрахунком вихідних показників вузла доступу для двох розглянутих методів, а також схему візуалізації руху трафіку для ресурсів доступу до послуг Multiplay. Проект виконано у програмному середовищі Eclipse. Користуючись перевагами ООП, наданими мовою Java, для кожного із складових елементів або процесів моделі створено клас, який описує структуру, принцип роботи та функціональність, необхідні для побудови конкретно даної моделі, уникаючи зайві деталі реалізації пристроїв. Для побудови мережі використано такі елементи, як програмний комутатор, сервер та кінцеві пристрої, до складу яких входять ПК, ноутбук та IP-телефон. Для кожного з них відповідно створені класи, - Switch, Server, Personal Computer, Laptop, Phone, в яких описано параметри та функції. На основній панелі класу WorkPanel розміщені усі комутатори мережі, з'єднані між собою за кільцевою топологією для демонстрації руху трафіку на магістральному рівні. Візуальне представлення симуляції трафіку продемонстровано на рис.1.

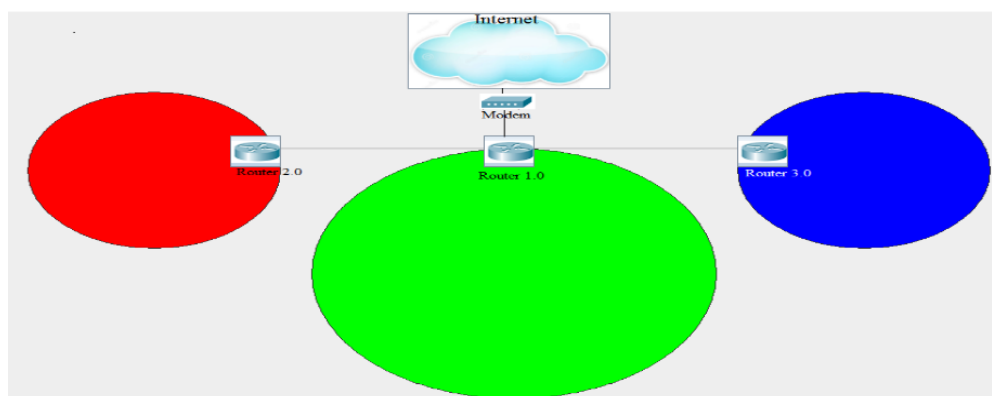


Рисунок 1 – Симуляція трафіку

ПЕРЕЛІК ПОСИЛАНЬ

1 Шилдт Г. Java 8. Полное руководство; 9-е изд.: Пер. с англ. – М.: ООО "И.Д. Вильямс", 2015. - 1376 с.

**МЕТРИКА ПАРАМЕТРІВ
ВИПРОМІНЮВАННЯ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ
ШИРОКОСМУГОВОГО ДОСТУПУ**

Мірось Ю.О., Сабурова С.О.

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: yurii.miros@nure.ua, факс (057) 702-13-20

The basic methods of measuring the frequency and bandwidth of radionuclide bandwidths of radio access systems (RAS), including wireless LAN equipment in the 2.4 GHz and 5 GHz frequency bands according to the technical requirements of the standards, are presented. Methodology for checking compliance of RAS characteristics with modern standards and radiation standards to ensure the electromagnetic compatibility of RAS and providing the necessary information for the needs of regulation of the use of the radio frequency resource of Ukraine.

Сучасне обладнання безпроводових мереж базується на міжнародних та європейських стандартах з телекомунікацій. Найбільше поширення в Україні отримали високошвидкісні стандарти безпроводових мереж IEEE 802.11a/b/g, IEEE 802.11n та IEEE 802.16, що вимагає використання у діяльності Українського державного центру радіочастот (УДЦР) національних стандартів України, згармонізованих з міжнародними та європейськими стандартами. Тому, актуальною є задача вивчення та практичного застосування відповідних національних стандартів, розроблених міжнародними організаціями, зокрема, Європейським інститутом стандартів телекомунікацій ETSI (European Telecommunications Standards Institute).

Метрика вимірювання центральної частоти радіоелектронного засобу (РЕЗ) широкосмугового радіодоступу без чітко виділеної несучої частоти можливо проводити як на антенному виході передавача, так і «з ефіру» на певній відстані від РЕЗ з використанням випробувальної антени, приєднаної до аналізатора спектра. При цьому використовується метод аналізатора радіочастотного спектра, суть якого полягає в розрахунку центральної частоти ($f_{\text{ц}}$) за результатами вимірювання ширини займаної смуги частот із значень її верхньої ($f_{\text{в}}$) та нижньої ($f_{\text{н}}$) частот за формулою $f_{\text{ц}} = (f_{\text{в}} + f_{\text{н}})/2$.

Допустиме відхилення частоти передавача згідно стандарту [1] складає $\pm 25 \times 10^{-6}$. Відповідно до вимог стандарту [2] фактичну центральну частоту носійного коливання для будь-якого заданого каналу, задекларовану виробником, треба підтримувати в межах $\pm 20 \times 10^{-6}$. Приклад результату метрики вимірювання центральної частоти випромінювання РЕЗ типу NanoBridge M2-G18 "Ubiquiti Network Inc.", що працює в режимі g з класом випромінювання 20M0G1Wображений на рис.1.

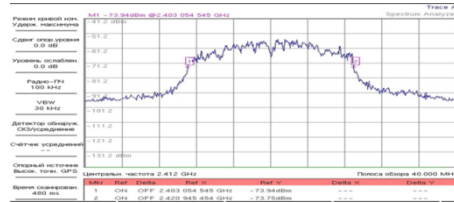
Частота, МГц		Відхилення частоти, 10 ⁻⁶											
За висновком	Виміряна	ETSI EN 300 328:2016	Виміряне										
2412	2412	±25	0										
Відповідає (так / ні) - так		Відповідає нормам (так / ні) - так											
		<table><tr><td>Маркер M1, МГц</td><td>2403,054545</td></tr><tr><td>Маркер M2, МГц</td><td>2420,945454</td></tr><tr><td>Частота згідно з висновком щодо ЕМС РЕЗ, МГц</td><td>2412,000000</td></tr><tr><td>Виміряна частота, МГц</td><td>2412,000000</td></tr><tr><td>Виміряне відхилення частоти, 10⁻⁶</td><td>0,00</td></tr></table>		Маркер M1, МГц	2403,054545	Маркер M2, МГц	2420,945454	Частота згідно з висновком щодо ЕМС РЕЗ, МГц	2412,000000	Виміряна частота, МГц	2412,000000	Виміряне відхилення частоти, 10⁻⁶	0,00
Маркер M1, МГц	2403,054545												
Маркер M2, МГц	2420,945454												
Частота згідно з висновком щодо ЕМС РЕЗ, МГц	2412,000000												
Виміряна частота, МГц	2412,000000												
Виміряне відхилення частоти, 10⁻⁶	0,00												

Рис.1. Метрика вимірювання центральної частоти

Рекомендовані параметри настроювання аналізатора спектра: в режимі g – роздільна здатність за смугою пропускання (RBW) 100 кГц, смуга пропускання відеофільтра (VBW) 30 кГц; в режимі b – RBW 100 кГц, VBW 100 кГц.

Метрика вимірювання ширини смуги частот радіовипромінювання РЕЗ широкосмугового радіодоступу здійснюється з використанням методу «Х дБ». Вимоги до ширини смуги та позасмуговим випромінюванням згідно стандартів [1] та [2] у вигляді спектральних масок випромінювання для обладнання радіодоступу діапазонів частот 2,4 ГГц та 5 ГГц зображені на рис. 2.

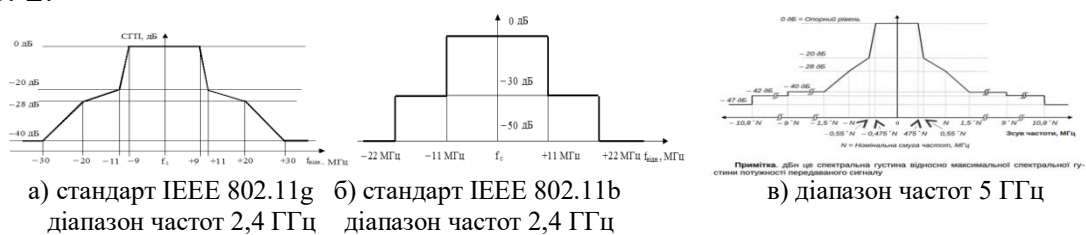


Рис. 2. Спектральні маски випромінювання

Висновки:

Розвиток сфери телекомунікацій безпосередньо пов'язаний з введенням в експлуатацію РЕЗ різноманітних радіотехнологій, систем та стандартів зв'язку. На даний час існує нагальна потреба у розробці методик перевірки відповідності характеристик РЕЗ сучасним стандартам та нормам випромінювання для забезпечення електромагнітної сумісності РЕЗ та надання необхідної інформації для потреб регулювання використання радіочастотного ресурсу України.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ETSI EN 300 328:2016, IDT (ДСТУ ETSI EN 300 328:2017 Електромагнітна сумісність і радіочастотний спектр. Системи з радіодоступом у діапазоні частот 2,4 ГГц. Загальні вимоги до радіоінтерфейсу).
2. ETSI EN 301 893:2017, IDT (ДСТУ ETSI EN 301 893:2017 Обладнання радіодоступу діапазону частот 5 ГГц. Загальні технічні вимоги та методи випробування).

БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ В СИСТЕМІ КОНТРОЛЮ ДОСТУПУ З ВИКОРИСТАННЯМ СЕНСОРНОЇ МЕРЕЖІ

Афанасьєв Ю.В.

Науковий керівник – д.т.н., проф. Лемешко О.В.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інфокомунікаційної інженерії
ім. В.В. Поповського, тел. (057) 702-13-20)
e-mail: testkivi204@gmail.com

Ensuring access control to facilities based on the use of telecommunication systems and networks is an urgent task. This problem is solved by finding effective ways to build access control systems. The paper studies the possibility of building an access control system based on one-factor and multi-factor authentication. A version of the hardware and software system implementation is proposed. For various system configuration options, the system availability time has been experimentally determined.

Аналіз публікацій з питань рішення задачі контролю доступу показує, що питання безпеки доступу до інформації є актуальним [1]. Існуючі методи автентифікації, такі як паролі, картки, різноманітні електронні ключі, не забезпечують в повній мірі захист від несанкціонованого доступу. Одним з ефективних методів забезпечення захисту інформації є застосування біометричних методів автентифікації.

За результатами дослідження питань реалізації технологій автентифікації визначено, що вартість апаратних засобів залежить від методу автентифікації, інформація про користувача зберігається в базі даних на сервері, що при певних умовах не забезпечує захист від доступу до неї. Удосконалення методів несанкціонованого доступу обумовлює розробку нових та удосконалення існуючих методів автентифікації. До них відносяться динамічні і статичні методи, методи багатокритеріального аналізу показників та інше [2].

В загальному випадку методи автентифікації повинні забезпечувати найменше значення частот помилкових спрацювань та відмов в обслугованні. Підвищення рівня безпеки в системах контролю доступу (СКД) можливе за рахунок застосування методу двофакторної автентифікації (two-factor authentication). Прикладами реалізації даного методу є способи автентифікації в соціальних мережах, банківській сфері де використовуються: SMS-автентифікація, одноразовий пароль, Google Authenticator та ін. [3]. Структура СКД залежить від наступних характеристик: кількості персоналу, для якого необхідно визначити заданий рівень доступу до певної інформації (об'єкту); просторових показників, які визначаються розмірами об'єкта, взаємному розташуванню окремих складових на місцевості; особливостями топології інформаційної

системи. Таким чином, зазначені системи представляють собою мережі, які поєднують в собі комплекс розподілених приладів автентифікації. Тому, такі мережі можна розглядати як сенсорні мережі.

В основу програмно-апаратної реалізації варіантів СКД покладено застосування наступних елементів: зчитувач відбитків пальців FPM10A; мікроконтролер ESP32 з інтегрованими Wi-Fi та Bluetooth контролерами та антенами; модуль RFID модуль RC522; мікроконтролер ESP8266; сервер одноплатний комп'ютер Raspberry Pi 3; Bluetooth-пристрої.

Розроблено алгоритм з автентифікацією по Bluetooth-пристрою. Він включає етап внесення даних користувача для автентифікації в базу даних та етап автентифікації користувача. В загальному випадку алгоритми роботи з автентифікацією по відбитку пальця та з використанням модуля RFID аналогічні. Загальними рисами реалізованих варіантів є наступне: необхідність наявності серверу, в якому зберігається база даних користувачів; використання мікроконтролеру ESP32 забезпечує реалізацію розглянутих методів; використання мікроконтролеру ESP8266 забезпечує реалізацію методів автентифікації без використання Bluetooth.

З метою визначення особливостей побудови мережі з використанням мікроконтролерів типу ESP32, в роботі проведено експериментальне дослідження часової характеристики мережі - часу готовності мережі. Розглянуто два варіанта налаштування мережі. Перший – один модуль ESP32 роздає свою WI-FI мережу а другий модуль підключається до неї за умови введення параметрів налаштування мережі вручну. Другий – один модуль ESP32 роздає свою WI-FI мережу, а другий модуль підключається до неї за умови передачі параметрів налаштування мережі автоматично по каналу WI-FI. В результаті аналізу отриманих даних визначено, що при налаштуванні мережі вручну, час підключення має більш стабільний характер і складає 1,35 сек. При автоматичному налаштуванні час готовності знаходиться в межах 1,3 – 44,3 сек.

ЛІТЕРАТУРА

1. Афанасьєв Ю.В. Шляхи забезпечення функціональної стійкості системи контролю та управління доступом до режимних об'єктів / Ю.В. Афанасьєв, Д.В. Сумцов // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 23-24 березня 2017 р.; Київський національний університет імені Тараса Шевченка. - К.: ВПЦ «Київський університет», 2017.- С. 8–13.
2. Кравченко Ю. В. Визначення проблематики теорії функціональної стійкості щодо застосування в комп'ютерних системах / Ю. В. Кравченко, С. В. Нікіфоров // Телекомунікаційні та інформаційні технології. – 2014. – № 1. – С. 12–18.
3. Кикина А.Л., Когельман Л.Г., Мишиев А.И. Вопросы безопасности беспроводных сенсорных сетей / Труды международной научно-технической конференции – Пенза, ПензГТУ, 2017, Вып. 25, с. 70.

АНАЛІЗ МЕТОДІВ ДОСЛІДЖЕННЯ ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ В SDN-МЕРЕЖАХ

Алексін В.В., Лемешко О.В.

Науковий керівник – д.т.н., проф. Лемешко О.В.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, кафедра інфокомунікаційної інженерії ім.
В.В. Поповського, тел. +38(095)8819735, e-mail: undershook@gmail.com)

The considered fail-safe routing methods have been researched and improved, both with and without balancing. The main thing in such networks is that routing protocols with an increased level of fault-tolerant solutions are used. As shown in practice, this technology is especially necessary for maintaining multiservice, as well as saving resources in some way. The use of special fail-safe routing protocols can increase the availability of routers acting as a gateway. And the use of a protection scheme FRR makes the network more resistant to overloads and more efficient in general.

Ускладнення в області телекомунікаційних технологій та інфраструктури призводять до того, що все більше вимог висуваються до параметрів якості обслуговування в системах та мережах. Ключову роль у забезпеченні заданих значень таких важливих показників якості обслуговування згідно вимог QoS(Quality of Service), такі як: середній час затримки, джиттер, ймовірність втрат та помилок пакетів, швидкість їх передачі відводиться контролю з боку протоколам маршрутизації.

Таким чином, актуальність проблеми маршрутизації полягає: у дослідженні методів та аналізу з оцінкою якості вибраного оптимального маршруту та недопущення перевантаження об'єктів мережі в часи найбільшого навантаження (ЧНН). Як показує аналіз з оцінкою недоскональності сучасних протоколів одношляховою та багатошляховою відмовостійкою маршрутизації, полягає в недоліках структури саме графів моделі і методів, які не в змозі враховувати в повній мірі параметри якості роботи мереж в реальному часі.

Для рішення цих проблем необхідно в умовах впровадження вибраної потокової моделі на основі SDN технології управління одношляховою та багатошляховою відмовостійкою маршрутизацією в тому числі з протоколами захисту шлюзу за замовчуванням для мережі доступу та протоколами балансування навантаження для транспортних ресурсів (GLBP, CARP, HSRP, VRRP) та необхідно також використовувати схеми захисту Fast ReRoute. Для вище вказаної потокової моделі у відмінності від графових характерне те, що вона може враховувати не тільки структуру мережі, а також параметри якості роботи каналів зв'язку та потоків трафіку навантаження, в межах норми.

Завдяки використанню досліджуємої потокової моделі, можна більш ефективно вирішувати складні задачі щодо збалансування навантаження у ЧНН в мережах доступу на основі SDN.

В рамках цієї моделі умови збереження потоку трафіка на кінцевих вузлах і в цілому мережі та в умовах запобігання перевантаженню каналів зв'язку необхідно забезпечити захист шлюзів за замовчуванням.

Висновки:

1. В результаті проведених досліджень було обґрунтовано та проаналізовано з оцінкою вибір потокової моделі згідно вимог QoS.

2. Структура досліджуємої моделі підходить, як для розв'язання задач одношляхової так і для багатошляхової відмовостійкої маршрутизації. Також потокова модель дає можливість використовувати метрики маршрутів такі, як переходи та пропускні здатності протоколів маршрутизації, що в свою чергу дозволяє точніше підходити до вибору основних та резервних маршрутів одношляхової та багатошляхової відмовостійкої маршрутизації.

3. Одночасно, схеми захисту Fast ReRoute дають можливість резервування, трактів, вузлів, і всього шляху/мультишляху в мережах доступу.

4. Використання протоколів балансування дає можливість забезпечити захист об'єктів від перенавантажень та ефективно використовувати ресурси мережі в ЧНН.

5. В продовження дослідження планується провести моделювання конфігурації мережі та аналіз протоколів захисту шлюзів за замовчуванням на симуляційному обладнанні "Cisco Packet Tracer" та реальному (лабораторному) обладнанні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вегешна Ш. Качество обслуживания в сетях IP [Текст]. – М.: Издательский дом "Вильямс", 2003. – 368 с.

2. Лемешко А.В. Модель отказоустойчивой маршрутизации многоадресных и широкополосных потоков в MPLS-сети [Текст] / А.В. Лемешко, К.М. Арус // Системи обробки інформації. – №9 (116). – 2013.

3. Єременко О.С. Огляд теоретичних рішень щодо відмовостійкої маршрутизації в телекомунікаційних мережах [Електронний ресурс] / О.С. Єременко, М.О. Євдокименко // Проблеми телекомунікацій. – 2018. – № 1 (22). – С. 25 - 42.

ВИБІР ТЕХНОЛОГІЇ ТА ТОПОЛОГІЇ ДЛЯ ПОБУДОВИ ЛОКАЛЬНОЇ МЕРЕЖІ НА ПРИДПРИЄМСТВІ

Миронов А.А.

Науковий керівник – доц., к.т.н. Токар Л.А.

Харківський національний університет радіоелектроніки (61166,
Харків, пр. Науки, 14, кафедра інфокомунікаційної інженерії ім. В.В.
Поповського, тел. +380958770569, email: myronov.andrey@gmail.com

The issue of building a network in the enterprise is investigated. The choice of topology for building a network is analyzed. The technology of building a network is analyzed.

Одним з найбільш перспективних варіантів вирішення проблеми передачі високосортного трафіку, одночасної передачі сигналів різних форматів є нове покоління технології пасивних оптичних мереж, що забезпечує надання широкого спектру послуг з високою якістю. Ця технологія вже зараз може забезпечує передачу даних на швидкості 1 Гбіт/с і вище на одного абонента, що визначає актуальність роботи.

Першим етапом розробки та побудови мережі на виробничому підприємстві з використанням технології PON є вибір топології, наступними етапами - вибір обладнання та впровадження доменної системи.

Зважаючи на те, що мережа підприємства містить 100 комп'ютерів, 20 принтерів та 20 ір-телефонів доцільно і економічно використовувати топологію "мультидерево з пасивним оптичним розгалуженням" PON (P2MP).

Головні переваги обраної топології:

- економічне використання волокна, всі системи працюють на одному волокні, поділ обміну інформаційних потоків виконується на основі WDM-технології, тобто на принципі хвильового поділу;
- деревоподібна структура передбачає, що кожен термінал користувача незалежний, має свій фізичний і логічний маршрут до концентратора, послідовні ланцюги виключені;
- широка смуга доступу, до 400 Мб / с на термінал;
- можливість резервування як активного обладнання, так і пасивних волоконних шляхів;

У якості технології обрана GPON, вона є найбільш економічна. Основні переваги технології GPON такі: підтримка до 256 логічних ONT на одну довжину хвилі; механізм розподілу смуги пропускання в висхідному потоці за допомогою маркерів в низхідному потоці; новий спосіб автоматичного і періодичного виявлення ONT; автоматичне масштабування при виявленні дрейфу вікна ONT; захист кожного ONT-з'єднання.

Проектована мережа має структуру з пасивним розподілом в напрямку від концентратора до абонента. Коефіцієнт розподілу може досягати до 64 на одне волокно (PON-гілка), тобто до одного

концентратора може бути підключено Nx64 терміналів. Топологія проектованої мережі приведена на рис. 1.

Користувачеві доступно все одночасно і в повному обсязі: телефонний зв'язок, потоки даних, відео, службові додатки, які цілком незалежні, ізольовані і захищені як в межах терміналу, так і в масштабі всієї проектованої мережі.

Для підвищення надійності мережі можлива організація гарантованого живлення концентратора і терміналів, резервування активного обладнання.

Згідно технічного завдання необхідно забезпечити такі сервіси: Local Area Network (LAN), Інтернет, високоякісна відеоконференція, відеоконференція низького рівня і Voice over IP (VoIP) - телефонія.

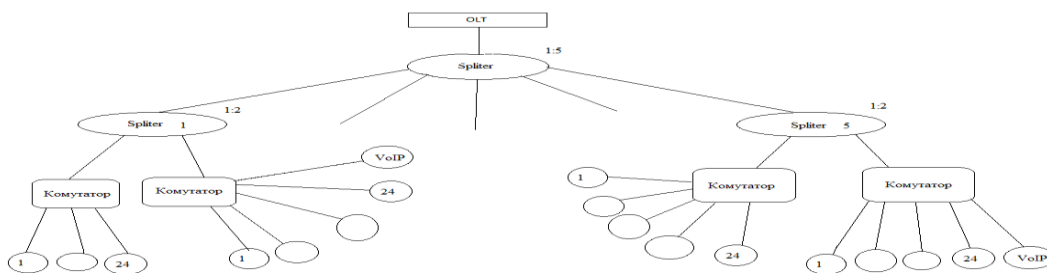


Рисунок 1 – Топологія проектованої мережі

Склад оптичної мережі містить оптичний розгалуждуювач (спліттер), пристрій для з'єднання декількох вузлів комп'ютерної мережі (коммутатор), абонентський термінал ONT, VoIP телефон.

Загальна необхідна швидкість передачі для всіх сервісів визначається формулою (1):

$$V = V_{\text{LAN}} + V_{\text{И}} + V_{\text{Bв}} + V_{\text{Bнy}} + V_{\text{VoIP}} \quad (1)$$

де V_{LAN} – необхідна швидкість сервісу LAN;

$V_{\text{И}}$ – необхідна швидкість сервісу Інтернет;

$V_{\text{Bв}}$ – необхідна швидкість сервісу високоякісної конференції;

$V_{\text{Bнy}}$ – необхідна швидкість сервісу низькоякісної конференції;

V_{VoIP} – необхідна швидкість сервісу IP телефонії.

Для розрахунку загальної швидкості необхідно скористатися параметрами швидкісних смуг для кожного з сервісів:

$$V = 100 + 20 + 6 + 0,512 + 0,256 = 126,768 \text{ (Мбіт/с)}$$

Таким чином, підтверджено створення мережі доступу з великою пропускнуою здатністю при мінімальних капітальних витратах.

УПРАВЛІННЯ РАДІОЧАСТОТНИМ СПЕКТРОМ В КОГНІТИВНИХ МЕРЕЖАХ ЗВ'ЯЗКУ

А.М.Ткаченко

Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії, тел. (057)
702-13-20)

e-mail: alyona.tka4enko2014@gmail.com факс (057) 702-13-20

The management of the radio frequency spectrum (RFS) is of great practical importance. This is due to the fact that the number of radio facilities operating in the common frequency bands in a limited area is constantly increasing. It has been investigated that the problem lies in the fact that the use of radio electronic equipment (radio-electronic means) without unacceptable mutual interference is becoming very common. It has not only a national, but also an international aspect, since radio waves do not know borders and radio stations should be designed in such a way that the RES of one state does not interfere with the operation of the RES of a neighboring state.

Радиочастотный спектр – один из наиболее дефицитных природных ресурсов, различные возможности использования которого расширяются день ото дня. Чем эффективнее этот ресурс используется, тем активнее происходит социальное и экономическое развитие страны.

К основным радиотехнологическим методам повышения эффективности использования частотного спектра относят:

- Использование видов модуляции высокого порядка (QAM-16, QAM-64)
- Использование мощного помехоустойчивого кодирования
- Многоантенные системы
- Оптимизация трафика (стандарты по сжатию заголовков)
- Оптимизация интернет-трафика

Для оценки общей эффективности использования РЧС вводится следующее выражение:

$$E = C_1 E_T + C_2 E_E + C_3 E_S \quad (1)$$

E_T , E_E , E_S – техническая, экономическая и социальная эффективности.

C_1 , C_2 , C_3 – корректирующие коэффициенты для выше перечисленных эффективностей. Они учитывают значимость той или иной эффективности, или её отсутствие. Общая сумма равняется единице.



Рис.1 – Алгоритм процедуры управления РЧС

Список литературы:

1. Управление радиочастотным спектром и электромагнитная совместимость радиосистем. [Текст] Учебн. пособие/ Под ред. д.т.н., проф. М.А. Быховского. - М.: Эко-Трендз, 2006. - 376 с.
2. Информационное управление эффективностью при использовании радиочастотного спектра/ В.А.Вишняков, А.В.Табаньков, 2014. – 32 с.
3. Восточно-европейский журнал передовых технологий. [Электронный ресурс]. URL: <http://openarchive.ua/bitstream/document/2415/1/12-1.pdf> (дата обращения: 15.02.202).

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ПАРАМЕТРІВ ЯКОСТІ ПОСЛУГ IoT 5G

Радченко В.В., Сабурова С.О.

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: vladyslav.radchenko.cpe@nure.ua, факс (057) 702-13-20

The Internet of Things can be considered as a global network infrastructure consisting of many connected devices that use touch, communication, network and information technologies. The introduction of IoT 5G services will take the prevailing approach to setting the level of service based on the quality of service provided by the subscribers themselves. Based on these requirements, the operator will form the initial parameters that determine the desired level of quality of service.

Технології NGN вже пройшли еволюційний шлях розвитку від гнучких комутаторів (Softswitch) до підсистем мультимедійного зв'язку IMS (IP Multimedia Subsystem) та безпроводових мереж довготривалої еволюції LTE (Long Term Evolution). При цьому завжди припускалось, що головним користувачем мереж NGN будуть споживачі - отже, максимальне число абонентів в таких мережах завжди буде обмежено чисельністю населення планети Земля.

Таким чином, в даний час відбувається еволюційний перехід від «Інтернету людей» до «Інтернету речей», IoT (Internet of Things) [1].

Мережі зв'язку «п'ятого покоління» - 5G, разом з аналізом великих даних (Big Data) і Інтернетом речей (IoT) покликані стати однією з основ цифрової економіки, головною рушійною силою якої повинен стати штучний інтелект (ШІ). Більш того, деяка кількість успадкованої інфраструктури мереж 3G і 4G органічно увійде до складу мобільних мереж п'ятого покоління 5G.

«Інтернет речей» можна розглядати в якості глобальної мережевої інфраструктури, що складається з безлічі підключених пристроїв, які використовують сенсорні, комунікаційні, мережні й інформаційні технології.

Забезпечення параметрів якості послуг Інтернету речей або Internet of Things (IoT) згідно вимог QoS (Quality of Service) залежить від:

- технологій безпроводових мереж з низьким енергоспоживанням (LPWAN, WLAN, WPAN);
- темпів впровадження мобільних мереж для Internet of Things (IoT): EC-GSM, LTE-M, NB-IoT і універсальних мереж 5G;
- темпів переходу мережі Інтернет на версію протоколу IPv6;
- технологій Smart Objects (сенсорів і актуаторов, забезпечених мікро контролером, пам'яттю і пристроєм зв'язку);

- спеціалізованих операційних систем зі стеком протоколів для мікроконтролерів сенсорів і актуаторов;
- широкого застосування стека протоколів 6LoWPAN / IPv6 в операційних системах мікроконтролерів сенсорів і актуаторов;
- ефективного використання Cloud computing для Internet of Things (IoT) платформ;
- розвитку технологій M2M (machine-to-machine);
- застосування сучасних технологій Software-Defined Networks (SDN), що знижують навантаження на канали інфокомунікацій. На рис. 1 представлено ринок послуг Інтернет - речей.



Рис.1. Ринок послуг Інтернету речей

Висновки:

1. При впровадженні послуг IoT 5G переважатиме підхід до встановлення рівня сервісу на основі якості послуг самих абонентів. Враховуючи ці вимоги, оператор сформує початкові параметри, що визначають бажаний рівень якості обслуговування.

2. Таким чином, операторам при забезпеченні послугами IoT 5G доцільно буде використовувати не тільки системи моніторингу для надзвичайних подій, але й системи управління якістю (SLA) та системи управління продуктивністю (Fault Management + SLA Management + Performance Management).

3. Відповідно до рекомендації G.1000 MCE-T («Якість послуг зв'язку: структура та визначення»), термін «якість обслуговування», крім технічних показників забезпечення послуг IoT 5G, також включає в себе якість відносин між абонентом і оператором мобільного зв'язку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. T. Kindberg et al. People Places and Things: Web Presence for the Real World. ACM J. Mobile Networks and Applications. — 2002. Vol. 7, № 5. P. 365–376.

2. S. Costanzo, S. Cherrier and R. Langar, "Network Slicing Orchestration of IoT-BeC³ applications and eMBB services in C-RAN", IEEE (INFOCOM) 2019, Paris, France, 29 April - 2 May 2019.

АЛГОРИТМ ДИСТАНЦІЙНОГО КЕРУВАННЯ ПРИВОДАМИ ЛАЗЕРНОЇ ОПТИКО-ЕЛЕКТРОННОЇ СТАНЦІЇ ПО CAN-ШИНІ

Шлома О.К.

Науковий керівник – д.т.н. Шостко І.С.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. *Інфокомунікаційної інженерії*,
тел. (057) 702-55-92)

E– mail: oleksandr.shloma@nure.ua

Observation of space is a very important factor when we testing flying object at the training ground. The use of laser-optical systems greatly facilitates the process of testing air bodies and monitoring them. To observe objects in space, the installation must be mobile and ready to accompany the object at high speed. This article discusses the algorithms of the Rozum RDrive servos and their communication with the computer via the CAN-bus. The principles of simplification of the switching system and the optimization of the working processes of servos are explained. We also examined RDrive operating modes and their protocols for communicating with a computer.

Для виявлення і супроводу цілей в повітряному просторі в ХНУРЕ розроблено дослідний зразок малогабаритної лазерної оптико-електронної станції (ЛОЕС) [1,2]. Установка має широкий спектр застосування, так її можна використовувати при проведенні випробувань зразків нових літальних апаратів, керованих ракет класу «повітря-поверхня», або ж як систему відеоспостереження і патрулювання територій з обмеженим доступом. Використовуючи лазерну оптико-електронну станцію, ми можемо зібрати велику кількість даних про параметри об'єкта - траєкторія руху, швидкість і прискорення. Всі параметри збираються і обробляються в реальному масштабі часу. Для збору даних використовується телевізійна камера з високою роздільною здатністю, тепловізор з телеоб'єктивом, лазерний далекомір, лазерний рівень горизонту і GPS приймач. Зібрані дані обробляються з використанням розробленого програмного забезпечення, в основі якого використовуються алгоритми і функції з бібліотеки алгоритмів комп'ютерного зору - OpenCV (Open Source Computer Vision Library). Технологія виявлення і стеження є впорядкованою послідовністю процедур отримання та аналізу відеопотоку. Відбувається захоплення цілі і потім в безперервному циклі вимірюється неузгодженість напрямку на цілі по відношенню до оптичної осі камери, видаються команди на сервоприводи опорно-поворотного пристрою.

В опорно-поворотному пристрої ЛОЕС ми використовуємо сервомотори RDrive від Rozum Robotics це закінчене рішення 3 в 1. RDrive об'єднує в одному корпусі ключові елементи: абсолютний енкодер (19 біт), контролер, хвильової редуктор і мотор змінного струму.

Для зв'язку з сервоприводами ми використовуємо CAN-шину. CAN-з'єднання сервоприводів RDrive це двухпроводова шина, яка транслює диференціальні сигнали: CAN_HIGH і CAN_LOW.

В інтерфейсі CANOpen можуть бути кадри даних, які передають команди до сервоприводу, або кадри, які запитують про передачу даних. Сервоприводи RDrive підтримують тільки стандартний формат фрейма CAN даних з 11-бітовим ідентифікатором. CANOpen охоплює п'ять верхніх рівнів моделі OSI: мережевий, транспортний, сеансовий, представлення і прикладний. Для реалізації CANOpen для сервоприводу RDrive використовуємо стек протоколів: SDO - сервіс об'єкта даних, NMT - управління станом мережі, Heartbet, EMCY - екстрений, SYNC -синхронізація.

Алгоритм спілкування сервоприводу з комп'ютером за допомогою CAN інтерфейсу складається з 3 обов'язкових етапів, після проходження яких сервопривід переходить в один з трьох режимів за які відповідає NMT стек. Перший етап - це включення сервоприводу (подача струму), другий етап - завантаження, що відбувається автоматично після включення сервоприводу, третій - ініціалізація, яка відбувається автоматично після успішного завантаження. Після успішного виконання трьох обов'язкових етапів RDrive може прийняти два стану 1) Pre-operational; 2) Operational. З цих двох станів сервопривід може перейти в режим Stopped, або перезавантажитися. Під час трьох перших етапів відбувається завантаження прошивки. У Pre-operational mode сервопривід доступний для комунікації, але не може виконувати команди, Operational mode - сервопривід може приймати всі CANOpen повідомлення, спілкуватися з ПК і виконує команди. Stopped mode – комунікацій відстуні за винятком NMT повідомлень.

Таким чином, розроблено алгоритм передачі команд управління на сервоприводи лазерної оптико-електронної станції з урахуванням особливостей технології виявлення і стеження цілі. Використання CAN інтерфейсу дозволило зменшити кількість проводів, що принципово важливо для систем з опорно-поворотним пристроєм.

Перелік посилань:

1. Тевяшев А. Д., Шостко І. С., Семенець В. В., Неофітний М. В., Колядін А. В. Лазерна оптико-електронна станція зовнішніх траєкторних вимірювань. Збірник XIX науково-технічної конференції «Створення та модернізація озброєння і військової техніки в сучасних умовах». Чернівці, 5–6 вересня 2019. С. 257–258.

2. Andrey Tevyashev, Igor Shostko, Mihail Neofitniy, Anton Koliadin Laser Opto-Electronic Airspace Monitoring System in the Visible and Infrared Ranges // IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments, APUAVD, 2019 KHAY C 127-129.

ИНЖИНИРИНГ ТРАФИКА С ИСПОЛЬЗОВАНИЕМ СЕГМЕНТНОЙ МАРШРУТИЗАЦИИ

Чеботарев И.А.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки, 14, каф. Инфокоммуникационной
инженерии им. В.В. Поповского, тел. +38 (057) 702-13-20)

Email: illia.chebotarov@nure.ua

Segment Routing provides complete control over the forwarding paths by combining simple network instructions. It does not require any additional protocol. Indeed, in some cases it removes unnecessary protocols simplifying your network. Segment routing does not require any path signaling. Hence, per-flow state only needs to be maintained at the ingress node of the SR domain increasing your network flexibility while reducing cost. Segment Routing runs natively on an MPLS or IPv6 data plane. A simple software upgrade will enable your hardware to run it. Also, Segment Routing can coexist with your existing LDP network, making the migration painless.

Сегментная маршрутизация (Segment Routing, SR) – новая технология инжиниринга трафика, разрабатываемая рабочей группой SPRING в составе IETF. Для SR определяется две инкапсуляции плоскости передачи (forwarding plane): MLPS (Multiprotocol Label Switching) и IPv6 с заголовком расширения сегментной маршрутизации (Segment Routing Extension Header). Домен SR – это непрерывный набор маршрутизаторов с поддержкой SR. Путь SR (т.е. LSP, просигнализированный по SR) осуществляет соединение в рамках домена SR. Актуальность данного вида маршрутизации заключается в том, что путь SR может проходить по пути наименьших затрат IGP между его начальной и конечной точками. Также он может проходить по пути, вычисленному с помощью инжиниринга трафика.

Передача SR. Когда входной SR-маршрутизатор получает пакет, он назначает ему класс FEC и инкапсулирует пакет с помощью стека меток MPLS. Затем он передает пакет следующему транзитному участку, связанному с данным FEC. Стек меток MPLS отражает путь SR, связанный с данным FEC. Каждая запись в стеке меток соответствует сегменту пути SR. Расширения IGP для сегментной маршрутизации. Каждый SR-маршрутизатор выделяет SID и метку: каждому префиксному сегменту или сегменту массовой рассылки, который заканчивается на этом маршрутизаторе; каждому сегменту соседства или привязки, который начинается на этом маршрутизаторе. Сделав это, он создает запись RIB (Routing Information Base) для каждого из вышеперечисленных сегментов и вносит записи RIB в FIB. Далее SR-маршрутизатор рассылает с помощью IGP следующую информацию: свои характеристики SRGB; все префиксные сегменты и сегменты массовой рассылки, которые заканчиваются на этом маршрутизаторе; все сегменты соседства или

привязки, которые начинаются на этом маршрутизаторе. IGP рассылает эти данные, в дополнение к ранее упоминавшимся атрибутам связи TE, по всему домену IGP. Поэтому каждый узел в рамках домена IGP содержит идентичную копию базы данных состояния связей (LSDB) и базы данных инжиниринга трафика (TED). LSDB описывает топологию IGP, включая SID и данные SRGB, а TED дополняет LSDB атрибутами связей TE.

Расчет путей. Функция расчета путей рассчитывает пути SR. Получив набор ограничений TE, функция расчета путей выдает на выходе стек меток MPLS, образующих путь SR, который соответствует ограничениям. Чтобы создать такой SR-путь, функция расчета путей обращается к LSDB и TED. Функция расчета путей может располагаться в центральном контроллере или, наоборот, распределяться по входным LSR.

Анализ. LDP и RSVP-TE – сквозные протоколы сигнализации, которые создают состояния передачи для каждого LSP в LSR. Поскольку LDP и RSVP-TE поддерживают все необходимые состояния передачи в LSR, то LSP, обработанный по LDP или RSVP-TE, может быть представлен одной записью стека MPLS. Напротив, методика SR перемещает часть состояний передачи (хотя только часть) из сети в пакет. Путь SR представлен стеком меток, где каждая запись соответствует сегменту на пути SR. Поэтому сеть поддерживает достаточно состояний, чтобы пересылать пакеты от входного сегмента к выходному, а пакет достаточно, чтобы пересылаться от сегмента к сегменту. Перенеся информацию о состояниях из сети в пакеты, SR снижает требования к памяти для LSR и объем вычислений, необходимый для поддержания состояний. А ведь проблема памяти и объема вычислений остается актуальной несмотря на то, что в последнее время маршрутизаторы стали оснащаться большим количеством вычислительных ресурсов и памяти, а также на доработки протокола RSVP-TE и его реализаций. Еще более важно то, что перенос информации о состояниях из сети в пакеты устранило потребность в сквозном протоколе сигнализации. Да, для работы SR требуется IGP и модуль расчета путей, но протокол сигнализации, подобный LDP или RSVP-TE, больше не нужен. Таким образом, каждый узел в IGP поддерживает LSDB и TED с достаточным количеством информации для работы функции расчета путей. В SR такого механизма нет. Поэтому на случай, когда ограничения TE включают в себя полосу пропускания, функция расчета путей должна быть централизованной и располагаться в контроллере, обладающем глобальной информацией о распределении полосы пропускания.

Список использованных источников

1. <https://www.ietfjournal.org/segment-routing-cutting-through-the-hype-and-finding-the-ietfs-innovative-nugget-of-gold/>
2. <https://www.segment-routing.net/>
3. <https://rtk-dc.ru/upload/iblock/ab4/ab441d4beb860ca678a61a1f0fbd33e6.pdf>

АЛГОРИТМ ОПТИМИЗАЦИИ СБОРА ИНФОРМАЦИИ В БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Галкин П.В.

Научный руководитель – к.т.н., проф. Ключник И.И.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. ПЭЭА, тел. (057) 702-14-94)

E-mail: galkinletter@ukr.net

The proposed ant algorithm using semaphores can be used not only for routing and traffic optimization problems, but also for other problems with large dimensions of search areas. It is proposed to use the semaphore method in order to restrict access to certain nodes, in the first case with a given number of threads, and in the second to nodes receiving an alarm. The results can be applied in the design of wireless sensor networks.

Беспроводная сенсорная сеть (БСС) – представляет собой распределённую в пространстве систему, важным аспектом работы БСС является ее структура [1]. В работе предлагается кластерная структура беспроводной сенсорной сети. Важным вопросом работы узлов БСС является энергопотребления узлов [2].

В работах [1-3] приведены подходы для построение БСС с применением кластеризации. Радиус действия и радиус радиосвязи только частично описывают возможный процесс сбора информации в БСС [4]. Для оптимизации управления информационным потоком предлагается использовать муравьиный алгоритм, классическая реализация которого рассматривалась в работе [5], а модифицированная версия – в работе [6].

В классическом варианте муравьиный алгоритм предложил Marco Dorigo в 1992 году для поиска оптимального пути в графе. Как отмечено в работе [6], на сегодняшний день существует пять основных модификаций муравьиного алгоритма Elitist Ant System, Ant-Q, Ant Colony System, Max-min Ant System, ASrank. Усовершенствования муравьиного алгоритма связаны с большим использованием истории поиска и более тщательным исследованием областей вокруг уже найденных удачных решений или с введением «элитных муравьев», новых механизмов выделения и испарения. Как отмечено в работе [6], на данный момент отсутствует универсальный алгоритм передачи данных, который сразу бы от конечного устройства направленно посылал пакет к координатору сети.

Методы генетических алгоритмов (муравьиного, алгоритма роя частиц) относятся к одному классу методов эволюционной оптимизации. Особенностью этих методов является высокая сходимость.

Муравьиные алгоритмы подходят для реактивных протоколов маршрутизации, где маршруты существуют только тогда, когда они необходимы, то есть когда по ним ведется передача данных. Данный метод соотносится с введённым нами алгоритмом управления передачей данных для узла БСС.

Муравей будет двигаться от узла i до узла j , используя вероятностно-пропорциональное правило с вероятностью [47]:

$$P_{i,j} = \frac{\tau_{i,j}^{\alpha} (\frac{1}{w_{i,j}})^{\beta}}{\sum_{j \in M} \tau_{i,j}^{\alpha} (\frac{1}{w_{i,j}})^{\beta}}, \quad (1)$$

где $\tau_{i,j}$ – количество феромонов на ребре от узла i до узла j ;

$w_{i,j}$ – расстояние между узлами i и j ;

M – множество узлов, которые можно посетить муравью;

α – коэффициент, контролирующий влияние количества феромонов

$\tau_{i,j}$;

β – коэффициент, контролирующий расстояние между узлами i и j на выбор муравья.

Если в выражении (10) $\alpha = 0$, то будет выбран ближайший узел, что соответствует жадному алгоритму в классической теории оптимизации. Если $\beta = 0$, тогда работает лишь феромонное усиление, что влечет за собой быстрое вырождение маршрутов к одному субоптимальному решению.

1. Галкін П.В. Аналіз моделей та оптимізації збору інформації в бездротових сенсорних мережах [Текст] / П. В. Галкін // Восточно-Европейский журнал передовых технологий. – 2014. – т.5, №9 (71). – С. 24-30.

2. Галкин П. В. Анализ энергопотребления узлов беспроводных сенсорных сетей // ScienceRise. – 2014. – №. 2 (2). – С. 55-61

3. Галкин П.В. Алгоритм управления и оптимизации информационных потоков в беспроводной сенсорной сети // Восточно-Европейский журнал передовых технологий. – 2014. – №. 6 (3). – С. 53-63.

4. Галкин, П.В. Модель сбора информации в беспроводной сенсорной сети / П.В. Галкин // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – №5(33). – С. 41–53

5. Галкін П.В, Ключник І.І. Спосіб збору інформації в бездротовій сенсорній мережі : пат. на корисну модель 100463 Україна / Галкін П.В., Ключник І.І. ХНУРЕ. – 2015.

6. Коваленко А.М. Разработка алгоритма направленной маршрутизации для беспроводных сенсорных сетей. [Текст] / А.М. Коваленко, В.А. Дидук, Е.Г. Трофименко // Труды Одесского политехнического университета. – 2011. – Вып. 1 (35). – С. 151–154.

СУЧАСНА МЕТОДИКА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ МЕРЕЖ СТАНДАРТУ IEEE 802.11

Гонтарь І.А., Згуїрі Іссам, Журавка А.В.

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 факс (057) 702-13-20

A research object is the process of information security of wireless networks of the standard IEEE 802.11.

The subject of research is the methods of pentests on wireless networks.

The aim of the work is to identify vulnerabilities of attacks on wireless networks, through using of upgraded system Kali Linux.

Methods of researched are an experiment with scanning and attacking on wireless networks.

Nowadays, wireless networks represent the main way of transferring information. In every company, every home has routers that provide wireless data transmission.

The pentest test is a technique for analyzing and evaluating network security systems or other systems by modeling malicious actions, ranging from unauthorized system actions to internal actions, that is, the intrinsic security of an authorized attacker. The main task of the penetration test is to identify the maximum possible number of vulnerabilities of the information system (IP) for a limited time under certain conditions and condition of the IP. When conducting a penetration test, the following tasks are solved: assessment of the current state of the IP information security system; identification of information system vulnerabilities; the use of identified vulnerabilities to gain unauthorized access or unauthorized access to information to demonstrate the existence of vulnerabilities and the existence of a highly likely threat to the information system; making recommendations to improve the effectiveness of information security in IP.

Simulating the attacker, the cyber security specialist actively analyzes the systems for vulnerabilities in all areas, for example: penetration of the corporate network through system defects.

Thus, the paper discusses the method of detection of IEEE 802.11 network vulnerabilities using Kali Linux [1]. At the same time, this package is a much-needed tool that can be used to find and simulate unauthorized actions to better protect the system, as well as for future cyber-defenses - it is a necessary practice to master and counter cyber attacks. This distribution can also be a very serious weapon in the hands of a hacker. Kali Linux is a very powerful network vulnerability tool for both cyber security (white hackers) and cyber criminals (black hackers), also a Linux distribution based on the Debian kernel. This

operating system contains a large number of tools and utilities that, on the one hand, help you identify security holes in your computer environment or can be a powerful weapon for corporate network damage. The distribution was created by Offensive Security staff. Therefore, the main goal is to find holes in the network. Kali Linux's main strength is its tools. It contains about a dozen tools for analysis, scanning for vulnerabilities, such as: Aircrack-ng is a suite of programs for hacking and testing Wi-Fi network security, allowing you to crack WEP, WPA / WPA2 keys, monitor traffic, sort through WPA-PSK keys, and grab Wi-Fi connection setup keys; Burp suite is a console application for finding vulnerabilities on Internet sites and web applications; Foremost is a console program for recovering files based on their headers, footers and internal data structure; John the Ripper is an open source console program for cracking passwords by the search method; Maltego is a console analytics program. It allows you to find connections between different entities and objects. Allows you to perform open source searches, combine data for analysis, and automatically build dependencies between them; Metasploit is a framework with sophisticated architecture, hundreds of contributors, which includes thousands of modules to automate the exploitation of a huge number of vulnerabilities; Nmap is an open source Kali Linux console application that can be used for network security audits and port scans; Wireshark is a program that allows you to analyze network packets. Has the ability to use it to troubleshoot network problems, analyze applications and communication protocols, and develop applications; jSQL Injection is a Java tool for automatic injection into SQL databases; Hydra is a console program for real-time password retrieval from various online services, as well as more secure applications such as Secure Shell (SSH) and other protocols. The search is performed not by hash, but directly by queries to the server, ie you can check whether the firewalls are properly configured, such attempts are blocked, and whether you can detect such an attack on the server at all. Not only can the Aircrack-ng suite of programs conduct DoS attacks, it can also intercept authentication packages and find keys and more. Along with its multifaceted and multifunctional tools, there are some features that make it more specialized than other distributions, such as: several boot options: standard download, safe mode (Failsafe) and forensic mode. There is also the LUKS Encryption Nuke option, which allows you to immediately remove keys for encrypted data.

Finally, Kali Linux is also a much-needed tool through which to search for and simulate unauthorized actions to better protect the system, as well as for future cyber-defenses - is a necessary practice for mastering and counteracting cyber attacks. This distribution may also be a serious weapon in the hands of a hacker.

References

1. Kali Linux. Official Documentation [Online Resource].- Access Mode <https://docs.kali.org/introduction/what-is-kali-linux>.

ОСОБЛИВОСТІ СУЧАСНОГО РОЗВИТКУ Wi-Fi МЕРЕЖ

Пантелєєв В.О, Ажраб Басіл Саліба, Нуїна Маруане

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 факс (057) 702-13-20

The object of the study is the convergent 4G communication network and the modern technology of wireless access to the Internet - Wi-Fi.

The subject of the research is the methods of security of elements and mechanisms of information protection in converged 4G and Wi-Fi networks.

The purpose of the work is to study the technologies and problems of the protection of modern wireless access technology and the convergent network of general use.

Research methods - the analysis of the prospects for the development of Wi-Fi and 4G and features of modern development has been carried out.

In the next few years we can expect further development of the Wi-Fi solutions line, with all major marketing directions. Mastering the 60 GHz band. The Wireless Gigabit Alliance (WiGig Alliance) is actively working on the development of 60 GHz Wi-Fi technology with peak transmission speeds of up to 7 Gb/s for picocell coverage. Such an increase in Wi-Fi performance is a major step forward, even compared to high-speed IEEE 802.11n in solutions up to 300 Mbps, which involve the use of two or three user streams and the integration of two 20 MHz radio channels. The limiting factor for this solution is the short range, as well as the need to simultaneously support basic Wi-Fi frequency bands - 2.4 GHz and 5 GHz. But the prospects for developing "cloud" services and services based on high-speed 60 GHz Wi-Fi seem quite realistic.

The development of Wi-Fi Direct solutions that allow for standard Wi-Fi speeds to provide direct connections between a variety of client devices (communicators, smartphones, printers, digital still cameras / video cameras, etc.), bypassing traditional hotspots and wireless routers. Following the example of Bluetooth technology, the Wi-Fi Alliance, as a developer of Wi-Fi Direct solutions, supports a number of specifications, in particular, for information security - Wi-Fi Protected Access 2 (WPA2). And also support for improved VoIP solutions with a new suite of protocols to further develop competitive alternative voice services.

An important advantage of cellular Wi-Fi networks is also the self-organization of the network modules and the ability to recover when some nodes fail. The introduction of the IEEE 802.11s specification will allow you to create simpler and less expensive Wi-Fi networks with alternative routes and increased reliability. Further improve the Wi-Fi radio interface. IEEE 802.11n

specification enhancements to radio parameters are complemented by enhanced chipset reliability, parity encoding technology, and improved access to access points by optimizing antenna beamforming.

The development of the IEEE 802.11v specification aims to support mechanisms for managing Wi-Fi radio network settings in terms of reducing power consumption. In turn, the introduction of 802.11k to improve radio resource management will allow Wi-Fi networks to identify weak signals or areas of uncertain reception and, accordingly, optimize wireless service.

Finally, let us identify the most important contemporary problems. At the same time, along with the growing popularity of Wi-Fi hotspots, a number of problems remain related to the lack of convenience and ease of use of this wireless technology [1]. Authorization procedure problem. During the hot spot access procedure, a Wi-Fi user through the browser enters authorization information, which in some cases may be blocked. For example, starting a Wi-Fi subscriber at a terminal of a certain program (such as e-mail). At the same time, the status of the established connection will be indicated on the Wi-Fi subscriber terminal. A time-limited access issue may occur in time-bound services, such as when using a Wi-Fi temporary service card in public places, such as in a hotel. After the set time of service, the connection to the Wi-Fi hotspot will be lost, although the user interface will indicate that the terminal is still connected. There was a problem choosing Wi-Fi hotspot. In many specific cases, the maintenance of the user terminal is in the area of simultaneous radio coverage of several Wi-Fi networks. The subscriber device recognizes the available Wi-Fi service identifier (SSID) and establishes a connection to this network. But if SSID is not recognized, the user will have to complete the entire procedure of Internet access, manually select SSID, enter a new URL in the browser and confirm the authorization information. In addition to being annoying to the user, this in itself is a rather cumbersome procedure that depletes the terminal device's battery and can lead to accidental errors. In some cases, the time spent may be critical, for example, when transmitting voice calls. The problem of supporting hotspots for roaming partners. In a situation where a Wi-Fi subscriber is authorized in a hot spot managed by a roaming partner. To overcome these problems, the Wi-Fi Alliance has proposed the specification of Wireless Internet Service Provider roaming (WISPr) 1.0. Equally important is the modern problem of maintaining the necessary level of information security in Wi-Fi hotspots.

References

1. Cisco Annual Internet Report (2018–2023) White Paper: [Electronic resource]. – Access Mode: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>

ОГЛЯД СУЧАСНИХ МЕТОДІВ МЕРЕЖНОЇ СТЕГАНОГРАФІЇ

Анна Щербак, Марина Шаповал, Дарраж Муад

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 факс (057) 702-13-20

An object of study is a process of stenographic information hiding, which counteracts the threat of unauthorized access to it.

A subject of the research is network steganography methods based on changes in header and data fields in protocols.

An aim of the work is to research and implement network steganography methods, with special emphasis on consideration of quality assessment indicators of stenographic methods. Choose a method that could be used to improve the system of remote user authentication in communication channels by increasing the resistance to cracking and noise immunity of the system.

Steganography is a science that studies ways and methods of hiding the existence of sensitive information when stored or transmitted to prevent third parties from discovering it. The hidden information is called a transcript. They are located in a specific medium. In network steganography, the role of the carrier is performed by a packet transmitted over the network. There are two mandatory requirements for stenographic transformation: invisibility and reliability (resistance to distortion of all kinds). In addition, when constructing a stenographic system, the following provisions should be taken into account [1]: acceptable computational complexity of the steganosystem implementation; providing the necessary bandwidth; ensuring the authenticity and integrity of the hidden message for the authorized person; the potential offender knows all about the steganosystem and its implementation except the key; if the fact of the existence of the hidden message becomes known to the offender, then it should not be possible to extract it until the key is known.

An important factor is also the choice of the most favorable media for hidden messages in communication networks. Consider the basic requirements that they must meet.

1) They should be popular, that is, the use of the media themselves should not be considered an anomaly. The more popular media present and used on the network, the better because they mask the existence of a hidden connection.

2) Their modification associated with the introduction of the steganogram should not be visible to a third party who is not aware of the existence of a hidden link.

The use of network steganography is that it does not rely on the deception of the human sense, as it does when using methods of steganography that conceal data in digital images, audio and video files. Let's look at three groups

into which methods of network steganography are divided [2]. 1) Steganography methods, the essence of which is to change the data in the network protocol header fields and in the payload fields; 2) Steganography techniques that change the structure of packet transmission, for example, change the sequence of packet transmission or deliberate introduction of packet losses during their transmission; 3) Hybrid methods of steganography - when used, the contents of the packages, the delivery time of the packages and the order of their transfer change. In turn, some of these methods are divided into several groups. Packet modification methods include three different subgroups. 1) Methods for changing data in the protocol header fields. They are based on modifications to the IP, TCP, Stream Control Transmission Protocol (SCTP) header fields, and more; 2) Package payload modification methods. In this case, various algorithms for watermarks, language codecs and other steganographic techniques for hiding data are used; 3) Mixed techniques. Methods for modifying the packet transmission structure also include three directions. 1) Methods in which the order of packets is changed; 2) Methods that change the delay between packets; 3) Methods, the essence of which is to introduce deliberate loss of packages by omitting sequence numbers from the sender.

Thus, the general information on network steganography is reviewed and particular attention is paid to the fact that there are mandatory requirements for stenographic transformation, such as invisibility and reliability. Also, it has been found that an important factor is the selection of the most favorable media for hidden messages. To implement network steganography, it is planned to consider software that uses Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), and Hypertext Transfer Protocol (HTTP) and network snippets to hide data on the network. These methods are planned to be compared by characteristics such as performance, efficiency, noise resistance and detection resistance. These characteristics make it possible to fully evaluate the effectiveness of the methods considered. The considered methods of steganography make it possible to successfully solve the problem of protecting information from unauthorized access.

References:

1. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures / [W. Mazurczyk, S. Wendzel, S. Zander et al.]. – Hoboken: Wiley-IEEE Press, 2016. – P. 296.
2. Handel T. G. Hiding data in the OSI network model / T. G. Handel, M.T. Sandford II // Information Hiding: First International Workshop Cambridge / T. G. Handel, M. T. Sandford II., 1996. – P. 23–38.

ВИДИ АТАК НА СТЕГОСИСТЕМУ ТА ЗАХИСТ ВІД НИХ

Грицюк В.К.

Науковий керівник – к.т.н., доц. Золотарьов В.А.

Харківський національний університет радіоелектроніки

(61166, Харків, просп. Науки, 14,

каф. Інформаційно – мережної інженерії, тел. (057) 702-14-29)

e-mail: vladyslav.hrytsiuk@nure.ua

In this publication, we consider the types of attacks on the stegosystem and methods for countering them.

Steganography is a communication method. The task of steganography is to hide the very fact of the existence of secret data during its transmission, storage or processing. In other words, hiding the existence of information means not only the impossibility of detecting a hidden message in an intercepted message, but also generally making it impossible to raise any suspicions about this. A common feature of steganographic methods is that the hidden message is embedded in a certain object (container) that does not attract attention, which is then openly forwarded to the addressee.

Існує два принципово різних способу передачі по відкритому каналу зв'язку конфіденційної інформації. Один із способів полягає в тому, щоб замаскувати передану секретну інформацію іншою інформацією. В цьому випадку секретні символи вбудовуються у відкритий текст. Завдання вбудовування та виділення повідомлень з іншої інформації виконує стегосистема. Стегосистема ж утворює стегоканал, по якому передається приховане повідомлення. Цей канал вважається підданим впливам з боку порушників.

Порушник може бути пасивним, активним і зловмисним.

Пасивний порушник може лише виявити факт наявності стегоканала і (можливо) читати повідомлення.

Діапазон дій активного порушника значно ширше. Приховане повідомлення може бути їм видалено або зруйновано.

Дії злочинного порушника найбільш небезпечні. Він здатний не тільки руйнувати, а й створювати помилкові стего.

Для здійснення тієї чи іншої загрози порушник застосовує атаки.

1. Атаки проти вбудованого повідомлення – спрямовані на видалення або псування ЦВЗ шляхом маніпулювання стего. Прикладами таких атак можуть бути лінійна фільтрація, стиск зображення, додавання шуму, вирівнювання гістограми, зміна контрастності і т. д.

2. Атаки проти стегодетектора – спрямовані на те, щоб ускладнити чи зробити неможливою правильну роботу детектора. При цьому водяний знак у зображенні залишається, але втрачається можливість його прийому. У цю категорію входять такі атаки, як афінне перетворення (тобто масштабування, зрушення, повороти), усічення зображення, перестановка пікселів і т. д.

3. Атаки проти протоколу використання ЦВЗ – в основному пов'язані зі створенням хибних ЦВЗ, помилкових стего, інверсією ЦВЗ, додаванням кількох ЦВЗ.

4. Атаки проти самого ЦВЗ – спрямовані на оцінювання і витяг ЦВЗ з стегоповідомлення. У цю групу входять такі атаки, як атаки змови, статистичного усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації.

Відповідно до цієї класифікації всі атаки на системи вбудовування ЦВЗ можуть бути розділені на чотири групи:

- 1) атаки, спрямовані на видалення ЦВЗ;
- 2) геометричні атаки, спрямовані на спотворення контейнера;
- 3) криптографічні атаки;
- 4) атаки проти використовуваного протоколу вбудовування та перевірки ЦВЗ.

Для підвищення надійності стегосистем можна запропонувати ряд поліпшень.

Різні методи протидії пропонувалися для вирішення проблеми прав власності. Перший спосіб полягає в побудові незворотного алгоритму ЦВЗ. ЦВЗ повинен бути адаптивним до сигналу і вбудовуватися за допомогою односпрямованої функції, наприклад, хеш – функції.

Другий спосіб вирішення проблеми прав власності полягає у вбудовуванні в ЦВЗ деякої тимчасової позначки, що надається третьою, довіреною стороною. У разі виникнення конфлікту особа, яка має на зображенні більш ранню тимчасову позначку, вважається справжнім власником.

Для захисту від атак типу афінного перетворення можна використовувати додатковий (опорний) ЦВЗ. Цей ЦВЗ не несе в собі інформації, але використовується для «реєстрації» виконуваних порушником перетворень. У детекторі ЦВЗ є схема, що виконує зворотне перетворення.

Іншим методом захисту від подібних атак є блоковий детектор. Модифіковане зображення розбивається на блоки, і для кожного блоку аналізуються всі можливі спотворення. Для кожної зміни визначається коефіцієнт кореляції ЦВЗ. Перетворення, після якого коефіцієнт кореляції виявився найбільшим, вважається реально виконаним порушником.

Перелік використаних джерел

1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН – ПРЕС, 2002. – 270 с.
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. – М.: Горячая линия – Телеком, 2010.

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПОПУЛЯРНИХ «ІАС» РІШЕНЬ ДЛЯ СТВОРЕННЯ ТА МЕНЕДЖМЕНТУ ХМАРНОЇ ІНФРАСТРУКТУРИ

Гусак М.В

Науковий керівник – д.т.н., проф. Безрук В.М
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14,
каф. Інформаційно-мережної інженерії, тел. (057) 721-14-29)
e-mail: maksym.husak@nure.ua

In this publication, we will consider some of the most popular solutions for a cloud infrastructure manager using the IAC approach for the most popular cloud solutions. It's no secret that cloud computing occupies a large part of the digital services market. In this way, the issue of managing and optimizing the infrastructure and its cost is relevant. And the IAC approach has established itself as one of the best from this point of view and has several advantages. It is fast, simple, provides structure consistency, increases efficiency, allows you to optimize cost and minimize risks. We will try to examine in more detail the tools currently offered on the market for implementing the IAC approach.

Cloud Computing на поточний момент є одним з найпопулярніших напрямків розвитку сфери інформаційних технологій. Багато компаній бажають мати всю свою ІТ-інфраструктуру в хмарі. Такі тенденції зумовлені рядом переваг які надають хмарні сервіси. Аби не бути голослівним приведу діаграму у якій наведено статистику з опитування більше ніж 300 компаній, та якими рішеннями вони користуються.

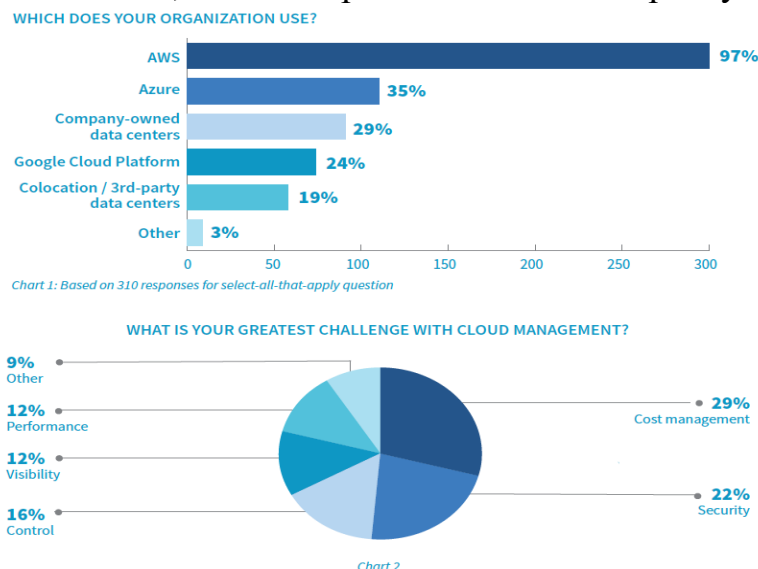


Рисунок 1 – Діаграма використання хмарних сервісів

Ми розглянули 3 основні на цей момент часу програми(підходи), до створення інфраструктури з використанням IaC(Infrastructure as Code) підходу. Це були рішення від компаній: Hashicorp з Terraform, AWS Cloud

з Cloud Formation, та Azure Cloud з ARM Templates. Було виділено декілька основних критеріїв оцінки для цих інструментів. Отже перше це простота використання та зрозумілість(прозорість), друге – ціна, третє – гнучкість в роботі, четверте – функціональність.

Таблиця 1 – Порівняння інструментів

Інструмент	Використання	Гнучкість	Функціональність
<i>Terraform</i>	2	4	4
<i>CloudFormation</i>	3	3	4
<i>ARM Templates</i>	3	3	4

А тепер детальніше, отже використання всі перераховані програми доволі прості у розумінні код для них пишеться в зрозумілому для людини вигляді(human readable code), для CloudFormation використовує yaml формат, ARM Templates – json формат, Terraform – власну мову HCL(подібна до json). З перерахованих, найбільше проблем може виникнути саме з Terraform тому за простотою використання він отримав найнижчий бал, а загалом ці інструменти потребують базових знань відповідної хмари та англійської мови.

Гнучкість як можна було здогадатись CloudFormation та ARM Templates можуть використовуватися тільки для AWS та Azure Cloud відповідно. В той час як Terraform програма з відкритим кодом та керується провайдерами і може бути використана для більше ніж 10 хмарних сервісів.

Функціональність – в рамках своїх хмарних сервісів CloudFormation та ARM Templates мають майже необмежений функціонал, Terraform програє в цьому аспекті, але він може використовуватися для управління інфраструктурою в декількох хмарах, таким чином він може бути більш дешевим в обслуговуванні.

Судячи з всього вище перерахованого середній бал усіх інструментів рівний, але ми виділили як переможця саме Terraform. Вирішальну роль в цьому рішенні відіграла його універсальність, та мультиклаудність.

Перелік посилань

1. Dignan L. Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud [Електронний ресурс] / Larry Dignan. – 2019. – Режим доступу до ресурсу: <https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/>

2. AWS CloudFormation Documentation [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://docs.aws.amazon.com/cloudformation/index.html>.

3. Terraform Documentation [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://www.terraform.io/docs/index.html>.

LTE UPLINK SCHEDULING IN MULTIPROCESSORS SYSTEM

Mahmoud Mahmoud Sayed Hussein

Scientific supervisor - PhD. Senior Researcher Kadatskaya. O

Kharkiev National University of Radio Electronic

(Infocommunication Engineering, 14. Nayku Ave. Kharkiev)

(057) 702-13-20)

E-mail: mahmoudsayed5197@gmail.com факс (057) 702-13-20

The main objective of the thesis is to design a parallel processing algorithm for LTE uplink in a multi processor system. In the thesis evaluate the performance of this algorithm with to throughput, efficiency and as algorithm complexity.

The uplink LTE scheduler algorithm can be parallelised efficiently over several digital signal processors in a multi-core environment. Is submitted algorithm are evaluated against each other in terms of throughput, time efficiency. Also, the result is compared with serial scheduling process. To simulated the uplink scheduler algorithm indicates that the parallel scheduling algorithm is able to achieve higher time efficiency than serial scheduling algorithm, while keeping the same throughput performance. The time improvement depends on the number of schedulable UEs in the system, processors number and the throughput trade-off.

In the equipment of the new generation Long Term Evolution (LTE), multi-core processors combine several microprocessors in one chip. They will be increasingly implemented in eNodeB LTE to achieve higher performance. Therefore, when developing and expanding the use of a multi-core processor system, it is necessary to modernize the current planning algorithm on a single processor platform. Scheduling in eNodeB LTE is a sequential process. The priority of planned users is set. Then for a given unit of the planning time, the scheduler assigns resources to users in accordance with the set priority level one by one until there are no more planned users or there are no spectral resources in accordance with the planning algorithm.

Such a scheduling algorithm has good efficiency for working on a single DSP platform. For a multi-core platform, it becomes very inefficient. This is due to the fact that during the process of allocating resources, low-priority user equipment cannot be scheduled. Previous users must be scheduled first. For a system of multi-core processors, the parallelism of their work does not provide parallel planning. In a sequential scheduling method, only one processor provides a scheduling process, even if there are other free processors that can provide service. The available time for the planning process is strictly limited and its value is directly proportional to the number of user devices that can transmit in one unit of time. This limits the number of serviced user devices. To enable the parallel launch of the planning process in a multiprocessor system, a larger number of user equipment can be allocated to the spectrum by increasing

the number of processors. Abstracts suggest parallel planning to increase current system performance and conduct research. The planning algorithm in this case consists of the following steps.

First, at the system level, effective parallelization to several DSPs in a multi-core environment occurs and the scheduling process is divided into several DSP cores of the uplink scheduler process. UEs are divided into separate user groups, and each processor UE is provided with one processor.

The frequency resource is also divided into separate fragments and then allocated to different groups of UEs. The planning process starts in multiprocessors independently of each other. One processor is responsible for only part of the entire set of UEs and, accordingly, has access to only part of the frequency resources. A reduced number of users leads to a reduction in planning time. Therefore, for the same period of time, it is possible to schedule more users. But this parallel scheduling method can also cause a decrease in system throughput.

Available frequency resources are divided into several fragments and map each of them to a specific group of UEs. Therefore, user equipment in one group can only move inside this fragment. They cannot cross the boundary of a fragment and are located in another part of the spectrum. Thus, in comparison with sequential scheduling, a parallel algorithm can even lead to users using the worst frequency resources.

The proposed algorithm can be divided into three stages. At the first stage, preliminary planning takes place, the user equipment and the frequency band are divided into groups and fragments in accordance with various rules. Each group is mapped to one piece. At the second stage, the multiprocessor platform takes on the planning process, performs the distribution of the spectrum in parallel flows with parallel planning. At this stage, two methods are developed and evaluated: maximizing throughput and maximizing equity. At the third stage, it is necessary to use the time saved to increase the spectrum efficiency.

Using two methods for solving the problems posed, the algorithms are evaluated with each other according to the criterion of bandwidth and efficiency of the time spent. The proposed algorithm is also compared with the sequential planning algorithm according to the same criteria. Efficiency of time use, memory usage and implementation possibilities are also evaluated. The proposed algorithm is simulated and simulated. The variety of simulations performed is based on a variation of the scheduling algorithm of the eNodeB LTE uplink scheduler process.

References

1. 3GPP TS 36.101; User Equipment (UE) radio transmission and reception (Release 8).
2. 3GPP TS 36.211; Physical Channels and Modulation (Release 8).

DEVELOPEMENT OF COMPLEX LABORATORY WORK ON RESEARCH OF MOBILE NETWORK SYSTEMS USING SDR TECHNOLOGY

Дриф Абденур

Научный руководитель – д.т.н., проф. Лошаков В.А

Харківський національний університет радіоелектроніки, Україна

E-mail:ut3ll.v@gmail.com

SDR (Software Defined Radio) is the most efficient technology which makes rapid modulation, encoding and signal processing in new generations of mobile communication systems by using custom software and rapid modification. However, the lack of training required to train specialists in this field. In this regard, the development of a complex laboratory work for the study of communication systems of new generations based on the use of SDR technology is relevant.

The research carried out in this us to develop a software to implement models of modern and advanced communication systems (GSM and LTE standards) using LimeSDR programmable radio platform [1]. This platform uses the Lime Microsystems LMS7002M radio chip, which contains low noise amplifiers, mixers of receivers and transmitters, filters of receivers and transmitters, gain control circuitry, transmitter power control circuit, ADC and DAC. It is important that it is fully open source, which means that the schematics of the device and the PCB are available, the source code of the FPGA programs as a PC client. The freeware Ubuntu GNU / Linux operating system was selected to implement the software for LimeSDR.

Laboratory work on the research of the GSM standard

With the widespread availability and the documentation of GSM, the digital mobile cellular standard is an ideal topic for learning the principles of cellular communication. Based on a comparative analysis of programmable SDR platforms, the LimeSDR radio platform was chosen to build the universal laboratory complex.

The LimeSDR platform gives students, inventors, and developers an intelligent and flexible device for manipulating wireless signals, so they can learn, experiment, and develop with freedom from limited functionality and expensive proprietary devices.

As part of the work, the GSM base station infrastructure (BS) has been deployed. This is done using the freely distributed osmocom software package (Fig. 1), which consists of dozens of software tools that can work both individually and form an integrated infrastructure. To interact the osmocom software package with LimeSDR, you must install an OsmoTRX receiver that implements the physical layer of the radio interface in accordance with the 3GPP technical specifications "Physical layer in the radio path"; and multiple access in the radio path; "Modulation"; "Synchronization of radio subsystems".

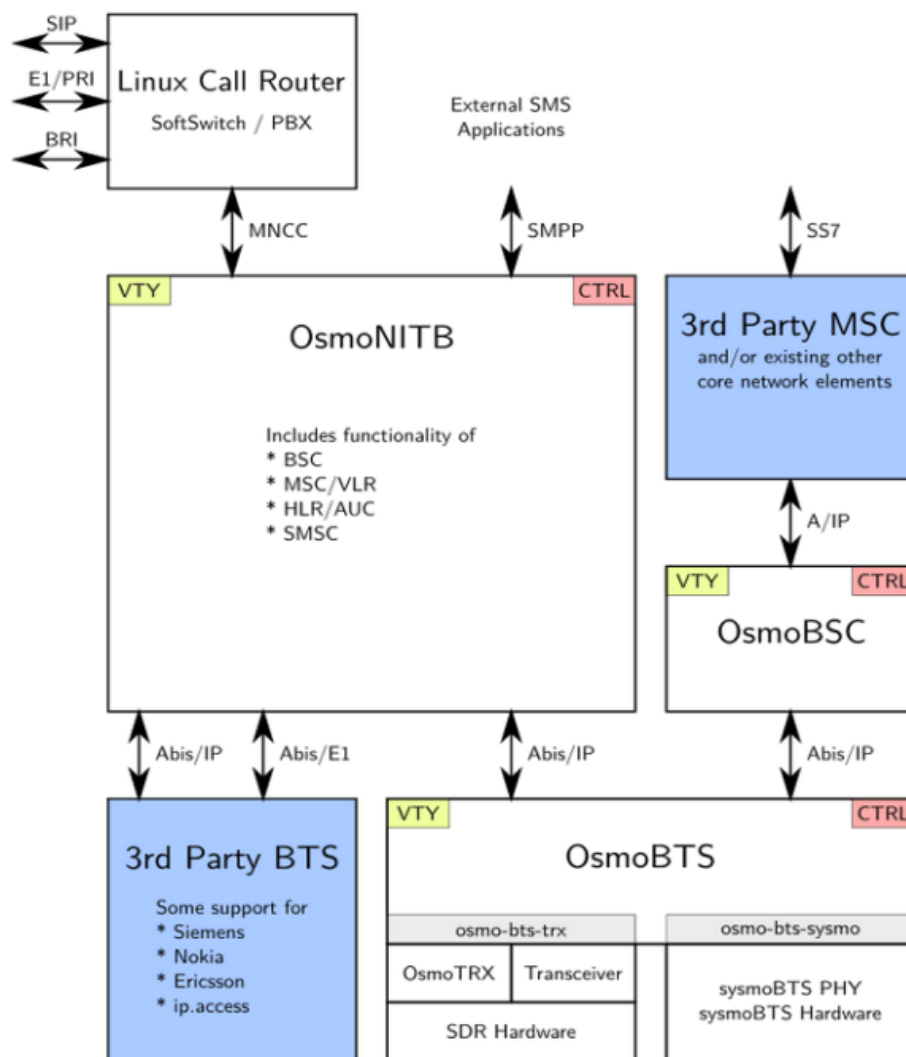


Fig.1

The developed physical models of GSM and LTE base stations allow us to make calls and connect to new subscribers from the existing standard equipment, as well as make calls through the SIP operator. The capabilities of the developed laboratory complex are not limited to the modeling of the above systems, they can also be used for the study of digital television systems (satellite DVB-S / S2, terrestrial DVB-T / T2 and cable DVB-C / C2 broadcast).

Literature

1. LimeSDR-USB User Guide [Электронный ресурс] / Myriad-RF– Режим доступа: http://wiki.myriadrfr.org/LimeSDR-USB_User_Guide – 2016.
2. Anthony Collins. All Programmable RF-Sampling Solutions.WP489 (v1.0.1) April 27, 2017.
3. Systems and Technologies of digital TV: навчальний посібник/ В.А. Лошаков, С.А. Сабурова та інш.; за заг. ред. проф. В.А. Лошакова. – Х.: ФОП Коряк С.Ф., 2019. – 416с. (ISBN 978 – 966 – 97643.

ДОСЛІДЖЕННЯ МЕТОДІВ КОНТОЛЮ ПОСЛУГ NB-IoT

Козубенко В.С., Сабурова С.О.

Науковий керівник – доц. Сабурова С.О.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. інфокомунікаційної інженерії
ім. В.В. Поповського,
тел. 38 (099) 529-65-31), vitalii.kozubenko@nure.ua

Using the NB-IoT standard provides improved indoor coverage and the ability to serve many low-traffic devices, especially those that are not too sensitive to delays. Narrowband IoT is converted to low-cost chipsets and devices and very low power consumption of these devices, which ensures long-lasting battery life

Стандарт NB-IoT був розроблений консорціумом 3GPP з урахуванням вимог, що пред'являються операторами: послуги IoT повинні передаватися за технологією передачі, відомої як «енергоєфективна мережу далекого радіусу дії» (Low-Power and Wide-Area, LPWA) і використовувати існуючу інфраструктуру операторів мобільного зв'язку - 4G. З точки зору універсальності, NB-IoT - це найкраще рішення LPWA для підприємств різних галузей, с допомогою якого можна підключати до мережі оператора лічильники комунальних послуг, датчики моніторингу, системи відстеження об'єктів і масу інших пристроїв. Однією з особливостей технології є можливість підключати до однієї соти базової станції до 100 тисяч пристроїв, що в десятки разів перевищує можливості існуючих стандартів мобільного зв'язку.

Використання низькочастотного діапазону дозволить забезпечити покриттям такі важкодоступні місця, як цокольні приміщення, підвали і т.д.

Технологія NB-IoT (Narrow Band IoT) зв'язку для Інтернету речей значно знижує споживання енергії кінцевими пристроями, забезпечує значно краще покриття і проникнення зв'язку, збільшує максимальну кількість підключених до мережі пристроїв.

Три варіанти розгортання «вузькосмугового NB-IoT» впливають на продуктивність не тільки для NB-IoT RAN (Radio access network; мережу радіодоступу в різних стандартах стільникового зв'язку), але і для одночасного розгортання і IoT, і MBW (mobile broadband, мобільний широкосмуговий доступ).

З точки зору мережі радіодоступу (RAN) існує три варіанти розгортання NB-IoT: варіант «всередині смуги», де NB-IoT розгортається всередині існуючого LTE спектра, використовуваного для надання мобільних широкосмугових (MBW) послуг; варіант «захищеної смуги» з використанням спектра по краях каналу (тобто в невикористаній частини спектра) існуючих LTE. Однак тут можливі перешкоди від суміжного

каналу на кордонах існуючих LTE базових станцій. «Захищені смуги» можуть бути використані без урахування потужностей основних базових станцій LTE); Третій варіант полягає в розгортанні NB-IoT з використанням присвоєння виділених частот (тобто «автономного» розгортання), а також використання сукупності різних виділених базових станцій спеціально для LTE iMBB. Два з цих варіантів підходять для розгортання в спектрі, який вже пройшов ліцензування.

Спеціально розроблені пристрої та датчики є основними компонентами в системах NB-IoT. Ці пристрої збирають інформацію з оточення і передають на базові станції NB-IoT або вузли передачі. Індивідуальні базові станції підключені до шлюзу IoT і серверів обласних додатків IoT для централізованого моніторингу та аналізу даних (рис.1).

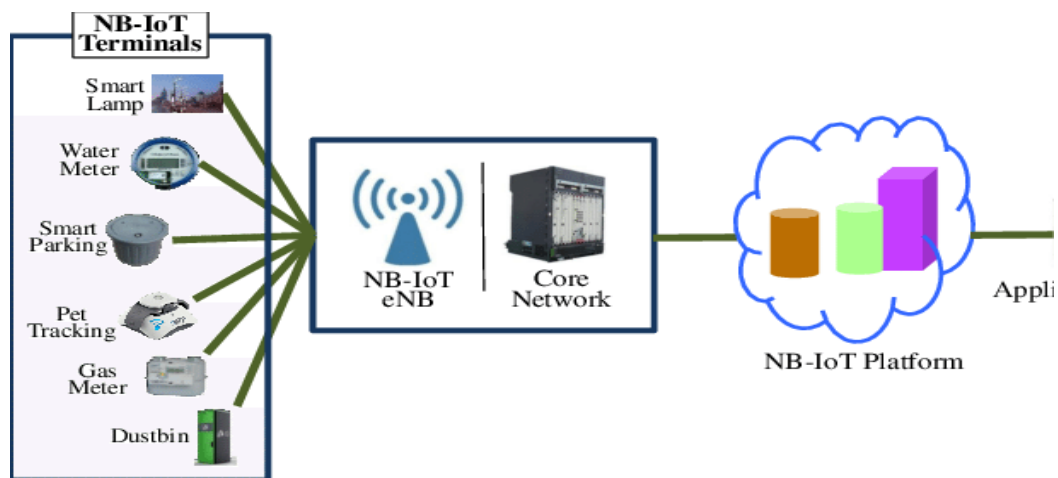


Рис. 1 Основні компоненти застосування NB-IoT

Висновки

Складні інструменти дослідження, аналізу та оцінки параметрів якості послуг NB-IoT дозволяють в режимі реального часу контролювати складну мережу за допомогою спеціальних мобільних додатків для зручності користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Багатоканальний електрозв'язок та телекомунікаційні технології (Ч.2) / Лемешко О.В., Лошаков В.А., Поповський В.В., Сабурова С.О., Епишкін С.О. – Х.: ТОВ «Компанія СМІТ», 2018р.р. – 482 с.
2. M. Satyanarayanan. Pervasive Computing: Vision and Challenges. IEEE Personal Comm. — 2001. Vol. 8, № 4. — P. 10–17.
3. M. Weiser, The Computer for the 21st Century. Scientific Am. — Sept 1991. Vol. 265, № 3. URL: <http://www.scientificamerican.com/article/the-computer-for-the-21st-century/> (датаобращення 15.03.15).

МОДЕЛЬ ПРИЙМАЛЬНОГО ТРАКТУ ПЕЛЕНГАТОРА

Білокурова А.О.

Науковий керівник – к.т.н, доц. Філіппенко О.І.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. ІКІ, тел. (057) 702-13-20)
e-mail:anastasiia.bilokurova@nure.ua

A model of the receiving path of the direction finder was proposed. To evaluate the adequacy of the solutions of the proposed model, a simulation of the system operation was performed using the Matlab/Simulink. In order to simplify the model and reduce the simulation time, certain assumptions were made - simulation just of the principle of processing of the received signal was performed.

Система радіопеленгації в основному є комбінацією антени та приймача, призначеної для визначення азимута віддаленого передавача [3]. Існують два принципово різних підходу до побудови приймального тракту. Це одноканальний приймальний тракт та багатоканальний. Побудова багатоканальних приймальних трактів пов'язана зі значними технічними проблемами, тому є значно дорожчими та складними у порівнянні з одноканальними.

У роботі було запропоновано модель приймального тракту пеленгатора. Для оцінки адекватності рішень запропонованої моделі було здійснено моделювання функціонування системи за допомогою пакету Matlab/Simulink. З метою спрощення моделі та зменшення часу моделювання були здійснені певні припущення - здійснене моделювання тільки принципу обробки сигналу, що підлягає аналізу. З моделі виключені гетеродини, перетворювачі частоти та фільтри проміжної частоти. Це не порушує адекватності моделювання оскільки усі частотні перетворення які використані у фізичній моделі необхідні для забезпечення селекції по сусідніх та дзеркальному каналах і здійснюють лише перенос спектру, але ніяк не змінюють спектральний склад та часові параметри сигналу, що обробляться. При створенні моделі здійснене припущення, що селекція сигналу, що підлягає аналізу вже здійснена.

Мета моделювання полягала 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 форми цього сигналу від співвідношення сигналу до шуму, що надходить з антени.

Антенний масив пеленгатора складається з 8 антен, які рівновіддалені відносно центру масиву. Для однозначного виміру фази відстань між окремими антенними елементами повинна бути менше половини довжини хвилі прийнятого випромінювання.

При побудові моделі системи кількість антен решітки було зменшено до чотирьох. Це зроблено з метою спрощення моделі. Сигнал формується за допомогою наступних модулів: Sine Wave – генератор синусоїдального сигналу призначений для формування сигналу; Gaussian Noise Generator – генератор шуму, що дозволяє імітувати ступень спотворення сигналу шумами; Gain1 – підсилювач, який призначений для регулювання потужності вхідного сигналу; Gain2 – підсилювач, який призначений для регулювання потужності шуму; Adder – суматор, що здійснює змішування сигналу та шуму, Score1 дозволяє контролювати форму вхідного сигналу.

Для плавного руху віртуальної антени треба послідовно змінювати амплітуди сигналів з попарно сусідніх антен, що надходять до суматора. Задля цього до складу моделі включено розподільувач сигналів трикутної форми. До складу розподільувача входить генератор трикутного сигналу та лінія затримки зі зворотнім зв'язком.

Комутатор антен – це керований атенюатор сигналів антен змодельований за допомогою Dot Product модулів, які здійснюють керування амплітудою сигналів, що надходять з антен та суматорів. Після формування сигналу від антени з електронним обертанням, він подається на модуль фазового розрізнення, де відбувається виділення сигналу, який несе інформацію про фазовий зсув вхідних сигналів антен. Для цього застосовується сигнал від нерухомої антени. В результаті після проходження виділеного сигналу через фільтр нижніх частот залишається сигнал, що несе інформацію про напрямок приходу сигналу від джерела радіовипромінювання.

Головна мета моделювання є аналіз залежності вихідних сигналів від співвідношення сигнал-шум на вході системи та від типу вхідного сигналу.

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. З результату моделювання видно, що сигнали каналів обробки дуже малі і практично відсутні, присутні тільки сигнали, що здійснюють електронне обертання антен. Джерело випромінювання випромінює гармонійний сигнал. Вхідний сигнал не містить шумів, відповідно на моделі $\text{Gain1}=0$, $\text{Gain2}=0$. На Score8 видно присутність та фазове співвідношення сигналів комутації антен та сигналу на виході каналу обробки.

Джерела:

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

2. J.A. Tsai, R.M. Buehrer, B.D. Woerner, .Spatial Fading Correlation Function of Circular Antenna Arrays With Laplacian Energy Distribution., IEEE Communications Letters, VOL. 6, No. 5, May 2002.

IMPROVING THE QUALITY OF 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.

MIMO (multiple-in, multiple-out) technology have become increasingly common over the past several decades, with notable examples being Wi-Fi networks and cellular 3G / 4G LTE.

As a result of the use of multiple antennas, MIMO wireless technology is able to considerably increase the capacity of a given channel, the more antennas a system has the more simultaneous data streams can be transmitted at once, improving the radio link.

A broadband V/H dual-polarized antenna is proposed for mobile communication base stations. The dual-polarized antenna achieves a HPBW (half power beam width) of $^{\circ}$ for both VP and HP elements, a bandwidth of about 48% (1.7–2.75 GHz) for $RL > 15$ dB, and an isolation of 30 dB. The antenna gain is about 9 dB for both vertical and horizontal polarization. An eight-element V/H dual-polarized antenna array is also developed. The antenna array has a bandwidth of 45% (1.7–2.7 GHz) and an antenna gain of 16 dB for both VP and HP, which may find potential applications in GSM/UMTS/LTE base stations.

Nowadays, radio communication systems demands more and more spectral bandwidth for channels, and to achieve effectiveness of data transmission through these channels, certain techniques are required to utilize the available bandwidth well. MIMO is a favorable technique. Note that 2x2 represents antennas which are MIMO and dual-polarity at the same time. The possibility of increasing the capacity of radio channels is an important task [1-3]. One of the possible methods of increasing capacity is the use of dual polarization antenna transmitting and receiving (Fig. 1). Such antennas may be substantially, MIMO antenna. The example of such a MIMO radio channel is shown in Fig. 1.

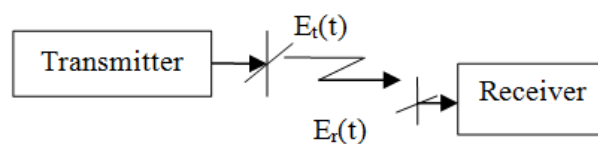


Fig.1. MIMO channel with dual polarization antenna

Dual-polarization is the ability for an antenna to function in two modes, known as vertical and horizontal polarization. A narrowband flat fading MIMO system is modeled as

$$Y = H \cdot X + n, \quad (1)$$

where – Y and X the receive and transmit vectors, respectively; H and n – the channel matrix and the noise vector, respectively.

Therefore, the use of principal component will find the transforming matrix to highlight the components of the information flow in the form

$$S(t) \Rightarrow \begin{pmatrix} S_1(t) \\ S_2(t) \end{pmatrix} = \vec{z}_{s_out_r}(t_i) = \begin{pmatrix} \vec{b}_1 & \vec{b}_2 \end{pmatrix}^T \cdot \vec{z}_{s_out}(t). \quad (2)$$

The main contribution of this work can be summarized in the following aspects, the proposed antenna focuses on the 5G, especially the special designed feeding structures allow the proposed antenna to out-perform other existing antenna on the whole compared with other designs, the proposed antenna satisfies the common requirement of mobile communication well and is more suitable for 5G application over the sub band .A large number of transmit antenna at a base station (BS) can remarkably improve performance Via increasing the multiplexing order to various human care IoT devices by higher degree of freedom and this performance analysis is achieved when various human care IoT devices are connected to network via a dual polarized massive MIMO.

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.

References:

1. Martynchuk A.A., Loshakov V.A., Oliver L.M. / Development of a transhorizon communication system based on dual polarization MIMO architecture // "Проблемы электромагнитной совместимости перспективных беспроводных сетей связи (ЕМС-2015). – Харьков: ХНУРЭ, 2015.
2. Larsson, E.; Edfors, O.; Tufvesson, F.; Marzetta, T. Massive MIMO for next generation wireless Systems. IEEE Commun. Mag. 2014,52, 186–195.

МОЖЛИВОСТІ ТЕХНОЛОГІЇ POWER OVER ETHERNET ПРИ МОДЕРНІЗАЦІЇ КОРПОРАТИВНИХ МЕРЕЖ

Мошенська Н.М.

Науковий керівник – доц., к.т.н. Харченко Н.А.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно-мережної інженерії,
тел. (057) 702-14-29)

e-mail: nataliia.moshenska@nure.ua

Power over Ethernet technology allows you to efficiently solve the power problems of wireless access points, CCTV cameras, IP phones, radio frequency identification (RFID) systems, etc. to deploy new networks and upgrade existing corporate networks. Power over Ethernet is a technology for the secure transfer of electricity and data using a “twisted pair”. The attractiveness and advantage of the technology lies in the fact that using only one set of wires for both data transfer and power supply reduces the time required to install the end systems and saves money on the cost of power cables and other components.

Тенденції появи нових послуг в сфері інформаційних мереж та швидкий розвиток технологій передачі даних роблять актуальним питання пошуку можливостей для впровадження нових методів та підходів для модернізації вже існуючих корпоративних мереж.

Традиційна мережа передачі даних передбачає наявність мережевого з'єднання та лінії електроживлення. Однак, застосування технології Power over Ethernet дає можливість використовувати лише один кабель Ethernet для передачі даних та живлення для пристроїв, які є елементами мережі Ethernet: бездротові точки доступу, камери відеоспостереження, IP-телефони, системи радіочастотної ідентифікації (RFID) тощо.

Power over Ethernet (PoE) – це технологія для безпечної передачі електроенергії та даних за допомогою «звитої пари». Умовами ефективної її роботи насамперед є щоб дані Ethernet та силова складова не заважали один одному, таким чином буде забезпечено одночасну передачу як даних так і живлення без будь-яких порушень.

Технологія PoE передбачає передавання електроживлення по «звитій парі» через роз'єм RJ45 відповідно до схеми розводки проводів, визначеної в стандарті IEEE 802.3 Ethernet через PoE сплітер на пристрої, які сумісні з PoE. Водночас мають місце втрати при передачі електроенергії. Стандарт IEEE 802.3af-2003 (PoE) забезпечує до 15,4 Вт постійного струму, але сумісний з PoE пристрій отримає лише 12,95 Вт. Однак цього достатньо для роботи таких мережевих пристроїв, як бездротові точки доступу, IP-телефони та елементів системи керування будівлі та контролю доступу. Оновлений стандарт IEEE 802.3at-2009 (PoE+) забезпечує до 25,5 Вт потужності для пристроїв. У 2018 році IEEE визначив стандарт 802.3bt, який вводить два додаткових типи живлення: до 55 Вт (тип 3) та до 90-100 Вт (тип 4).

Використання технології Power over Ethernet для модернізації вже існуючих корпоративних мереж має низку суттєвих переваг:

- застосування технології PoE значно спрощує та здешевлює модернізацію вже існуючої корпоративної мережі (за рахунок відмови від розгортання нових ліній електроживлення скорочуються витрати на придбання та прокладку кабелю);

- використання PoE дозволяє виконувати монтаж пристроїв в місцях, де організація нової лінії електроживлення викликає труднощі, наприклад, за підвісною стелею;

- застосування в корпоративній мережі робить можливим скорочення кількості кабелів та електричних розеток в серверній кімнаті або в комутаційній шафі;

- PoE дозволяє скоротити використання електророзеток і інших елементів енергомереж;

- PoE має підвищену експлуатаційну безпеку: стандарт IEEE 802.3af (PoE) і стандарт IEEE 802.3at (PoE +) забезпечують захист від короткого замикання, падіння напруги, перевищення споживаного струму тощо;

- простота розгортання мережі при модернізації, особливо в складних просторових умовах (дахи та зовнішні огорожі будівель, внутрішні приміщення в аеропортах і вокзалах, кафе, кінотеатри тощо);

- можливість виконувати керування електроживленням бездротових точок доступу, IP-телефонів, систем керування будівлі та контролю доступу з метою підвищення енергоефективності (відключення електропостачання певного ряду пристроїв, що підтримують технологію PoE після того, як користувачі мережі покинули приміщення за відсутності необхідності в цілодобовій наявності електроживлення для цих пристроїв).

На сьогоднішній день найбільш перспективними в області корпоративних мереж є бездротові технології стандарту 802.11. Так як переважна більшість пристроїв, що потребує підключення, є мобільними, необхідність у повному покритті зони обслуговування мережі становиться основним питанням при модернізації. Вагомий вклад при цьому має технологія Power over Ethernet. Її переваги дозволяють спростити етапи модернізації на рівні структурованої кабельної системи існуючих корпоративних мереж, так і для розгортання нових інформаційних мереж.

Список використаних джерел

1. Стандарт IEEE 802.3af
2. Федоров, А. Новые возможности Power over Ethernet / А.Федоров / Компоненты и технологии. - 2008. - № 83. - С.86-88.
3. Тестирование систем с поддержкой питания через Ethernet (PoE) [Електронний ресурс] - Режим доступу: <http://oskc.ru/?%20p=5687>

ANALYSIS OF THE COVERAGE AREA OF THE ACCESS POINT USING NETSPOT SIMULATION

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 research aims to map the territory of blankspot on that location, so that it can be used as a reference for optimizing the placement of access points. The research method used was the experiment through the drive test using Nestpot software. The analysis performed includes: Signal level, Signal-to Interference ratio, and Quantity of Access point. Experimental results indicate the quality of the reception on location observed is not the same, some point receive very strong signals from more than one access point, while some other point still entered into the realm of blankspot. Of research results also gained some room located near some of the access point are having Signal to Interference Ratio.

Currently the ease of accessing the internet has become a fundamental requirements primarily a college surroundings. The requirement to always be connected to the internet network is seen with the growing number of access points that are installed to meet these needs. Installation of the access point is often not structured properly so that the area of scoped in the area of coverage is uneven. On the research of the simulation is done against the signal strength of the access point toward the receiver Wi-Fi in the room and the room of the student learning lecturer electrical engineering building 3 and 4 floors.

The current utilization of access to internet network is already widely used. Request student and lecturer for the always connected to the internet network on the rise. The number of access point installed should be able to meet the needs, but the reality that there are currently mounting point of the access point was not arranged properly, so that the laying on of access point at some locations are outside the range of the area. In line with the development of many current technologies utilized for communication through the medium of the internet. The current wireless network has been developing very rapidly with the latest technology refers to the IEEE 802. 11n [1]. At this time there have been many schools, colleges and agencies that utilize wireless networks. In planning a wireless network we need to know the condition of the room as well as a place to placing the access point to work optimally, and every client in every room can capture the signals properly.

This research was conducted to analyze wireless network in the building of the lecture with attention to parameters: Signal level, Signal-to-interference ratio, Quantity and access point. The methods used in this research is a method of experimentation through a test drive using Netspot PRO Software. Nespot PRO serves as the scanning software used for Wi-Fi networks with the primary SSID parameter and can keep track of the strength of the signal. Signal Level

Signal strength can make quality reliable network, the signal level on a wireless reliability can be measured by knowing the value of a quantity specified dBm when scanning for Wi-Fi. The more positive approach the dBm value then the signal is getting good and reliable. Data retrieval is performed for 3 times and the average was taken. The results signal level from the SSID on every space lecturer FPTK electro 3rd floor can be seen in figures 1-2.

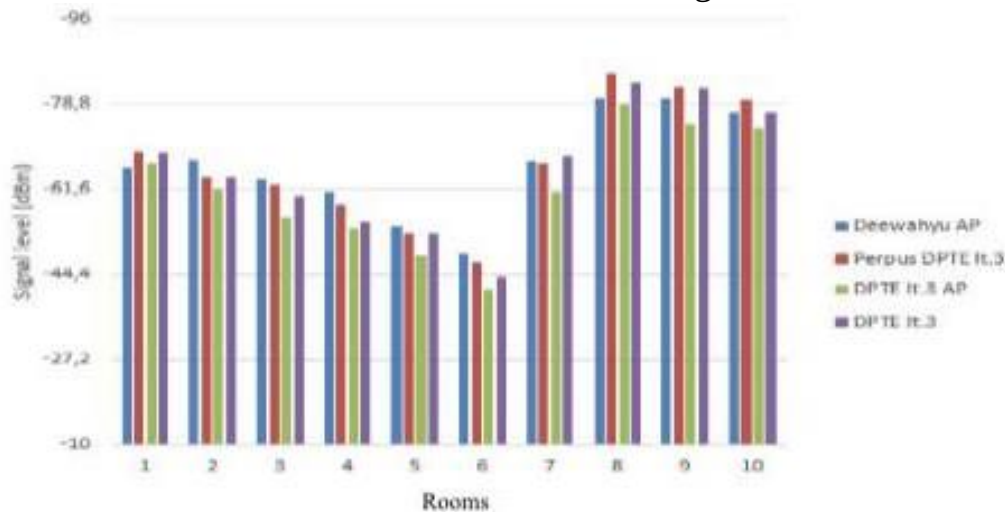


Fig. 1. Comparison of the Signal level from the SSID on every space Lecturer Electro floor 3

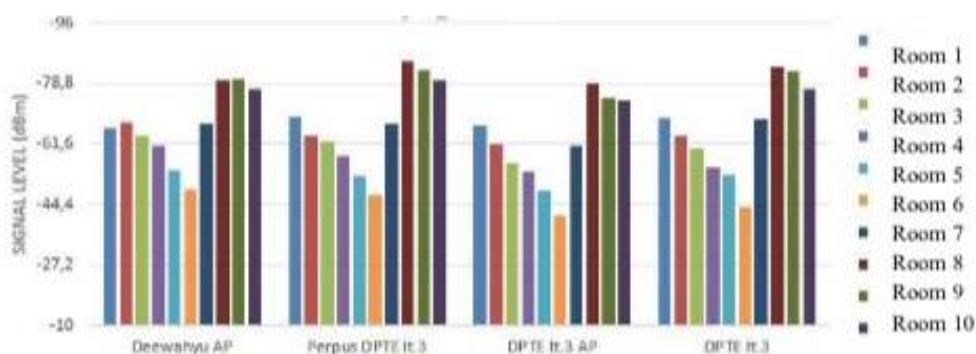


Fig. 2. Comparison of the Signal Level of the Lecturer FPTK Spaces Every third floor to a different SSID

Based on testing and analysis that has been done on this research, the following conclusions can be drawn: Based on the results of the simulation are represented on the graph can be known that the signal level on the 3rd floor is uneven for the entire space, there is a buildup of electrical lecturer SSID on the one room that causes beberapa other blankspot.

Reference:

Martynchuk A.A., Loshakov V.A., Oliver L.M. / Development of a transhorizon communication system based on dual polarization MIMO architecture // "Проблемы электромагнитной совместимости перспективных беспроводных сетей связи (ЕМС-2015). – Харьков: ХНУРЭ, 2015.

CCTV – LAMP CAMERA FOR SMART HOME SOLUTION

Reginald Tannor

Scientific Supervisor – Prof. Martynchuk A.A.

Kharkov National University of Radio Electronics,

Infocommunications Department,

Nauky Ave. 14, Kharkiv, 61166, Ukraine, e-mail: tannorreginald@gmail.com

The report contains the results of a study of the communication quality parameters of a remote wireless channel for controlling a lamp as a remote access for monitoring the security status of a home, workplace or company. Closed Circuit Television Cameras (CCTV) have become an important crime prevention and security measure. Cameras collect images and transfer them to a monitoring-recording device where they are available to be watched, reviewed and/or stored.

CCTV is a situational measure that enables remote surveillance of a locale. This makes it possible for the police and other law and regulatory agencies such as private security to respond to incidents when alerted and to have information about what to look for when they arrive. The storing of images facilitates post-incident analysis that may be helpful to an investigation. There are many different types of CCTV systems and they have different capacities to meet a variety of objectives.

Despite the tendency within the criminological literature to discuss CCTV as if it were a single measure, CCTV systems can differ quite markedly. Cameras can be: static (focusing on a single view); able to pan, tilt and zoom (moved by operators or placed on ‘tours’ to survey a succession of scenes); fixed (permanently installed in one location); redeployable (moved around power points within an area); mobile (placed in vehicles and transported to where they are needed).

Speaking as correctly as possible, the camera in Figure 1 does not transmit video, but allows remote viewing of video in online mode. Viewing video from the camera is possible from almost any modern mobile device (smartphone, tablet). The principle of transmitting data to the Internet is very simple, the camera connects to a wireless WiFi network (with Internet access), after which video viewing from the camera becomes available. Thus, the router to which this camera is connected becomes a “gateway” to the Internet and makes it possible to remotely work with the camera. Access to the camera from mobile devices is possible through the free icsee or xmeye application. This application is free and available for owners of Android phones, as well as for owners of phones with iOS. The camera works according to the P2P principle, while connecting to this Wi-Fi camcorder can be carried out in two options - either directly or via the Internet (using a Wi-Fi network).



Fig. 1. Panoramic IP Wi-Fi Camera Fisheye Light Bulb

The camera will be an excellent assistant and an unobtrusive observer in a situation when you need to observe a person, be it an elderly person, a child, a nanny, a housekeeper or colleagues at work. Moreover, this camera can be an excellent means of protection against burglars. Not every robber will immediately determine that this lamp is not just a lighting lamp, but also has a camera. In this case, as soon as the camera detects movement, you will receive a notification in the application and you can call law enforcement agencies to prevent robbery. In view of the widespread use of smartphones and tablets, this camera will be very useful for young parents, who often, in addition to caring for the child, are engaged in other important tasks. With this camera, you can constantly monitor whether the child is sleeping or not, and what happens to him at all directly from your smartphone anywhere in the house. Simply put, if you are looking for an inexpensive camera with a panoramic view, then this panoramic IP Wi-Fi fisheye camera will pleasantly please you with its capabilities.

They can transmit analog or digital images via cable or wireless links. The images can be recorded in different ways with different implications for quality. The many methods of storing and manipulating images have different implications for the type and speed of monitoring that can be carried out. The availability of specialized uses such as number plate and facial recognition has generated yet more potential applications of this flexible technology

ДОСЛІДЖЕННЯ МЕТОДІВ ОПТИЧНОЇ РЕФЛЕКТОМЕТРІЇ

Колтаков О.А.

Науковий керівник –доц. Ковальчук В.К.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. ІКІ ім. В.В. Поповського тел.70 21 320)

e-mail: oleksandr.koltakov@nure.ua, тел. (050) 030-59-12

OTDR measurements are an essential component of the work carried out during the installation and operation of fiber-optic communication lines. With their help, the quality of the optical lines is determined. One of the main advantages of an OTDR is that it can be used to test fiber from only one end, according to the principle of a radar system. The principle of operation Optical Time Domain Reflectometer is based on measuring the power of light radiation.

Рефлектометричні вимірювання є важливою частиною робіт, що проводяться при монтажі волоконно-оптичної лінії зв'язку. За видами рефлектометри поділяються на: релеєвський, бріллюєновський, поляризаційний, рамановський.

Метою даної роботи є аналіз видів та методів оптичної рефлектометрії, їх основних параметрів, розрахунок динамічного діапазону релеєвського рефлектометру.

До основних параметрів оптичних рефлектометрів належать: динамічний діапазон (дБ), мертва зона (м) та порогова потужність.

Один з найбільш важливих параметрів рефлектометру є динамічний діапазон. Він показує максимальну довжину волокна, яку можливо виміряти з максимальною амплітудою. Для оцінки динамічного діапазону необхідно знати час усереднення імпульсів t , період їх слідкування T та тривалість імпульсів τ .

Динамічний діапазон рефлектометру визначається як:

$$D_{rms} = \frac{P_c - P_{ш}}{2} \quad (1)$$

А розраховується за формулою:

$$D_{rms} = \frac{P_c - \eta + q - P_{np} + 10 \lg \sqrt{\frac{0.9t}{T}}}{2} \quad (2)$$

де P_c - потужність, розсіяна назад до початку волокна, $P_{ш}$ - еквівалентна шумова потужність на вході фотоприймача, P_v - потужність джерела випромінювання, η - втрати у відгалужувачі, q - коефіцієнт зворотного релеєвського розсіювання, P_{np} - порогова чутливість фотоприймача.

Мертва зона характеризує часове «осліплення» фотодетектора при потраплянні на нього великої відображеної потужності.

Порогова потужність зростає зі збільшенням ширини спектру лазерного джерела. Більш точніші випромінювачі мають більшу ширину спектру. На рис. 1 наведені результати розрахунку динамічного діапазону.

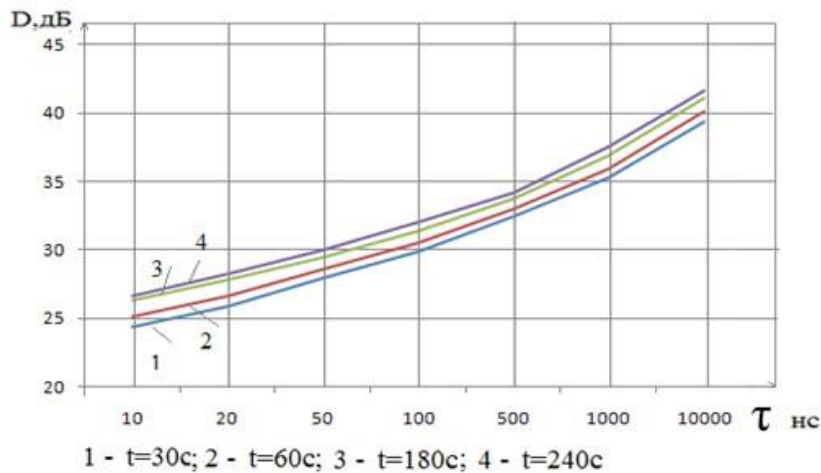


Рис. 1 - Залежність динамічного діапазону від тривалості імпульсу та часу

З наведеного графіку видно, що зі збільшенням тривалості імпульсу і часу усереднення сигналу зростає динамічний діапазон. Такий великий динамічний діапазон досягається, за рахунок збільшення енергії імпульсу.

Релеєвський рефлектометр найбільш поширений. Він використовується на всіх етапах будівництва та експлуатації волоконно-оптичної лінії, та дозволяє визначити місця обриву і дефектів волокон. Також дозволяє отримати графічне представлення стану лінії при фіксуванні потужності зворотного відображеного світлового потоку лінії.

Бріллюєновський рефлектометр дозволяє виміряти натяг в оптичних волокнах – основний параметр терміну служби оптичного кабелю. Головною відмінністю бріллюєновського розсіювання від релеєвського є те, що викликають його акустичні неоднорідності які є рухомими.

Поляризаційний рефлектометр використовується для вимірювання розподілу довжини биття вздовж волокна. Від традиційного OTDR відрізняється тим, що на виході лазера встановлений поляризатор, а на вході в фотоприймач встановлений аналізатор стану поляризації відображеного від волокна випромінювання.

Рамановський рефлектометр використовується в системах з WDM. Він дозволяє проводити вимірювання на різних довжинах хвиль. Для фільтрації рамановського розсіювання від загального випромінювання, яке розповсюджується вздовж волоконної лінії, використовується тонкоплівковий фільтр.

Вибір рефлектометра для вимірювання тої чи іншої волоконно-оптичної лінії визначається її технологією та необхідністю вимірювання стану лінії.

Перелік посилань:

1. Хамадулин Э.Ф. Основы Радиоэлектроники: Методы и средства измерений. Москва, 2018 – 365 с.
2. Портнов Э.Л. Волоконная оптика в телекоммуникациях. 2018. – 392 с.

АНАЛІЗ СИСТЕМ МОНІТОРИНГА В СИСТЕМАХ WDM

Лаптів П.О.

Науковий керівник - старший викладач кафедри інфокомунікаційної інженерії імені В.В.Поповського Ковальчук В.К.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії імені В.В.Поповського)

e-mail: pavlo.laptiev@nure.ua, тел. (099) 680-15-23

The given work is devoted developments in the field of fiber networks and in monitoring systems. One of the most important tasks in transport networks, this is maintaining the characteristics of fiber and other optical elements at the proper level. Monitoring systems allow continuous monitoring. Different algorithms can describe monitoring. Monitoring has different modes. The presented algorithm is associated with the observation mode. The proposed algorithm helps to understand the principle of operation of this mode. This mode already exists in one of the specialized programs.

Проблема надійності волоконно-оптичних мереж і систем з оптичним мультиплексуванням охоплює широке коло питань і по своїй суті є комплексною. Її рішення вимагає застосування відповідних методик контролю і оцінки стану всіх оптичних пристроїв. Особливістю систем з WDM є можливість мультиплексування десятків і навіть сотень оптичних сигналів, кожен з яких передається на відведеній йому довжині хвилі в єдиний мультиплексний сигнал, при цьому рознос по довжині хвилі може не перевищувати декількох десятих нанометра. У таких системах використовуються оптичні підсилювачі, тому необхідний контроль шумових параметрів.

Одне з найважливіших завдань - підтримання характеристик волокна і інших оптичних елементів на належному рівні. Саме тому системи безперервного моніторингу оптичних волокон набувають особливої значущості. Моніторинг забезпечує безперервний контроль стану активних каналів за допомогою відповідних наборів тестів, дозволяє виявляти різні відхилення в характеристиках оптичних елементів мережі, які, в свою чергу, можуть вплинути на її працездатність. Моніторинг дає можливість визначати поточний стан системи, а також дає можливість аналізу цього стану. Завдяки цьому можна запобігти виходу системи з ладу і не допустити погіршення показників якості системи.

Існує кілька методик моніторингу: моніторинг активних волокон, моніторинг з використанням каналу контрольного оптичного каналу, моніторинг з використанням одного з робочих каналів, моніторинг з використанням систем дистанційного тестування. Моніторинг можна організувати, як і на активних схемах, так і на пасивних. Активні і пасивні схеми складаються з пасивних мультиплексорів і демультиплексорів. Різницею між ними є ряд недоліків і особливостей підключення. Основний

недолік пасивних схем це - виділений канал з невеликою потужністю, який несе в собі відповідь на задані тести. Дана проблема призводить до необхідності додаткових розрахунків з урахуванням різних похибок.

У даній роботі був розроблений алгоритм, схема якого показана на рис.1, для тестування волокон активної схеми.

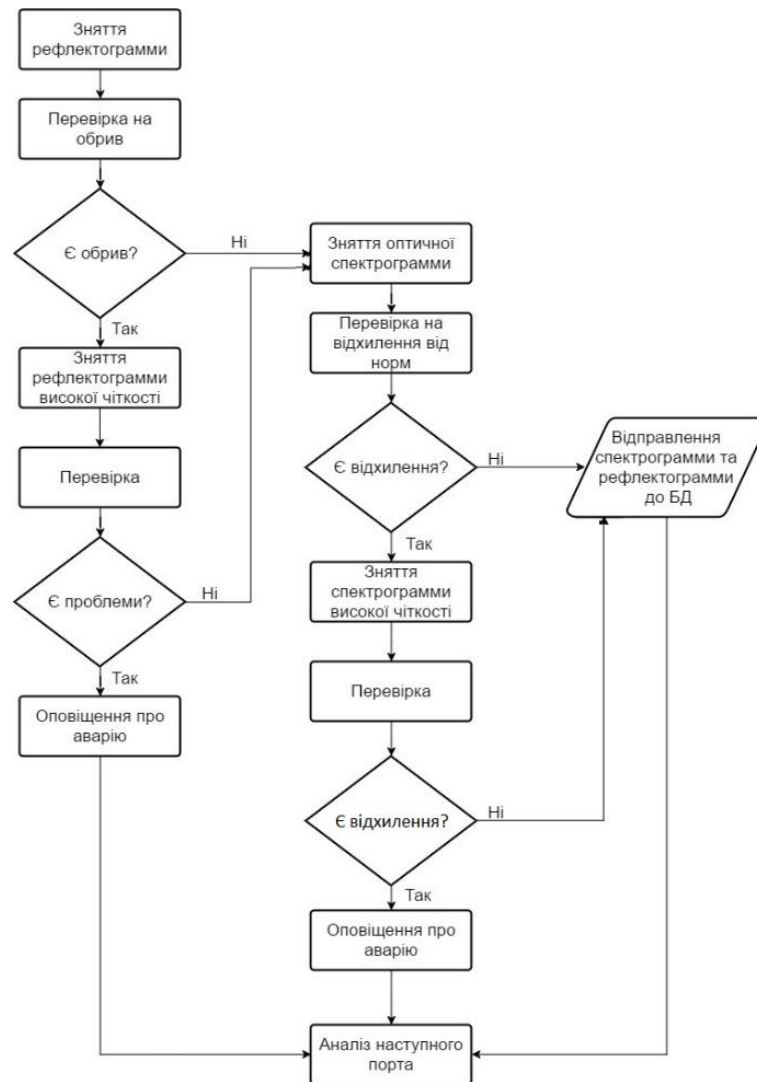


Рис 1. Алгоритм моніторингу

Даний алгоритм пов'язан з програмою-клієнтом, він дозволяє проконтролювати і відстежити процеси які відбуваються у волокні під час його експлуатації, а також дає можливість накопичення банку даних.

Список літератури

1. Хмелев К. Ф. Основы фотонного транспорта / К. Ф. Хмелев. – Киев: Техника, 2008. – 678 с.
2. Мониторинг ВОЛС [Електронний ресурс] – Режим доступу до ресурсу: https://iron-harry.ua/monitoring_VOLS/

ХМАРНА АТС НА БАЗІ СИСТЕМИ ВІРТУАЛІЗАЦІЇ

Циліорик В.Є.

Науковий керівник – к.т.н., доц. Токарь Л.О.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інфокомунікаційної інженерії
ім. В.В. Поповського, тел. (057) 702-13-20)
e-mail: v.foxgate@gmail.com

An overview and comparison of the dedicated virtual servers with the services of operators and providers is conducted. The main tasks in the development of cloud PBX on virtualization systems are highlighted. A network model and a model for setting up the PROXMOX VE virtualization environment are developed. The performance of the developed model on the dedicated virtual server is analyzed.

При використанні хмарних АТС, на ринку пропонується готові рішення, які вимагають додаткові витрати. В даній роботі віртуальна АТС розглянута не як додатковий сервіс, а як окрема конфігурація виділеного сервера. Таким чином поєднуючи всі переваги хмарних технологій і систем віртуалізації, залишаємо гнучкість і повну доступність для налаштування конфігурацій.

Віртуальна АТС Asterisk для офісу є найкращим і оптимальним рішенням для середнього та малого бізнесу. Будучи безкоштовним програмним забезпеченням, він підтримує безліч VoIP протоколів і всіма функціями класичної міні-АТС. Asterisk працює на низькому рівні під операційною системою Linux

Надання хмарних АТС — лише один із напрямів розвитку проектів систем віртуалізації. Вони дозволяють поєднувати переваги інтернет-сервісів з простотою класичної телефонної станції. Основна частина заліза функціонує на стороні сервіс-провайдера, а клієнт отримує послугу в чистому вигляді. Телефонним апаратом у віртуальній АТС може бути як фізичний телефон з підтримкою VoIP, так і додаток, запущене на чому завгодно. Підтримка протоколу SIP з'явилася ще в четвертій версії Android, тому дзвінки через віртуальну АТС можна робити зі смартфона. Управління хмарної АТС виконується через веб-інтерфейс, а значить з будь-якого пристрою підключеного до інтернету.

Практичне значення роботи полягає у веденні в експлуатацію хмарних АТС не вдаючись до послуг операторів та провайдерів, за допомогою відкритого програмного забезпечення Asterisk і системи віртуалізації PROXMOX VE. При використанні контейнерів LXC для Asterisk, на виході вийде досить мобільна, компактна і сучасна АТС, яка споживає в спокої 100-220Мб ОЗУ.

В роботі проведено огляд та порівняння виділених віртуальних серверів з послугами операторів, провайдерів. Виділено основні завдання

при розробці хмарової АТС на системах віртуалізації, розроблено програмно-апаратну модель виділеного серверу, середовища віртуалізації PROXMOX VE. Проведено аналіз ефективності розробленої моделі на виділеному сервері.

Апаратна та програмна складова включає наступні елементи: виділений сервер; система віртуалізації PROXMOX VE; віртуальна АТС Asterisk, програмне забезпечення для навантажувального тесту SIPP.

Сервер, що генерує тестові дзвінки, розміщений на віртуальній машині. Сервер, що приймає дзвінки - фізичний сервер. Програмне забезпечення для навантажувального тесту SIPP підключено до сервера Asterisk, що генерує тестові дзвінки. Між серверами Asterisk був створений SIP-транк.

Моделювання реального навантаження включало обробку медіа потоку, переданого по протоколу RTP.

Результати аналізу демонструють, що хмарна АТС, встановлена на виділеному сервері, який має мінімальні параметри конфігурації і конкурентну ціну, здатна обслуговувати приблизно до 1900 паралельних розмов.

Медіапоток передавався в основному в одну сторону - в напрямку від SIPP сервера до сервера Asterisk. Однак він був безперервним, а не періодичним. Можна припустити, що в цілому створювана таким чином навантаження була не нижче тієї, що має місце при реальних розмовах.

Оцінити негативний вплив статистичних факторів, на достовірність отриманих результатів, в застосуванні до реальних навантажень важко, проте припустимо, що взявши значний запас, можна цілком розраховувати на те, що для обслуговування 800-1000 паралельних дзвінків, описана конфігурація буде працювати якісно і надійно.

ЛІТЕРАТУРА

1. Баскаков И.В. IP–телефония в компьютерных сетях / Баскаков И.В., Пролетарский А.В., Мельников С.А., Федотов Р.А. – М.: Бином. Лаборатория знаний, Интернет–университет информационных технологий, 2008. – 226 с.

2. Гольдштейн А.А. Справочник по телекоммуникационным протоколам. Протокол SIP. / Гольдштейн А.А. – М.: Санкт-Петербург: БХВ–Петербург, 2014. – 348 с.

ANALYSES OF EUROPEAN CYBERSECURITY FRAMEWORKS

Maryna Yevdokymenko, Sebastian Floderus,

Linus Rosenholm, Vincent Tewolde

Kharkiv national university of radio electronics

(61166, Kharkiv, Nauky ave,14, V.V. Popovskyy department of

Infocommunication engineering, phone. (057) 702-13-20)

e-mail: marina.ievdokymenko@nure.ua

The main purpose of the paper is to analyze the EU cybersecurity frameworks and policies, to compare the development strategies of European countries and Ukraine, to identify compatibility and gaps between them for further developing recommendations for creating a more reliable and safe ecosystem through integrating EU cybersecurity frameworks.

EU is developing a suite of European cybersecurity standards that aim to deter and respond to cyber-attacks which constitute an external threat to the EU and its partner states by producing practices and guidelines on how to implement and enhance security, how to prevent attacks and provide cybersecurity hygiene. The European Cyber Security Organization (ECSO), European Union Agency for Cybersecurity (ENISA), IoT Security Foundation are the leading organizations for providing businesses, companies, and individuals with best practices in area of the security. Collectively, such organizations provide Frameworks for exchanging cybersecurity information between stakeholders as well as establish regulatory documents such as the EU Cybersecurity plan to protect open Internet and online freedom and opportunity, National Information Security (NIS) directives, Principles for IoT Security, standards in support of the Cybersecurity Certification, etc. While they represent the emerging common practice, such frameworks and regulatory documents are relatively new for the Ukrainian businesses and individuals.

The purpose of the paper is to provide of strategic documentation and cybersecurity approaches of the EU frameworks for exchanging cybersecurity information with further using of European experience in cybersecurity practices to the business, legal regulatory bodies, government institutes of Ukraine, as well as to the scientific and educational institutions.

Implementation of these EU cybersecurity frameworks will contribute to the creation of a single secure digital ecosystem. To do this, consider the main European frameworks for cybersecurity:

1. *Cybersecurity Strategy interlinks: European Agenda on Security's, Digital Single Market Strategy and Global Strategy*, which describe EU's cyber ecosystem, EU Cybersecurity Strategy and their goals.
2. *Cyber Defence Policy Framework*, which connected with EU's Cyber Defence Policy Framework, cyber defence capabilities, as well as the protection of the EU Common Security and Defence Policy (CSDP)

communication and information networks, Permanent Structured Cooperation Framework (PESCO) and EU-NATO cooperation.

3. *EU's Joint Framework on countering hybrid threats*, which connected with studying cyber threats to both critical infrastructure and private users, highlighting that cyberattacks can be carried out through disinformation campaigns on social media.
4. *Network and Information Security (NIS) Directive*, which connected with a blueprint for a quick and coordinated response to a major attack, and for the swift implementation of the NIS Directive.
5. *EU cybersecurity certification framework*, which connected with the creation of tailored and risk-based EU certification schemes, because certification plays a critical role in increasing trust and security in products and services that are crucial for the Digital Single Market.
6. *European Union Agency for Cybersecurity (ENISA)* as one of the most important organization for ensuring a high and effective level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations

The main result of this paper is analyzing and comparing the development strategies of European countries and Ukraine, identifying compatibility and gaps between them and further developing recommendations for creating a more reliable and safe ecosystem through integrating EU cybersecurity frameworks.

References

1. <https://ec.europa.eu/digital-single-market/en/cyber-security>
2. Robert Ackerman. 2019. Too few cybersecurity professionals is a gigantic problem for 2019. Tech Crunch. Retrieved January 29, 2019 from <https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019>
3. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
4. S. N. Matheu, J. L. Hernandez-Ramos and A. F. Skarmeta, "Toward a Cybersecurity Certification Framework for the Internet of Things," in *IEEE Security & Privacy*, vol. 17, no. 3, pp. 66-76, May-June 2019. doi:10.1109/MSEC.2019.2904475

ACCESS TECHNOLOGIES FOR MACHINE TYPE COMMUNICATION NETWORKS

Eltayh Mostafa Tarek Ahmed

Scientific supervisor - PhD.Senior Researcher Kadatskaya O.

Kharkiev National University of Radio Electronic
(Infocommunication Engineering , 14. Nayku Ave.Kharkiev)
(057) 702-13-20)

E-mail: mahmoudsayed5197@gmail.com ; fax (057) 702-13-20

Machine-type communication (MTC) has it provides connections for of MTC devices, forming a basis for the Internet of things. Physical layer has a pivotal role in M2M communications. M2M should be made efficient enough in terms of its power consumption and spectrum utilisation for to accommodate a large number of MTC devices. In this work is studied the issues on PHY-layer designs relevant to M2M communications. We surveyed related research works based on MTC network designs and the issues in this respect.

For wireless communications, multiple access technology plays a critical role, which determines how a common medium is shared among users. To develop an optimal air interface supporting M2M traffic, there are numerous features that are unique in MTC, which should be taken into account. As the technical requirements specified in 3GPP LTE-A for the fourth generation of mobile networks and defined by the International Telecommunication Union, downlink data rates need to go up to 100 Mb/s for mobile devices and 1 Gb/s for pedestrian users, respectively.

Based on the vision as proposed by LTE-A (i.e., LTE release 12), HetNets help to enhance the wireless network performance in different aspects. Different transmission devices with different transmission powers and coverage distances between transmitters and receivers pose a big challenge to improve spectrum efficiencies and data transmission rates over different radio links. However, as the number of MTC devices increases, which come with an increasing demand on ubiquitous wireless coverage and high data rates for MTCs, cognitive gateways become an alternative [1]. The use of cognitive gateways in MTC networks promotes a better utilisation of the radio resources (such as an improved spectral reuse factor), because the gateways act as data aggregation points for lowpower and low data rate MTC devices. Nevertheless, the LTE-A standard only defines S1 interface and X2 interface back haul for macro-cells and picocells. For femtocells , it is preferred to use IP as a backhaul protocol .Nevertheless, the existing S1 and X2 interface backhauls in LTE-A do not serve well for the MTC networks, which carry heterogeneous network properties with different cell sizes (such as femtocells and small cells). For this reason, S1 and X2 will not be applicable for MTC, and thus, it is necessary to find a new air-link interface for small-cell environment, which is a vital issue in MTC.

Normally, the transmission links between MTC devices and gateways (also referred to as M2M device grouping issue) play an important role. Moreover, transmission technology from gateways to femtocell (or small-cell AP) is an open issue, which has not been well defined by either 3GPP or other standardisation bodies. Nevertheless, the interference problem caused by multiple paths in HetNets is in particular challenging. In the text followed, we will discuss the interference issues and propose some possible solutions to implement the air-links between MTC devices and gateways.

The macro-cellular networks in LTE are named as evolved NodeBs (eNBs). Using the same backhaul and access schemes as in macro-cells, a picocell is formed by a group of low-power nodes in HetNets. New Long Term Evolution (LTE)-Advanced features like enhanced inter-cell interference coordination (eICIC) and carrier aggregation (CA). Because of its transmit power ranging from 23 to 30 dBm typically, it covers a distance of 300 m or less for serving for a few tens of users [2]. Femtocell base stations are intended for indoor deployments with their transmit powers less than 100 mW (or less than 23 dBm) typically. They are used in indoor environments such as homes or enterprises, serving a dozen active users by using consumers' broadband connections, such as cable, fiber or digital subscriber line. We studied the issues on PHY-layer designs relevant to M2M communications. We surveyed related research works based on MTC network designs and discussed the issues in this respect. We gave a brief introduction to the major PHY characteristics of Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15.1), Zigbee (IEEE 802.15.4) and SUN (IEEE 802.15.4g) technologies.

In a multi-cell environment, a new air-link design based on CC-CDMA for gateways to small-cell APs (G2S) interface was suggested in this paper as a complement to existing technologies and standards. CC-CDMA was proposed as a candidate to overcome interferences occurred in G2S air-links. We also provided a review on the works on CC-CDMA via discussing the characteristics and properties of CCs.

We identified various challenging or open issues for the implementation of MTC in wireless communication systems.

References

1. 3GPP Organizational Partners: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for Machine-type Communications (MTC); Stage 1 (Release 11). In Technical Specification TS 22.368 V11.5.0, 3GPP Sophia Antipolis, France, 2012.
2. 3GPP Organizational Partners: 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on Provision of Low-cost Machine-type Communications (MTC) User Equipments (UEs) based on LTE (Release 12). In Technical Report TR 36.888 V12.0.0, 3GPP, AW – Oranjestad, 2014.

ANALYSIS OF GOALS AND TASKS OF FHRP IN MODERN NETWORKS

Олатунџи Джон

Olatunji John

Scientific Supervisor – Amal Mersni. PhD, Senior Lecturer of V.V. Popovskyy
Department of Infocommunication Engineering,
Kharkiv National University of Radio Electronics,
Infocommunication Faculty,
Nauky Ave. 14, Kharkov, 61166, Ukraine, e-mail: pemiolatumji@gmail.com

The object of study is to analyze the goals, tasks and performance of FHRP in modern networks.

The goal of the work is to study the impact of FHRP on modern networks.

Research methods- Analysis of standards and technologies.

Hops in networks occurs when a packet is passed from one network segment to the next [1]. If that first hop ever goes down, that particular network will become incapable to communicate to the outside world and only local communication across the switched domain will be possible.

The main goal is to improve throughput. It requires multiple routes or paths to divide the traffic or load distributed equally between the paths. [1] Load balancing is implemented to improve the redundancy and throughput.

To implement load balancing different routing protocols are used which equally distribute the traffic and utilizes the available bandwidth. In some cases, the term load balance can be used interchangeably with the load sharing

The first hop redundancy protocols include three protocols Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP). Each protocol has its own purpose and has its own advantages and disadvantages.

FHRP was developed to also reduce traffic loss. These protocols help particular organization to successfully send the traffic from source to destination without loss of many packets. In case of the failure of one system, there is a standby system which automatically activates itself and continues sending the traffic. The HSRP protocol and GLBP protocol are Cisco propriety whereas the VRRP protocol is the Institute of Electrical and Electronics Engineers (IEEE) standard. [2]

Operation

HSRP is a Cisco proprietary protocol that enables the network engineer to add more than one redundant device to achieve network reliability. The different routers in the HSRP group will communicate to select a single active router gateway that handles all the network traffic. When configuring a router to be an active router, the standby router at this point is also selected. Both the standby and the active router will communicate through sending a Hello messages and will detect if the active router fails. [2] When the failure occurs one of the

standby router take the duties of the active router with minimum delay and at the same time another standby router is selected.

VRRP is an open standard that can be used where the equipment of various companies exists. Its operation is nearly the same as that of HSRP but differs in a couple of ways. In VRRP, like with HSRP, a group of routers are configured in which the network engineer selects one master router and the other a backup router [2].

The physical IP address of the master router is used by the clients as a default gateway. The backup members of the VRRP group will communicate with the master gateway through hello messages and take over the duties of the master router when the master router goes down or some error occurs.

The IP address used always belongs to the master router which is referred to as the IP address owner. When the master router recovers from error it will again take its responsibilities back and will forward the network traffic itself.

To achieve load sharing between the routers along with redundancy, Cisco has a new protocol called the GLBP. It is a Cisco proprietary that improves the efficiency of the FHRP by allowing automatic load balancing. [2]

The current study specifically aims to answer following research questions: Which protocol is suitable according to a particular environment? How to effectively configure the protocols. How long would it take to changeover to the backup router?

Conclusion

FHRP is a cisco proprietary protocol which is the earliest First Hop Redundancy Protocol (FHRP). that provides backup to a network and it facilitates a successful transmission from source to destination. Also provide a load balancing facility.

Major Drawback of FHRP includes, it is a Cisco propriety hence it works on only Cisco devices. There is a high packet loss which is more compared to the other technologies. Also to enable the preemption it is to be configured manually every time. [2]

References

1. Performance Evaluation of First HOP Redundancy Protocols (HSRP, VRRP & GLBP) ; Zia Ur Rahman.
2. Chapter: FHRP - HSRP Multiple Group Optimization. Link https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/x-e-16/fhp-xe-16-book/fhp-hsrp-mgo.html

BASIC CONCEPTS OF: MPLS

Abdelfattah Mohamed

Scientific Supervisor – Amal Mersni. PhD, Senior Lecturer of V.V. Popovskyy

Department of Infocommunication Engineering,

Kharkiv National University of Radio Electronics,

Infocommunication Faculty,

Nauky Ave. 14, Kharkiv, 61166, Ukraine, e-mail:m.zaki178@gmail.com

The main objective of the thesis is to investigate and study MPLS (multi-protocol label switching), its background and technology basics, to define what is MPLS, its features and concepts.

MPLS (Multi-protocol label switching) is a technology that enables very fast switching of data. MPLS is packet forwarding method using labels to make data forwarding decisions. MPLS is used to connect one site to another, both sites are connected through a service router cloud on a private tunnel.

Unlike IP routers, packet forwarding is not based on source and destination addressing MPLS labels each packet with a unique label which connected devices checks, which allows faster and more efficient data transmitting.

As networks grow it required more efficient, faster solutions to forward data, MPLS was introduced to avoid delay as it forwards data using MPLS instead of IP address. Originally MPLS was used to allow core networking devices simpler, more efficient and faster packet switching method by simplifying the header. As MPLS is a “multi-protocol” it doesn’t specify one protocol which allows various types of data to be exchanged.

MPLS labels packets with different labels, first router does a normal routing lookup but instead of finding only the next hop it finds the final destination router and adds a “label”, since the path is pre-determined devices in the path uses the label to route the traffic without any extra IP lookup. When packet reaches its final destination router it removes the label then the packet is delivered using normal IP routing. [3]

MPLS offers some great features, one of its attractive features is interface independency which means each site can use different connection method than the other, for example one site can use T1 connection and the other can use fiber optic connection and MPLS connect them all together to communicate. Furthermore, MPLS is one to many, which allows networks to connect easily and expand, from a customer perspective MPLS provides full freedom and full control on the connection between sites.

Comparing to VPN technology MPLS is not cost beneficial as it's more expensive, on the other hand MPLS provides faster performance because there is no encryption to deal with also MPLS provides guaranteed quality of service as it is reliable and secure. [4]

MPLS concepts is divided in two parts Edge and Core, at edge the edge labels switch router (ATM switch or router) classifies packets and label them (Label Impastation). In core Label switch router (ATM switch+ Label switch or router) forward using labels, each label indicates service class and destination which is known as Label swapping or switching. At the other Edge the Edge label switch router is responsible for removing labels and forward packets (label disposition). This Label distribution provides the ability to setup bandwidth guaranteed paths in addition to providing fast and reliable data transmission. [1]

Conclusion

It can be concluded that Multiprotocol Label Switching (MPLS) enables Service Providers and customers a simple and efficient solution with its scalability and reliability. By allowing enterprises to expand their networks and by adding additional sites without any additional configurations and by its interface independency MPLS is considered a better choice for enterprises as it is more secure and reliable than VPN.

MPLS advantages:

- MPLS Label
- Quality of service
- Interface independence
- One to many

References

- [1] Steve smith. Introduction to MPLS.
- [2] Mayank Tripathi. MPLS explained.
- [3] Richard A Steenbergen. MPLS
- [4] CBT Nuggets. What is MPLS and How does it work?

ОЦІНКА ПОТЕНЦІЙНИХ МОЖЛИВОСТЕЙ БЕСПРОВОДНИХ СЕНСОРНИХ МЕРЕЖ СИСТЕМ ЗВ'ЯЗКУ 5G

Яценко С.В., Гнітецький В. А.

Науковий керівник – старший викладач Булашенко А. В.;
Київський політехнічний інститут ім. Ігоря Сікорського, м. Київ, Україна
(03056, Київ, пр. Перемоги, 37, каф. теоретичних основ радіотехніки)
e-mail: an_bulashenko@i.ua, 095-702-99-09

The traffic model takes into account the features of H2H and M2M traffic. The traffic model and its service systems make it possible to estimate the delay in message delivery from M2M devices, taking into account packet loss and retransmissions. This allows you to select communication network resources and parameters of M2M devices to ensure guaranteed quality of serviced.

Беспровідні сенсорні мережі інтенсивно розвиваються завдяки відносно низькій вартості, швидкості розгортання та можливості використання в місцях, де не можна розгорнути кабельні мережі. Вони є складовою частиною для майбутніх мереж 5G [1].

У таких мережах важливе місце має якість функціонування мережі, одним із ключових елементів якої є зв'язність. Під зв'язністю розуміють ймовірність доступності сенсорного вузла відносно інших вузлів. Він характеризується ймовірністю зв'язності, що виражає потенційну можливість доставки даних. Відсутність зв'язності призведе до часткового або повного порушення працездатності мережі.

Ймовірність зв'язності беспроводних сенсорних мереж з рухомими вузлами є складним, тому скористаємося наближеною оцінкою зв'язності через пропускну здатність [2]. Якщо пропускна здатність вище нуля, то зв'язність між вузлами існує. Залежність ефективної зв'язності від кількості транзитів n апроксимується

$$f(n) = \frac{1}{1 + n^\alpha},$$

де α – константа (прийняли $\alpha = 0.5$).

Залежність ймовірності зв'язності від швидкості руху вузлів апроксимується

$$p(v) = e^{-v/b},$$

де b – константа (прийняли $b = 5$).

Одержані залежності подані на рис. 1.

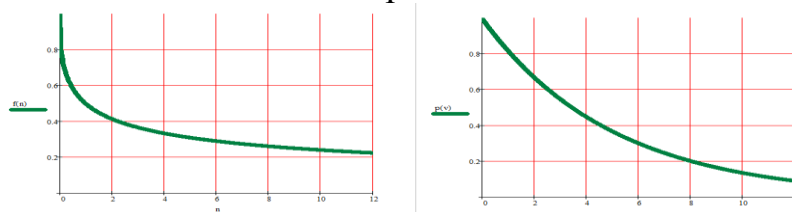


Рисунок 1

Таким чином, на основі отриманих залежностей сформуємо комплексний показник залежності від кількості транзитних вузлів та середньої швидкості руху вузлів

$$q(n, v) = f(n) \cdot f(v) = \frac{e^{-\frac{v}{b}}}{1 - n^a}.$$

Записаний вираз є функцією двох змінних, що подана на рис. 2.

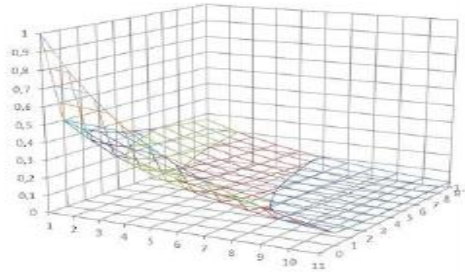


Рисунок 2

Використовуючи отримані залежності визначимо ймовірність ефективної зв'язності із врахуванням якості маршруту

$$p_{зв.эф.} = p_{зв} \cdot F(n),$$

де $p_{зв}$ – оцінка ймовірності зв'язності, $F(n)$ – функція розподілу довжини маршруту.

Звідси визначимо

$$n = \sqrt[a]{1 - \frac{1}{B_0}},$$

де B_0 – задане мінімально допустиме значення пропускної здатності маршруту.

Таким чином, показник ефективної зв'язності відображає потенційну можливість доставки даних між вузлами мережі із самоорганізацією з врахуванням необхідної кількості параметрів, що впливають на якість обслуговування трафіка. При використанні різних технологій побудови мережі ймовірність ефективної зв'язності може суттєво різнитися, оскільки вона залежить від якості маршруту та вимог до його якості, в то й час коли оцінка зв'язності буде однаковою, оскільки визначається лише потенційними можливостями встановлення з'єднання. Отже, з точки зору її потенціальних можливостей мережі буде більш інформативним використання показників ефективної доступності мережі.

Перелік посилань

1. Zhang Z. On Swarm Intelligence Inspired Self-Organized Networking: Its Bionic Mechanisms, Designing Principles and Optimization Approaches / Z. Zhang, K. Long, J. Wang, and F. Dressler // IEEE Commun. Surveys & Tutorial. – 2014. – Vol. 16, No. 1, pp. 513-537. DOI: 10.1109/SURV.2013.062613.00014.

2. Нуриллов И.Н. Эффективная связность беспроводной сенсорной сети / И.Н. Нуриллов, А.И. Парамонов // Электросвязь. – 2018. – №3. С.68-74.

ОЦІНКА ТРАФІКА M2M У МЕРЕЖАХ 5G

Демченко І.В.

Науковий керівник – старший викладач Булашенко А. В.

Київський політехнічний інститут ім. Ігоря Сікорського, м. Київ, Україна
(03056, Київ, пр. Перемоги, 37, каф. теоретичних основ радіотехніки)

e-mail: an_bulashenko@i.ua, 095-702-99-09

The work describes the estimation of M2M traffic in 5G communication systems. Features of M2M traffic should be considered when building traffic monitoring and network management systems. The proposed traffic model allows us to estimate the delay in message delivery from M2M devices, taking into account packet losses and retransmissions. The traffic model uses a combination of M2M and H2N traffic.

Бурхливий розвиток мереж зв'язку веде до збільшення їх потенційних можливостей у сфері обслуговування трафіка, що призводить до збільшення його об'ємів. Суттєвою складовою трафіка є Інтернет речей IoT, що використовує технологію M2M (machine-to-machine). M2M-комунікація вважається основним елементом в майбутніх системах [1-2].

Особливість трафіка M2M полягає в тому, що він формується великою кількістю пристроїв, які потенційно можуть сильно перевищувати кількість звичайних користувачів [3].

Залежно від технології, у безпроводних каналах використовуються протоколи керування доступом до мережі, що веде до затримки або повторної передачі пакету. Використовуємо модель обслуговування трафіка для загального середовища поширення сигналу (рис. 1). Модель трафіка враховує особливості трафіків H2N (human-to-human) та M2M [4].

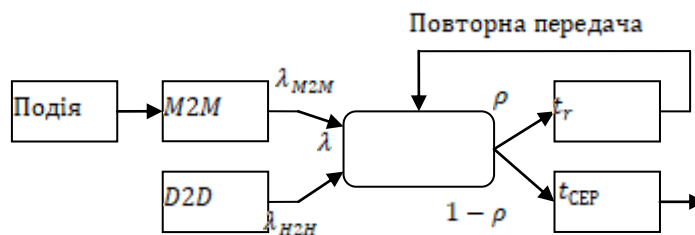


Рис. 1

Ймовірність доставки пакета із врахуванням багатократної передачі

$$p_d = 1 - p_0^k = 1 - \left(\frac{\rho_{BX}}{1 + \rho_{BX}} \right)^k,$$

де k – кількість спроб передачі пакета; p_0 – ймовірність зайнятості каналу.

Оцінка кількості спроб передачі каналу

$$k = \frac{\ln(1 - p_d)}{\ln(\rho)} = \frac{\ln(1 - p_d)}{\ln\left(\frac{\rho_{BX}}{1 + \rho_{BX}}\right)}.$$

Ймовірність того, що для доставки пакету необхідно k спроб передачі

$$p_k = (1 - p_0) \cdot p_0^{k-1} = (1 - \rho) \rho^{k-1}.$$

Середня кількість спроб передачі

$$k_m = \sum_{k=1}^{\infty} k p_k = \sum_{k=1}^{\infty} k (1 - \rho) \rho^{k-1}.$$

Залежність числа спроб передачі від інтенсивності навантаження та ймовірності доставки подана на рис. 2

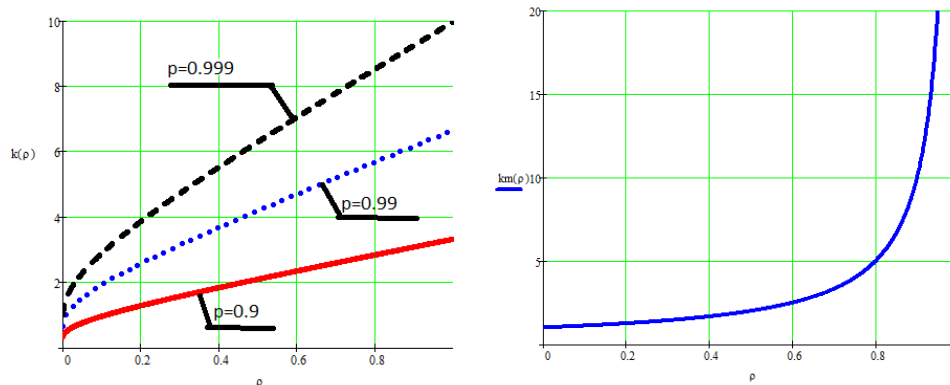


Рис. 2

Із рис. 2 та рис. 3 бачимо, що при досить високій ймовірності доставки, в області відносно малої кількості спроб передачі (до 5) використання каналу не перевищує 0.2. При більшому використанні каналу кількість спроб різко збільшується. Тому спроба передачі може розглядатися як проба стану каналу.

Таким чином, модель запропонованого трафіка дозволяє оцінити затримку доставки повідомлень від M2M пристроїв з врахуванням втрат пакетів та повторних передач. Це дозволяє обирати ресурси мережі зв'язку та параметри M2M пристроїв для забезпечення гарантованої якості обслуговування.

Перелік посилань

1. Ghavimi F. M2M communications in 3GPP LTE/LTE-A network: architectures, service requirements, challenges, and applications / F. Ghavimi, H.-H. Chen // IEEE Communications Survey and Tutorials. – 2015. – Vol. 17, No. 2. – p. 525–549. DOI: 10.1109/COMST.2014.2361626.
2. Парамонов А.И. Модели потоков трафика для сетей M2M / А.И. Парамонов // Электросвязь. – 2014. – № 4., С. 11-16.
3. Дао Ч.Н. Модели концентрации трафика M2M и оценка его влияния на QOS в сетях 5G / Ч.Н. Дао, А.И. Парамонов // Электросвязь. – 2018. – № 4. С. 47-54.
4. Gu B. Power control for cognitive M2M Communications underlaying cellular with fairness concerns / B. Gu, C. Zhang, H. Wang, Y. Yao, X. Tan // IEEE Access – 2019. – Vol. 7. – p. 80789-80799. DOI: 10.1109/ACCESS.2019.2914157.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

ОСОБЕННОСТИ ОЦЕНКИ ЧАСТОТЫ ОСНОВНОГО ТОНА ГОЛОСОВОГО СИГНАЛА ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ

Куценко Е.Е., Пастушенко Н.С.

Научный руководитель – к.т.н., проф. Пастушенко Н.С.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки, 14, каф. Инфокоммуникационной
инженерии, тел. (097)2332744
e-mail: Yehor.kutsenko@nure.ua

The security of financial, information and computing resources in modern computer networks largely depends on the quality of user authentication systems. One of the directions for improving the quality of authentication systems is the use of biometric features of the user. The most promising in terms of efficiency/cost are voice authentication systems. The scientific problem of improving the quality of voice authentication systems by using phase data of the voice signal is solved.

Современные информационные технологии и компьютерные сети пронизывают все существующие известные системы и связывают все государственные службы, науку, транспорт, связь, энергетику, оборону, здравоохранение, банковский сектор и промышленность. Опасность современных кибератак, воздействия которых приводят не только к материальным потерям, но и к экологическим, социальным, макроэкономическим потрясениям. Особенно велика опасность компьютерных атак для организаций и объектов жизненной важности.

Известно, что первым барьером в обеспечении безопасности компьютерных и информационных сетей разного назначения является система аутентификации пользователей [1]. Одно из главных направлений совершенствования современных систем аутентификации – использование биометрических признаков пользователя, и в первую очередь, его динамических (поведенческих) признаков [2, 3]. Наиболее интенсивно исследуемыми биометрическими системами аутентификации информационных сетей являются системы голосовой аутентификации (СГА), которые отличаются экономичностью, простотой и удобством использования. По критерию эффективность/стоимость это наиболее перспективные системы. Вместе с тем, как и все биометрические системы аутентификации, СГА имеют качественные показатели, которые не отвечают возрастающим требованиям к их характеристикам.

Современные СГА при формировании шаблона пользователя используют амплитудно-частотные данные его голосового сигнала [1]. Вместе с тем, известно, что наиболее информативным параметром, в том числе, и голосового сигнала, являются его фазовые данные [2, 3]. Поэтому в работе исследуется актуальная научно-техническая задача повышения

качественных характеристик СГА за счет использования фазовых данных голосового сигнала.

При формировании признаков шаблона широкое применение нашли следующие признаки голосового сигнала пользователя: частота основного тона, формантная информация, спектральные и кепстральные коэффициенты. Среди признаков особое место занимает частота основного тона (ЧОТ), которая позволяет дополнительно решать следующие задачи: распознавание эмоций, определение пола, сегментации аудио с несколькими голосами и разделения речи на фразы, определять патологические характеристики голоса в медицине и др.

Для уточнения величины и качества оценки ЧОТ предложено использовать фазовую информацию голосового сигнала и процедуры расчета кепстральных коэффициентов.

Методика проводимых исследований включала использование преобразования Гильберта для формирования квадратурной составляющей голосового сигнала на основе, которой формировались фазовые данные. Далее рассчитывались амплитудный и фазовый спектры, максимум которых, как правило, совпадает с ЧОТ (имеет значение в диапазоне от 50 до 400 Гц). Последующие процедуры связаны с использованием соотношений расчета кепстральных коэффициентов. Известно, что рассчитывается до сорока этих коэффициентов. Для этого используются семплы голосового сигнала в несколько десятков миллисекунд с перекрытием. Для выбранных семплов выполняется преобразование Фурье, спектр которого логарифмируется, а затем выполняется обратное преобразование Фурье. После выполнения последней процедуры можем оценить частоту максимума спектра – оценку ЧОТ. Таким образом, получим до сорока оценок ЧОТ. Далее выполняется статистическая обработка полученных результатов и уточняется оценка ЧОТ. Расчет кепстральных коэффициентов (частоты основного тона) выполняется как по амплитудной, так и по фазовой информации голосового сигнала. В заключение приводятся результаты моделирования, которые подтверждают адекватность и достоверность изложенного подхода.

Список литературы:

1. Beigi H. Fundamentals of Speaker Recognition. – NY: Springer, 2011. – 1029 p.
2. Oppenheim A.V., Lim J.S. The Importance of Phase in Signals: Article in Proceeding of the IEEE, 1981, t. 69(5), P. 529 - 541.
3. Пастушенко Н.С. Исследование информативности фазовых данных голосового сигнала пользователя системы аутентификации / Н.С. Пастушенко, В.Г. Педро, О.Н. Файзулаева [Электронный ресурс] // Проблемы телекомунікацій. – 2018. – № 1 (22). – С. 67 - 74. – Режим доступа к журн.: http://pt.nure.ua/2018/181_pastushenko_voice.pdf.

АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ І ПЕРСПЕКТИВА ВИКОРИСТАННЯ ПРОТОКОЛІВ У ГРУПАХ КОС

Кавуненко Я.О.

Науковий керівник – к.т.н., доц. Єпішкін С.О.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікацій, тел. (057) 702-55-92)
e-mail: yana.kavunenko@nure.ua

The given work is about researching of general weaknesses of protocols in braid groups.

Протягом декількох останніх років помітно зріс інтерес до криптографічних додатків, заснованих на перетвореннях в некомутативних групах. Групи КОС зокрема представляють особливий інтерес в силу своєї ефективності при забезпеченні трудомістких обчислювальних процесів. Різними групами дослідників були запропоновані протоколи з перетвореннями в групі КОС. У той же час можливості практичного застосування перетворень в групах КОС обмежені через недостатнє їх аналізу, як раз в криптографічних додатках. Метою цієї статті є розгляд і аналіз основних криптографічних перетворень і криптографічних протоколів в КОС групах, а також розгляду проблемних питань [1].

Коса з n -ламаних ниток – об'єкт який складається з двох паралельних площин P_0 і P_1 в трьохвимірному просторі R^3 , який складається з впорядкованої множини точок $a_1, a_2, \dots, a_n \in P_0, b_1, b_2, \dots, b_n \in P_1$ і з n -простих ламаних $l_1, l_2, \dots, l_n$, які не перетинаються між собою, перетинаючи кожену площину P_t між P_0 і P_1 і з'єднують точки $\{a_i\}$ з точками $\{b_i\}$ (рис. 1).

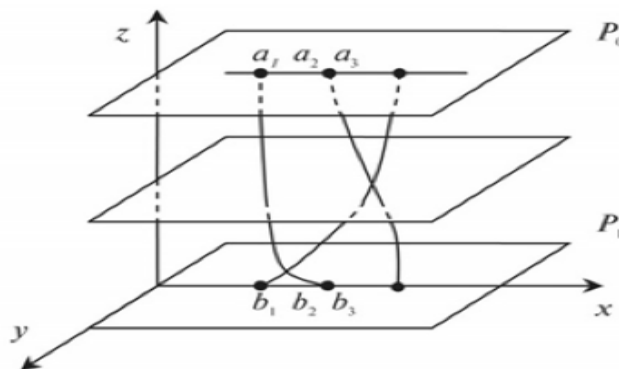


Рисунок 1 – Графічне представлення КОС

Фундаментальною в теорії КОС є теорема Артїна: група КОС B_n ізоморфна абстрактній групі, породженої утворювальними $b_1, b_2, \dots, b_{n-1}$, які задовольняють певним співвідношенням.

Грунтуючись на отриманих знаннях, були розглянуті наступні види криптографічних перетворень в КОС групах:

1. системи обміну ключами;

2. схеми шифрування / дешифрування;
3. протоколи аутентифікації;
4. механізм електронного цифрового підпису.

Стійкість криптосистем ґрунтується на наступних проблемах:

1. **Завдання пошуку сполучень (CSP):** нехай $(x, y) \in V_n V_n$ такі, що $y = a^{-1}xa$, де $a \in V_n$ або однієї з підгруп V_n . Завдання знайти таке b , що $y = b^{-1}xb$.

2. **Завдання одночасного пошуку безлічі сполучень (MSCSP):** нехай $(x_1, a^{-1}x_1a) \dots (x_r, a^{-1}x_ra) \in V_n V_n$ такі, що $y = a^{-1}xa$, де $a \in V_n$ або однієї з підгруп V_n . Завдання знайти таке b , що $y = b^{-1}x_1b = a^{-1}x_1a, \dots, b^{-1}x_rb = a^{-1}x_ra$.

3. **Завдання декомпозиції (BDP):** нехай $(x, y) \in V_n V_n$ такі, що $y = a_1xa_2$ для $(a_1, a_2) \in LB_n LB_n$. Завдання знайти $(b_1, b_2) \in LB_n LB_n$ таку, що $y = b_1xb_2$.

4. **Завдання одночасної множинної декомпозиції (MSBDP):** Нехай $(x_1, a_1x_1a_2) \dots (x_r, a_1x_ra_2) \in V_n V_n$ для $(a_1, a_2) \in LB_n LB_n$. Завдання знайти пару $(b_1, b_2) \in LB_n LB_n$ таку, що $y = b_1x_1b_2 = a_1x_1a_2, \dots, b_1x_rb_2 = a_1x_ra_2$.

5. **Завдання пошуку кореня (RP):** Нехай $x =$, де $a, x \in V_n$ та $p \in \mathbb{N}$. Завдання пошуку для експоненти p знайти таку косу $b \in V_n$, щоб $= x$.

6. **Завдання вибору пов'язаних елементів (CDP):** Нехай $(x, y) \in V_n V_n$. Завдання встановити, чи є x і y сполученими, тобто встановити, чи існує таке $a \in V_n$ або однієї з підгруп V_n , що $y = a^{-1}xa$.

Виходячи з вищенаведеного, існує три основні різновиди атак:

- 1) використання рішення задачі пошуку сполучень;
- 2) використання імовірнісного підходу в V_n ;
- 3) використання допоміжної групи, як правило, в уявленні Бурау [2].

Аналіз розглянутих криптографічних систем показує, що розробка алгоритмів, що використовують групи КОС є перспективним напрямком у розвитку криптографії. Основні характеристики систем наведені в таблиці 1.

Таблиця 1 – Основні характеристики криптографічних систем, що використовують групи КОС

Вхідне повідомлення, біт	$pn \log(n)$
Зашифроване повідомлення, біт	$4pn \log(n)$
Швидкість шифрування, операцій	$O(p^{2n} \log(n))$
Швидкість розшифрування, операцій	$O(p^{2n} \log(n))$
Довжина персонального ключа, біт	$0.5pn \log(n)$
Довжина відкритого ключа, біт	$3pn \log(n)$
Складність атаки «груба сила»	$((n/2)!)^p = \exp(0.5pn \log(n))$

Перелік посилань:

1. D. Garber, S. Kaplan, M. Teicher, B. Tsaban and U. Vishne, Length-based conjugacy search in the braid group, Contemp. Math. 418 (2006), 75–87.
2. E. Artin, Theory of Braids, Ann. of Math. 48 (1947) 101–126.

МЕТОДИ ТЕСТУВАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Стрілець А.М. Чернікова В.Г Скирда С.О.

Науковий керівник – док.т.н. Шостко І.С.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)

E-mail: andrii.strilets@nure.ua

This work is devoted to actual of choosing a method of testing information security tools. Because, at any stage in the life cycle of an automated system, be it design, configuration or operation, the administrator must know whether the system actually meets the required security level. The paper describes two methods of testing information security tools. And also we are talking about automated means of exploitation and their algorithm of work. The main tools of automatic information audit were also considered.

Останнім часом зростає значимість інформаційної безпеки, так як з'являється безліч незаконних способів отримання доступу до інформації. Тому, на будь-якому етапі життєвого циклу автоматизованої системи, будь то проектування, конфігурація або експлуатація, адміністратор повинен знати, чи дійсно система задовольняє необхідному рівню захищеності.

Існує кілька підходів до тестування безпеки системи. По-перше, можна провести ряд тестів на проникнення (пентестов), тобто, використовуючи всілякі утиліти, бази даних вразливостей і експлойтів спробувати отримати доступ до цільової системі, серверу, комп'ютера, обійти тестуючу програму. Перевага пентестов в тому, що їх проводять люди, відповідно, вони можуть в реальному часі приймати ті чи інші рішення, змінювати стратегії, засоби атак та інше. Однак, в цьому ж і недолік даного підходу - все залежить від компетентності тих, хто ці пентести проводить. Не можна після проведення ряду атак стверджувати, що система володіє потрібним рівнем захисту. Адже можливо, що просто були вибрані не ті засоби або використовувалися застарілі вразливості.

Другий метод полягає у відтворенні попередньо записаного трафіку комп'ютерних атак. Налаштовується спеціальний стенд, до якого підключається тестуюча система. Перевагою цього підходу є можливість забезпечення багаторазової повторюваності умов експерименту за умови, що трафік комп'ютерних атак кожен раз буде відтворюватися ідентичним чином. Відсутність у складі стенду реальних атакованих систем усуває проблему відновлення стану окремих його елементів після проведення атак. Але розглянутий спосіб тестування не дозволяє варіювати параметри атак (наприклад, кодування HTTP-запитів і використовуваний експлойтом shell-код) в процесі тестування, оскільки це вимагає серйозної модифікації вже сформованих пакетів мережевого трафіку.

Оскільки проводити тестування цільової системи вручну дуже складно, останнім часом стали з'являтися автоматизовані засоби експлойтинга. Такі програми дозволяють в автоматичному режимі виявити уразливості цільового хоста, а потім провести ряд атак для експлуатації цих вразливостей. Загальний алгоритм роботи таких засобів складається з наступних кроків:

1. Сканування портів і ідентифікація сервісів на досліджуваних об'єктах.
2. На основі бази знань висувається припущення про наявність вразливостей в виявлених сервісах.
3. Перевірка можливості експлуатації передбачуваних вразливостей.

Розглянемо найпопулярніші засоби автоматичного аудиту безпеки:

- Core Impact - це програмний продукт для проведення тестування несанкціонованих проникнень в систему. Перевіряє досліджувані системи на наявність вразливостей. За допомогою нього можна протестувати безпеку веб-додатків, мережевих систем, кінцевих пристроїв, мобільних пристроїв, бездротових мереж і т.д. Дозволяє моделювати багатоступінчасті атаки і взаємодіяти з успішно атакованою системою. Має свою БД експлойтів, яка щомісяця поповнюється власною командою розробників. З недоліків можна відзначити досить високу ціну;

- CANVAS / D2 / Nessus Bundle. Збірка CANVAS з D2 Exploit Pack інтегровані сканером виявлення вразливостей Nessus дозволяють досягти аналогічного підходу, закладеного в продукті CORE IMPACT. На відміну від свого конкурента, під платформу CANVAS, крім власних експлойтів, можливий імпорт сторонніх експлойтів. Це дозволяє CANVAS-у охопити набагато більше вразливостей для проведення атак в порівнянні з іншими рішеннями даного сегмента;

- SAINT Vulnerability Scanner & SAINTExploit. Аналог інтегрованого CANVAS і Nessus з тією лише відмінністю, що у SAINT Vulnerability Scanner і SAINTExploit один виробник. Функціональність же практично повністю ідентична.

За результатом аналізу можна констатувати, що на даний момент не існує комплексної методології проведення тестування на проникнення. Кожен з розглянутих методів фокусується на певних питаннях, і як наслідок, при проведенні комплексного тестування на проникнення неможливо повністю опиратись лише на одну методологію. Також є очевидно, що використання автоматизованих засобів тестування значно збільшує ймовірність успішного виконання тесту на проникнення.

Перелік посилань:

1. Автоматизований експлойтинг [Електронний ресурс].— Режим доступу до ресурсу: <https://www.securitylab.ru/blog/personal/evteev/13705.php>. (дата звернення: 10.02.2020).

КІБЕРБЕЗПЕКА ХМАРНИХ ОБЧИСЛЕНЬ ТА БАЗ ДАНИХ

Тертичний В.О. Куценко Є. Є.

Науковий керівник – док.т.н. Шостко І.С.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)

E– mail: vladtertychnyi@gmail.com

For any company, the most significant and valuable asset is data, since any possible data leakage can lead to the loss of critical important information, which will entail losses for the company. This means that its protection is one of the most difficult tasks facing the departments responsible for ensuring information security. The article describes methods for protecting cloud services and databases. Possible security threats in the area of cloud computing security and database protection were examined. It also considered recommendations for eliminating security threats in the field of cloud computing and also in the field of databases.

Захист баз даних є однією з найскладніших завдань, що стоять перед підрозділами, відповідають за забезпечення інформаційної безпеки. З одного боку, для роботи з базою необхідно надавати доступ до даних усім співробітникам, хто за службовим обов'язком повинен здійснювати збір, обробку, зберігання та передачу конфіденційних даних. Контроль і управління хмарами – є проблемою безпеки. Гарантій, що всі ресурси хмари порашовані і в ньому немає неконтрольованих віртуальних машин, не запусцене зайвих процесів і не порушена взаємна конфігурація елементів хмари немає. Основні відомі загрози для хмарних обчислень: труднощі при переміщенні звичайних серверів в обчислювальній хмарі, динамічність віртуальних машин, уразливості всередині віртуального середовища, захист бездіяльних віртуальних машин, захист периметра і розмежування мережі

Для вирішення даних проблем компанією Cloud Security Alliance (CSA) були розроблені найбільш ефективні способи захисту в області безпеки хмар. До них відносяться такі методи як шифрування хмари яке є одним з найефективніших методів захисту даних. Провайдер, що надає доступ до даних повинен шифрувати інформацію клієнта, що зберігається в ЦОД, а також у випадку відсутності їх необхідності, безповоротно видаляти. Також провайдер для захисту даних при передачі повинен використовувати надійні протоколи такі як: AES, TLS, IPsec. Дані не вийде прочитати або зробити зміни, навіть у випадку доступу через ненадійні вузли. Також рекомендується використовувати аутентифікацію або ж для більшої надійності токени або сертифікати. Для прозорості взаємодії провайдера з системою ідентифікацію при авторизації, також рекомендується використовувати протоколи LDAP і SAML .

Також має сенс ізолювати користувачів використанням індивідуальної віртуальної машини і віртуальної мережі, які в свою чергу повинні бути розгорнуті з використанням таких технологій, як VPN, VLAN і VPLS.

Що стосується баз даних то існує кілька методів їх захисту. По-перше необхідно контролювати доступ до бази даних. Запобігти атаки кіберзлочинців допоможуть обмеження дозволів і привілеїв.

По-друге для компанії необхідно визначити критично важливі дані. Первим кроком має стати аналіз важливості захисту конкретної інформації.

Безумовно для запобігання витоку даних необхідно проводити моніторинг активності бази даних. Аудит і відстеження дій всередині бази даних передбачає знання про те, яка інформація була оброблена, коли, як і ким. Однак найкращим способом захистити базу даних – зашифрувати її для осіб, які намагаються отримати доступ без авторизації. Для цього використовуються технології шифрування для перетворення інформації, що зберігається в базі даних, в шифротекст, що робить її прочитання неможливим для осіб, що не володіють ключами шифрування. Існує два основних способи шифрування інформації: симетричний та асиметричний. Асиметричне шифрування є більш безпечним, у порівнянні з симетричним, але в той же час воно істотно повільніше. Основні підходи можна класифікувати по тому, на якому рівні відбувається шифрування: на рівні сховища, на рівні бази даних, на рівні додатку.

На рівні сховища використовується так зване «прозоре» шифрування (англ. Transparent Database Encryption, TDE). Дані шифруються перед записом на диск і дешифруються під час читання в пам'ять, що вирішує проблему захисту «неактивних» даних, але не забезпечує збереження інформації при передачі по каналах зв'язку або під час використання.

Одним із прикладів шифрування на рівні бази даних є шифрування на рівні стовпців яке записує в базу даних вже зашифровані дані, а саму базу даних без подальшого шифрування в сховище.

У шифруванні на рівні додатків процес шифрування здійснюється додатком, яке створює або змінює дані, тобто він відбувається перед записом в базу даних.

Таким чином в доповіді запропоновані рекомендації щодо запобігання найбільш популярних атак на хмари і на бази даних, що дозволяє адаптувати запропоновані механізми захисту в будь-яку компанію.

Перелік посилань:

1. Загрози хмарних обчислень і методи їх захисту [Електронний ресурс].– Режим доступу до ресурсу: <https://habr.com/ru/post/1831/> (дата звернення: 13.02.2020).

2. Захист баз даних – запорука безпеки корпоративної мережі [Електронний ресурс]. – Режим доступу до ресурсу: <https://eset.ua/ru/blog/view/14/> (дата звернення: 13.02.2020)

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ БІОМЕТРИЧНОГО ШАБЛОНУ РАЙДУЖНОЇ ОБОЛОНКИ ОКА

Чернікова В.Г. Стрілець А.М. Скирда С.О.

Науковий керівник – к.т.н., доцент Філіппенко О.І.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)

E-mail: valerii.chernikova@nure.ua

This work is devoted to actual problem of choosing a method for protection biometric template of the iris based on using fuzzy extractors. The above-mentioned protection method was also investigated under the conditions of a combination with methods of processing the iris image from the CASIA-Iris-Interval database. The scientific novelty of the work is to further improve the methods of protection biometric template of the individual by the iris for remote biometric authentication.

На зміну захисту інформації за допомогою паролів приходять біометричні системи, деякі з яких за останні роки придбали досить велику популярність серед користувачів завдяки своїй захищеності та зручності використання. Біометрична система розпізнавання встановлює відповідність конкретних поведінкових або фізіологічних характеристик користувача деякому заздалегідь заданому шаблону. Цей процес відбувається наступним чином. На етапі реєстрації виконується запис зразка біометричної риси користувача за допомогою датчика. Наприклад, при проведенні автентифікації по райдужній оболонці ока таким датчиком виступатиме камера, а зразком буде око користувача. Далі система витягує індивідуальні риси з біометричного зразка. Тобто, в зазначеному вище прикладі на даному етапі буде відбуватися виділення окремої ділянки райдужної оболонки та її перетворення в код. На наступному етапі система зберігає виділені риси в якості шаблону поряд з іншими ідентифікаторами. Це може бути ідентифікаційний номер, ім'я користувача та ін. Для отримання доступу користувач пред'являє датчику ще один біометричний зразок. При автентифікації шаблон, що зберігається в базі, порівнюється з новим зразком за допомогою алгоритму зіставлення, і повертається рейтинг відповідності, що відображає ступінь схожості між шаблоном і запитом. Після цього системою приймається рішення про надання даному користувачу доступу до певної інформації або об'єкту. Основною проблемою всіх біометричних ознак є їх відносна нестабільність. Тобто в двох послідовних пред'явленнях їх образи будуть побітно нестійкими. Через це неможливе застосування шифрування і звичайних хеш-функцій з подальшою перевіркою результатів різних пред'явлень на рівність. Одним із шляхів вирішення проблеми, що найбільш задовольняють вимогам є використання нечітких екстракторів.

Використання нечітких екстракторів дозволяє однозначно відновлювати секретний ключ з неточно відтворюваних біометричних даних. Довжина ключа задається у вигляді параметра, при цьому для відтворення ключа потрібні додаткові відкриті дані, які відповідні ключу і зберігаються в пам'яті.

Метод нечітких екстракторів витягує випадкову рівномірно розподілену послідовність з первинних вхідних даних і відновлює її з будь-яких даних, які є достатньо схожі на початкові. Нечіткий екстрактор дозволяє отримувати тільки один ключ, якість вихідної ключової послідовності якого задовольняє всім критеріям якості криптографічних ключів.

Захист біометричних шаблонів необхідно здійснювати криптографічними перетвореннями з використанням ключових даних. До перетворень, які не змінюють відстань Хемінга при порівнянні, відносяться шифрування гамуванням, перестановкою, підстановкою. Шифрування гамуванням визначається простотою реалізації.

Отже, до зашумленого біометричного шаблону за операцією побітового складання додаються біти гамми і таким чином отримується результуюча послідовність.

Виходячи з вищенаведеної інформації можна зробити наступні висновки. Застосування шифрування гамуванням є ефективним засобом для створення багаторазових нечітких екстракторів. За рахунок ключової гамми збільшується ентропія біометричного шаблону, що забезпечує стійкість до криптографічних атак. Ключова послідовність гамми зберігається у пристрої користувача і використовується тільки при початковій фазі реєстрації, або при поновленні бази даних і повинна постійно додаватися до зашумленого біометричного образу. Застосування коротких кодів, що коректують помилки для зашумлення біометричних шаблонів, є ефективним засобом побудови захищених біометричних образів.

Перелік посилань:

1. Конахович Г.Ф. Цифрова стеганографія / Г.Ф. Конахович, А.Ю. Пузиренко. – К.: МК-Пресс, 2006, 40 с.
2. Колешко В.М. Традиційні методи біометричної аутентифікації і ідентифікації / В.М. Колешко, Е.А. Воробей, П.М. Азізов. – М. : БНТУ, 2009, 107 с.

МЕТОДИ БЛОКУВАННЯ САЙТІВ

Семенченко О. А.

Науковий керівник – д.т.н. доцент Золотарьов В. А.

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

In today's world, billions of people are facing a form of blocking when surfing the internet. Access to Internet content in countries is blocked using Internet service providers. Individual countries resort to technical restriction of access, usually for reasons of national security and to implement specific laws.

Many users are also blocking access to resources that have been blocked for various reasons.

By comparing all kinds of blocking and bypassing the blocking of sites, I brought them a classification. Also, for each criterion I have assigned my coefficient.

У сучасному світі мільярди людей стикаються з тією чи іншою формою блокувань при серфінгу в інтернеті. Доступ до інтернет-контенту в країнах блокується за допомогою обладнання інтернет-провайдерів. До технічного обмеження доступу окремі країни вдаються, як правило, з міркувань національної безпеки і з метою виконання конкретних законів.

Громадська організація Internet Society виділяє кілька способів блокування доступу до інтернету, серед яких: блокування по IP, блокування сайту по URL, блокування із застосуванням системи DPI, блокування в рамках конкретних платформ (особливо пошукових систем) і блокування по DNS [1].

Також багато користувачів обходять блокування для отримання доступу до ресурсів які були заблоковані за різними причинами. Найвідоміші методами являються: використання CGI-проху, DNS, перекладача, VPN, кеш Google, зміни IP-адреси або використання браузеру TOR.

Розглядаючи усі способи блокування можемо зазначити два загальні недоліки:

1. Вони не вирішують проблему Блокування не видаляє контент з Інтернету, не перешкоджає незаконній діяльності і не допомагає переслідувати злочинців; вона усього лише приховує контент від очей широкої публіки. Сам по собі контент нікуди не зникає.

2. Вони заподіюють непрямий збиток Кожен спосіб блокування і надмірний, і недостатній одночасно - неминуче блокується дозволений

контент і пропускається заборонений. Проте збиток Інтернету цим не обмежується - блокування збільшує ризики кінцевих користувачів, пов'язані із спробами обійти блокування, знижує прозорість Інтернету, руйнує атмосферу довіри, заганає інтернет-служби в підпіллі і вторгається в приватне життя користувачів. Крім того, необхідно враховувати усі витрати, пов'язані з блокуванням.

На мою думку найкращий спосіб боротьби з нелегальним контентом і незаконною діяльністю в Інтернеті - протидія порушникам на місці скоєння злочину. Застосування фільтрів, блокуючих доступ до онлайн-контенту, слід визнати неефективним поставленим завданням, що не відповідають. Ці фільтри заподіюють непрямий збиток законослухняним користувачам Інтернету.

Законодавці, заклопотані проблемою поширення нелегального контенту через Інтернет, повинні звернути увагу на дві основні стратегії:

1. Вирішувати проблему на місці виникнення. Найбільш щадний для Інтернету підхід - прибирати нелегальний контент звідти, де він зберігається, і боротися з незаконною діяльністю там, де вона відбувається. Видалення нелегального контенту з місць зберігання і вжиття примусових заходів проти правопорушників дозволяє уникнути негативних наслідків блокування контенту і є ефективнішим підходом до видалення нелегального контенту. Співпраця юрисдикцій і зацікавлених осіб - запорука успішного рішення проблеми нелегального контенту в Інтернеті, для якої не існує державних кордонів.

2. Правильно розставляти пріоритети і використати альтернативні підходи. Деякі обставини допускають інші, ефективніші способи вирішення цієї проблеми.

Література:

1. Закон України «Про основні засади забезпечення кібербезпеки України» // (Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403

2. Конвенція Ради Європи «Конвенція про кіберзлочинність» // http://zakon.rada.gov.ua/laws/show/994_575

3. Internet Society «Internet Society — обзор перспектив блокировки интернет-контента» 2017 р.

**МЕРЕЖНА БЕЗПЕКА,
СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ,
ВІДМОВСТІЙКІСТЬ МЕРЕЖ**

Тертичний В.О.

Науковий керівник – док.т.н. Шостко І.С.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)

E-mail: vladtertychnyi@gmail.com

In recent years, the number of deliberate interventions (hacker or cyber attacks) in the work of information systems of all state and commercial structures has sharply increased in Ukraine. In almost all cases, after the implementation of hacker attacks, the work of enterprises is blocked from several hours to several days, which leads to significant financial losses. The article describes the main points of network security in general, It also talks about network resiliency. A set of measures to protect the network was also proposed.

Мережною безпекою називаються дії, спрямовані на захист працездатності і цілісності мережі і даних. Основне завдання мережної безпеки – це збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації. До основних методів мережної безпеки можна віднести такі методи як:

1. авторизація користувачів;
2. антивірусне ПЗ;
3. безпека електронної пошти;
4. сегментування мережі;
5. використання систем виявлення та протидії атакам;
6. використання брандмауеру;
7. відмовостійкість мережі.

Для того щоб захистити мережу необхідно в першу чергу захистити периметр мережі, тобто її зовнішній кордон. Захист периметра вважається обов'язковим елементом системи забезпечення інформаційної безпеки корпоративної мережі і включає в себе шлюзи безпеки, засоби міжмережевого екранування, організацію віртуальних приватних мереж (VPN), системи виявлення та запобігання вторгнень (IDS / IPS).

Замість того щоб боротися з наслідками інцидентів безпеки, а виявити їх відразу необхідно використовувати системи виявлення вторгнень, які призначені для визначення фактів несанкціонованого доступу до комп'ютерної системи чи мережі або несанкціонованого управління ними в основному через Інтернет.

Зазвичай архітектура системи виявлення вторгнень включає такі компоненти як: сенсорну систему, призначену для збору подій; підсистему

аналізу, призначену для виявлення атак; сховище в якому зберігаються результати аналізу; консоль управління. Системи виявлення вторгнень можна поділити на дві основні категорії: пасивні (IDS) і активні (IPS).

Різниця між ними ж полягає в тому, що в активній системі виявлення вторгнень, системою відразу ж приймаються відповідні дії на порушення такі як скидання з'єднання тощо.

Використання ноутбуків і смартфонів дозволяє співробітникам працювати, перебуваючи поза офісом. Їм необхідно забезпечити захищений віддалений доступ до корпоративних додатків, не знижуючи при цьому рівня безпеки. Тому систему мережної безпеки необхідно доповнити системами управління мобільними пристроями, додатками і даними.

Найчастіше вибір падає на так звані брандмауери наступного покоління (NGFW) — системи корпоративного класу, що забезпечують багаторівневий захист на базі одного пристрою. Таким чином, система захисту периметра розширюється і доповнюється іншими рішеннями, але ні в якому разі не скасовується.

Якщо говорити про відмовостійкість мережі то рівень надійності мережі залежить від рівня і типу відмовостійких рішень, застосованих в мережі. Відмовостійкість мережі визначається двома факторами: рівень надмірності мережної інфраструктури; час відновлення мережі, тобто час, необхідний для перемикання потоків даних на працездатні частини мережі в разі відмови її частини. Для підвищення відмовостійкості необхідно приймати такі міркування при проектуванні мережі: архітектура мережевого обладнання; дублювання з'єднань; рознесення каналів зв'язку.

У висновку роботи хочеться додати, що для забезпечення високого рівня корпоративної безпеки потрібно використовувати цілий комплекс заходів захисту. Перш за все потрібно побудувати зовнішній периметр мережі з використанням технологій VPN, систем виявлення та запобігання вторгненням, а також міжмережевими екранами. Також необхідно організувати захищені з'єднання для віддалених користувачів. Адже боротьба з новими атаками вимагає рішень по забезпеченню мережної безпеки і розробки мережної стратегії безпеки, що відповідає вимогам надійності, вартості та питань інтеграції з іншими ІТ системами. Вироблені рішення повинні бути надійними, забезпечувати захист від атак на рівні додатків і дозволяти ідентифікувати трафік.

Перелік посилань

1. Що таке мережева безпека? [Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/products/security/what-is-network-security.html (дата звернення 15.02.2020)

2. Мережева безпека. Замість введення? [Електронний ресурс]. – Режим доступу до ресурсу: <https://habr.com/ru/company/hpe/blog/261913/> (дата звернення 15.02.2020)

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ З ХМАРНОЮ ТЕХНОЛОГІЄЮ

Скирда С.О. Стрілець А.М. Чернікова В.Г

Науковий керівник – проф. Марчук В.С.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії
ім.Поповського В.В.,
тел. (057) 702-55-92)

E-mail: stanislav.skurda@nure.ua

The paper analyzes the methods of security audit of telecommunications networks with cloud technology. In the case of SaaS service, the audit is organized according to the classical scheme. It is assumed that the cloud has a sufficient level of protection. When using PaaS and IaaS services, the system audit is complicated. In this case, you need to use the technology of auditing software products that are delivered to the cloud users.

В наш час безліч людей використовують віддалений доступ в Інтернет через ноутбук, смартфон, планшетний комп'ютер для роботи поза офісом, в тому числі і з конфіденційною інформацією. Такий спосіб роботи має перевагу, однак несе за собою збільшення ризиків інформаційної безпеки.

Існують три види хмарних сервісів.

1. Програмне забезпечення як послуга Software as a Service (SaaS). Контроль і управління фізичною і віртуальною інфраструктурою хмари виконується хмарним провайдером. Тільки обмежена кількість налаштувань конфігурації додатків може бути доступна користувачам.

2. Платформа як послуга Platform as a Service (PaaS). Користувач має можливість розмістити програмне забезпечення для подальшого розміщення на ньому своїх додатків. Та частина програмного забезпечення, що встановлюється користувачем доступна йому для корегування.

3. Інфраструктура як сервіс Infrastructure as a Service (IaaS). В цьому випадку користувач має можливість використовувати хмарну інфраструктуру для самостійного управління ресурсами обробки, зберігання інформації. Користувач може ставити своє програмне забезпечення. Але контроль і управління фізичною і віртуальною інфраструктурою хмари виконується хмарним провайдером.

Самим захищеним з трьох сервісів є SaaS. Інші менш захищені, тому що користувач може ставити своє програмне забезпечення в хмару. А це відкриває дорогу до встановлення додатків з шкідливим кодом.

Якщо допустити, що провайдер хмарного сервісу забезпечує достатній рівень інформаційної безпеки, то основним каналом вразливості системи є лінія зв'язку до сервера провайдера.

Для забезпечення основного захисту лінії може використовуватися VPN технологія і антивірусне забезпечення, що ставиться в обладнанні

користувача. Антивірусний захист вимагає додаткових обчислювальних потужностей і постійного оновлення антивірусних програм.

Одним з методів зниження цих ризиків є застосування хмарних сервісів безпеки. Наприклад, може використовуватися антивірусне програмне забезпечення "із хмари".

Після розгортання телекомунікаційної мережі з хмарною технологією і вибраними засобами інформаційного захисту потрібно забезпечити аудит телекомунікаційної системи.

Під аудитом інформаційної безпеки розуміється системний процес отримання об'єктивних якісних і кількісних оцінок поточного стану ІБ організації відповідно до визначених критеріїв та показників на всіх основних рівнях забезпечення безпеки: нормативно-методологічному, організаційно-управлінському, процедурному і програмно-технічному.

Результати кваліфіковано виконаного аудиту дозволяють побудувати оптимальну по ефективності і витратам систему забезпечення інформаційної безпеки (СЗІБ), що представляє собою комплекс технічних засобів, а також процедурних, організаційних і правових заходів, об'єднаних на основі моделі управління ІБ.

На першому етапі спільно з Замовником розробляється регламент, який встановлює склад і порядок проведення робіт.

На другому етапі, відповідно до узгодженого регламенту, здійснюється збір вихідної інформації.

Третій етап робіт передбачає проведення аналізу зібраної інформації з метою оцінки поточного рівня захищеності системи.

По результатам проведеного аналізу на четвертому етапі проводиться розробка рекомендацій щодо підвищення рівня захищеності автоматизованої системи від загроз інформаційної безпеки.

Організація аудиту інформаційної безпеки телекомунікаційних мереж з хмарною технологією має ряд особливостей.

У випадку сервісу SaaS аудит організується по класичній схемі. При цьому передбачається, що хмара має заданий достатній рівень захисту.

При використанні сервісів PaaS і IaaS аудит системи значно ускладнюється. В цьому випадку потрібно розробити технологію аудиту програмних продуктів, що поставлені в хмару користувачами. Ці продукти можуть бути джерелом загроз для системи з хмарною технологією. Тому потрібно організувати систему постійного контролю програмного забезпечення користувачів.

Перелік посилань

1. Прудникова А.А., Садовникова Т.М. Анализ облачных сервисов с точки зрения информационной безопасности // Т_Comm, 2012. - №7. – С. 153-156.

КОМПЛЕКСНИЙ ПІДХІД ПРИ ВИБОРІ МЕТОДОЛОГІЇ ОЦІНКИ РИЗИКІВ СЕРВЕРНОЇ КІМНАТИ ЯК ОБ'ЄКТУ ПІДВИЩЕНОГО РИЗИКУ КОМПАНІЇ

Подолька Н.В., Кавуненко Я.О.

Науковий керівник – к.т.н., доцент Добринін І.С.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. ІКІ, тел. (057) 702- 55- 92)

E-mail: nataliia.podoliaka@nure.ua

This work reflects the choice of a comprehensive approach to assessing the risks of a corporate network server room in the organization. The main task of the information security management system is to preserve the confidentiality, integrity, and availability of information. This work provides propositions about the usage method of cause-effect relationships for determination risks in corporate networks. Risk assessment is recommended based on the received data using the methodology of factor analysis of the information risks.

Так як головним сховищем найціннішого ресурсу будь-якої компанії - інформації - є серверна кімната, вона має бути обладнана належним чином і задовольняти міжнародні стандарти, прийняті в конкретній компанії. Будь-який витік інформації може стати причиною серйозних проблем для компанії - від значних фінансових збитків до повної її ліквідації.

Аналіз загроз стає підґрунтям для оцінки ризиків інформаційних активів серверної кімнати, адже очевидним є той момент, що усі найважливіші інформаційні активи компанії зберігаються в серверному приміщенні, тому і оцінку ризиків доцільно починати саме з нього.

У наш час для вирішення задач з оцінки інформаційних ризиків використовуються кілька методологій. Найбільшу популярність завдяки масовому використанню здобули методологія OCTAVE, методологія NIST та методології, зазначені в стандарті ISO/IEC 31010. Проте з цілої низки критеріїв неможливо визначити однозначну першість того чи іншого методу оцінки ризиків, адже вони розрізняються ступенем деталізації, вимогами до підготовки персоналу і необхідними ресурсами.

Наразі лишається актуальною проблема - немає універсальної методології, яка б відповідала всім критеріям і задовольняла всі потреби підприємств. Наявність такої є важливим моментом, так як до цих пір деякі керівники не розуміють важливості проведення оцінки інформаційних ризиків у їхніх мережах, в тому числі і з причини неповного досконалості наявних на ринку програм. У більшості існуючих методологій та стандартів основна увага приділяється побудові комплексного процесу

управління ризиками. В той час як питання безпосередньої оцінки ризиків розглядаються досить поверхнево. Методологія FAIR розроблена саме для усунення цього недоліку. Вона містить детальну класифікацію факторів, що обумовлюють виникнення ризику, визначає їх вплив один на одного і взаємозв'язок між ними. Це дозволяє адекватно оцінити частоту реалізації ризиків і масштаби втрат - саме те, що найчастіше викликає труднощі.

Ретельний аналіз даної методології показав, що в розрахунках інформаційних ризиків вона передбачає матричний підхід та переведення кількісних значень параметрів до якісних за допомогою відповідних шкал.

Процесу оцінювання ймовірностей реалізації загроз і вразливостей необхідно приділяти особливу увагу, для цього пропонується скористатися методом встановлення причинно-наслідкових зв'язків. Даний підхід дасть нам чітке розуміння основних загроз, які є актуальними для серверної кімнати корпоративної мережі.

Аналіз причинно-наслідкових зв'язків - це структурований метод, який застосовується для визначення можливих причин небажаної події чи проблеми. Він систематизує можливі чинники, які мають вплив в узагальнені категорії таким чином, що дозволяє розглядати всі можливі гіпотези. Аналіз причинно-наслідкових зв'язків дозволяє отримати структуроване графічне відображення переліку причин конкретного впливу.

Незважаючи на те, що методологія FAIR дає якісну оцінку ризику, цей підхід може застосовуватися достатньо ефективно. Проте, щоб він застосовувався найбільш ефективно, доцільно формувати причинно-наслідкові зв'язки по відношенню до серверної кімнати корпоративної мережі. Саме комплексний підхід дозволяє сформувати модель загроз для серверної кімнати, точно ідентифікувати ризики та спростити застосування методології FAIR для оцінки інформаційних ризиків.

Перелік використаної літератури:

1. Менеджмент риска. Методики оценки риска. // ISO/IEC 31010:2009, IDT. – 2009.
2. I. Dobrynin, T. Radivilova, N. Maltseva and D. Ageyev, "Use of Approaches to the Methodology of Factor Analysis of Information Risks for the Quantitative Assessment of Information Risks Based on the Formation of Cause-And-Effect Links, 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 229-232.

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ НА КАНАЛЬНОМУ РІВНІ ЗА ДОПОМОГОЮ ПРОТОКОЛУ OPENVPN

Кодаченко Р. Ю.

Науковий керівник – доц. Токар Л. О.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. інфокомунікаційної інженерії
ім. В.В. Поповського),
тел. 38 (095) 448-95-81, rusik.ka16@gmail.com

In the article the different approaches to the organization and for ensuring the protection of information in networks in data link layer using OpenVPN. The author select the best option of organization of specialized disciplines in terms of the minimum amount of time and material resources. The article focuses on the use of information in the Internet and the providing their protection. The effectiveness of information security in global networks is discussed.

Одним з програмних продуктів, що реалізують захист на каналному рівні, є OpenVPN (www.openvpn.net). Даний продукт дозволяє організувати закриту мережу на базі мережі Інтернет. При підключенні до такої мережі клієнт проходить процедуру криптографічної аутентифікації по цифровому сертифікату, що забезпечує захист від несанкціонованого доступу до ресурсів цієї мережі. Крім того, забезпечується шифрування мережевого трафіку при роботі в мережі. OpenVPN підтримує режими роботи "міст" і "маршрутизатор". При роботі в режимі "міст" відбувається шифрування і інкапсуляція кадрів Ethernet. Слід зазначити, що якщо шифрування забезпечує захист від доступу до інформації, що передається, то через інкапсуляцію зловмисник не зможе з'ясувати адресата переданої інформації.

Розглянемо завдання, які можливо вирішити за допомогою OpenVPN в режимі "міст":

- Підключення віддаленого співробітника до корпоративної мережі (VPN-шлюз)

Рішення даного завдання передбачає використання серверної частини OpenVPN в якості додаткового шлюзу в мережі організації. Сегмент мережі, що доступний через VPN-шлюз, зазвичай називають доменом шифрування. Робочі місця і сервера, що входять в домен шифрування не підключаються до VPN. При підключенні до сервера OpenVPN клієнт отримує прозорий доступ до всіх машин, що знаходяться в домені шифрування. Чи отримають подібний доступ до машин клієнта машини з домену шифрування, залежить від налаштувань сервера OpenVPN.

- Об'єднання мереж філій організації в єдину мережу

Іншим завданням, яке можна вирішити за допомогою OpenVPN є об'єднання мереж філій організації в єдину мережу через Інтернет. В цьому

випадку сервери OpenVPN встановлюється в якості додаткових шлюзів у власних мережі, а потім з'єднуються між собою.

- Об'єднання сегментів декількох організацій в єдину мережу для ведення спільного проекту (міжкорпоративний портал)

Основною проблемою при створенні міжкорпоративного порталу є логічний поділ мережі організації на два сегменти, один з яких надає свій ресурс організаціям-партнерам, а інший закритий для них. Для вирішення даної проблеми одна з організацій розгортає на зовнішній адресі сервер OpenVPN. На все робочі місця і сервера, які беруть участь в порталі, встановлюється клієнт OpenVPN, і ці машини підключаються до сервера.

- Підключення до мережі віддалених користувачів з низьким рівнем довіри

Рішення даного завдання потрібно для мереж, до яких підключаються "зовнішні" користувачі (наприклад, замовники або клієнти). Рівень довіри до них набагато нижче, ніж до співробітників компанії, тому потрібне забезпечення спеціальних "рубежів" захисту, що запобігають або обмежують доступ останніх до особливо цінної, конфіденційної інформації.

- Створення декількох логічних мереж в одній фізичній мережі

Рішення даного завдання потрібно, наприклад, коли треба розділити трафік між внутрішніми департаментами організації, які звертаються до серверів з одного фізичного сегмента. Особливість даного варіанту в тому, що VPN будується між вузлами, що знаходяться, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером. Цей варіант схожий на технологію VLAN, але замість поділу трафіка, використовується його шифрування.

- Анонімний серфінг

Під серфінгом розуміються будь-які дії користувача в Інтернеті. При цьому інтернет-провайдеру даного користувача стають відомі web-сайти, що відвідував користувач; адресати листів користувача і т.п. Використання OpenVPN в якості додаткового "логічного" шлюзу в Інтернет, встановленого на території організації, в якій працює користувач, забезпечує анонімність серфінгу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Оліфер В.Г. Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи: Навчальний посібник для вузів. 4-е изд. - СПб.: Пітер, 2010. - 944 с.

2. Арестова О.Н., Бабанін Л.Н., Войскунский А.Є. Комунікація в комп'ютерних мережах: психологічні детермінанти і наслідки // Вісник МГУ. Серія XIV. Психологія. 2008. №4. С. 65-84.

ПЕРСПЕКТИВИ ТА КІБЕРБЕЗПЕКА ЦИФРОВІЗАЦІЇ БІЗНЕСУ ТА ПРОМИСЛОВОСТІ

Іващенко М.Д.

Науковий керівник – к.т.н., доц. Ляшенко О.С.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Безпеки інформаційних технологій)
e-mail: max.ivas01@gmail.com

The up-to-date trend is digitalization and digital transformation of business and industry. It has enabled small companies, startups to quickly create their products and market them in the same way as large companies that are already present on the market. It is revealed that the opportunities for Ukraine will be to increase the competitiveness of the economy; overall development of the digital economy and relevant labor market; creation of new industries; accelerating the development of innovative entrepreneurship. The barriers will be: the imperfection of the education system, the lack of a strategy and national program for digitizing the various spheres of society.

Кінець XX – початок XXI століття ознаменували стрімким розвитком сучасних комунікацій та зв'язку в світі. Якщо вчасно аналізувати такі цифрові тренди, то з'являється можливість якісного прогнозування конкретного технологічного, економічного чи навіть соціального явища в найближчому майбутньому. Цей тренд створює неабиякі можливості для України [1]. По суті можливий розвиток нової галузі економіки і нових робочих місць для населення. Науковцям необхідно буде виробити нову методологію та підходи до розуміння середовища цифрової економіки і збору інформації в ній. Разом з тим виникне потреба в нових ефективних інструментах управління. Отже, такий тренд почне свій вплив як на мікро- так і на макрорівні.

Надсучасним трендом є так звана цифровізація (диджиталізація) і цифрова трансформація бізнесу та промисловості. На сьогодні основою для створення нових продуктів стали цифрові технології, і, відповідно, вони також перетворились на своєрідний критерій конкурентних переваг на ринку. Цифровізація змогла перевернути ринок. Вона дала можливість невеликим компаніям, стартапам швидко створювати свої продукти та виводити їх на ринок рівно так, як це роблять великі компанії, які вже присутні на ринку. Це призвело до зміщення «інформаційного центру» до дрібних компаній.

Цифрова трансформація веде до появи унікальних систем і процесів, що лягають в основу вартості нових продуктів (наприклад, UBER, AirBed and Breakfast (Airbnb), інтернет-банкінг тощо). Трансформації у промисловості вибудовуються відповідно до відомої концепції «Індустрія 4.0» та з розвитком роботизованих виробництв, кіберсистем та роботів.

Можливостями для України у цьому аспекті буде підвищення конкурентоздатності економіки; загальний розвиток цифрової економіки і відповідного ринку праці; створення нових індустрій; пришвидшення розвитку інноваційного підприємництва.

Але при цьому, на наш погляд, в Україні існує низка бар'єрів для швидкого розвитку цифровізації:

- відсутність стабільних середньої та вищої систем освіти для нарощення цифрових підприємницьких навичок у суспільстві в цілому;
- відсутність розробленої стратегії щодо способів та підходів до оцифровування різних сфер життя суспільства на державному рівні;
- відсутня національна програма підтримки, мотивації і стимулювання бізнесу до використання цифрових інструментів, рішення мають поодинокий та епізодичний характер з відсутністю системного підходу.

Процес цифровізації вимагає від держави створення умов для його безпечного становлення. Зокрема, це виражається у прийнятті законів, нормативно-правових актів органами державної влади і цим відбувається легалізація і легітимація або навпаки осудження будь-яких правовідносин.

Наразі в Україні правова база для регулювання суспільних відносин у сфері цифрової економіки та кібербезпеки розвинута слабо. Нормативно-правові акти представлені таким чином:

ЗУ «Про телекомунікації», ЗУ «Про авторське право і суміжні права», № 67-р «Про схвалення концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації», Проекти Законів №9083 та №9083-1 «Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами в Україні», та інші [2];

Таким чином, використовуючи системи захисту інформації та завдяки формуванню сучасного правового поля, що відповідає загальносвітовим вимогам, можливо збільшення довіри громадян до цифрових технологій.

Список використаних джерел

1. Work on Digital Labour Platforms in Ukraine: Issues and Policy Perspectives. URL: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/--travail/documents/publication/wcms_635370.pdf

2. Указ Президента №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL: <https://zakon5.rada.gov.ua/laws/show/96/2016>

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

ИСПОЛЬЗОВАНИЕ МНОГОКРИТЕРИАЛЬНОГО ПОДХОДА К ОПТИМИЗАЦИИ ТКС

Бухаров А.С., Барсук В.А., Кривошапка Н.В.

Научный руководитель – к.т.н., доц. Мельникова Л.И.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки, 14, каф. Инфокоммуникационной инженерии
им. В.В. Поповского, тел. (057) 702-13-20)

e-mail: liubov.melnikova@nure.ua

The solution of some Pareto-optimal problems in the field of telecommunications is considered and an analysis of methods for solving them is carried out. It is noted that additional information is information on the relative importance of particular criteria. The determination of weights encounters serious difficulties and usually comes down to expert judgment. A heuristic procedure is proposed to clarify the solution obtained.

Развитие инфокоммуникационных технологий приводит к необходимости применения эффективных методов решения оптимизационных задач именно в многокритериальной постановке [1]. В докладе приведены примеры решения задач многокритериальной оптимизации в области инфокоммуникаций, отмечена особенность методов решения таких задач и предложена процедура, позволяющая уточнять полученное решение в интерактивном режиме. В работе [2] сформулирована многокритериальная модель качества обслуживания при управлении сервисом (SLM – Service Level Management) в системах абонентского радиодоступа. В качестве частных критериев выбраны три основных параметра качества услуг: достоверность передаваемой информации, задержка при передаче пакетов, процент потерянных пакетов. Разработанная в [3] методика многопутевой маршрутизации, включает в себя процедуру многокритериальной оптимизации, и позволяет определить оптимальное число независимых кратчайших путей. В качестве частных критериев использованы величина максимального потока по мультипути и задержка передачи пакета. В работе [4] решается задача обеспечения качества передачи голосовой информации в беспроводных сетях, как задача многокритериального выбора кодека. Проведено исследование влияния параметров сети на качество передачи голосовой информации в беспроводных сетях. С помощью Е-модели получена оценка качества передачи для основных кодеков, использующихся в IP-телефонии. Задача выбора кодека решена как задача многокритериальной оптимизации. Кодеки должны удовлетворять нескольким требованиям, которые и определили следующий набор частных критериев: скорость передачи, устойчивость к потере пакетов, коэффициент снижения качества оборудования. При решении этих задач проявились некоторые особенности решения задач многокритериальной оптимизации.

Как известно, задача многокритериальной оптимизации в общем случае может быть сформулирована следующим образом, пусть x - решение, определенное, на множестве допустимых решений X . Качество решения оценивается множеством критериев. Известно отображение $f : x \rightarrow K$, и относительная важность критериев $\Lambda = \{\lambda_1, \lambda_2, \dots, \lambda_n\}$. Необходимо найти оптимальное решение $x^\circ = \text{opt}G[K(x), \Lambda]$, где x° - эффективное решение, $\text{opt}G[K(x), \Lambda]$ - схема компромисса (обобщенный критерий оценки эффективности). Решение поставленной задачи не вызывает затруднений в том случае, если известен вектор Λ и определен вид оператора $\text{opt}G[\cdot]$. Определение весовых коэффициентов сталкивается с серьезными трудностями и обычно сводится к экспертной оценке. В работе предлагается процедура уточнения оптимального решения лицом принимающим решение (ЛПР). Поиск оптимального решения проводится по следующей процедуре. Исследуется множество всех вариантов решения и проводится оптимизация по каждому из нормированных частных критериев. Полученные максимумы образуют вектор, который используется далее ЛПР для принятия решения. Проводится оптимизация по обобщенному критерию, наибольшему значению критерия соответствует вариант который предъявляется ЛПР в качестве решения. Перед ЛПР ставится вопрос: «Все ли показатели имеют удовлетворительное значение?» При ответе на этот вопрос используется вектор наилучших значений частных критериев. В случае отрицательного ответа ЛПР выделяет частный критерий, который имеет наименее удовлетворительное значение, а также указывает его значение, которое можно считать удовлетворительным. Предложенная процедура поиска решения задачи многокритериальной оптимизации позволяет получать и уточнить решение в интерактивном режиме при любой степени неопределенности априорной информации о важности частных критериев.

Список использованных источников:

1. Многокритериальный анализ и выбор средств телекоммуникаций: монография / В.М. Безрук, Д.В. Чеботарева, Ю.В. Скорик. – Харьков: ФОП Коряк С.Ф. 2017. - 268 с.
2. Мельникова Л.И., Горяева С.Н., Андрушко Д.В. Многокритериальная модель качества обслуживания в системах абонентского радиодоступа. Радиотехника. Респ. межвед. Сборник. - 2006. - Вып. 144. - С. 102-106.
3. Мельникова Л.И., Горяева С.Н., Андрушко Д.В. Многопутевая маршрутизация с использованием оптимального алгоритма распределения сетевых ресурсов для сетей MPLS-TE. Радиотехника. Респ. межвед. сб. - 2006. - Вып. 144. - С. 35-38.
4. Бухаров А.С., Тарасов Р.А. Оценка качества речи в телемедицинских сетях. VI международная научно-техническая конференция "Информатика, управление и искусственный интеллект (ИУИИ-2019)", г. Харьков.

РОЗРАХУНОК ЛІНІЙНИХ СПЕКТРАЛЬНИХ ЧАСТОТ З ВИКОРИСТАННЯМ ДИСКРЕТНОГО ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ ДЛЯ ОБРОБКИ ЕЛЕКТРОКАРДІОГРАМИ

Самочорнов М.Б.

Науковий керівник – к.т.н., доц. Кривенко С.А.

Харківський національний університет радіоелектроніки

(61166, Харків, пр. Науки, 14, каф. Інформаційно-мережної інженерії)

e-mail: nick.samochernov@gmail.com, тел. (068) 450-95-91

An approach for glucose meters was improved. We process electrocardiograms of patients to detect change of glucose concentration in the blood. The technique uses discrete wavelet transform for electrocardiograms processing. Standard oral glucose tolerance test used to check fifty-six patients complains of type 2 diabetes symptoms. It has been achieved high sensitivity and specificity to determine, hemoglobin, blood pressure, lipoproteins and low-density cholesterol, ion exchange performance (potassium, sodium, and calcium), triglycerides. The square of the Matthews correlation coefficient 0.93 has been achieved on examination.

Keywords: discrete wavelet transform, glucose meter, electrocardiogram, line spectral frequencies.

Існує два основних типи діабету. Лише 10-15% від у людей діабет 1 типу. Цукровий діабет другого типу є найбільш поширеним форма захворювання. Невеликий відсоток хворих на діабет припадає на вагітних жінок (3-5%, також відомих як гестаційний). Через високу поширеність діабету 2 типу особливий інтерес викликає моніторинг пацієнтів з такими цукровий діабет. 5% населення США (близько 18 мільйонів) страждають на діабет. Це сьома провідна причина розвитку смерть. До 2020 року витрати, пов'язані з лікуванням[1].

Метою даної статті є розгляд методики вдосконалення обробки електрокардіограми пацієнта (ЕКГ) для виявлення зміни концентрації глюкози в крові за допомогою обчислення лінійних спектральних частот за допомогою дискретного вейвлет-перетворення.

У нашому дослідженні для вирішення цієї проблеми використовується дискретна вейвлет-трансформація.

А. Лінійне прогнозування та ЕКГ

Спостережувана послідовність даних є випадковим вектором

$$X^m = (X_0, X_1, \dots, X_{m-1})^t$$

Оптимальний одношаговий лінійний прогноз - це оптимальний лінійний предиктор

$$\hat{X}_m = (a_{m-1}, \dots, a_2, a_1)^t X^m.$$

Алгоритм Левінсона-Дурбіна є ефективною інверсією для пошуку векторних елементів (a_m) з вектора автокореляції.

Б. Дискретне вейвлетське перетворення

Наступним методом пропонуються коефіцієнти квантування (a_m) лінійного прогнозування. Основою вважається швидке вейвлет-перетворення Хаара для порядку послідовностей $m = 16$.

1) Один рівень перетворення.

Дискретне вейвлет-перетворення (DWT) сигналу (a_m) обчислюється, пропускаючи його через ряд фільтрів. Спочатку зразки пропускають через фільтр низьких частот з імпульсною характеристикою $g[n]$. Сигнал також розкладається одночасно за допомогою високочастотного фільтра $h[n]$. Виходи дають коефіцієнти деталізації від високочастотного фільтра та коефіцієнти наближення від фільтра низьких частот. Важливо, щоб два фільтри були пов'язані один з одним, і вони відомі як квадратурний дзеркальний фільтр [2].



Рис. 1. Структурна схема аналізу фільтру

Однак, оскільки половина частоти сигналу тепер була видалена, половину зразків можна відкинути відповідно до правила Найквіста.

Це розкладання вдвічі зменшило часовий дозвіл, оскільки лише половина кожного виходу фільтра характеризує сигнал. Однак кожен вихід має половину смуги частот входу, тому роздільна здатність частоти була подвоєна.

2) Каскадні та фільтруючі банки

Це розкладання повторюється для подальшого збільшення роздільної здатності частоти та наближення коефіцієнтів, розкладених за допомогою фільтрів високого та низького пропускання, а потім зменшення вибірки.

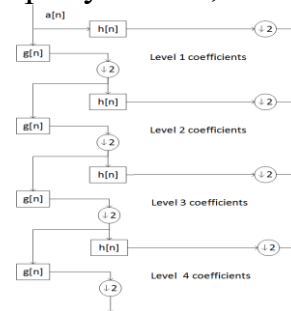


Рис. 2. Структурна схема аналізу фільтру

Список використаної літератури

1. Nguyen LL. "Non-invasive detection of hyperglycaemia in type 1 diabetic patients using electrocardiographic signals", Thesis, University of Technology Sydney, 2014.
2. "Discrete wavelet transform," 14 2 2016. [Online]. Available: https://en.wikipedia.org/wiki/Discrete_wavelet_transform [Accessed 15 2 2016].

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СТИСНЕННЯ ЗОБРАЖЕНЬ, ПРЕДСТАВЛЕНИХ В ФОРМАТІ JPEG

Курлан О.О.

Науковий керівник – к.т.н., доц. Золотарьов В.А.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ІМІ, тел. (057) 702-14-29)

e-mail: oleksandr.kurlan@nure.ua

Object of research – methods to improve efficiency of JPEG image compression.

The purpose of this work is a research into methods to improve efficiency of JPEG image compression.

The main methods of compression of images are considered. Their comparative analysis was carried out. Methods of increasing the compression efficiency of images presented in JPEG format will be investigated. In the practical part there will be a software implementation of the investigated methods and a comparative characteristic.

Мета роботи: дослідження методів підвищення ефективності стиснення зображень, представлених в форматі JPEG – метод теоретичного вибору порогового значення та метод вибору порогового значення з використанням cross-validation.

Експериментальним шляхом було проаналізовано 31 напівтонове зображення та отримані перші низькочастотні ДКП коефіцієнти близькі до нуля, які можна обернути в нуль без втрати якості зображення; побудовано зображення коефіцієнту пікового відношення величини сигналу до шуму PSNR у порівнянні з розміром для цих зображень, стиснених з використанням згаданих порогових методів RD-OPT квантуванням.

Крім того, отримані графіки PSNR-розміру для цих зображень, стиснених з використанням таблиць квантування «за замовчуванням JPEG»; графіки частот PSNR для випадків RD-OPT квантування без порогу (оптимізації таблиці квантування). Оцінки на цих ділянках є фактичними показниками результату стиснення JPEG з кодуванням Хаффмана, а не оцінок ентропії. Було виявлено, що метод теоретичного порогового значення з таблицею квантування в відношенні розміру-спотворення приводить до збільшення PSNR на 2 дБ, порівняно з алгоритмом RD-OPT квантування без порогової обробки, та на 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, що і схема кодування RD-OPT без порогового значення, в низьких бітових швидкостях. Втім, 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 класичних зображень у градаціях сірого «Lena» (рис. 1.а) і «Boat» (рис. 1.б).

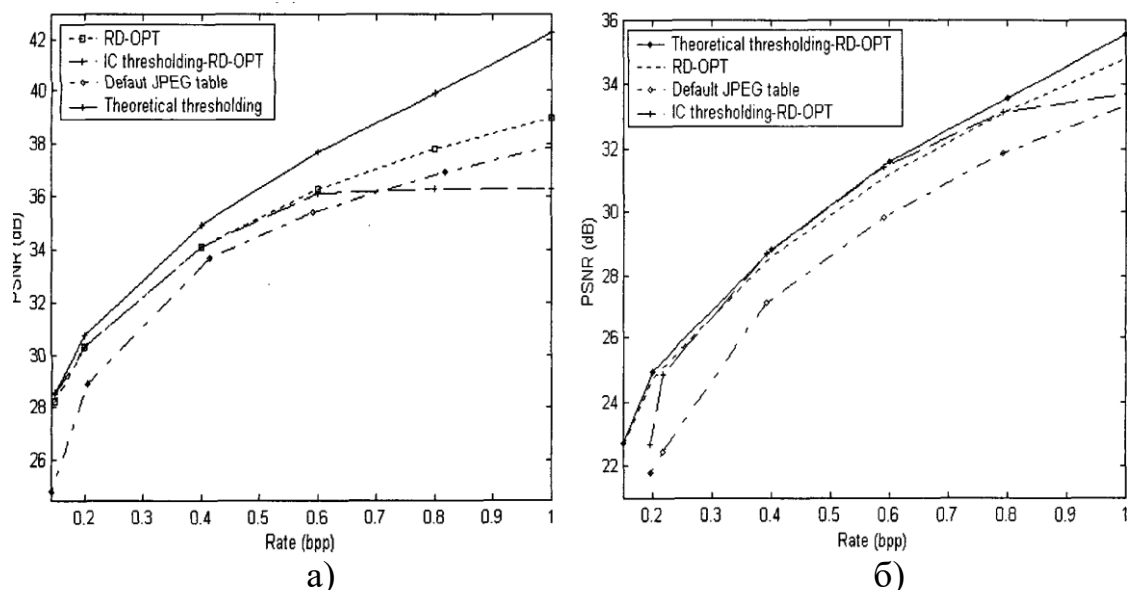


Рис. 1 – а) порівняння показників глобального порогу з φ_β для зображення «Lena»; б) для зображення «Boat»

Результати експерименту доводять, що метод вибору порогового значення з використанням cross-validation, дозволяє обрати більше порогове значення, ніж метод теоретичного вибору порогового значення; а метод з використанням інформаційного критерію не задовольняє умовам стиснення зображень і не дає суттєве підвищення ефективності.

Проведене дослідження довело можливість істотного підвищення ефективності стиснення зображень, представлених у форматі JPEG та зниження розміру файлу без помітного зниження якості зображення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Transform image coding with global thresholding: application to baseline JPEG. // in Proceedings XIV Brazilian Symposium on Computer Graphics and Image Processing. – 2001. – С. 164 – 171.
2. Wasserman L. All of Nonparametric Statistics / Larry Wasserman. – New York, NY, United States: Springer-Verlag New York Inc., 2007. – 270 с.

СТАТИСТИЧНИЙ АНАЛІЗ ДКП КОЕФІЦІЄНТІВ JPEG ЗОБРАЖЕНЬ

Курінний А.А.

Науковий керівник – доц., к.т.н. Золотарьов В.А.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. інформаційно-мережної інженерії)
тел. (095) 418-74-74, e-mail: artem.kurinyi@nure.ua

Digital technologies allow people to receive and process enormous general information and securely store it. Presently, one of the most important tasks is the creation of compression methods, the use of which allows improving the characteristics of the system of transmission, processing and data registration. The purpose of this work is to substantiate the expediency of choosing the Laplace distribution for the statistical description of DCT coefficients from a statistical point of view. The main idea of the work is to use a double stochastic model, according to which not only DCT coefficients but also the variance of these coefficients will be considered random.

JPEG широко використовуються для стиснення з втратами нерухомих кадрів. Втім відкритим лишається питання визначення результуючого статистичного розподілу після виконання дискретного косинусного перетворення (DCT) для кожного з блоків та отримання відповідних коефіцієнтів.

Такі знання були б корисні, наприклад, у внутрішньому устрої квантувача і шумозаглушувача для покращення зображення.

Верхній лівий коефіцієнт називається постійним коефіцієнтом, а решта – змінними коефіцієнтами.

Масштабування гістограми зберігається однаково для всіх постійних коефіцієнтів в цьому графіку.

Важливою характеристикою

типових зображень є те, що вони мають змінну дисперсію блоків. Тому ми моделюємо зображення за допомогою подвійної стохастичної моделі, причому дисперсія розподілів Гауса також є випадковою величиною. Це виявляється визначальним фактором для форми розподілу коефіцієнтів. Через унітарність ДКП, дисперсія гаусівського розподілу, отримана шляхом застосування центральної граничної теореми, прямо пропорційна дисперсії блоку. Однак константа пропорційності різна для різних

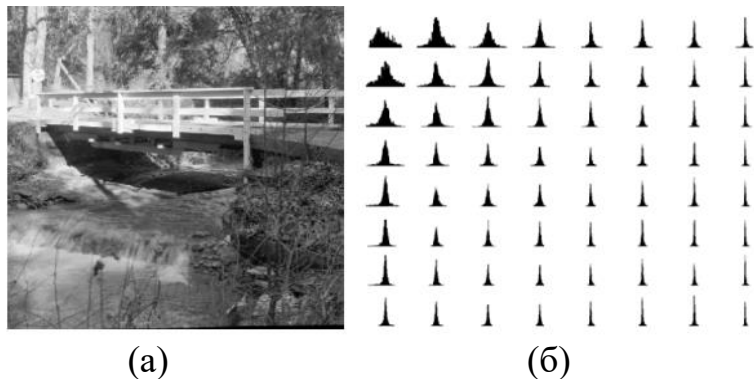
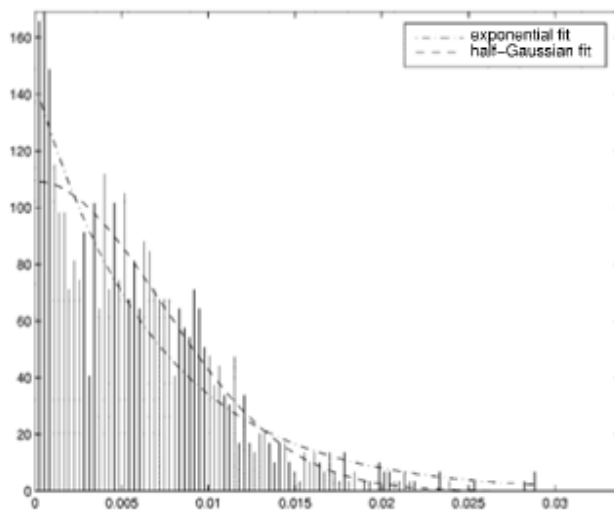


Рис. 1 – Зображення «bridge» (a) та гістограма DCT коефіцієнтів зображення «bridge» (б)

коефіцієнтів: вона менше в міру того, як ми йдемо до більш високих частотних коефіцієнтів. На низьких частотах, ваги сусідніх пікселів близькі, тому підсумкове підсумовування зазвичай призводить до великих величин. Однак на високих частотах ваги сусідніх пікселів близькі за величиною, але протилежні за знаком. Коли пікселі корельовані просторово, загальний ефект полягає в тому, що вони схильні взаємовиключні один одного в підсумовуванні, і тому отриманий DCT коефіцієнт зазвичай має малу величину.

Існує альтернативне пояснення цього явища з більш традиційної перспективи обробки сигналів. Поблочно ДКП можна інтерпретувати як



(а) (б)
Рис. 2 – Зображення: «baboon» (а)
та гістограма і апроксимація
для зображення «baboon» (б)

розкладання піддіапазонів після повторного компонування коефіцієнтів. Тому розподіли коефіцієнтів насправді еквівалентні гістограмам різних підзон. Оскільки всі природні образи володіють певними ступенями просторової кореляції, їх енергія зазвичай зосереджена в нижчій смузі частот.

В результаті природно очікувати більшої енергії – отже, більшою дисперсії – в низькочастотних піддіапазонах вихідного зображення, ніж ми очікуємо від високочастотних

підзон. Тому, коли ми дивимося на гістограму, ширина розподілу Лапласа зменшується при русі до високочастотного піддіапазону.

Оскільки сплески грають велику роль для стиснення зображення за допомогою JPEG 2000 і цифрове стиснення відео стає все популярнішим, ми вважаємо, що ці аналізи будуть корисні для розвитку мультимедійних систем.

Перелік джерел:

1. Куріний А. А. Використання апарату ймовірнісних Р-Р графіків для дослідження розподілу ДКП коефіцієнтів JPEG зображень // 23-й Міжнародний молодіжний форум «Радіoeлектроніка та молодь у ХХІ столітті». Зб. Матеріалів фаруму. Т.4. – Харків: ХНУРЕ. 2019. – С. 78-79.
2. Родигін М.В., Федоров О.В. Врахування структурних властивостей зображення при оцінюванні якості стиснених JPEG зображень // Східно-Європейський журнал передових технологій. – 2015. – Vol. 6/4, № 78. – Р. 54-64.

ДОСЛІДЖЕННЯ АЛГОРИТМІВ РОЗПІЗНАВАННЯ ГЕНДЕРНОЇ ПРИНАЛЕЖНОСТІ ЛЮДИНИ ЗА ЇЇ ГОЛОСОМ

Єрмолаєв А.А.

Науковий керівник к.т.н., доц. Золотарьов В.А.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ІМІ, 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 та впровадити методи 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.

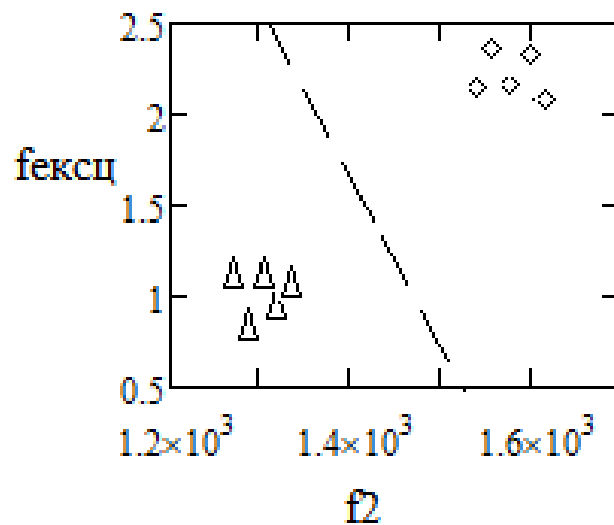


Рисунок 1 – Зосередження пар вимірювань середнього значення другої формантної частоти основного тону і коефіцієнта ексцесу для жіночих голосів (трикутники) і чоловічих голосів (квадрати)

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 по частоті основного тону та 2-ої формантної частоти.

ПЕРЕЛІК ПОСИЛАНЬ

1. Пресняков И.Н. Автоматическое распознавание отдельных 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.

ДОСЛІДЖЕННЯ ІМОВІРНОСТІ ВИНИКНЕННЯ РИЗИКУ ТА АНАЛІЗ ЗЛОВМИСНИХ ПРОГРАМ

Пестєрева С. Є.

Науковий керівник – к.т.н., доц. Золотарьов В.А.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ІМІ, тел. (057) 702-14-29)

e-mail: sofiia.pestierieva@nure.ua.

The technological advances in computing devices have created great impact for wide range of application. Since computing devices may be coupled with third-party software applications, so, many security and privacy difficulties can be stimulated by malwares.

Object of research – methods to improve safety for computer systems as for home users and business users.

The purpose of this work is a research malware and threat analysis. Build classification certain malware.

Мета роботи – дослідження тенденції розвитку зловмисних програм у світі за останні роки.

У ході роботи були розглянуті 10 актуальних вірусів (а саме GoBot2, Formbook, Joao, TrojanDownloader.FakejQuery, Remaiten, Prikormka, Mooze/AdWare.LoadMoney, Mumblehard, Aibatook) та розглянуто методи та етапи їх розповсюдження, встановлення, запуск та виконання зловмисних програм (команд)

У ході дослідження було проаналізовано 5 вірусів (GoBot2, Remaiten, Prikormka, Mooze, AdWare.LoadMoney, які мають більш обширні відомості) за такими факторами: імовірність, складність реалізації та застосовність.

Під імовірністю розуміється ймовірність підхоплення та розраховується, як 0,1 за актуальність ресурсу та 0,5 від кількості вразливостей, а саме на що він спрямован (файл, тека, виконання команд та ін.).

Під складністю реалізації розуміється необхідність наявності у порушника режиму ІБ та залежить від кількості етапів встановлення один етап має вагу 0,05, якщо встановлення вірусу потребує 4 етапи, то складність реалізації 0,2.

Під застосовністю розуміється можливість застосовувати кібератаку на рівні різних архітектур, фреймворків, операційних систем, мов програмування. В нашому випадку від актуальності операційної системи для звичайного користувача та її версії. Коефіцієнти я розділила так, що для ОС Linux=0,05; для Win32=0,1; для Win64=0,15.

Було побудовано таблицю з розрахунком імовірність виникнення ризику, яка наведена в табл. 1

Таблиця 1 – Розрахунок імовірності виникнення ризику

Фактор	Класифікатор	Коефі- цієнт	Назва вірусу				
			GoBot2	Remai- ten	Prikor- mka	Mooze	AdWare.- LoadMoney
Імовірність	Актуальність						
	Торент-файл	0,05	+				
	Браузер	0,1		+	+	+	+
	Кількість вразливостей						
	Тека	0,05	+		+		
	Файл			+	+		
	Виконання файлів		+				
	Запис реєстра		+			+	
	Виконання команд					+	
	Крадіжка облікових даних			+	+		+
Сума			0,2	0,2	0,25	0,2	0,15
Складність реалізації	Кількість етапів встановлення	0,05	5	1	2	4	1
Сума			0,25	0,05	0,1	0,2	0,5
Застосовність	Операційна система						
	Linux	0,05		+			
	Win32	0,1			+	+	+
	Win64	0,15	+		+		
Сума			0,15	0,05	0,25	0,1	0,1
Загальна сума			0,6	0,3	0,6	0,5	0,3

За результатами проведеного дослідження були розглянуті різноманітні віруси та проаналізувала імовірність виникнення ризику в залежності від різних умов.

Перелік джерел:

1. SECURITY REPORT 2017/18 [Електронний ресурс] // <https://www.av-test.org/en/news/>. – 2018.
2. Threat Encyclopaedia [Електронний ресурс] // https://www.virusradar.com/en/threat_encyclopaedia/filter?page=. – 2019.
3. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] // Постанова Національного банку України. – 2017.

ЗАСТОСУВАННЯ МЕТОДУ ТЕОРІЇ СИСТЕМ ЩОДО АНАЛІЗУ ЕЛЕКТРИЧНИХ ПРИСТРОЇВ

Бондар О.Д.

Науковий керівник: – к.т.н. Скорик Ю.В.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. інформаційно-мережної інженерії,
(057) 702-14-29)

e-mail: olha.bondar@nure.ua тел. 098-440-18-05

The increasing complexity of processes and events in science, technology and other fields of activity is the ever-expanding use of mathematical and computational methods. In connection with these circumstances, the concept of “system” is enriched in content and acquires quantitative characteristics. The concepts of complex and large systems, systems engineering, systems theory, systems approach are widely used. Traditional scientific directions and educational disciplines are influenced by the theory of systems and systems approach. terminological and mathematical apparatus. Here we consider an example of applying a systematic approach to the analysis of electrical devices.

Система – це сукупність об'єктів, пов'язаних будь-якими формами взаємодії або взаємозалежності.

З точки зору математичної моделі система має форму сукупності змінних та співвідношень, що їх пов'язують.

Модель фізичної системи пов'язує між собою змінні трьох типів:

- вхідні $[V] = [v_1, v_2, v_3, \dots, v_m]$;
- вихідні $[Y] = [y_1, y_2, y_3, \dots, y_r]$;
- внутрішні (проміжні) $[X] = [x_1, x_2, x_3, \dots, x_n]$.

Внутрішні змінні також мають назву змінних стану.

Аналіз системи ґрунтується на розв'язанні системи матричних рівнянь:

$$\begin{cases} \frac{d}{dt} x(t) = F[x(t), v(t)]; \\ y(t) = \varphi[x(t), v(t)]. \end{cases}$$

Перше рівняння є рівнянням стану системи. Розв'язок цього рівняння повинен задовольняти початковій умові $x_0 = x(t_0)$.

$$x(t) = \psi[x(t_0), v(t)].$$

Друге рівняння називається вихідним рівнянням, оскільки визначає вихідні змінні в залежності від вектору вхідних впливів та вектору станів системи.

У випадку коли функції правих частин рівнянь є лінійними, система вважається лінійною.

$$\begin{cases} \frac{d}{dt} x(t) = A(t)x(t) + B(t)v(t); \\ y(t) = C(t)x(t) + D(t)v(t). \end{cases}$$

де $A(t)$ – матриця системи, є квадратною n -го порядку; $B(t)$ – матриця керування розміром $n \times m$; $C(t)$ – матриця виходу розміром $r \times n$; $D(t)$ – матриця входу розміром $r \times m$. Оскільки елементи матриць залежать від часу, система є нестационарною (параметричною).

Якщо Матриці A , B , C , та D не залежать від часу, то система є лінійною стаціонарною і рівняння набувають вигляду:.

$$\begin{cases} \frac{d}{dt} x(t) = Ax(t) + B v(t); \\ y(t) = Cx(t) + D v(t). \end{cases}$$

Для того, щоб побудувати в такій формі математичну модель електричного пристрою слід виконати наступні кроки:

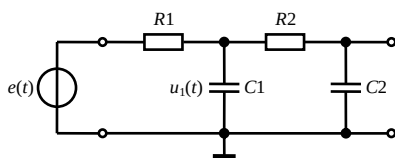
1. На схемі пристрою замінити кожен індуктивність L_k ідеальним джерелом струму величиною $i_k(t)$, кожен ємність C_m – ідеальним джерелом напруги $u_m(t)$.

2. У колі, що утворилося та складається лише з джерел та опорів, розрахувати на підґрунті законів Кирхгофа та Ома струми через джерела напруги та напруги на джерелах струму. Слід розглядати тільки ті джерела, якими було замінено ємності та індуктивності.

3. Провести заміну змінних розрахованих напруг та струмів за правилом: $u_m(t) = L_m \frac{di_m(t)}{dt}$; $i_k(t) = C_k \frac{du_k(t)}{dt}$.

Внаслідок цих кроків буде утворена система лінійних диференціальних рівнянь першого порядку, виражена через змінні стану, якими є струми через індуктивності та напруги на ємностях.

Приклад утворення системи на підґрунті пасивного фільтру нижніх частот наведено на рис. 1.



$$\tau_1 = R1C1; \quad \tau_2 = R2C2; \quad k = \frac{R1}{R2};$$

$$\frac{d}{dt} \begin{bmatrix} u_1(t) \\ u_2(t) \end{bmatrix} = \begin{bmatrix} -\frac{1+k}{\tau_1} & \frac{k}{\tau_1} \\ \frac{1}{\tau_2} & -\frac{1}{\tau_2} \end{bmatrix} \begin{bmatrix} u_1(t) \\ u_2(t) \end{bmatrix} + \begin{bmatrix} \frac{1-k}{\tau_1} \\ 0 \end{bmatrix} \cdot [e(t)]$$

Рисунок 1 Схема ФНЧ та відповідна система рівнянь в просторі станів

Перелік джерел

1. Сигорский В.П., Математический аппарат инженера [Текст]: – Киев, «Наука», 1977, 770 с.

2. Заде Л., Дезоер Ч., Теория линейных систем. (Метод пространства состояний). Под редакцией Г. С. Поспелова [Текст]: – М., «Наука», 1970, 704 с.

РОЗГОРТАННЯ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ЗА ДОПОМОГОЮ ДОКЕРА

Васільєва Ю.С., Курило О.В.

Науковий керівник – ст.викл. каф. ІМІ Малінін О.П.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно – мережної
інженерії, тел. (057) 702-14-29)

e-mail: juliya1999@gmail.com, тел. (096) 234-14-68

oleksandr.kurylo@nure.ua, тел. (099) 563-03-58

A recent Nginx study found that 36% of businesses currently use microservices, while another 26% conduct research on how to implement them. This paper discusses the benefits of microservices as well as how they interact with docker. The advantages of the microservices that we are talking about in the work helps to flexibly configure applications and takes care of data persistence. Containerization is very widely used in modern programming, and this is what we will consider in our work. We will also consider docker, which is the most popular and used platform for the development, operation and delivery of applications.

Мікросервіси - все більш популярна архітектура для створення масштабних додатків. Вони також відомі як мікросервісні архітектури - це архітектурний стиль, який структурує додаток як набір сервісів, які:

- Ремонтопридатні та легко перевіряються;
- Незалежно розгортаємі;
- Належить невеликій команді.

Мікросервісна архітектура забезпечує швидку, часту і надійну доставку великих і складних додатків. Це також дозволяє організації розвивати свій технологічний стек. Існує безліч плюсів, пропонованих архітектурою Microservices. Ось кілька з них:

• Мікросервіси можуть легко адаптуватися до інших систем або технологій.

- Відмова одного процесу не впливає на всю систему.
- Надає підтримку великих підприємств, а також невеликим командам.
- Може бути розгорнутий незалежно і у відносно короткі терміни.

Плюси:

- Свобода використання різних технологій.
- Кожен мікросервіс орієнтований на одну можливість.
- Підтримує окремі розгортаємі блоки.
- Дає змогу частим випускам програмного забезпечення.
- Забезпечує безпеку кожного сервісу.
- Кілька сервісів паралельно розробляються і розгортаються.

Мінуси:

- Збільшує проблеми усунення неполадок.

- Збільшення зусиль для налаштування та інших операцій.
- Складно підтримувати безпеку транзакцій.
- Важко відстежувати дані через різні кордони.

Контейнеризація - це тип стратегії віртуалізації, що з'явився в якості альтернативи традиційної віртуалізації на основі гіпервізора. При контейнеризації операційна система може використовуватися спільно контейнерами, а не клонується для кожної віртуальної машини. Наприклад, Docker надає платформу віртуалізації контейнерів, яка служить гарною альтернативою угодам на основі гіпервізора.

Основна особливість контейнерів - це те, що вони є незмінними (immutable). Якщо ви створили контейнер один раз, він зберігає повний зліпок файлової системи. У будь-який момент, незалежно від середовища запуску, це буде повністю ідентична копія сервісу, включаючи ОС та всі необхідні вам dll-бібліотеки. Такий контейнер буде працювати скрізь однаково: на машині розробника, в тестовому оточенні або в production.

Докер - це відкрита платформа для розробки, доставки і експлуатації додатків. Docker розроблений для більш швидкого викладання ваших додатків. За допомогою docker ви можете відокремити ваш додаток від вашої інфраструктури і поводитися з інфраструктурою як керованим додатком. Docker допомагає викладати ваш код швидше, швидше тестувати, швидше викладати додатки і зменшити час між написанням коду і запуску коду. Docker робить це за допомогою легковагової платформи контейнерної віртуалізації, використовуючи процеси і утиліти, які допомагають керувати і викладати ваші програми.

У своєму ядрі docker дозволяє запускати практично будь-який додаток, безпечно ізольоване в контейнері. Безпечна ізоляція дозволяє вам запускати на одному хості багато контейнерів одночасно.

Docker - відмінний інструмент для управління і розгортання мікросервісів. Кожен мікросервіс може бути далі розбитий на процеси, що виконуються в окремих контейнерах Docker, що можна вказати в файлах конфігурації Dockerfiles і Docker Compose. У поєднанні з інструментом забезпечення, таким як Kubernetes, кожний мікросервіс може бути легко розгорнутий, масштабований і спільно використан командою розробників. Вказівка середовища таким чином також спрощує об'єднання мікросервісів для формування більшого додатку.

Список використаних джерел:

1. <https://www.linode.com/docs/applications/containers/deploying-microservices-with-docker/>
2. <https://habr.com/>
3. <https://vps.ua/blog/docker-and-linux-containers/>
4. <https://microservices.io/>

РОЗРОБКА СИСТЕМИ СТЕЖУВАННЯ ЗА РУХОМИМИ ОБ'ЄКТАМИ

Гнилицький Я. В.

Науковий керівник – ст. викл. каф. ІМІ Малінін О.П.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно – мережної інженерії ,
тел. (057) 702-14-29)

e-mail: grimesarisao@gmail.com, тел. (095) 157-91-41

The given work is devoted to the ability to track and store routes of moving objects. The modern level of technologies makes it possible to use navigation devices in the environment of mobile operators. In this work, compact trackers are used that perform the work of a terminal device of a mobile communication network based on the exchange of SMS messages. To be able to commit the routes of objects it is necessary to create application for the smartphone and connect the database to store related information. The task being solved is widely used in companies and everyday life to control cars, people and other objects.

У сучасних умовах з наявністю розвинених інформаційних мереж стала реальною можливість відстеження переміщень рухомих об'єктів у режимі реального часу та фіксація маршрутів руху на веб-сервері.

Сучасний рівень цифрових технологій дозволяє використовувати доступні широкому колу користувачів навігаційного обладнання працюючого в середовищі операторів мобільного зв'язку.

Представляє інтерес застосування компактних трекерів, виконуючих функцію термінального пристрою мережі мобільного зв'язку, заснованих на обміні СМС-повідомлень. В даній роботі використовується трекер ТК102В. Для роботи у трекер необхідно встановити SIM карту одного з операторів мобільного зв'язку України. Була обрана SIM карта оператора Київстар. Для взаємодії з трекером також необхідно мати смартфон або планшет із встановленою SIM картою будь-якого мобільного оператора. У роботі використовується смартфон Samsung A7 2017. Для зберігання інформації о трекерах використаних користувачем, їх пройдений шлях, призначених для користувача налаштувань та іншої необхідної інформації використовувалася база даних Cloud Firestore.

Для фіксації маршруту пересування трекеру можливі декілька варіантів, серед яких було розглянуто два. Перший спосіб, що був використаний в даному проєкті, передбачає наявність контролюючого мобільного терміналу, наприклад смартфона або планшету маючого SIM карту мобільного оператора. Смартфон посилає виклик на трекер, який у свою чергу відповідає на виклик відправляючи смартфоні свої координати

у вигляді СМС-повідомлення. Другий спосіб полягає в становленні треку такого режиму роботи, при якому він через певні інтервали часу посилає інформацію про власні координати на сервер в мережі інтернет.

Для розробки мобільного застосування використовувався рушій Flutter - SDK з відкритим вихідним кодом, розроблений компанією Google. Переваги використання даної платформи полягають у кількості підтримуваних ним пристроїв, таких як стаціонарні комп'ютери та мобільні пристрої на базі Android і iOS. У якості мови програмування Flutter використовує Dart, який компілюється в бінарний код, зарахунок чого досягається швидкість роботи нарівні з нативними додатками.

Зберігання всієї інформації відбувається у базі даних Cloud Firestore - базі типу document-model, що дозволяє зберігати всі дані в об'єктах, які називаються документами, у вигляді ключ-значення. Де значення може бути чим завгодно, від строкової змінної до бінарного файлу, що дозволяє динамічно і швидко оновлювати і отримувати інформацію. Документи в свою чергу групуються в колекції, що дозволяє отримувати лише потрібну інформацію зменшуючи обсяг одержуваних даних і швидкість обробки запиту.

Алгоритм роботи програми, встановленої на призначеному для користувача пристрої, полягає в організації передачі команд треку та прийомі від нього СМС-повідомлень. Отримане СМС-повідомлення обробляється і отримані з нього координати записуються до бази даних пристроя і синхронізуються з базою даних на сервері. Після чого пройдений трекером маршрут можна побачити на google-мапі у вигляді з'єднаних точок-маркерів. При натисканні на маркер можна дізнатися детальну інформацію про трекер на момент часу перебування в зафіксованому місці. Так само, трекери можна персоналізувати, давши їм особливі імена, іконки чи фотографії.

Розглянуте в роботі завдання показує наскільки широко засоби інформаційних мереж та телекомунікацій увійшли у життя сучасного суспільства і відкриває нові можливості пов'язані з обміном інформації, зокрема з моніторингу переміщень мобільних об'єктів будь-якої природи і походження.

Список використаних джерел:

1. <https://www.munstergps.ie/wp-content/uploads/TK102B-Manual.pdf>
2. <https://flutter.dev/docs>
3. <https://firebase.google.com/docs>

РОЗГОРТАННЯ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ЗА ДОПОМОГОЮ ДОКЕРА

Резнік Я.В.,

Науковий керівник – ст.викл. каф. ІМІ Малінін О.П.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно – мережної інженерії ,
тел. (057) 702-14-29)

e-mail: sipkowski@gmail.com, тел. (099) 6638874

The Face Recognition (FR) is growing as a major research area because of the broad choice of applications in the fields of commercial and law enforcement. Traditional FR methods based on Visible Spectrum (VS) are facing challenges like object illumination, pose variation, expression changes, and facial disguises. Unfortunately these limitations decrease the performance in object identification and verification. To overcome all these limitations, the Infrared Spectrum (IRS) may be used in human FR. So it leads and encourages the researchers for continuous research in this area of FR.

Технології розпізнавання облич – це бізнес, що дуже швидко розвивається. Десятки стартапів та технічних компаній продають послуги з розпізнавання облич готелям, магазинам, і навіть школам та літнім таборам. Бізнес розквітає завдяки новим алгоритмам, здатним ідентифікувати людей з набагато більшою точністю, ніж іще кілька років тому. Для того, щоб покращити точність цих алгоритмів, компаніям необхідно «натренувати» їх на мільярдах облич. Такі обсяги зображень неможливо зібрати, кожного разу запитуючи дозвіл у людини, чиє обличчя зображене на фото. Тож, існуючі бази даних, зібрані за згодою зображених на фото людей, є дуже малими і містять зазвичай лише кілька тисяч облич.

Офіційні бази даних мають і низку інших недоліків – у багатьох базах не вистачає різноманітності за ознакою раси або ж замало фотографій, зроблених у нестандартних умовах – з тінями на обличчі, у капелюсі або з макіяжем. Якщо алгоритм не тренуватиметься на таких «ускладнених» обличчях, то він виявиться абсолютно неефективним у реальному світі.

Тож, компанії часто обирають легший шлях, як-то просто брати з Інтернету фотографії, де позначено імена зафіксованих на них людей. Насправді, є досить висока ймовірність, що і ваше обличчя є частиною «бази для тренування» алгоритму розпізнавання облич якоїсь компанії.

Фактично, для тренування алгоритму необхідна база даних, де до кожної людини прив'язано багато фотографій з її обличчям у різних обставинах, ракурсах та при різному освітленні. Наприклад, якщо користувач робить багато селфі, то отримавши доступ до цих фотографій, компанія має багато різних фотографій, прив'язаних до однієї людини.

Або ж багато користувачів викладають безліч фотографій у соцмережі, позначаючи на них себе та своїх друзів. Такої інформації теж буде достатньо для тренування алгоритму розпізнавання облич.

Цікаву історію має одна американська компанія, яка запустилася у 2012 році під назвою EverRoll як телефонний додаток для організації фотографій. Компанія вирізнялася досить агресивною маркетинговою політикою. Так, щойно додаток завантажувався, він отримував доступ до усіх контактів, збережених на телефоні, і змушував користувача відправити усім цим контактам повідомлення із запрошенням також завантажити цей додаток. Наступним кроком цього додатку було завантаження усіх фотографій з телефону у хмарне середовище.

Такі агресивні маркетингові кроки навіть змусили Apple прибрати цей додаток з Apple Store у 2016 році. Сьогодні, це вже компанія Ever AI, що спеціалізується на технології розпізнавання облич та займає перші місця у змаганнях з точності розпізнавання людей у складних умовах. Як зазначають експерти, такому успіху компанія завдячує своїй величезній базі даних, яка налічує близько 13 мільярдів фотографій.

Варто зазначити, що законодавче регулювання в цій сфері є важливим не лише через проблему приватності, а й через велику частку помилок, яких припускаються системи розпізнавання облич на даному етапі розвитку технології. Цікаво, що першим містом, яке повністю заборонить використання систем розпізнавання облич державними структурами може стати Сан-Франциско – один з основних осередків розробки цих самих систем. Адже, саме розробники краще за інших розуміють наскільки ненадійними є наразі ці системи.

Отож, на сьогодні ми не можемо уберегтися від того, щоб наші фото використовувалися для тренування алгоритмів розпізнавання облич. Однак, у світі вже зрозуміли необхідність регулювання цієї сфери і процес створення відповідних нормативних вимог вже запущено. А поки, не варто надто вже довіряти цим системам – вони помиляються так само як і люди.

Список використаних джерел:

1. Vijayakumari, V. Face Recognition Techniques: A Survey. World Journal of Computer Application and Technology. Vol. 1, N. 2. 2013. P. 41–50.
2. Bui T.T.T., Spitsyn V.G. Digital image dissection by two-dimensional discete wavelet transform and fast Haar wavelet transform. Bulletin of the Tomsk Polytechnic University, vol. 318, no. 5, pp. 73–76, 2011.
3. ORL Face Databases AT&T (Olivetti) Research Laboratories, Cambridge. ORL face databases http://www.uk.research.att.com/pub/data/orl_faces.zip.

ПОРІВНЯННЯ ПРОТОКОЛІВ VPN ДЛЯ ОРГАНІЗАЦІЇ КОРПОРАТИВНОЇ ПРИВАТНОЇ МЕРЕЖІ

Рябко М.С.

Науковий керівник – доц. Костромицький А.І.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно-мережної інженерії
тел. (057) 702-14-29)

e-mail: mykyta.riabko@nure.ua.

This paper considers a comparison of the VPN protocols that are most commonly used when deploying a corporate virtual private network. An Internet-based enterprise VPN is required for the exchange of private information between physically remote equipment and employees. Building a VPN requires knowledge of the protocol features that will be used to transport and encrypt personal data. An understanding of the principles of working via the Internet and the equipment features of network participants is also required. The comparison was based on protocol characteristics such as data transfer rate, security, availability, complexity of blocking and implementation.

Дані, що передаються корпоративною мережею, представляють собою приватну інформацію, яка повинна залишатись конфіденційною під час її транспортування. Оскільки майже всі підприємства, що використовують корпоративну мережу фізично розташовані за межами однієї локальної мережі, є необхідність об'єднати віддалені офіси або окремих співробітників в єдину мережу, використовуючи мережу загального доступу Інтернет. Для об'єднання декількох локальних мереж створюють VPN, що забезпечує шифрування даних і їх наскрізну передачу між користувачами мережі.

Вірний вибір протоколів є основою для VPN, так як всі протоколи мають певні характеристики та вимоги, що до налаштування і реалізації. Тому існує необхідність перед вибором протоколів, виявити, який трафік буде маршрутизуватися, тип та характеристики обладнання користувачів мережі, сумісність протоколів і обладнання, що плануються для використання.

Найчастіше використовують такі протоколи:

- PPTP;
- L2TP/IPsec;
- OpenVPN.

Серед інших протоколів, їх перевагами є сумісність з багатьма операційними системами та доступність.

PPTP це протокол тунельного зв'язку, який працює на каналному рівні. Він створює тунель через мережу Інтернет до сервера-одержувача і передає PPP-пакети віддаленого клієнта, використовуючи інкапсуляцію IP-пакетів. Для автентифікації використовує протокол MS-CHAPv2.

Шифрування – MPPE-128 біт[1]. Середня швидкість 70 Мбіт/с при широкосмуговому з'єднанні 100 Мбіт/с.

Його перевагами являються: швидкість, простота реалізації, стабільність з'єднання, підтримка всіх операційних систем.

Недоліки: низький рівень безпеки – 128 - бітне шифрування, легкий спосіб блокування, працює лише через 1723 порт.

L2TP – це протокол тунельного зв'язку, оскільки він не забезпечує шифрування, разом з ним використовується протокол шифрування IPsec, для забезпечення конфіденційності даних. Використовує 500 UDP-порт. На даний момент IPsec вважається безпечним рішенням при використанні алгоритмів шифрування AES[1].

Переваги: простота реалізації, підтримка всіх операційних систем, високий рівень безпеки та стабільність з'єднання.

Недоліки: низька швидкість та високий рівень використання ресурсів CPU для забезпечення подвійної інкапсуляції, легкий спосіб блокування.

OpenVPN – інструмент з відкритим вихідним кодом. Працює в режимі точка-точка або клієнти-сервер. Має три режими автентифікації:

- за допомогою встановленого ключа;
- автентифікація по сертифікату;
- по логіну і пароллю.

Існує підтримка з'єднання VPN з динамічними віддаленими вузлами, тунелі поверх NAT або за допомогою повноцінного брандмауера. Безпеку і шифрування забезпечено бібліотекою OpenSSL або PolarSSL і протоколом транспортного рівня Transport Layer Security. Дозволяє підключатися через UDP-порт або TCP-порт. При підключенні по UDP підвищується швидкість передачі даних, а при підключенні по TCP підвищується надійність за рахунок збільшення часу затримки.

Переваги: гнучке налаштування, високий рівень безпеки, може працювати крізь брандмауери, використовує широкий спектр алгоритмів шифрування, підтримка багатьох операційних систем.

Недоліки: складність інсталяції, необхідність встановлювати додаткове програмне забезпечення, обмежена підтримка портативними пристроями.

Оскільки кожен з протоколів має певні переваги та недоліки в порівнянні з іншими, зробити однозначний висновок, який з протоколів краще використовувати, можна, тільки провівши більш детальний розбір, що буде виконано в магістерській роботі.

Перелік джерел:

1. Charlie Scott Virtual Private Networks, Second Edition / Charlie Scott, Paul Wolfe, Mike Erwin. – O'Reilly Media, Inc., 1999.

ПОРІВНЯННЯ ІНСТРУМЕНТІВ УПРАВЛІННЯ КОНФІГУРАЦІЄЮ ANSIBLE ТА CHEF

Маслій В.П.

Науковий керівник – доцент Власова В.О.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14 каф. Інформаційно-мережевої інженерії,
тел. (096)595-65-40) e-mail: vladyslav.maslii@nure.ua

Tools for managing the Chef and Ansible buzz conceived to simplify the setup and servicing of the ten, hundreds and thousands of servers. You can automatically unload these configurations to your server in the middle of the server. This thesis will compare these configuration management tools.

Швидкий розвиток віртуалізації укупі зі збільшенням потужності серверів, які відповідають промисловим стандартам, а також доступність “хмарних обчислень” привели до значного зростання числа серверів які потребують управління. Зараз ми повинні управляти набагато більшою кількістю серверів, які можуть бути розподілені по всій земній кулі. У цей момент інструменти управління конфігураціями і вступають в гру. У багатьох випадках, ми управляємо групами однакових серверів, на яких запущені однакові програмами і сервіси. [1]

Ansible та Chef - це два найпопулярніших інструменти управління конфігурацією, які використовуються сьогодні. [2] Хоча обидва інструменти можуть виконувати багато одних і тих самих завдань, кожен з них має свої переваги, і вони виконують завдання помітно по-різному. Порівняймо ці інструменти за такими параметрам:

1. Архітектура

Chef працює по моделі клієнт-сервер, де є сервер Chef, в якому зберігаються ваші Cookbooks і на якому зареєстровані всі сервери або вузли, за які він відповідає. Цей Chef-сервер часто називають «концентратором». Самі вузли запускають клієнтське програмне забезпечення Chef, яке фактично виконує управління автоматизацією і конфігурацією в цій системі після отримання інструкцій від сервера Chef. Chef клієнти регулярно опитують сервер Chef на наявність змін в Cookbooks і, якщо зміни виявляються, виконують необхідні зміни стану в своїх системах. Основною перевагою цієї моделі є те, що вона вимагає дуже мало роботи для сервера Chef, оскільки все, що йому потрібно зробити, це надати клієнтам Chef відповідну інформацію при опитуванні. На відміну від Chef, Ansible не спирається на модель клієнт-сервер. Ansible не використовує агентів і нічого не вимагає для цільових хост-систем, крім ssh і Python. Це значно полегшує початок роботи з Ansible і звичайно, це означає, що на одну систему доводиться менше послуг, які ви повинні відслідковувати і обслуговувати.

Підсумок: почати роботу з Ansible легше, так як він не потребує агентів.

2. Мова

Іншою важливою відмінністю є Cookbooks написані на мові програмування Ruby в Chef і Playbooks написані на мові розмітки YAML в

Ansible. Для написання і читання Cookbooks необхідний досвід роботи з Ruby в той час як Playbooks написані на YAML, легкою для читання людиною мовою серіалізації, такий досвід не обов'язковий. Це значно спрощує створення нових Playbooks, а також дозволяє читати і розуміти Playbooks, написані кимось іншим, але має обмеження, що полягає в тому, що ви не завжди можете виконувати складні завдання з налаштування таким чином, щоб це було природно. Chef дозволяє простіше вирішувати завдання зі складною логікою роботи. Насправді, складні завдання в Ansible іноді можуть здатися дуже «хакерськими», і вам іноді доведеться покладатися на Jinja2 для цих цілей. З огляду на, що Ansible почав розробку тільки в 2012 році, можна очікувати, що з часом випадковий «хакерський» обхідний шлях поступиться місцем більш природнім рішенням в більш пізніх випусках програмного забезпечення.

Підсумок: Playbooks в порівнянні з Cookbooks набагато простіше створювати і розуміти, але вони обмежені в складності завдань конфігурації, які ви можете виконувати з їх допомогою.

3. Статична і динамічна інвентаризація

Ще однією перевагою Ansible перед Chef є те, як він керує своєю системою хост-систем. З Chef хости повинні бути індивідуально зареєстровані на сервері Chef. Однак Ansible пропонує кілька варіантів для джерела інвентаризації: простий INI-файл з хостами, класифікованими по розділах; база даних; або інше джерело, можна опитувати, для визначення того, які на ньому сучасні системи. Така гнучкість дозволяє Ansible використовувати запаси, які є статичними або динамічними.

Підсумок: на відміну від Chef, Ansible може використовувати динамічні і статичні списки хост-систем.

Проте, якщо ви повинні вибрати між ними, спочатку ретельно продумайте свої власні потреби і порівняйте їх з тим, що пропонує кожне рішення.

Переваги Ansible. Швидкий та простий при розгортанні та написанні Playbooks. CLI підтримує майже всі мови програмування. Гарна безпека яка забезпечується використанням SSH ключів.

Недоліки. Відносно новий та недостатньо тестований. Недопрацьований GUI та погана підтримка Mac Os.

Переваги Chef. Більш розвинений та має гарну документацію. Має багато модулів для вирішення складних задач доволі просто.

Недоліки. Досвід роботи з Ruby. Використання формату JSON замість більш дружнього для користувача YAML.

Список джерел

1. Огляд: Puppet, Chef, Ansible, Salt [Електронний ресурс] – Режим доступу до ресурсу: <https://habr.com/ru/post/211306/>

2. Chef vs Ansible [Електронний ресурс] – Режим доступу до ресурсу: <https://www.loomsystems.com/blog/single-post/2017/07/20/chef-vs-ansible-comparison-of-configuration-management-tools>

ВИБІР ОПТИМАЛЬНОГО ВАРІАНТУ МІНІ-ПК ДЛЯ ОРГАНІЗАЦІЇ МЕРЕЖІ ІоТ

Братійчук І.Ю., Чеботарьова Д.В.

Науковий керівник – ст. викл. Малінін О.П.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. інформаційно-мережної інженерії,
тел. (057) 702-14-29)
e-mail: dariia.chebotarova@nure.ua

Application mini PC is actual at the construction of clever houses. Thus important is an optimal choice mini PC for organization of effective central element of network. The most recent mini PC configurations were reviewed in this work: Raspberry PI 4B, nVIDIA Jetson Nano, Radxa Rock pi 4b, Odroid – XU4Q, Odroid C2, Nano Pi M4, Nano PCT2, Orange Pi3, Banana Pi M3, Banana Pi M64. For more detailed analysis and selection of the best variant of mini PCs were tested with the help of service programs Phoronix Test Suite, Benchmark, Sysbench and Iperf. The requirements for the central IoT device (performance, data rate and peripherals, etc.) that have been tested are most in line with the Raspberry PI 4B mini PC.

На сьогоднішній день велику популярність набуває застосування мінікомп'ютерів (міні ПК) при розробці інформаційних систем та мереж в багатьох галузях науки і техніки, особливо при побудові розумних будинків. Саме тому задача вибору оптимальних варіантів міні ПК для побудови мереж є актуальною.

Для організації мережі ІоТ необхідно виконати вибір міні ПК, який буде виконувати роль центрального елементу в мережі. Центральний елемент є локальним сервером, що виконує збір та обробку інформації, підтримує локальну базу даних (БД), приймає необхідні рішення та підтримує роботу всієї мереж ІоТ.

В роботі було виконано огляд найбільш актуальних конфігурацій міні ПК, а саме: Raspberry PI 4B, nVIDIA Jetson Nano, Radxa Rock pi 4b, Odroid – XU4Q, Odroid C2, Nano Pi M4, Nano PCT2, Orange Pi3, Banana Pi M3, Banana Pi M64. Було детально розглянуто основні параметри та виконано аналіз переваг та недоліків досліджуваних міні ПК. Для отримання більш детальної інформації було проведено тестування всіх розглянутих варіантів міні ПК за різними характеристиками.

Тестування є невід'ємною частиною оцінки продуктивності і якості будь-якого обладнання та програмного забезпечення. Саме тому, в роботі велику увагу приділено тестуванню міні ПК.

Для тестування міні ПК було обрано сервісні програми Phoronix Test Suite, Benchmark, Sysbench, Iperf. Утиліта Phoronix є кросплатформним рішенням, вона має дуже широкий набір найбільш популярних та

ефективних тестів, а також готові комплексні тести для тестування окремих компонент. Утиліта тестування Phoronix – це потужний і універсальний інструмент тестування обладнання і системи в цілому. Активна підтримка і розвиток даного проекту роблять його дуже перспективним [1].

За допомогою Phoronix Test Suite, Benchmark, Sysbench та Iperf для міні ПК виконано наступні тести: тестування швидкості роботи CPU; тест AOBench, що аналізує перетворення масиву даних; тест encode-mp3-1.7.0, що аналізує реакцію процесора на перекодування аудіо формату wav в формат mp3 за допомогою codec lame; тест rybench для CPU; тест cashebench, що фіксує швидкість обміну даними між cashe пам'яттю процесора і ОЗП міні ПК; тести швидкості роботи ОЗП (ramspeed, tinymembench, Memory Read та Memory Write); тест швидкості роботи з БД OLTP, тестування пропускної здатності мережі Ethernet та пропускної здатності мережі WiFi; тест швидкості роботи з картою пам'яті SD; тест швидкості роботи з USB; тест копіювання файлу 9 Гб по Ethernet; тест на споживану потужність та вимірювання температури SoC під навантаженням.

В результаті тестування було виявлено, що вимогам, які висуваються на центральний пристрій мережі IoT (продуктивність, швидкість роботи з даними та перефрією, вартість тощо), найбільше відповідає міні ПК версії Raspberry PI 4B. Тому саме Raspberry PI 4B можна рекомендувати для використання в якості центрального елемента при розробці мережі IoT.

Характеристики міні ПК версії Raspberry PI 4B наведено в табл.1.

Таблиця 1 – Характеристики міні ПК Raspberry PI 4B

Характеристика	Значення	Інше
SoC	Boadcom BCM2711	USB-C (5B), Dual HDMI
CPU cores	4 x Cortex A72	
CPU freq	1500	
RAM size	4 Gb	
RAM type	LPDDR4	
Ethernet	1000 Mbit/s	
WiFi	2.4 GHz; 5 GHz	
USB	2 x USB3.0; 2 x USB2.0	

ПЕРЕЛІК ПОСИЛАНЬ:

1. Утиліта тестирования Phoronix Test Suite [Електронний ресурс]
Режим доступу: <https://itproffi.ru/utilita-testirovaniya-phoronix-test-suite/> –
(дата звернення 11.02.2020 р.) – Назва з екрана.

АНАЛІЗ ТА ПОРІВНЯННЯ ОРГАНІЗАЦІЇ ХМАРНОЇ ІНФРАСТРУКТУРИ РІЗНИХ ПРОВАЙДЕРІВ

Абіх І.В.

Науковий керівник – к. т. н., доц. Костромицький А. І.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережна інженерія»,
тел. (057) 702-14-29; e-mail: iryna.abikh@nure.ua)

In today's information technology world, cloud technologies are actively deployed in all developed countries, providing fundamentally new, cost-effective business, management, education and research opportunities.

This study analyzes its cloud infrastructure options for three popular providers: Amazon Web Services, Google Cloud Platform, and Microsoft Azure. The advantages and disadvantages are analyzed, as well as the comparison of virtual machine deployment speeds, delays in some regions and the cost of computing services, and the comparison of services and features.

У сучасному світі інформаційних технологій хмарні інфраструктури знаходять широке застосування у всіх розвинених країнах, забезпечуючи принципово нові, економічно ефективні можливості для бізнесу, управління, освіти і наукових досліджень.

Хмарні сервіси є комбінацією існуючих технологічних рішень, які взаємно інтегровані для забезпечення максимальної автоматизації і мінімізації участі людини в роботі комплексу.

Використання хмарних технологій є актуальним питанням для всіх галузей, а відповідно і вибір провайдера, як постачальника послуги набуває особливого значення. Тому мета нашого дослідження провести аналіз та порівняння організації хмарної інфраструктури Amazon Web Services, Google Cloud Platform і Microsoft Azure.

Можна знайти досить багато різних порівнянь провайдерів, які досить повно дають уявлення про сервіси і особливості топових провайдерів [1,2], однак автори не дають однозначних рекомендацій через різні потреби та умови використання ресурсів, а також питання бізнесу та конкуренції не позбавлене сенсу.

Порівняння хмарних провайдерів у дослідженні засноване на аналізі часу розгортання інфраструктури та складається з таких сервісів: віртуальних машин, бази даних та балансувальника навантаження.

Віртуальні машини є основою для будь-якої інфраструктури, яка в свою чергу необхідна для розгортання додатків. Балансування навантаження важливий елемент інфраструктури який автоматично розподіляє трафік додатків із зміною навантаження в одній або між декількома зонами доступності. Забезпечуює високу доступність, автоматичне масштабування та надійни захист, необхідний для

забезпечення безпеки та відмовостійкості. Також важливою складовою хмарної інфраструктури є бази даних вони автоматично масштабуються, розширюючи і зменшуючи можливості для обробки пікових навантажень, та оптимізує витрати.

Кожен з наведених хмарних провайдерів, безперечно, має свої переваги. Amazon Web Services – один из перших провайдерів. Він має величезну популярність та велику підтримку ІТ-суспільства. Є найбільш розгалуженою мережею центрів обробки даних, має прогресивно зростаючий набір послуг, які випереджають час, володіє ресурсами для машинного навчання, віртуальної реальності, робототехніки, супутникового зв'язку, мобільного зв'язку, квантових технологій та ін.

Основним плюсом Microsoft Azure є те, що він тісно інтегрований з програмним забезпеченням Microsoft, має найрозвиненішу інфраструктуру з великою кількістю регіонів по всьому світу, у порівнянні з іншими постачальниками хмарних служб. Azure має унікальний сервіс - Azure DevOps - корисний та зручний сервіс, який допомагає вправно та легко організувати CI/CD процес.

Google Cloud Platform пропонує зрозумілий інтерфейс, значний масштаб і балансування навантаження, швидкий доступ до ресурсів та обробку даних, порівняно низьку ціну. Компанія Google розробила стандарт Kubernetes, тобто GCP, має найзручніший сервіс контейнеризації.

Результатами дослідження та дискусії серед DevOps спеціалістів є такий висновок, що Microsoft Azure – більш дорогий, Google Cloud Platform – більш швидкий, а Amazon Web Services – більш надійний та широкоживаний провайдер. У кожного провайдера є партнерські програми та знижки на зарезервовані ресурси, навчальні програми, та зручні ресурси для менеджменту та бізнесу.

У даній роботі було проаналізовано та визначено загальні принципи хмарних технологій та сервісів, хмарних обчислень, аналіз чинників розвитку хмарних технологій, а також визначено напрями реалізації цих питань. Проведений аналіз різних провайдерів хмарних технологій, визначено всі недоліки і переваги.

Список джерел

1. AWS vs GCP vs Azure [Електронний документ] - Режим доступу до ресурсу <https://www.educba.com/aws-vs-azure-vs-google-cloud/> - 19.02.2020 р.
2. Compare Top Public Cloud Providers [Електронний документ] - Режим доступу до ресурсу <https://www.flexera.com/blog/cloud/compare-top-public-cloud-providers-aws-vs-azure-vs-google/> - 17.07.2018 р.
3. Cloud Comparison [Електронний документ] - Режим доступу до ресурсу <https://www.datamation.com/cloud-computing/aws-vs-azure-vs-google-cloud-comparison.html> - 19.02.2020 р.

ЗАХИСТ ІНФОРМАЦІЇ В КЛІНІЧНОМУ ІНТЕРНЕТІ РЕЧЕЙ

Кирсанов О.О. Безлуцький В.О.

Науковий керівник – к.т.н., доц. Кривенко С.А.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. інформаційно-мережної інженерії)
e-mail: kirsanov7008@gmail.com, тел. (066) 480-98-56

This document illustrates a considered approach for analyzing the security considerations for components, systems and operational environments related to Clinical IoT Data and Devices. The determination of usefulness and applicability of this approach and the viability of the resulting recommendations for a specific component, device, system or operational environment is the joint responsibility of the parties who engineer the systems and devices; the parties who determine the suitability of components, devices and systems in a given operating environment.

Стандарт P2733 встановлює рамки з принципами TIPSS (Довіра, Ідентичність, Конфіденційність, Захист, Безпека, Безпека) для даних клінічного Інтернету речей (IOT) та перевірки та сумісності пристроїв. Сюди входять клінічні IOT та сумісність із системами охорони здоров'я, включаючи Електронні записи здоров'я (EHR), Електронні медичні записи (EMR), інші клінічні пристрої IOT, на лікарняних пристроях та майбутні пристрої та підключені системи охорони здоров'я [1].

Метою даної роботи є аналіз міркувань безпеки для компонентів, систем та операційних середовищ, пов'язаних з клінічними даними і пристроями інтернету речей.

Зловмисними суб'єктами можуть бути або люди, або ті, що не є особами, наприклад, комп'ютерні боти, віруси, хробаки тощо. Зловмисні суб'єкти здійснюють атаки на свої цілі. Зловмисна поведінка зазвичай має один з двох шляхів: (1) зловживання процесом, технологією або даними людей; або (2) використання вразливостей і недоліків в дизайні, конфігурації і експлуатації пристроїв на які базуються пристрої.

Аналіз безпеки складається з перерахування атак, сценаріїв атак, кампаній атак та оцінки релевантності цих атак, сценаріїв атак і кампаній атак для конкретного пристрою, системи та операційного середовища. Актуальність будь-якої атаки заснована на оцінці серйозності, ймовірності та впливу атаки на передбачувану операцію і передбачуваний результат роботи компонента та системи.

Зловмисник заражає пристрої з метою масового злому пристроїв для отримання доступу до внутрішніх корпоративних мереж для одного з наступних:

- встановити програмне забезпечення для вимагання в корпоративній мережі;
- для вилучення даних;
- для зараження систем, що за корпоративною прошивкою;
- зловмисне перенастроювання пристроїв IoT для шахрайських цілей.

Приклад переліку кампаній нападів на клінічні системи IoT: порушення ділових операцій: шахрайський суб'єкт проникає в клінічне IoT-операційне середовище з метою негативного впливу на функціонування одного або декількох бізнес-процесів; фінансовий прибуток через вимагання: шахрайський суб'єкт проникнув у клінічне операційне середовище IoT з метою утримання даних для подальшого викупу; крадіжка інтелектуальної власності: шахрайський суб'єкт проникнув у клінічне операційне середовище IoT з метою збору і вилучення програмного забезпечення та операційних даних.

Сценарії атаки:

- несправний або погано налаштований пристрій має порти, піддані доступу до Інтернету. Націлене зловмисне програмне забезпечення визначає та розпізнає його та заражає його;
- Несправний або погано налаштований пристрій має порти, піддані надійному з'єднанню. Націлене зловмисне програмне забезпечення визначає та розпізнає його та заражає його;
- ПК або ноутбук у мережі які були заражені зловмисним програмним забезпеченням або іншим чином піддаються ризику. Потім цей пристрій використовується для пошуку вразливих пристроїв [2].

Список використаної літератури

[1] T. Thompson, «P2733 - Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS,» 20.02.2020. [Онлайновий]. Available: <https://standards.ieee.org/project/2733.html>.

[2] М.-Б. Александр. 20.02.2020. [Онлайновий]. Available: <http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/10448>. [Дата звернення: 20.02.2020].

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВЗАЄМОПОВ'ЯЗАНИХ ГІПЕРТЕКСТОВИХ ДОКУМЕНТІВ ВСЕСВІТНЬОЇ ПАВУТИНИ ТА ІНФРАСТРУКТУРИ ДЛЯ ПІДТРИМКИ ЕЛЕКТРОННОЇ ПОШТИ

Ключников Є.Ю.

Науковий керівник – к.т.н, доцент Кривенко С.А.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно-мережної інженерії,
тел. +38(057) 702-14-29)

e-mail: yevhen.kliuchnykov@nure.ua

Artificial neural networks are computing systems that simulate decision making in the biological nervous systems of animals. The biological nervous system is composed of neurons (nerve cells) connected to each other. Using the hypertext transfer protocols of the World Wide Web and the email infrastructure, it is possible to use the computing power of devices connected to the network. Using the above protocols, the calculation of the individual elements of the neural network is performed on clients (computing devices connected to the network). The regulation of the neural network operation is performed by the server.

Штучні нейронні мережі [1] - це обчислювальні системи, які симулюють процес прийняття рішень у біологічних нервових системах тварин. Біологічна нервова система складається з нейронів (нервових клітин), пов'язаних між собою. Нейронні імпульси приймаються тілом нейрона та передаються далі через аксон, та через синоптичне з'єднання, до інших нейронів. За допомогою протоколів передачі гіпертекстових документів всесвітньої павутини та інфраструктури для підтримки електронної пошти можливо використовувати обчислювальні потужності обчислювальних приладів, підключених до мережі. SMTP і HTTP - це протоколи прикладного рівня, які використовуються для передачі інформації між хостами. SMTP використовується для передачі електронних листів між поштовими серверами, тоді як HTTP використовується для передачі даних з веб-сервера до веб-клієнта.

Мета роботи розглянути суттєві відмінності між SMTP та HTTP [2]

HTTP (HyperText Transfer Protocol) [3] – це протокол прикладного рівня створений для передачі гіпертекстових документів у форматі .html, сьогодні також використовується для передачі будь-яких типів даних.

SMTP (Simple Mail Transfer Protocol) [4] – це комунікаційний протокол прикладного рівня для пересилання електронної пошти.

За допомогою вище вказаних протоколів розрахунок окремих елементів нейронної мережі виконується на клієнтах (обчислювальних приладах, підключених до мережі). Регулювання роботи нейронної мережі виконується сервером.

Така модель нейронної мережі надає можливість використовувати окремі обчислювальні обладнання, пов'язані за допомогою всесвітньої павутини, для реалізації роботи однієї нейронної мережі.

SMTP	HTTP
Це протокол push, тобто сервер, що відправляє, поштовхує дані на поштовий сервер, ініціюючи з'єднання TCP.	Це протокол витягування, тобто клієнт витягує інформацію, доступну на сервері, ініціюючи з'єднання TCP.
SMTP використовує стійке з'єднання.	HTTP може використовувати як стійке, так і непостійне з'єднання.
За замовчуванням SMTP використовує порт 25.	За замовчуванням HTTP використовує порт 80.
Він вимагає кодування бінарних мультимедійних даних у 7-бітному ASCII.	Він не вимагає кодування двійкових мультимедійних даних у 7-бітовому ASCII.
Він розміщує всі об'єкти в одному повідомленні.	Він розміщує кожен об'єкт у власному HTTP-повідомленні.

Список використаних джерел:

[1] D. Graupe, Principles of Artificial Neural Networks, London: World Scientific, 2013.

[2] "SMTP vs. HTTP," 21 2 2020. [Online]. Available: <https://www.educative.io/edpresso/smtp-vs-http>. [Accessed 21 2 2020].

[3] M. Belshe, R. Peon, M. Thomson, Ed., "Hypertext Transfer Protocol version 2," 15 2 2015. [Online]. Available: <https://tools.ietf.org/html/draft-ietf-httpbis-http2-17>. [Accessed 21 2 2020].

[4] J. Klensin, "Simple Mail Transfer Protocol," 4 2001. [Online]. Available: <https://www.ietf.org/rfc/rfc2821.txt>. [Accessed 21 2 2020].

ПОДАННЯ ФУНКЦІЙ ЩІЛЬНОСТІ ЙМОВІРНОСТІ РОЗПОДІЛІВ ДКП КОЕФІЦІЄНТІВ JPEG ЗОБРАЖЕНЬ КРИВИМИ ПІРСОНА

Цариценко С.Д., Федоров О.В.

Науковий керівник – ст. викл. Федоров О.В.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно-мережної інженерії,
тел. (057) 702-14-29)

e-mail: semyon4k777@gmail.com

The paper employs technique of Person's curves to approximate and discover properties of the DCT coefficient densities of JPEG images. In particular, the conducted research has shown that beta distribution of the 2-nd type provides good agreement with the empirical data. Despite the fact that our research is focused on JPEG images, research output is going to be applicable to a much broader selection of contemporary image formats as many of them are DCT based.

Відмітною рисою сучасності є можливість оперувати великими обсягами даних. Для ефективної передачі та зберігання мультимедійних даних застосовують методи стиснення із втратами інформації. Такі методи хоча і не забезпечують зберігання ідеально точного зображення або аудіо запису, але дозволяють значно збільшити коефіцієнт стиснення в порівнянні із методами стиснення без втрат за рахунок незначного для сприйняття людини спотворення.

Зазвичай методи стиснення із втратами працюють у просторі деякого перетворення, що має властивість компактифікувати енергію перетворюваного сигналу [1]. Так, якщо, відповідно до алгоритму роботи JPEG, розбити зображення на блоки розміром 8x8 пікселів, а потім застосувати до них двомірне дискретне косинусне перетворення (ДКП), для кожного блоку отримаємо його частотне представлення. Побудувавши гістограму розподілу кожної з частотних складових можна зауважити, що для більшості натуральних зображень емпірична щільність імовірності АС ДКП коефіцієнтів виявляється симетричною відносно нуля.

Коли ми маємо справу із стисненням зображення, одразу постають два суттєвих питання. А саме: вибір оптимальних параметрів алгоритму стиснення зображення, таким чином аби досягти найкращої якості зображення з огляду на його розмір, або навпаки: гарантувати найменший розмір стисненого зображення при заданій якості. Адекватно підібрані статистичні моделі ДКП коефіцієнтів вирішують обидва із зазначених вище питань. На практиці часто використовується апроксимація за допомогою розподілу Лапласа [2]. Для досягнення більшої точності апроксимації варто використовувати узагальнений гаусів розподіл [3].

Інтуїтивно зрозуміло, і це підтверджується експериментальними дослідженнями, що форма емпіричного розподілу ДКП коефіцієнтів

визначається структурними особливостями певного зображення. Наприклад, для зображень, що містять у своєму складі суттєві області монотонності, розподіл Лапласа погано узгоджується з емпіричними даними, отже забезпечує неприйнятну точність прогнозування (оцінювання) якості зображення (що є суттєвим для задач компресії зображень). Навпаки, для зображень з ярко вираженими текстурними ознаками, модель Лапласа добре спрацьовує. Таким чином, для коректного врахування структурних властивостей зображення при оцінюванні (прогнозуванні) якості стиснених JPEG зображень слід використовувати альтернативні моделі розподілу ДКП коефіцієнтів. Ефективне застосування таких моделей можливе лише за умови, що вони не будуть надто складними та матимуть економні з обчислювальної точки зору методи оцінювання їх параметрів.

Цим вимогам задовільняє система кривих Пірсона, зокрема бета-розподіл 2-го роду [4]:

$$f(x) \propto \frac{|x|^{p-1}}{(1+|x|)^{p+q}}, \quad -\infty < x < \infty, \quad (1)$$

де p, q – параметри розподілу, значення яких визначається за методом моментів з урахуванням $f(0)$.

Зауважимо, що при $p=1$ (1) стає розподілом Sallee [5]:

$$f(x) \propto \left(1 + \frac{|x|}{s}\right)^{-q}, \quad -\infty < x < \infty \quad (2)$$

де $q > 1, s > 0$ – параметри розподілу.

Проведені експериментальні дослідження з напівтоновими JPEG зображеннями розміру 256×256 пікселів показали гарну узгодженість класу моделей (1) із значеннями ДКП коефіцієнтів зображень.

Список використаних джерел:

1. Lim, J. S. (1990). Two-Dimensional signal and image processing. New Jersey: Prentice-Hall, 694.
2. Lam, E. Y., Goodman, J. W. (2000). A mathematical analysis of the DCT coefficient distributions for images. IEEE Transactions on Image Processing, 9 (10), 1661–1666.
3. Nadarajah, S. (2009). Gaussian DCT coefficient models. Acta applicandae mathematicae, 106(3), 455-472.
4. Kendall, M., Stuart, A. (1977). The advanced theory of statistics. Vol. 1: Distribution theory. London: Griffin, 1977, 4th ed.
5. Sallee, P. (2004). Model-based steganography. Digital Watermarking. Lecture Notes in Computer Science. Berlin: Springer, 2939, 154–167.

ОГЛЯД ОСОБЛИВОСТЕЙ ТА ВЛАСТИВОСТЕЙ ПЕРЕТВОРЕННЯ УОЛША ІНФОРМАЦІЙНИХ СИГНАЛІВ

Туренко А.В.

Науковий керівник: – к.т.н. Бондар Д.В.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. інформаційно-мережної інженерії,
(057) 702-14-29)

e-mail: kyritta@gmail.com. тел. 093-392-28-57

Currently, interest in studying orthogonal signal transformations, and among them Walsh transforms, continues to grow. This is facilitated by the availability of high-speed digital computers, as well as significant advances in digital circuit technology and the development of specialized digital processors. Recently, the trend of more active use of discrete Walsh transforms continues to develop rapidly.

Numerous studies of Walsh functions and related theoretical and practical issues, in particular, problems of their effective formation, are due to a wide range of applications of these functions.

Застосування електричних сигналів для будь-яких цілей, зокрема і для формування, передачі та прийому інформації, передбачає опору на використання методів перетворення сигналів. Основним з перетворень безумовно є перетворення Фур'є, яке передбачає пов'язування сигналів з відповідними до них спектральними функціями або спектрами. Перетворення Фур'є виконується в ортогональному базисі гармонічних сигналів. Але відомі ще інші перетворення і також в негармонічному базисі.

Перетворення Уолша є найбільш відомим серед негармонічних ортогональних перетворень. Перетворення Уолша широко застосовується при цифровій обробці сигналів, так як воно може бути обчислено тільки з використанням операцій обчислення суми та різниці. Внаслідок цього апаратурна та програмна реалізація перетворення Уолша є простішими відносно інших перетворень.

Уявлення сигналу $s(t)$ у вигляді ряду Уолша аналогічне до представлення його у вигляді ряду Фур'є.

$$s(t) = \sum_{k=0}^{\infty} d_k \text{wal}(k, t);$$
$$d_k = \int_0^1 s(t) \text{wal}(k, t) dt.$$

Базис сигналів Уолша є не тільки ортогональним але і нормованим. Самі сигнали складаються з серій прямокутних імпульсів, що максимально спрощує їх генерування та добре пристосовує для обробки пристроями цифрової схемотехніки.

Успішному використанню функцій Уолша і перетворення Уолша в відповідних областях науки і техніки сприяло вивчення наступних питань: властивості функцій Уолша; властивості спектрів Уолша; загальні питання застосування функцій Уолша при виконанні перетворень; алгоритми БПУ; обчислення кореляційних функцій і виконання згорток на базі функцій Уолша; застосування функцій Уолша для дослідження випадкових процесів; використання функцій Уолта при побудові цифрових фільтрів.

Практично важливим є використання функцій Уолша для формування сигналів, які передаються по лініях радіозв'язку. Запропоновано використовувати їх в якості носіїв при поширенні сигналів в радіоканалі над поверхнею Землі, опрацьовані питання генерування і прийому сигналів цього виду. Функції Уолша застосовані при розробці багатоканальних систем зв'язку, в яких одночасно передаються різні сигнали по кожному каналу зв'язку, тобто реалізовано метод багатоканального зв'язку на підґрунті розподілу каналів за формою сигналів. Вони знайшли в галузі зв'язку та ряд інших застосувань, зокрема, на основі використання функцій Уолша розроблені вдосконалені методи завадостійкого кодування сигналів, раціональним чином вирішені питання декодування кодів Ріда-Малера і проведені інші дослідження і розробки в цьому напрямі.

Здійснення перетворення Уолша технічними засобами можливе декількома способами:

- безпосереднє, що передбачає генерування сигналів Уолша з наступним апаратним або програмним розрахунком скалярного добутку з досліджуванним сигналом;
- метод матричного добутку;
- використання швидких алгоритмів перетворення Уолша;
- шляхом цифрової фільтрації на засадах парадигми вейвлет-перетворення.

Як це завжди буває: жоден з перелічених методів не є найкращім. Уподобання в застосуванні визначається умовами задачі, яка підлягає розв'язанню. Однак останній з означених методів винайдено та опрацьовано відносно недавно, а тому він ще має підвищений інтерес для вивчення.

Перелік джерел

1. Ахмед Н., Рао К. Р., Ортогональные преобразования при обработке цифровых сигналов: Пер. с англ./Под ред. И. Б. Фоменко. [Текст]: – М.: Связь, 1980.—248 с.
2. Залманзон Л.А., Преобразование Фурье, Уолша, Хаара и их применение в управлении, связи и других областях [Текст]: – М., «Наука». Гл. ред. физ.-мат. лит., 1989, 496 с.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ VPN НА ПРОИЗВОДИТЕЛЬНОСТЬ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ВО ВРЕМЯ БРАУЗИНГА

Назаренко Ю.В.

Научный руководитель – к.т.н., ст. преп. Иваненко С.А.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки, 14, каф. ЭВМ, тел. (057) 702-13-54)
e-mail: yuliia.nazarenko@nure.ua

In today's world, developers are increasingly worried about the security of personal data on the network. Constantly is being developed to improve security programs and eliminate computer weaknesses. But you always have to pay for such improvements. We pay computer productive capacity for secure site isolation.

Информационные услуги занимают существенное место в жизни современного человека. При этом большая ее часть доступна посредством использования интернета. В последнее время многие пользователи стали обращать внимание на нехватку производительности ПК, при использовании браузера. При оценке объёма занимаемой оперативной памяти приложениями можно обнаружить, что браузер является одной из самой ресурсоёмких программ. В данной работе рассматривается влияния субфреймов на производительность ПК.

Субфрейм — это функция изоляции сайтов, которая используется для борьбы с уязвимостью Spectre. Данная уязвимость была обнаружена исследователями североамериканской корпорации Google. Это группа аппаратных уязвимостей, ошибка в большинстве современных процессоров, имеющих динамическое выполнение команд. Spectre открывает доступ ко всем данным пользователя за счет подключения служб браузера для изъятия информации о паролях, банковских картах, истории поиска и так далее.

Субфреймы разделяют каждый процесс, протекающий в браузере, и ограничивают их с помощью встроенной защиты. Таким образом, предотвращается прямой доступ вредоносного ПО к памяти устройства.

Браузер автоматически разделяет и ограничивает процессы каждого отдельного домена и с помощью встроенной защиты от Spectre предотвращает прямой доступ к памяти компьютера через каждый отдельный процесс. Данное решение повышает уровень безопасности веб-серфинга, однако платить за него приходится оперативной памятью, которая наряду с быстродействием процессора устройства определяет общую производительность ПК.

Рассмотрим более подробно вариант возникновения проблемы с ухудшением производительности во время интернет-серфинга.

Ни для кого не секрет, что содержимое сайтов в изобилии содержит встроенную рекламу, имеющую различные источники происхождения. Для

того, чтобы исключить из отображения назойливую рекламу используются программы блокировщики (ABP, uBlock). Так же многие пользователи используют бесплатные VPN-сервисы, которые могут позволять некоторую анонимность пользователю, и позволяют получать доступ к различным сервисам, которые могут быть недоступны по тем, или иным причинам в некоторых странах.

В результате проведения эксперимента была выявлен следующее: при совместном использовании VPN (в браузере Opera использовался встроенный сервис, в Chrome использовалось расширение TouchVPN) и какого-либо блокировщика (например ABP) с течением времени наблюдалось значительное увеличение объёма оперативной памяти занимаемой браузером.

Для выяснения причины подобного поведения решено было воспользоваться встроенным диспетчером задач браузера Google Chrome, который позволяет отслеживать различные процессы интернет страниц, в том числе и их ресурсоемкость.

В результате исследования была выявлена тенденция к увеличению объёма занимаемой оперативной памяти некоторых субфреймами, которые по своей сути являлись рекламными баннерами известных интернет площадок, социальных сетей и т.д. Размеры таких отдельных субфреймов с течением времени увеличивались до 1,5 ГБ, при этом счётчик заблокированных элементов блокировщиком рекламы постоянно увеличивал значение. Следует отметить, что при отключении блокировщика, проблема исчезала, ровно, как и при отключении VPN. В первом случае, субфреймы оставались, но не увеличивались в размере. Во втором случае, некоторые из них исчезали вовсе, что свидетельствует о том, что бесплатные VPN сами являются источниками дополнительной рекламы на страницах. Когда же они начинают отфильтровываться блокировщиками, это видимо приводит к их повторной попытке открытия, что в результате и приводит к засорению оперативной памяти субфреймом.

Эксперимент был проверен в нескольких браузерах на разных компьютерах. Таким образом, бесплатные VPN являются источниками дополнительной рекламы и ухудшением общей производительности ПК.

Литература:

1. Что такое Субфрейм в Google Chrome [Электронный ресурс].// chromeum.ru – 2019. – Режим доступа до ресурсу: <https://chromeum.ru/faq/what-is-subframe-in-google-chrome>.
2. Изоляция сайтов в Chrome [Электронный ресурс] // gadgetstyle.com.ua. – 2019. – Режим доступа до ресурсу: <https://www.gadgetstyle.com.ua/47168-chrome-site-isolation-feature/>.

ДОСЛІДЖЕННЯ ШУМОПРИГНІЧУЮЩИХ ФІЛЬТРІВ ІМПУЛЬСНИХ ЗАВАД

Коновалова. К. Ю.

Науковий керівник – к.т.н., ст. викл. Іваненко С.А.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно-мережної інженерії,
тел. +38(057) 702-14-29

e-mail: kateryna.konovalova@nure.ua

Impulse noise is one of the main factors that worsen the transmission quality of various ones, and can occur both during the transmission of signals carrying information over communication channels and directly during their processing, for example, due to decoding errors.

На сьогоднішній день питання електромагнітної сумісності радіоелектронної апаратури стає все більш актуальним. Зростаюча кількість радіоелектронних засобів підвищує вимоги до якості функціонування обладнання. Проте електромагнітна обстановка залишається досить напруженою через велику кількість завад із різноманітними джерелами походження.

Досить розповсюдженими є імпульсні завади (ІЗ), джерелами яких можуть бути: електромеханічне обладнання, наприклад, електродвигуни та імпульсні джерела вторинного електроживлення створюють високочастотні електромагнітні перешкоди (ЕМП).

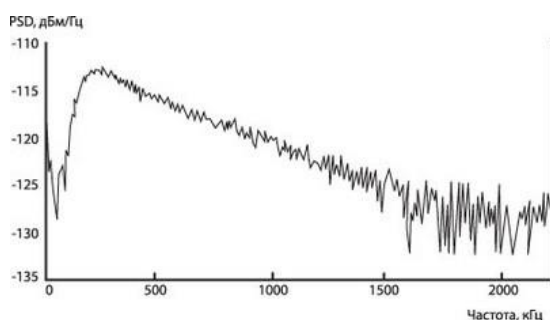


Рис. 1 Спектральна щільність імпульсних перешкод

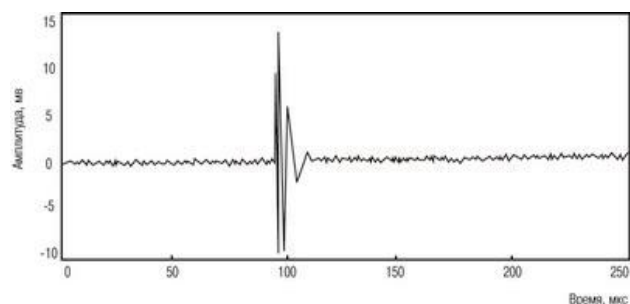


Рис. 2 Часова характеристика імпульсної завади

Найбільш чутлива до ЕМП є радіоприймальна апаратура. Для боротьби із таким типом завад використовуються придушувачі NB (Noise Blanker).

Використання аналогових реалізацій таких придушувачів розраховано на певний тип перешкод, і, як наслідок мають обмеження

щодо налаштування оптимальних параметрів придушувача в залежності від властивостей завади. Тому перспективною є розробка программно-налагоджуваних придушувачів ІЗ, які мають більші можливості щодо адаптації до завади та, як наслідок, якості її придушення. Розглянемо детальніше принцип роботи фільтра NB.

На вхід фільтра надходить повільно мінливий сигнал та періодичний імпульсний сигнал з амплітудою, що значно перевищує амплітуду корисного сигналу. Тривалість імпульсу сигналу дуже коротка, а період досить великий, хоча на слух він здається суцільним. Завдання фільтра – вирізати короткі імпульси з корисного сигналу і утворені провали заповнити апроксимованим корисним сигналом. Важливо встановити поріг спрацьовування фільтра NB таким чином, щоб корисні сигнали виявилися нижчими, а імпульси його

перевищували. Якщо цього не зробити фільтр почне різати корисні сигнали.

Застосування таких типів фільтрів дозволить підвищити відношення «сигнал-завада», та тим самим підвищити ефективність функціонування радіоприймальної апаратури у сучасних електромагнітних умовах.

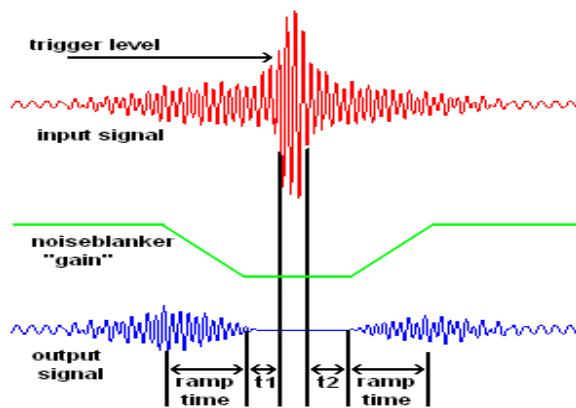


Рис. 3 Результат роботи NB фільтра

Список використаних джерел:

1. Ільїн, А. А., and Н. Ф. Денисова. "Методи шумозаглушення при цифровій обробці сигналів і зображень." Журнал зареєстрований в Міністерстві культури, інформації та спорту РК. Свідоцтво про постановку на облік ЗМІ № 5888-ж від 11.04. 2005.

**ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ
ПРОГРАММНО-АППАРАТНОЙ ПЛАТФОРМЫ HACKRF
ЛЯ ЗАДАЧ ТЕСТИРОВАНИЯ УЯЗВИМОСТЕЙ
БЕСПРОВОДНЫХ СРЕДСТВ УПРАВЛЕНИЯ**

Попаденко М.О.

Научный руководитель – к.т.н., ст. преп. Иваненко С.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки, 14,
каф. информационно-сетевой инженерии,
тел. (057) 702-14-29)
e-mail: mariia.popadenko@nure.ua

Currently, information resources are becoming the main target of attacks by attackers. The attacker actively uses the most common system vulnerabilities: memory leaks, encryption weaknesses, incomplete verification of input data, etc. The attacked party, in turn, tries to find vulnerabilities in the system by developing and improving barriers that protect the protected information object from unauthorized access. The aim of this work is to investigate the use of the HackRF software and hardware platform for vulnerabilities. Since HackRF is allows you to receive or transmit signals in a large frequency range.

В настоящее время информационные ресурсы становятся главной целью атак со стороны злоумышленников. Атакующая сторона активно использует наиболее распространенные уязвимости систем: утечки памяти, недостатки шифрования, переполнение буфера, неполную проверку входных данных. Атакуемая сторона, в свою очередь, старается находить уязвимые места системы, разрабатывая и совершенствуя барьеры, ограждающие защищаемый информационный объект от несанкционированного доступа. HackRF позволяет тестировать уязвимости беспроводных средств управления.

Программно определяемое радио (SDR) использует цифровую обработку сигналов для реализации функции радио. С SDR можно создать виртуальный передатчики или приёмники для любого радиосигнала в виде программы, используя всего одно аппаратное устройство и компьютер. HackRF — это уникальное устройство, созданное для тестирования и разработки современных радио-технологий.

HackRF One это открытая аппаратная платформа которая может быть использована как USB периферийное устройство или же запрограммировано на автономную работу.

HackRF One выдает тактовый сигнал 10 МГц на CLKOUT. Сигнал представляет собой прямоугольную волну 10 МГц от 0 В до 3 В, предназначенную для нагрузки с высоким импедансом.

HackRF одна из многих программных радиосистем, однако она является распространенной. Устройство имеет огромное количество преимуществ: широкий диапазон рабочих частот (1 МГц – 6 ГГц); широкополосная полоса пропускания (max - 20 МГц); совместимый с другим, так и с другими источниками сигнала; портативный (питается от USB); поддерживает множество ОС. Однако, она имеет небольшую мощность и КПД штатной антенны менее 1%.

Передача информации в HackRF осуществляется двумя способами:

- первый способ – общение напрямую с устройством (HackRF имеет библиотеку с открытым API. Необходимо программно сформировать комплексный (IQ) сигнал для всей требуемой полосы приемника, чтобы его ЦАП в свою очередь, отправил сигнал в эфир. Также необходимо задать ряд настроек (частота, усиление, полоса пропускания);

- второй способ – использованию пакета GNU Radio (GNU Radio – это открытый и бесплатный пакет программ, предназначенный для цифровой обработки сигналов в научных, образовательных или коммерческих целях).

С помощью программно-аппаратной платформы HackRF можно прослушивать эфир, а также фальсифицировать отправителя.

В настоящее время компьютерные мыши и клавиатуры с радиоинтерфейсом и USB-трансивером пользуются популярностью, но такие устройства не защищены от взлома. С помощью HackRF можно перехватить данные, дешифровать трафик. Из-за данных уязвимостей могут быть утрачены пароли, платёжные реквизиты, персональные данные и ещё много важной информации.

HackRF может анализировать трафик GSM сетей (результатом данного анализа будет доступ к различным системным сообщениям), управлять радиоуправляемой машиной или дверным звонком.

Литература:

- *Cognitive Radio Technology*. Bruce Fette. Elsevier Science & Technology Books, 2006. 656 pags.

- *Галкин В. А.* Основы программно-конфигурируемого радио. – М.: Горячая линия - Телеком, 2013. – 372 с.

- *Positive technologies* Сборник исследований по практической безопасности 2017 – 69 с.

A TECHNIQUE TO IMPROVE CONVERGENCE OF THE LLOYD-MAX QUANTIZATION SCHEME FOR THE EXPONENTIAL FAMILY MEMORYLESS SOURCES

Stepanov O.O., Fedorov O.V.

Scientific supervisor - senior lecturer Fedorov O.V.

Kharkiv National University of Radio Electronics

(61166, Kharkov, Nauky Ave. 14, dep. of Information and Network

Engineering, tel. (057) 702-14-29)

e-mail: oleksandr.stepanov@nure.ua

This paper considers the Lloyd-Max algorithm for designing optimal quantizers for memoryless sources. Usually Lloyd-Max's algorithm requires a relatively large number of steps to yield optimal spacing of the partitioning points. The objective of this note is to introduce a technique to improve convergence of the Lloyd-Max algorithm for the exponential family of memoryless sources.

Sampling and quantization are two major operations performed when digitizing analog signals. Nowadays, the theory is well developed for both of these operations and for signals of arbitrary nature: deterministic or random. To deal with random signals, a famous Lloyd-Max quantizer is used [1]. Also, there are several generalizations of the mentioned above algorithm exist, Farvardin & Modestino's entropy constraint quantizer [2] and Sullivan's dead-zone plus uniform threshold quantizer [3] to name a few. It deserves noting that entropy constrained quantization underlies all the modern algorithms of lossy compression of multimedia data. However, efficient algorithms exist only for memoryless probability distributions, namely, for exponential and double exponential ones [4].

Usually Lloyd-Max's algorithm requires a substantial number of steps (30 and more) to yield optimal spacing of the partitioning points. It appears that for certain types of memoryless sources there becomes possible to improve the algorithm's convergence. These sources are described by distributions from the exponential family of distributions. That is, the objective of the paper is to introduce a technique to improve convergence of the Lloyd-Max quantizer for the exponential family of memoryless sources.

Let $\{X_t\}$ be a discrete-time memoryless stationary process and $X_t \sim f(x)$, where $f(x)$ is a probability density function. The N -level quantizer is thought of as a function $q_N(\cdot)$ which maps $\{X_t\}$ onto one of $\{Q_n\}_{n=1}^N$ levels. In terms of threshold values $\{T_n\}_{n=1}^{N-1}$, $q_N(\cdot)$ can be defined as [2]:

$$q_N(x) = \sum_{i=1}^N Q_i I_i(x),$$

where $I_l(x)$ equals 1 if $x \in (T_{l-1}, T_l]$ and 0 otherwise.

To assess the total alteration of $\{X_t\}$ introduced by the N -level quantizer, an average distortion function is used:

$$D_N(\vec{T}, \vec{Q}) = \sum_{i=1}^N \int_{-\infty}^{\infty} d(x, Q_i) I_i(x) f(x) dx,$$

where $d(\cdot, \cdot)$ is the non-negative measure of distortion and $\vec{T} = [T_1, T_2, \dots, T_{N-1}]^T$, $\vec{Q} = [Q_1, Q_2, \dots, Q_N]^T$. Here we deal with $d(x, Q_l) = \int_{T_{l-1}}^{T_l} (x - Q_l)^2 f(x) dx$.

Optimal values of $\vec{T}$ and $\vec{Q}$ are minimizers of $D_N(\vec{T}, \vec{Q})$. Thus we naturally come up with the system of $2N - 1$ equations, namely

$$\begin{cases} \frac{\partial}{\partial T_l} \int_{T_{l-1}}^{T_l} (x - Q_l)^2 f(x) dx = 0, \\ \frac{\partial}{\partial Q_l} \int_{T_{l-1}}^{T_l} (x - Q_l)^2 f(x) dx = 0, \end{cases} \Rightarrow \begin{cases} (T_l - Q_l)^2 f(T_l) = 0, \\ \int_{T_{l-1}}^{T_l} x f(x) dx = Q_l \int_{T_{l-1}}^{T_l} f(x) dx. \end{cases} \quad (1)$$

It is obvious, there is no explicit solution to (1) and here the Lloyd-Max algorithm comes to play. To improve the convergence of the algorithm for the exponential family of memoryless sources, we employ the following approximation, which is a direct consequence of the 2-nd remarkable limit:

$$e^x \approx (2 \cdot n + x)^n \cdot (2 \cdot n - x)^{-n}. \quad (2)$$

Let us illustrate the proposed technique by example of the exponential distribution with the PDF $f(x) = \beta^{-1} \exp(-x/\beta)$; $x > 0$, the system (1) becomes

$$\begin{cases} T_l = Q_l, \\ \alpha_l = 1 + \delta_l \left(1 - \frac{1}{1 - e^{-\delta_l}}\right); \alpha_l = \frac{Q_l - T_{l-1}}{\beta} \text{ and } \delta_l = \frac{T_l - T_{l-1}}{\beta}. \end{cases} \quad (3)$$

Results of substituting (2) for (3) are summarized below.

$n = 1$	$n = 2$	$n = 3$	$n = 4$
$\alpha_l \approx \frac{\delta_l}{2}$	$\alpha_l \approx \frac{\delta_l}{2} \left(1 - \frac{\delta_l}{8}\right)$	$\alpha_l \approx \frac{\delta_l}{2} \left(1 - \frac{16\delta_l}{\delta_l^2 + 108}\right)$	$\alpha_l \approx \frac{\delta_l}{2} \left(1 - \frac{\delta_l}{32} - \frac{8\delta_l}{\delta_l^2 + 64}\right)$

Subject to the first equation of the system (3), Q_l and T_l are interchangeable and for $n = 1$ we get a conventional Lloyd-Max scheme. In turn, for $n > 1$ one gets improved convergence.

References

1. S. Lloyd. Least squares quantization in PCM. *IEEE Transactions on Information Theory*, 28(2):129–137, March 1982.
2. N. Farvardin and J. Modestino. Optimum quantizer performance for a class of non-Gaussian memoryless sources. *IEEE Transactions on Information Theory*, 30(3):485–497, May 1984.
3. G. J. Sullivan. On embedded scalar quantization. In *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 4, May 2004, pp. 605–607.
4. G. J. Sullivan. Efficient scalar quantization of exponential and laplacian random variables. *IEEE Transactions on Information Theory*, 42(5):1365–1374, Sep 1996.

РОЗРОБКА ПРИСТРОЮ УСУНЕННЯ СИНФАЗНОЇ ПЕРЕШКОДИ РАДІОПРИЙОМУ

Рижов О. О.

Науковий керівник – к.т.н, ст. викл. Іваненко С. А.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Інформаційно-мережної інженерії,
тел. (057) 702-14-29)

e-mail: oleksandr.ryzhov@nure.ua

This article discusses the problem associated with hindrance from radio receivers. In-phase hindrance is considered in more detail, to combat which a device has been developed to suppress this hindrance. The developed device can be used for the operation of various radio receivers, including for radio monitoring.

Радіоприймальні пристрої – це системи електричних ланцюгів, вузлів і блоків, призначені для уловлювання радіохвиль, які поширюються у відкритому просторі природного або штучного походження і перетворення їх до виду, що забезпечує використання інформації, яка в них міститься. Перші радіоприймальні пристрої створені в 90-х роках 19 століття.

Сучасна електромагнітна обстановка індустриального міста є несприятливою через те, що прийом амплітудно-модульованих сигналів радіостанцій, які працюють в діапазонах довгих, середніх і коротких хвиль сильно утруднений. Джерелом електромагнітних перешкод є потужне електрообладнання промислових підприємств, електротранспорт, освітлювальні прилади, комп'ютери, побутова техніка тощо [1].

Перешкоди можна розділити на зовнішні і внутрішні. Зовнішні перешкоди виникають поза радіоприймального пристрою і проходять на його вихід через весь тракт від антени або проникають безпосередньо через елементи приймача, а також через ланцюги живлення. Внутрішні перешкоди виникають безпосередньо в самому приймачі. Джерелом внутрішніх перешкод можуть бути транзистор, резистор і т.п. Зовнішні перешкоди можна класифікувати за походженням. При цьому розрізняють: атмосферні перешкоди, що виникають в результаті електромагнітних процесів в атмосфері Землі; космічні перешкоди, обумовлені радіовипромінюванням зірок і міжзоряного газу; промислові перешкоди, які створюються різними електроустановками, які застосовуються на виробництві та в побуті; перешкоди від радіостанцій інших систем радіозв'язку [2].

Перешкоди будь-якого походження розрізняються на періодичні, імпульсні і гладкі (або флуктуаційні). Періодичні перешкоди – це, перш за все, перешкоди, створювані радіостанціями інших систем радіозв'язку. Імпульсні і гладкі перешкоди мають безперервний спектр. Гладкі або

флуктуаційні перешкоди можна уявити як велике число дуже коротких імпульсів, які розміщені в хаотичному порядку один за одним. Прикладом імпульсних перешкод можуть служити атмосферні перешкоди, прикладом гладких перешкод - внутрішні шуми приймача [2].

Також, перешкоди діляться на активні і пасивні. Активні перешкоди створюються генеруючими джерелами. До них відносяться всі види перешкод атмосферного, космічного, промислового і внутрішнього походження. Пасивні перешкоди виникають в результаті особливостей поширення електромагнітних хвиль. До них відносяться замирання і ехо-сигнали [2].

Радіопередавач радіостанції віддалений від радіоприймача на десятки, сотні і тисячі кілометрів, а відстань до джерела електромагнітної перешкоди часто не перевищує десятих часток довжини хвилі. При цьому антена радіоприймача виявляється, в так званій ближній зоні випромінювання джерела перешкоди, в міру наближення, до якого модуль вектору напруженості магнітної складової електромагнітного поля перешкоди зростає пропорційно $1/r^2$ (де r – це відстань до джерела випромінювання), а модуль вектору напруженості електричної складової – пропорційно $1/r^3$, тобто швидше. Іншими словами, чим ближче джерело перешкоди, тим більш явно в випромінюваному їм електромагнітному полі електрична складова переважає над магнітної, причому зі збільшенням довжини хвилі ця особливість проявляється в більшій мірі. Для дальньої зони цей ефект відсутній [1].

Тому для боротьби з синфазною перешкодою використовується магнітна прийомна антена, яка входить до складу пристрою усунення синфазної перешкоди, та є нечутливою до електричної складової електромагнітного поля, і яка має до того ж спрямовані властивості, які дозволяють шляхом відповідної орієнтації в просторі додатково відбудовуватися від радіоприйому випромінювання що заважає. Використання для радіоприйому в таких умовах саме магнітної антени дає найкраще відношення сигнал/перешкода на вході радіоприймача. Це пов'язано з іншою структурою електромагнітного поля поблизу джерела випромінювання в ближній зоні.

Перелік посилань:

1. Подавление синфазной помехи радиоприему [Электронный ресурс]. – Режим доступа: <http://sezador.radioscanner.ru/articles/cmreject.html> – Загл. с экрана.
2. Классификация радиопомех [Электронный ресурс]. – Режим доступа: <https://studopedia.info/1-110664.html> – Загл. с экрана.

**ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ,
МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ,
СТАНДАРТИЗАЦІЯ І СЕРТИФІКАЦІЯ**

ЗАБЕЗПЕЧЕННЯ ПРЕЗУМПЦІЇ ВІДПОВІДНОСТІ. СПЕЦІАЛЬНІ ВИМОГИ ДО ПРИЗНАЧЕНИХ ОРГАНІВ З ОЦІНКИ ВІДПОВІДНОСТІ

Фоменко В.Д.

Науковий керівник – доцент Штефан Н.В.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Метрології та технічної експертизи,
тел. 066-175-1092)

E-mail : lightwoodvel@gmail.com

The given work is devoted to presumption of conformity. The system of technical regulation (metrology, standardization, conformity assessment, market surveillance) aims at ensuring the safety and conformity of goods and services, protecting the domestic market and expanding the country's foreign market, contributing to the development of new technologies and improving the competitiveness of the economy. By far, the most effective model is the European approach to technical regulation, which is based on the relevant harmonized legislation and promotes the free movement of goods, healthy competition, the introduction of innovation into production, but at the same time ensures the safety of products.

Оцінка відповідності є складовою системи технічного регулювання, що пов'язана з доведенням того, що задані вимоги, які стосуються продукції, процесу, послуги, системи, особи чи органу, були виконані. Вимоги, що забезпечують безпечність продукції, наводяться в технічних регламентах. В Україні оцінка відповідності технічним регламентам є обов'язковою. Для того, щоб органи могли працювати у сфері оцінки відповідності технічним регламентам, вони мають бути призначеним.

Для того щоб ООВ набули призначення, вони повинні відповідати загальним вимогам до призначених органів та спеціальним вимогам.

Щодо визначення спеціальних вимог можливо декілька джерел:

- відповідні технічні регламенти, якими передбачене застосування процедур оцінки відповідності із залученням призначених органів;
- Постанова Кабінету Міністрів України щодо спеціальних вимог до призначених органів.

Презумпція відповідності спеціальним вимогам призначених органів визначається в Законі України від 03.07.2019 № 124-VIII «Про технічні регламенти та оцінку відповідності» та полягає у відповідності вимогам міжнародних стандартів щодо органів з оцінки відповідності.

Презумпція відповідності – припущення, яке визнається достовірним, поки не буде доведено інше, про те, що продукція, пов'язаний з нею процес або метод виробництва чи інший об'єкт відповідає вимогам відповідного технічного регламенту, що визначені в ньому, а орган з оцінки відповідності відповідає спеціальним вимогам до призначених органів з оцінки відповідності чи визнаних незалежних організацій.

Доведення органом з оцінки відповідності своєї відповідності критеріям, установленим відповідними національними стандартами, перелік яких затверджений центральним органом виконавчої влади, що забезпечує формування державної політики у сфері технічного регулювання, або частинами цих стандартів, надає такому органу з оцінки відповідності презумпцію відповідності спеціальним вимогам до призначених органів у тій мірі, в якій національні стандарти, що застосовуються, охоплюють зазначені вимоги.

Доведення відповідності органу вимогам цих стандартів здійснюється через акредитацію ООВ.

Загальні вимоги здебільшого стосуються юридичного оформлення діяльності ООВ.

Спеціальні вимоги безпосередньо описують «технічні» характеристики ООВ. Вони можуть вказуватися або Кабінетом Міністрів України, або технічними регламентами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Штефан Н.В. Розвиток технічного регулювання в Україні. Метрологія та прилади. – 2014. - №1(45). – С.250-253

2. Про технічні регламенти та оцінку відповідності: Закон України від 03.07.2019 № 124-VIII

3. Про затвердження спеціальних вимог до призначених органів з оцінки відповідності: Постанови Кабінету Міністрів України від 13.01.2016 № 56

АВТОМАТИЗОВАНА СИСТЕМА СТАТИСТИЧНОЇ ОБРОБКИ ДАНИХ БАГАТОРАЗОВИХ ВИМІРЮВАНЬ

Яхновська Д.С.

Науковий керівник – к.т.н., доц. Запорожець О.В.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. метрології та технічної експетризи,
тел. (057) 702-13-31), e-mail: daria.mysic27@gmail.com

The problem of automation of routine calculations for statistical processing of multiple measurements results is considered. The proposed software has a user-friendly graphical user interface and displays the results in the form of numerical values of the estimates of distribution laws, cumulative curve, histogram, and allows you to save the report with the results in a text file.

Методи обробки експериментальних даних спрямовані насамперед на аналіз, зменшення та оцінку похибок результатів вимірювань. Найбільш важливими є чисельні методи обробки, засновані на описі та аналізі невизначеностей вихідних даних, серед них переважають статистичні методи. У загальному випадку результати вимірювань (спостережень) можна вважати випадковими величинами. Як і всяка випадкова величина, результат вимірювання повністю характеризується законом розподілу, інформацію про який одержують, опрацьовуючи результати багаторазових спостережень методами математичної статистики. У результаті з'являється можливість не тільки оцінити характеристики випадкової похибки, але і підвищити точність вимірювання.

При проведенні різноманітних метрологічних регламентів досить часто доводиться використовувати процедури статистичної обробки даних багаторазових вимірювань, які вимагають значного обсягу обчислювальних операцій, що потребує багато часу. Тому досить актуальним є завдання автоматизації таких процедур.

Виходячи із цього, було розроблено програмний засіб мовою MATLAB, що реалізує такі основні функції:

- 1) файловий ввід/вивід даних;
- 2) інтерактивний режим взаємодії з користувачем;
- 3) побудова гістограми та кумулятивної кривої для найбільш типових законів розподілу (рівномірний, нормальний, Лапласа, трикутний та арксинус);
- 4) обчислення описових статистик результатів багаторазових спостережень (середнього арифметичного, середнього квадратичного відхилення, медіани, розмаху, асиметрії, ексцесу);
- 5) функція відсіювання недостовірних даних за допомогою критеріїв Райта та Смирнова;
- 6) перевірка гіпотези про відповідність статистичних даних вибраному закону розподілу за критерієм Пірсона та Колмогорова;
- 7) побудова інтервальних оцінок випадкової похибки.

Програма має зручний графічний інтерфейс користувача (рис. 1) і відображає результати у вигляді числових значень оцінок параметрів законів розподілу, кумулятивної кривої, гістограми, а також дозволяє зберігати звіт з результатами в текстовому файлі.

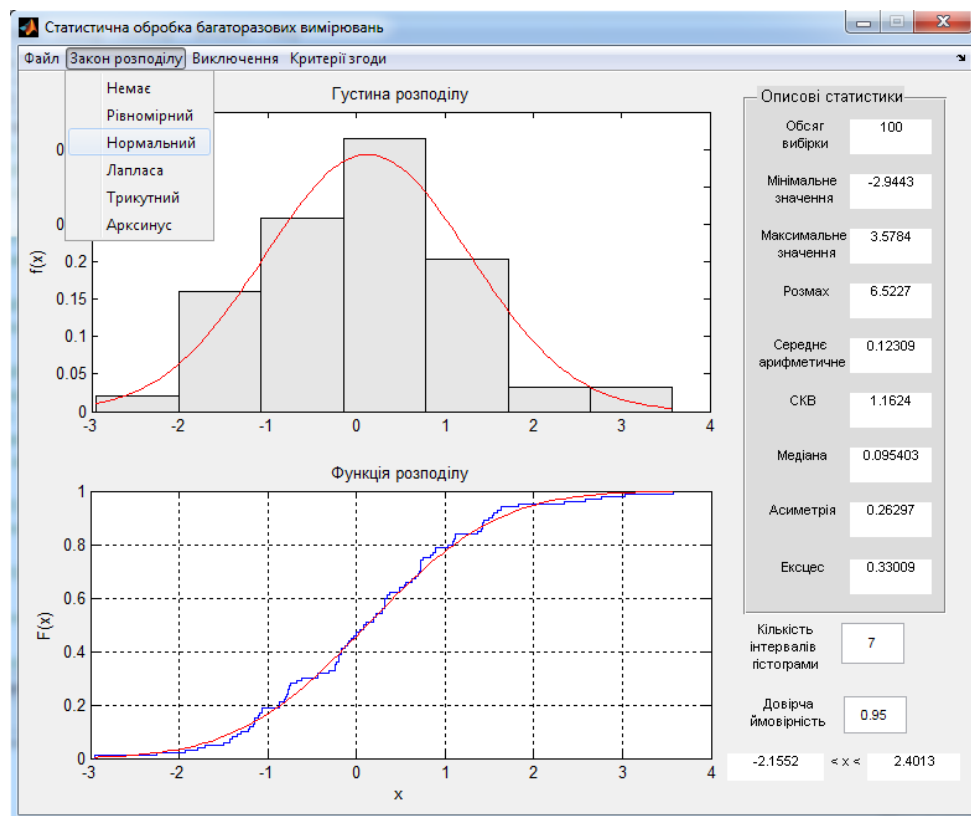


Рис. 1 – Інтерфейс програми

Перевагами розробленої автоматизованої системи є можливість обробляти значні обсяги даних та працювати з різними форматами вхідної інформації, вона може застосовуватись при здійсненні наукових досліджень, проведенні метрологічних регламентів та у навчальному процесі.

Список використаних джерел

1. Грановский, В.А. Методы обработки экспериментальных данных при измерениях [Текст] / В.А. Грановский, Т.Н. Сирая. – Л.: Энергоатомиздат, 1990. – 288 с.
2. Захаров, И.П. Обработка результатов измерений [Текст] : учеб. пособие / И.П. Захаров. – Харьков : Изд-во НУВД, 2002. – 126 с.
3. Захаров, И.П. Теоретическая метрология [Текст] : учеб. пособие / И. П Захаров. – Харьков : ХТУРЭ, 2000. – 172 с.
4. Романов, В.Н. Теория измерений. Анализ и обработка экспериментальных данных [Текст] : учеб. пособие / В.Н. Романов, В.В. Комаров. – СПб : СЗТУ, 2002. – 127 с.
5. Дьяконов, В.П. MATLAB. Полный самоучитель [Текст] / В.П. Дьяконов. – М.: ДМК Пресс, 2012. – 768 с.

МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ АНЕМОМЕТРУ

Цис М.Б.

Науковий керівник - к.т.н., доц. Сергієнко М.П.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. МТЕ, тел. (057) 702-13-31
e-mail: maryna.tsys@nure.ua)

An anemometer is a device for measuring the flow velocity and the direction of air movement, gases and liquids. This applies both restricted flows, such as air movement in air ducts, and unrestricted flows, such as atmospheric wind. The technical and metrological performances of an anemometer M-95-CM are considered in the work. The estimation procedure of measurement uncertainty, including model, components of uncertainty, their contributions to the total uncertainty, taking into account the distribution law, is developed.

Анемометр - це прилад для вимірювання швидкості потоків та напрямки руху повітря, газів і рідин. Це стосується як обмежених потоків, наприклад руху повітря в повітропроводах, так і необмежених потоків, наприклад атмосферного вітру. Анемометри насамперед призначені для метеорології, адже зміна таких параметрів, як швидкість і напрям вітру, вказують нам на зміни погодних умов, попереджають про наближення грози, шторму, інших небезпечних природних явищ, що дуже важливо для пілотів, моряків, інженерів, та й для усіх нас. Як правило, це легкі портативні прилади, зручні у використанні навіть в складних польових умовах.

Принцип роботи анемометра полягає у виявленні зміни деякого фізичного властивості потоку, або в дії цього потоку на механічний пристрій, поміщене в потік. При цьому анемометр може вимірювати повну величину швидкості, величину швидкості в площині, або компоненту швидкості в певному напрямку. Крім того, сучасні анемометри в залежності від моделі можуть вимірювати напрямок вітру, об'ємний витрата повітря, вологість, температуру, тиск. Таким чином, анемометри перетворюються в портативні метеостанції.

В роботі розглянуті технічні характеристики анемометру М-95-ЦМ:

- діапазон вимірювань швидкості повітряного потоку (1,8...55) м/с;
- межі допустимої основної абсолютної похибки при вимірюванні $\pm(0,5 + 0,05 V)$ м/с, де V - вимірювана швидкість повітряного потоку;
- діапазон установки порогів спрацьовування сигналізації:
 - швидкості повітряного потоку (12...40) м/с;
 - часу впливу поривів вітру (2...5) с;
- межі допустимої основної абсолютної похибки установки порога спрацьовування сигналізації по швидкості повітряного потоку при температурі $(20 \pm 5) ^\circ\text{C} \pm 0,4$ м/с;

- межі допустимої додаткової похибки при зміні температури навколишнього повітря від $(20 + 5) ^\circ \text{C}$ у межах робочих умов, в долях від основної похибки:

- при вимірюванні швидкості повітряного потоку: $\pm 0,5$;
 - при спрацьовування сигналізації швидкості повітряного потоку: $\pm 0,5$;

- поріг спрацьовування попередньої сигналізації швидкості повітряного потоку від встановленого значення порогу швидкості повітряного потоку $(75 \pm 5) \%$;

- дискретність установки порогів спрацьовування сигналізації по швидкості повітряного потоку $0,1 \text{ м/с}$;

- дискретність встановлення часу спрацювання сигналізації по швидкості повітряного потоку $0,1 \text{ с}$;

- поживана потужність $10 \text{ В} \cdot \text{А}$: 10;

Метрологічне забезпечення представляє собою комплекс організаційно-технічних і економічних заходів, які забезпечують необхідну єдність і точність вимірювань у відповідності з вимогами нормативно – технічної документації, а також впровадження прогресивних технологій, що забезпечують оптимальне здійснення виробничих режимів. Якість вимірювань залежить від якості засобів вимірювань, методів вимірювань, кваліфікації кадрів, якісної експлуатації й обслуговування вимірювальних приладів.

Метрологічне забезпечення охоплює весь життєвий цикл анемометрів – наукові дослідження, включаючи оцінювання невизначеності вимірювань, підготовку й виробництво, сферу обігу і експлуатації.

В роботі розроблено процедуру оцінювання невизначеності вимірювань, включаючи модельне, складові невизначеності, їх внески в загальну невизначеність з урахуванням закону розподілу.

Список використаних джерел

1 Р.В. Бичківський, П.Г. Столярчук, П.Р. Гамула. Метрологія, стандартизація, управління якістю і сертифікація. - Львів: Видавництво Національного університету Львівська політехніка, 2004. - 288 с.

2 Боженко Л.І. Метрологія, стандартизація, сертифікація та акредитація: Навчальний посібник. - Львів: Афіша, 2006. - 328 с.

3 Величко О.М., Коломієць Л.В., Гордієнко Т.Б. Оцінювання результатів вимірювань:основи і нормативне забезпечення: підручник. - Одеса: ВМВ, 2010.- 188 с.

4 Терещенко М.Д. Вимірювання параметрів руху. Навчальний посібник. – Одеса: ОКСМС, Укртехснаб, 1999. - 108 с.

ПРИНЦИПИ ДІЇ ТЕПЛОЛІЧИЛЬНИКА УВР-Т

Тимчук І.В.

Науковий керівник – к.т.н., проф.. Єгоров А.Б.

Харківський національний університет радіоелектроніки

(61166, Харків, просп. Науки, 14, каф. Метрології та технічної експертизи, тел.. (057) 702-13-31)

e-mail: yegorov.rik@gmail.com

The heat meter implements an ultrasonic time-pulse method of measuring flow. The heat meter is configured from the built-in keyboard or via the RS-232/485 interface with a PC. There is a protection of settings and archive data from unauthorized changes by restricting access to management using a password system and the presence of hardware configuration protection against overwriting.

Heat meters are designed for commercial and technological accounting of thermal energy, water and other liquids, can be included in the composition of measuring systems, ACS systems.

Лічильники призначені для вимірювання теплової потужності та кількості теплової енергії, об'єму, маси, об'ємних та масових витрат теплоносія у двох трубопроводах відповідно до діючих правил обліку споживання теплової енергії води та інших рідин на промислових підприємствах та об'єктах комунального господарства, можуть бути включені у склад вимірювальних систем, автоматизованих систем управління технологічними процесами (АСУ ТП).

Лічильник дозволяє виміряти об'ємну витрату води у двох трубопроводах: «подавальному» та «зворотному» або «підживлення», температуру і тиск у трьох трубопроводах «подавальному», «зворотному» та холодної води або «підживлення».

Шляхом конфігурації лічильник адаптується до експлуатації в системах теплопостачання (СТП) згідно зі схемами теплообліку 1 ÷ 8, які наведено у додатку Б.

Лічильник забезпечує:

- вимірювання та індикацію поточного значення об'ємних витрат теплоносія;
- вимірювання та індикацію поточних значень температури у трьох трубопроводах;
- вимірювання та індикацію поточних значень тиску у трьох трубопроводах;
- обчислення та індикацію поточних масових витрат теплоносія, який пройшов по двох трубопроводах за ЗПЧ;
- обчислення теплової енергії, яка передається по тепловому виходу;
- обчислення теплової потужності;
- архівування у енергозалежну пам'ять результатів вимірювань та обчислень;

- архівування у енергозалежну пам'ять відомості про аварії;
- архівування у енергозалежну пам'ять відомості про втручання оператора;
- вимірювання тривалості паузи в обліку теплової енергії відповідно до «Тимчасових правил обліку споживання теплової енергії»;
- передачу вимірювальної, діагностичної, архівної та іншої інформації через послідовні інтерфейси RS-232 та RS-485, Ethernet;
- відображення результатів вимірювань та обчислень на РКІ;
- захист параметрів налаштувань та архівних даних від несанкціонованих змін шляхом обмеження доступу до управління за допомогою системи паролів та наявності апаратного захисту конфігурації від перезапису.

Межі допустимої відносної похибки лічильника під час вимірювання об'єму рідини:

- клас 1 (врізні ПЕА, врізні секції) – $\pm (1 + 0.01 Q_n/Q) \%$.
- клас 2 (накладні ПЕА) – $\pm (2 + 0.02 Q_n/Q) \%$.

Межі допустимої відносної похибки лічильника при перетворюванні вхідних сигналів від термоперетворювачів опору та обчисленні кількості тепла: $\pm (0,5 + \Delta T_{min}/\Delta T) \%$.

Межі допустимої відносної похибки лічильника при вимірюванні кількості тепла.

Межі допустимої відносної похибки лічильника при вимірюванні кількості тепла - схеми обліку тепла 4 – 6 Додаток Б:

- 1) При застосуванні витратомірів класу 1 – $\pm (2 + 0.01 Q_n/Q + 4 \Delta T_{min}/\Delta T) \%$;
- 2) При застосуванні витратомірів класу 2 – $\pm (3 + 0.02 Q_n/Q + 4 \Delta T_{min}/\Delta T) \%$;

Література:

1. ДСТУ 3339-96 Теплолічильники. Загальні технічні вимоги
2. Кремлевский П.П. Измерение расхода и количества жидкости, газа и пара. - М.: Изд-во стандартов, 1980.
3. Лепявко А.П. Измерение расхода жидкости и газа. Части 1 и 2. - М.:АСМС, 2008.
4. Цейтлин В.Г. Техника измерения расхода жидкостей, газов и паров. - М.: Изд-во стандартов, 1981.
5. <http://energo.kh.ua/ru/>

ИССЛЕДОВАНИЯ ПАРАМЕТРОВ СЧЕТЧИКА ГАЗА ГУВР-011

Токарева М.С.

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: maryna.tokarieva@nure.ua,

Ultrasonic gas meters GUVR-011 are used for commercial and technological accounting of various gases - natural, associated petroleum, compressed air, oxygen, nitrogen, etc. The diameter of pipelines is from 50 to 4,000 mm. The main relative measurement error is from $\pm 0.3\%$ to $\pm 2\%$. Meters are used for gas metering, including commercial gas, at gas distribution points, industrial facilities, energy facilities and utilities. Meters can be used to measure the flow of clean gases, contaminated gases, on the plumes of wells, on underground gas storages, on gas flares, etc.

В докладе приведены метрологические и технические характеристики прибора, а также его принцип работы. Данный прибор разработан на предприятии ЧАО «Энергоучет».

Ультразвуковой расходомер-счетчик газа типа ГУВР-011 предназначен для измерения в рабочих условиях скорости потока, объемного расхода и объема природного газа и других газов, которые транспортируются по трубопроводам круглого сечения в прямом или обратном направлении, а также для измерения времени наработки и простоя.

Пределы допускаемой относительной погрешности счетчика

Диапазон объемного расхода	Пределы допускаемой основной относительной погрешности, %			
	с врезной секцией		с врезными ПЭА	
	2 пары ПЭА	1 пара ПЭА	2 пары ПЭА	1 пара ПЭА
от Q_{min} до Q_r	± 2	± 3	± 4	± 5
от Q_r до Q_{max}	± 1	$\pm 1,5$	± 2	± 3

По принципу работы счетчик относится к время - импульсным ультразвуковым расходомерам, работа которых основана на измерении разности времени прохождения (УЗС – ультразвукового сигнала) по направлению потока газа в трубопроводе и против него.

Работой счетчика управляет встроенный ОМК (однокристалльный микроконтроллер) согласно алгоритму рабочей программы и значений настроечных параметров, которые записываются в ОМК при конфигурировании счетчика.

Для обеспечения проведения поверки счетчика без вывода его из эксплуатации, в каждый измерительный канал счетчика может быть встроен кварцевый калибратор. В ходе поверки калибратор вносит в сигналы, распространяющиеся сквозь газ в трубопроводе, неодинаковые (для направлений «по» и «против» потока газа) эталонные задержки, кратные целому числу периодов кварцевого генератора счетчика. Калибратор в ходе поверки управляется с помощью ПК, оснащенного специализированным ПО

Счетчик, при его использовании в составе узла учета природного газа, подключается к корректору (вычислителю) для передачи информации об объемах газа, прошедшего через него, для последующей обработки.

Счетчик может быть подключен к корректору двумя способами: либо по импульсному выходу, либо по интерфейсу RS-232 или RS-485.

Взрывобезопасность счетчиков обеспечивается схемными и конструктивными решениями в соответствии с видом защиты «Искробезопасная электрическая цепь» по ДСТУ 7113:2009 «Вибухонебезпечні середовища. Частина 0. Електрообладнання. Загальні вимоги».

Внешний вид счетчика



Литература:

1. Кремлевский П.П. Измерение расхода и количества жидкости, газа и пара. - М.: Изд-во стандартов, 1980.
2. Лепявко А.П. Измерение расхода жидкости и газа. Части 1 и 2.-М.: АСМС, 2008.

ДОСЛІДЖЕННЯ МЕТРОЛОГІЧНИХ ХАРАКТЕРИСТИК ТЕПЛОЛІЧИЛЬНИКА УВР-Т

Гапоненко Д.О., Єрохіна М.Я., Кірко О.С.

Науковий керівник – д.т.н., проф. Єгоров А.Б.

Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Метрології та технічної експертизи
тел. (057) 702-13-31)
e-mail: yegorov.rik@gmail.com

Heat meters are designed for commercial and technological accounting of thermal energy, water and other liquids, can be included in the composition of measuring systems, ACS systems.

The heat meter implements an ultrasonic time-pulse method of measuring flow. The heat meter is configured from the built-in keyboard or via the RS-232/485 interface with a PC. There is a protection of settings and archive data from unauthorized changes by restricting access to management using a password system and the presence of hardware configuration protection against overwriting.

Даний лічильник розроблений на підприємстві ЧАО «Тахіон». У доповіді наведені технічні та метрологічні характеристики, а також принципи дії пристрою.

Лічильник дозволяє виміряти об'ємну витрату води у двох трубопроводах: «подавальному» та «зворотному» або «підживлення», температуру і тиск у трьох трубопроводах «подавальному», «зворотному» та холодної води або «підживлення».

Технічні характеристики лічильника УВР-Т

Тип та кількість каналів вимірювання:	
канали вимірювання витрат	1 або 2
канали вимірювання температури	до 3
канали вимірювання тиску	до 3 (надлишкового або абсолютного)
Номінальний внутрішній діаметр трубопроводу (DN):	
Накладні ПЕА (перетворювачі електроакустичні)	від 70 до 3200 мм
Врізні ПЕА	від 200 до 4000 мм
Врізні секції	від 25 до 1600 мм
Комунікаційний канал	RS-232 або RS-485;
Протокол обміну	ModBus RTU;
Швидкість обміну	4800;9600;19200;38400;57600;115200 біт/с;
Довжина лінії зв'язку	для RS-232 – до 15 м; для RS-485 – до 1200 м;
Кількість приладів в мережі RS-485	до 255

Лічильник обчислює поточні об'ємні витрати теплоносія, як відношення виміряної швидкості потоку та площі внутрішнього поперечного перерізу трубопроводу згідно з виразом:

$$Q = 2,827 \cdot 103 \cdot S_g \cdot V \cdot D^2$$

де Q — поточні об'ємні витрати, м³/г;
 S_g — гідродинамічний коефіцієнт;
 V — виміряна швидкість потоку, м/с;
 D — внутрішній діаметр трубопроводу, м.

Межі допустимої відносної похибки лічильника під час вимірювання об'єму рідини:

- клас 1 (врізні ПЕА, врізні секції) – $\pm(1 + 0.01 Q_n/Q) \%$,
- клас 2 (накладні ПЕА) – $\pm(2 + 0.02 Q_n/Q) \%$.

Витрати рідини вимірюються витратомірним вузлом лічильника, принцип дії якого заснований на вимірюванні часу розповсюдження ультразвукового сигналу через рідину, яка проходить через трубопровід. Різниця між часом розповсюдження ультразвукового сигналу у прямому та зворотному напрямках відносно руху рідини пропорційна швидкості її потоку.

Випромінювання та прийом ультразвукового сигналу проходять по чергово парою ПЕА, яка змонтована на вимірювальній ділянці трубопроводу.

ПЕА можуть бути накладним (монтуватися на поверхні трубопроводу) або врізними (монтуються у отвори, що знаходяться у стінках трубопроводу або врізної секції).

Управління лічильником може здійснюватися з клавіатури або за допомогою ПК, який підключено до інтерфейсу RS-232/RS-485.

Клавіатура дозволяє керувати відображенням даних на дисплеї - індикаторі з метою:

- перегляду поточних значень об'ємних витрат та об'єму, поточних значень тиску та температури, поточної дати та часу, поточних значень теплової потужності, теплової енергії та маси теплоносія, дані архівів, значень параметрів налаштування;
- спостереження на дисплеї у режимі «Осцилограф» форму вимірювального сигналу, який проходить по акустичному каналу скрізь рідину, регулювати посилення приймача окремо для випромінювання «за потоком» та «проти потоку», оцінювати візуально зміщення за часом між вимірювальними сигналами, зумовлене потоком рідини.

Література:

- 1 ДСТУ 3339-96 Теплолічильники. Загальні технічні вимоги
- 2 <http://energo.kh.ua/ru/>

ВИПРОБУВАННЯ ПОКАЗНИКІВ БЕЗПЕКИ РУЧНОГО ЕЛЕКТРОІНСТРУМЕНТУ

Єрмак А.Р.

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 essence, goals, tasks and content of the conformity assessment of a hand-held power tool are considered. Regulatory documents are proposed to test safety parameters. The program of testing of safety parameters is developed. Test methods are proposed. Testing and testing equipment for testing safety parameters is offered. Test results are given.

Ручний електроінструмент – механізований інструмент, у якого приводним двигуном є електродвигун. Джерелом енергії для електричного інструменту може бути електрична мережа (220 В, 110 В і 380 В), джерело височастотного струму у промислового електроінструменту (як правило, 220 В, 50 Гц), або електричний акумулятор. Електроінструмент широко використовується в будівельних роботах для зварювання, різання, свердління, шліфування, полірування, фарбування та є затребуваним товаром на ринку України. Відповідно до законодавства України в сфері технічного регулювання введення в обіг продукції вимагає оцінки її відповідності національним технічним регламентам (ТР) [1]. ТР – нормативно-правовий акт, в якому визначено характеристики продукції або пов'язані з ними процеси, методи виробництва, дотримання яких є обов'язковим. Виконання вимог ТР є обов'язковим. У ТР наводяться основні вимоги безпеки до потенційно небезпечного обладнання.

Відповідно до Технічного регламенту безпеки машин (Постанова КМУ №62 від 30.01.13 р., Наказ від 10.11.2016 № 1885 гармонізований з Директивою 2006/42/ЕС Machinery (від 2017/05/2006 р.)) ручний електроінструмент підлягає оцінці відповідності за обов'язковими вимогами [2,3]. Оцінка відповідності – процес доведення того, що задані вимоги, які стосуються продукції, процесу, послуги, системи, особи чи органу, були виконані. Випробування – визначення однієї чи кількох характеристик об'єкта оцінки відповідності згідно з процедурою [1].

Метою даної роботи є забезпечення оцінки відповідності ручного електроінструменту шляхом розробки метрологічного забезпечення випробувань. Завдання даної роботи: аналіз нормативного забезпечення випробувань ручного електроінструменту; аналіз технічних характеристик об'єкта випробувань; розробка метрологічного забезпечення випробувань ручного електроінструменту.

Необхідність підтвердження відповідності ручного електроінструменту виникає з двох причин:

1. Підтвердження безпеки для здоров'я і життя людини, його майна і навколишнього природного середовища;

2. Завоювання ринку, тобто підвищення конкурентоспроможності виробів.

Завдання проведених випробувань параметрів безпеки - отримання якісних або кількісних характеристик продукції, тобто проведення оцінки здатності продукції в заданих умовах виконувати покладені на неї функції. Випробування проводяться у відповідності до положень, що містяться в законі, методами, викладеними в ДСТУ або інших нормативних документах, прийнятих відповідно до чинного законодавства.

Нормативним забезпеченням випробувань параметрів безпеки ручного електроінструменту в Україні є такі гармонізовані європейські стандарти: ДСТУ ІЕС 60745-1:2010 «Інструмент ручний електромеханічний. Безпека. Частина 1. Загальні вимоги (ІЕС 60745-1:2006, IDT)»; ДСТУ ІЕС 60745-2-3:2010 «Інструмент ручний електромеханічний. Безпека. Частина 2-3. Додаткові вимоги до шліфувальних, полірувальних та дискових шліфувальних інструментів (ІЕС 60745-2-3:2006, IDT)». Відповідно до даних нормативних документів розроблені програма і методика випробувань параметрів безпеки ручного електроінструменту.

Програма випробувань включає наступні процедури:

- 1) Підготовка випробувального устаткування.
- 2) Виконання необхідних вимірів і випробувань: випробування на стійкість до механічних зовнішніх чинників, випробування на стійкість до кліматичних зовнішніх діючих факторів, випробування на відповідність ступеня захисту, випробування на безпеку (вимірювання опору ізоляції, перевірка електричної міцності ізоляції), вимірювання температури корпусу, перевірка зразка в ненормальному режимі роботи, випробування на теплостійкість, перевірка маркування, упаковки, комплектності.
- 3) Обробка отриманих даних та оформлення протоколів випробувань.
- 4) Оформлення документації.

Перечень ссылок:

1. Закону України Про технічні регламенти та оцінку відповідності // База даних «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/124-19>.
2. ДСТУ ІЕС 60745-2-3:2010 Інструмент ручний електромеханічний. Безпека. Частина 2-3. Додаткові вимоги до шліфувальних, полірувальних та дискових шліфувальних інструментів (ІЕС 60745-2-3:2006, IDT) – Київ : Держспоживстандарт України, 2010. – 38 с.
3. ДСТУ ІЕС 60745-1:2010 Інструмент ручний електромеханічний. Безпека. Частина 1. Загальні вимоги (ІЕС 60745-1:2006, IDT) – Київ : Держспоживстандарт України, 2006. – 38 с.

ВЛИЯНИЕ НЕНУЛЕВОЙ НЕОПРЕДЕЛЕННОСТИ МЕЖДУНАРОДНОГО ПРОТОТИПА КИЛОГРАММА НА ПРОСЛЕЖИВАЕМОСТЬ ИЗМЕРЕНИЙ

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

After a new redefinition of the kilogram, the International Prototype of Kilogram has its own uncertainty. The paper describes the impact of this uncertainty on the global traceability. The requirements OIML R 111-1 for weights are considered. The ability of laboratories to distribute mass at the level of accuracy classes E1 and E2 after redefinition is analyzed.

Keywords: kilogram, uncertainty, traceability.

Точность гирь должна соответствовать строгим законодательным метрологическим и техническим характеристикам, указанным в таких документах, как OIML R 111-1 [1]. В этом нормативном документе содержатся подробные требования к гирям и наборам гирь, а также рекомендации по их правильному использованию.

К контролируемым и требуемым характеристикам относятся: материал, форма, плотность, качество поверхности, допуск относительно номинального значения, неопределенность условной массы, электрические и магнитные свойства и идентификационные маркировки.

Наиболее строгие требования предъявляются к гирям класса точности E1. Согласно OIML R 111-1, эти гири предназначены для обеспечения прослеживаемости между национальными эталонами массы (со значениями, полученными от проведения сличений с Международным прототипом килограмма) и гирями класса точности E2 и ниже.

При обеспечении прослеживаемости к национальным эталонам массы допустимая стандартная неопределенность условной массы для гирь класса точности E1 должна быть более строгой, чем у класса E2, у E2, чем для гирь класса точности F1 и так для всей цепи прослеживаемости. Допустимая расширенная неопределенность, U ($k = 2$), при определении условной массы для гирь классов точности E1 и E2 должна быть меньше или равна одной трети максимально допустимой погрешности при номинальном значении массы.

Согласно старому определению единицы массы – килограмма [2], Международный прототип не имел неопределенности. Его масса всегда составляет ровно один килограмм после очистки, хотя известно, что его масса со временем изменяется по сравнению с другими аналогичными эталонами-копиями [3].

Наибольшее влияние на цепочку прослеживаемости после переопределения оказывает ненулевая неопределенность, которая присваивается Международному прототипу килограмма – 0,020 мг. Эта неопределенность будет распространяться по всей цепочке массового распространения и, приведет к большей неопределенности калибровки, чем в настоящее время присваивается.

Требования для калибровки класса E1 выполняются в случае, когда начальная неопределенность от Международного прототипа килограмма равна 0,020 мг, и даже для случая с 0,050 мг. Это не случайно, так как критерии для переопределения, представленные СКК CGPM, были сделаны таким образом, что неопределенности E1 все еще могли быть удовлетворены после переопределения [4].

Таблица 1 - Распространение неопределенности ($k = 1$) от Международного прототипа килограмма после переопределения до гирь класса точности E1

Уровень в цепи прослеживаемости	Комбинированная стандартная неопределенность (мг)	
	Случай 1	Случай 2
Международный прототип килограмма	0,020	0,050
Рабочие эталоны ВІРМ	0,030	0,071
Национальные первичные эталоны	0,030	0,071
Гири класса точности E1 других лабораторий	0,044	0,077

Увеличение неопределенности не повлияет на способность распространять массу на уровне класса точности E1, так как условия переопределения килограмма были тщательно выбраны, таким образом предотвращая любой «скачок» или разрыв в масштабе массы.

Литература:

1. ДСТУ OIML R 111-1:2008 Гирі класів точності E1, E2, F1, F2, M1, M1-2, M2 і M3. Частина 1. Загальні технічні вимоги та методи випробування (OIML R 111-1:2004, IDT)
2. Unit of mass (kilogram). Si Brochure: The International System of Units (SI); 8th edition, 2006; updated in 2014
3. Calibration campaign against the international prototype of the kilogram in anticipation of the redefinition of the kilogram part I: comparison of the international prototype with its official copies. Michael Stock, Pauline Barat, Richard S Davis, Alain Picard and Martin J T Milton. Published 24 March 2015, Metrologia, Volume 52, Number 2.
4. Consultative Committee for Mass and Related Quantities (CCM) Report of the 12th meeting (26 March 2010) to the International Committee for Weights and Measures. Bureau International des Poids et Mesures, Sevres.

ОЦІНЮВАННЯ НЕВИЗНАЧЕНОСТІ ВИМІРЮВАНЬ ПРИ КАЛІБРУВАННІ ФОТОТАХОМЕТРІВ

Засядько В.М.

Науковий керівник - д.т.н., проф. Захаров І.П.

Харківський національний університет радіоелектроніки
(61166), Харків, просп. Науки, 14, каф. Метрології та технічної експертизи,
тел.057(702-13-31)

e-mail: Victorybox17@ukr.net

Currently, in order to ensure the uniformity of measurements, special attention is paid to the harmonization of regulatory documents in accordance with international norms and standards.

To assess the accuracy of the measurement results, in accordance with international norms and standards, uncertainty calculations are used.

Measurement uncertainty (according to VIM) is a non-negative parameter that characterizes the scattering of quantities that are attributed to the measurand based on the information used. Measurement uncertainty includes components due to systematic effects, such as those associated with corrections and the assigned values of the standards, as well as the definitional uncertainty.

Розглядається методика калібрування фототахометра з використанням стробоскопу як еталона та допоміжної апаратури токарного верстату методом безпосереднього порівняння [1].

Визначаються метрологічні характеристики фототахометру порівнянням вимірів частоти обертів вала верстату токарного в заданих умовах проведення калібрування:

$$\Delta f = f_{max} - f_{cmp} = \frac{1}{n} \sum_{i=1}^n f_{maxi} - \bar{f}_{cmp},$$

де f_{max} - показання фототахометра;

n - кількість спостережень за даний інтервал;

$\bar{f}_{cmp}$ - середньоарифметичне значення результатів вимірювань стробоскопа,

який прийнято за еталонну міру;

f_{maxi} - показання для кожної серії спостережень каліброваного приладу.

При обробці результатів вимірів враховують основну похибку еталонного фототахометра, що повинна бути у 3 рази менша основної похибки фототахометра, що калібрується, та визначають на всіх частотах обертання в кожному діапазоні вимірювання [5].

Проводиться оцінювання невизначеності вимірювань за типами А та В згідно з керівництвом по виразу невизначеності вимірювань [2].

За типом А оцінюється стандартна невизначеність за допомогою статичного аналізу ряду спостережень, тобто експериментальним стандартним відхиленням середнього значення [2], [3], [4].

За типом В оцінюється стандартна невизначеність. Цей метод, при якому враховують додаткові обумовлені внутрішньою нестабільністю об'єкту вимірювання для поправки на нестабільність фототахометра, що калібрується та поправки на нестабільність роботи еталонного стробоскопу [2], [3], [4].

Сумарну стандартну невизначеність результатів калібрування обчислити за формулою, згідно закону розповсюдження невизначеності:

$$u_{B(\bar{f}_{cmp})} = \sqrt{u_{A(\bar{f}_{max})}^2 + u_{B(\Delta f_{max})}^2 + u_{A(\bar{f}_{cmp})}^2 + u_{B(\bar{f}_{cmp})}^2 + u_{B(\Delta f_{cmp})}^2},$$

де: $u_{A(\bar{f}_{max})}$ - стандартна невизначеність вимірювань фототахометра за типом А;

$u_{B(\Delta f_{max})}$ - стандартна невизначеність для поправки на нестабільність фототахометра за типом В;

$u_{A(\bar{f}_{cmp})}$ - стандартна невизначеність стробоскопа за типом А;

$u_{B(\bar{f}_{cmp})}$ - стандартна невизначеність стробоскопа за типом В;

$u_{B(\Delta f_{cmp})}$ - стандартна невизначеність для поправки на нестабільність стробоскопа за типом В.

В результаті проводиться оцінка відповідності фототахометра заявленої у паспорті на прилад згідно технічних умов до приладів [4].

Список літератури

1. МКУ 07-479:2018 Метрологія. Фототахометр. Дійсне значення фототахометра. Калібрування з використанням стробоскопа методом звірення.
2. ДСТУ-Н РМГ 43:2006 Метрологія. Застосування «Руководства по выражению неопределенности измерений» (IDT РМГ 43:2001) – 28 с.
3. Захаров І.П. «Теория неопределенности в измерениях». - 2002, 256 с. 2017-52 с.
4. ISO/IEC 17025:2005. General requirements for the competence of testing and calibration laboratories.
5. ДСТУ ГОСТ 21339:2009 Тахометры. Общие технические условия, 23 с.

ПАРАМЕТРЫ БЕЗОПАСНОСТИ ДОРОЖНО-ТРАНСПОРТНЫХ СРЕДСТВ В ПРОЦЕССЕ ИХ ИСПЫТАНИЙ

Свинарь М. Е.

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: smariya_1997@ukr.net

The structural safety parameters of wheeled vehicles are considered. A review of regulatory documents governing the methods for measuring these parameters during testing is carried out. The features of the approaches used in the tests are considered, their generality is determined.

Keywords: wheeled vehicles, structural safety parameters, methods for measuring

Безопасность дорожного движения (БДД) определяет одно из основных качеств дорожно-транспортных средств (ДТС). Являясь основополагающим фактором обеспечения и повышения безопасности ДТС и их составных частей на стадиях их проектирования, производства и эксплуатации, сертификация оказывает существенное влияние на БДД. Именно поэтому основной целью проведения сертификационных испытаний ДТС можно считать подтверждение их конструктивной безопасности.

Конструктивную безопасность ДТС условно разделяют на активную, пассивную и экологическую.

Активная безопасность ДТС обеспечивается комплексом его конструктивных и эксплуатационных свойств, направленных на предотвращение дорожно-транспортного происшествий.

При проверке активной безопасности на управляемость можно выделить такие виды испытаний для тормозной системы, системы устойчивости и рулевого управления соответственно: испытание эффективности торможения; измерение высоты рисунка протектора; измерение рулевого усилия.

При проверке активной безопасности на информативность виды испытаний для освещения обзора и габаритов следующие: измерение освещенности; измерение прочности безопасного стекловидного материала применяемого для изготовления ветровых стекол и др; измерение наружных выступов.

Оцениваемые параметры для данных видов испытаний – это видимость освещаемой поверхности; дробление, механическая прочность, удар модели головой на воздействие окружающей среды; контур поверхности.

Вспомогательные параметры можно разделить на основные и дополнительные.

К основным относятся высота огней, наклон луча, количество огней; параметры выступов. К дополнительным: вибрация, температура устройства, угол видимости, фототермические параметры, направление фар; протяженность закругления, твердость материала, утапливание, радиус кривизны.

Пассивная безопасность обеспечивается совокупностью конструктивных свойств ДТС, позволяющих при возникновении дорожно-транспортного происшествия исключить или уменьшить тяжесть его последствий для водителя, пассажиров и пешеходов.

Виды испытаний, которые проводятся при проверке пассивной безопасности – это измерение прочности сидений и их креплений. Основным оцениваемым параметром является непосредственно прочность креплений, а дополнительными – угол наклона, сила осевого сжатия, показатели ускорения, критерий травматизма, тип сидения.

Экологическая безопасность достигается ограничением излучений и выделений от ДТС, оказывающих отрицательное влияние на участников дорожного движения и окружающую среду.

При исследовании выбросов в атмосферу для определения дымности, видимых выбросов и оксид углерода и углеводорода необходимы испытания: измерения дымности; измерения выброса выхлопных газов; измерения содержания CO_2 и CH_4 в отработавших газах автомобилей.

Оцениваемым параметром является коэффициент поглощения. Вспомогательные параметры: коэффициент ослабления светового потока, плотность выхлопных газов, номинальный расход газов.

Дополнительные вспомогательные параметры: температура, частота вращения вала дизеля, чувствительность, свободное ускорение, давление; число оборотов, мощность, температура воздуха, атмосферное давление, давление в системе впуска и выхлопа, свободное ускорение; рабочая температура, частота вращения вала двигателя, гранично-допустимые значения CO_2 и CH_4 .

Исследуя акустические шумы, измеряются внешний и внутренние шумы, которые характеризуются коэффициентом звукопоглощения. Вспомогательные параметры при таком испытании – число оборотов двигателя, габариты транспортного средства, температурные параметры, параметры окружающей среды, покрытие, атмосферное давление.

При проведении испытаний радиопомех, нужно измерять радиоэлектрические помехи и контролировать их уровень. Вспомогательными параметрами будут высота антенны, частота измерения, а дополнительными – рабочая температура, расстояние от антенны до ближней металлической части, погодные условия.

ШЛЯХИ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПРОЦЕСУ КАЛІБРУВАННЯ ЦИФРОВИХ МУЛЬТИМЕТРІВ

Семеніхін В.С.

Науковий керівник – д.т.н., проф. Захаров І.П.

Національний науковий центр «Інститут метрології»

(61002, Харків, вул. Мироносицька, 42, тел. (057) 700-34-09)

e-mail: kh1856ua@gmail.com

The development of instrument technology has led to a decrease in the cost of manufacturing digital measuring instruments and has greatly expanded their functionality, which has led to a significant increase in the number of measurement tools that need to be calibrated and complicated due to the multifunctionality of devices and the need for complex calculations.

Significantly reducing the cost of digital measuring instruments and increasing the complexity of their calibration process in terms of cost-effectiveness make it necessary to optimize the calibration process by increasing its productivity.

Збільшити продуктивність процесу калібрування, тобто збільшити кількість відкаліброваних засобів вимірювань за одиницю часу, у випадку з цифровими мультиметрами можливо двома способами. Перший полягає у тому щоб одночасно калібрувати декілька приладів, другий полягає у пришвидшенні процесу калібрування і оформлення результатів за допомогою автоматизації.

Для того щоб з'ясувати на скільки збільшується продуктивність процесу калібрування використовуючи наведені шляхи її підвищення порівняно зі стандартним методом калібрування уручну одного приладу за раз було проведено розрахунковий експеримент.

Для зручності розрахунків експерименту було обрано партію зі 100 цифрових мультиметрів типу «APPA 505» для яких експериментальним шляхом, за допомогою багатофункціонального калібратора Fluke 5520A, були визначені витрати часу на проведення вимірювань і оформлення їх результатів – на кожну точку вимірювань у стандартному ручному режимі в середньому необхідно 10 секунд без урахування часу на перемикання та впливу оператора, на внесення результатів вимірювань і розрахунків до сертифікату калібрування витрачається в середньому 20 хвилин на один прилад. Для дослідження способу підвищення продуктивності за допомогою автоматизації процесу калібрування було використано спеціалізоване програмне забезпечення (далі – ПЗ) Fluke MET/CAL® Plus.

Калібрування проводилося для всіх вимірювальних величин, на всіх діапазонах вимірювань, що вимірює даний цифровий мультиметр – на кожному діапазоні обиралися по 3 точки калібрування (5 %, 50 % та 95 % від діапазону) на кожній з яких було знято по 5 вимірюваних значень. Дані про кількості вимірювань у процесі калібрування наведено у Таблиці 1.

Таблиця 1 – Кількості вимірювань при калібруванні одного мультиметра

Вимірювана величина	Кіл-сть діапазонів вимірювань	Кіл-сть частотних діапазонів	Кіл-сть точок калібрування	Кіл-сть вимірювань у точці	Загалом кількість вимірювань(точок)
DCV	5	-	3	5	725 (145)
ACV	2	3			
	3	3			
	2	4			
DCI	3	-			
ACI	1	1			
	2	1			
R	6	-			
C	7	-			
T	2	-			
F	-	6			

Таким чином вручну на процес калібрування партії зі 100 цифрових мультиметрів за розрахунками витрачається 73,61 години (з них на проведення вимірювань 40,28 годин, на оформлення – 33,33 години), продуктивність складає 1,36 од/год без урахування часу перемикання та впливу втоми оператора.

Технічно одночасно можливо проводити калібрування 5-ти мультиметрів у режимах вимірювання напруги постійного та змінного струму і частоти. При використанні цього способу на процес калібрування партії зі 100 мультиметрів за розрахунками витрачається 47,23 години (на проведення вимірювань – 13,9 годин, на оформлення – 33,33 години), продуктивність складає 2,12 од/год без урахування часу перемикання та впливу втоми оператора.

Іншим способом збільшення продуктивності процесу калібрування є використання ПЗ для автоматизації ПЗ Fluke MET/CAL® Plus, яке дозволяє проводити калібрування цифрового мультиметра в середньому за 0,5 год (без урахування часу на перемикання) та в автоматичному режимі здійснювати обробку та оформлення результатів [1]. Таким чином при використанні спеціалізованого ПЗ для автоматизації процесу калібрування продуктивність складає 2 од/год.

Таким чином продуктивність порівняно із ручним режимом проведення калібрування з використанням автоматизації зростає на 47 %, а при одночасному калібруванні 5 мультиметрів за напругою та частотою на 55 %, якщо не враховувати вплив оператора.

Література:

1. Зуйков А.А. Автоматизация работы метрологической службы – программное обеспечение Fluke MeT/CAL. ЭЛЕКТРОНИКА. Наука/технология/бизнес. 2015. №8 (00148). С. 127-134

АЛФАВІТНИЙ ПЕРЕЛІК

A

Ayodele Tega Ajadi	64
Abdelfattah Mohamed	80

I

Ikeza Obasi A. D	60
------------------	----

O

Olatunji John	78
---------------	----

M

Mahmoud Mahmoud Sayed Hussein	52
Eltayh Mostafa Tarek Ahmed	76

T

Reginald Tannor	66
-----------------	----

A

Алексин В.В	28
Афанасьев Ю.В	26
Абіх І.В	139

Б

Бондаренко О.С	8
Білокурова А.О	58
Бухаров А.С	113
Барсук В.А	113
Бондарь О.Д	125

В

Волокітіна О.І	22
Васільєва Ю.С	127

Г

Галкін П.В	40
Греков І.С	12
Галушка А.В	18
Гонтарь І.А	42
Грицюк В.К	48
Гнилицький Я. В	129
Гапоненко Д.О	171
Гусак М.В	50
Гнітецький В. А	82

Д

Дарраж Муад	46
Дриф Абденур	54
Демченко І.В	84

Е

Евдокименко М.А	74
Ермолаев А.А	121
Ермак А.Р	173

З

Засядько В.М	177
--------------	-----

Ж

Журавка А.В.	42
--------------	----

И

Иващенко М.Д	109
--------------	-----

К

Кавунеко Я.О	91,105
Козубенко В.С	56
Колтаков О.А	68
Куценко Е.Е	89,95
Кодаченко Р.Ю	107
Курлан О.О	117
Куріний А.А	119
Кирсанов О.О	141
Ключников Е.Ю	143
Коновалова К.Ю	151

Л		Ф	
Лябах А.С	20	Фоменко В.Д	161
Лаптев П.О	70		
М		Х	
Маслій В.П.	135	Ходаківський М.М	16
Муляр Б.П	10	Хачиров Е.Ф	20
Мірось Ю.О	24	Ц	
Миронов А.А	30	Цилюрик В.Є	72
Мошенська Н.М	62	Цариценко С.Д	145
		Цис М.Б	165
Н		Ч	
Назаренко Ю.В	149	Чурсанов М.О	6
П		Чеботарев И.А	38
Пушкарьов В. В	14	Чернікова В.Г	93, 97, 103
Пантелєєв В.О	44	Чеботарьова Д.В	137
Подолька Н.В	105		
Пестерєва С. Є	123	Ш	
Попаденко М.О	153	Шлома О.К	36
Паценко А. Н	175	Шаповал М	46
Р		Щ	
Радченко В.В	34	Щербак А	46
Резнік Я.В	131		
Рижов О. О	157	Я	
Рябко М.С	133	Ященко С.В	82
		Яхновська Д.С	163
С			
Самочорнов М.Б	115		
Семенченко О. А	99		
Скирда С.О	93, 97, 103		
Стрілець А.М	93, 97, 103		
Степанов О.О	155		
Свинарь М. Е	179		
Семеніхін В.С	181		
Т			
Ткаченко А.М	32		
Тертичний В.О	95, 101		
Тимчук І.В	167		
Токарева М.С	169		
Туренко А.В	147		

ЗМІСТ

Проблеми інфкомунікацій	5
Управління інформаційною безпекою	87
Інфокомунікаційні технології.....	111
Інформаційно-вимірювальні технології, метрологічне забезпечення, стандартизація і сертифікація	159
Алфавітний перелік.....	182

ДЛЯ ПОДАТОК

ДЛЯ ПОДАТОК

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У ХХІ СТОЛІТТІ»

Матеріали XXIV Міжнародного молодіжного форуму

Відповідальний за випуск О.С. Невзорова

Комп'ютерна верстка О.І. Ільїна, В.Г. Чепела

Матеріали збірника публікуються
в авторському варіанті без редагування

План 2020 (перше півріччя), поз. _____

Підп. до використання 02.04.2020 Формат pdf. Об'єм даних 3,6 Мб

Підп. до друку 02.04.20. Формат 60x84 _{1/16}. Спосіб друку – ризограф.

Умов.друк.арк. 10,4. Облік. вид.арк. 10,0. Тираж 100 прим.

Ціна договірна Зам № _____

ХНУРЕ. Україна. 61166, Харків, просп. Науки, 14, E-mail: info@nure.ua

Підготовлено в редакційно-видавничому відділі ХНУРЕ
Свідоцтво суб'єкта видавничої справи ДК №1409 від 26.06.2003

Віддруковано в редакційно-видавничому відділі ХНУРЕ
61166, Харків, просп. Науки, 14

NURE

