ISSN 1311-3321

РУСЕНСКИ УНИВЕРСИТЕТ "Ангел Кънчев"
UNIVERSITY OF RUSE "Angel Kanchev"

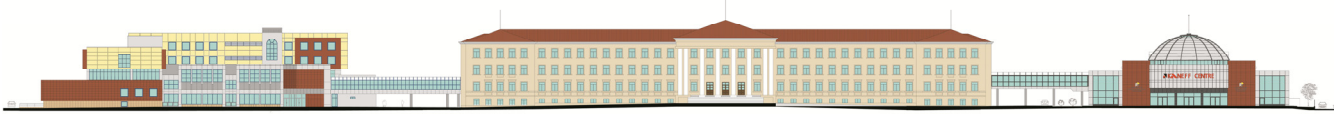
Факултет „Електротехника, електроника и автоматика"
Faculty of Electrical engineering, Electronics and Automation

СБОРНИК ДОКЛАДИ
на
СТУДЕНТСКА НАУЧНА СЕСИЯ – СНС'17

СБОРНИК ДОКЛАДОВ
СТУДЕНЧЕСКОЙ НАУЧНОЙ СЕСИИ – СНС'17

PROCEEDINGS
of
the SCIENTIFIC STUDENT SESSION – SSS'17

Русе
Ruse
2017



ISSN 1311-3321

РУСЕНСКИ УНИВЕРСИТЕТ "Ангел Кънчев"
UNIVERSITY OF RUSE "Angel Kanchev"

Факултет „Електротехника, електроника и автоматика "
Faculty of Electrical engineering, Electronics and Automation

СБОРНИК ДОКЛАДИ

на

СТУДЕНТСКА НАУЧНА СЕСИЯ – СНС'17

СБОРНИК ДОКЛАДОВ

СТУДЕНЧЕСКОЙ НАУЧНОЙ СЕСИИ – СНС'17

PROCEEDINGS

of

the SCIENTIFIC STUDENT SESSION – SSS'17

Русе
Ruse
2017

Сборникът включва докладите, изнесени на студентската научна сесия **СНС'17**, която е организирана и проведена във факултет **„Електротехника, електроника и автоматика"** на Русенския университет "Ангел Кънчев".

Докладите са отпечатани във вида, предоставен от авторите им.
Доклады опубликованы в виде, предоставленном их авторами.
The papers have been printed as presented by the authors.

ISSN 1311-3321

- **СТУДЕНТСКАТА НАУЧНА СЕСИЯ се организира от АКАДЕМИЧНОТО РЪКОВОДСТВО и СТУДЕНТСКИЯ СЪВЕТ на РУСЕНСКИЯ УНИВЕРСИТЕТ с цел да се предостави възможност на студенти и докторанти да популяризират основните резултати от своята учебно-изследователска работа и да обменят опит.**

- **ОРГАНИЗАЦИОНЕН КОМИТЕТ**

• **Съпредседатели:**

проф. д-р Велизара Пенчева – Ректор на Русенския университет

чл.-кор. проф. дтн Христо Белоев, DHC – Председател на СУ – Русе и ОС на Русенски университет

Станимир Бояджиев - Председател на Студентски съвет

• **Научни секретари:**

проф. д-р Диана Антонова – Зам. ректор НИД
dantonova@uni-ruse.bg; 082-888 249

доц. д-р инж. Галина Иванова – Координатор докторанти
giivanova@uni-ruse.bg; 082-888 855.

• **Членове:**

Факултет „Аграрно-индустриален"

доц. д-р инж. Калоян Стоянов - kes@uni-ruse.bg, 082-888 542;

Здравко Стоянов - студент plox@abv.bg, 0883486551

Факултет „Машинно-технологичен"

доц. д-р Велина Боздуганова - velina@uniruse.bg, 082-888 572;

маг. инж. Виктория Карачорова - vkarachorova@uni-ruse.bg, 082-888 653

Факултет „Електротехника, електроника и автоматика"
доц. д-р Милко Маринов - mmarinov@ecs.uni-ruse.bg , 082 888 356

доц. д-р Цветелина Георгиева - cgeorgieva@uni-ruse.bg, 082 888 668

гл. ас. д-р Иванка Цветкова - itsvetkova@uni-ruse.bg, 082 888 836

Георги Георгиев - jorch123@abv.bg

Факултет „Транспортен"
доц. д-р Симеон Илиев – spi@uni-ruse.bg, 082-888 331;

Салим Куйтов – salimsv1996@gmail.com

Факултет "Бизнес и мениджмънт"
доц. д-р Драгомир Илиев – diliev@uni-ruse.bg; 082 888 704
гл. ас. д-р Елизар Станев – eastanev@uni-ruse.bg, 082 888 703

Факултет „Юридически"
гл. ас. д-р Ваня Пантелеева - vpanteleeva@uni-ruse.bg, тел. 0887412662

Факултет „Природни науки и образование"
доц. д-р Юрий Кандиларов - ukandilarov@uni-ruse.bg, 0889 518 824
Слави Георгиев - georgiev.slavi.94@gmail.com

Факултет „Обществено здраве и здравни грижи"
Секция „Здравни грижи"
доц. д-р Теодора Недева, дм - tsherbanova@uni-ruse.bg, 0887468695
Кристина Мариянова – студент, 0876134124

Секция „Промоция на здравето и социални дейности"
доц. д-р Ирина Караганова - ikaraganova@uni-ruse.bg, 0884203004
Надежда Колева – студент, 0895859574

Филиал Разград
доц. д-р Цветан Димитров - tz_dimitrow@abv.bg , 0887 631 645

Атанас Атанасов - manager.atanasov@gmail.com , 0893 339 749

Филиал Силистра
доц. д-р Галина Лечева - glecheva@uni-ruse.bg; 086 821 521
Катрин Нивелинова - Ladykathrin95@abv.bg

СЕКЦИЯ
„Електротехника, електроника и автоматика"

С Ъ Д Ъ Р Ж А Н И Е

СЕКЦИЯ
„Комуникационна и компютърна техника"

С Ъ Д Ъ Р Ж А Н И Е

Хармоници в захранващата мрежа, създавани от ретрофит LED лампи

автор: маг. инж. Петя Петрова
научни ръководители: доц. д-р Орлин Петров, доц. д-р Вяра Русева

Harmonics in the power supply network developed from retrofit LED Lamps: *The paper presents the study of the generated higher harmonics in the electrical network of different types of retrofit LED lamps. The study was conducted with over 30 types of LED products with different characteristics and from different manufacturers. The results obtained are presented in a summarized form and the relevant analysis and conclusions are made. It turns out that some of the LEDs tested show relatively good indicators, but there are also those that cause significant "pollution" of the electrical network.*

Key words: *LED Lighting, Harmonic distortion, Retrofit LEDs.*

ВЪВЕДЕНИЕ

През последните няколко години, сме свидетели на навлизането на светодиодните източници все по-масово в бита. Предпоставка за това, е разработването на т.нар. ретрофит светодиодни лампи, при които е възможна директната замяна на съществуващ конвенционален светлинен източник с модерен светодиоден.

Тъй като светодиодните продукти са полупроводникови устройства, тяхното захранване трябва да става с постоянен ток. Това предполага използването на специализиран захранващ модул (драйвер), за да може да се осигури правилно функциониране на устройството [1].

В резултат на това се наблюдават нарушения на качеството на електрическата енергия, които могат да причинят повреда в оборудването и генериране на висши хармоници, които водят до увеличаване на тока [2].

Въпреки, че мощността на единичен светодиод е малка, при голям брой потребители използващи светодиодни лампи в помещенията, може да възникнат значителни проблеми с качеството на електрическата енергия [3].

ИЗЛОЖЕНИЕ

В доклада е представено изследване на генерираните висши хармоници в електрическата мрежа от различни видове ретрофит светодиодни лампи. Изследването е извършено с над 30 вида светодиодни продукти с различни характеристики и от различни производители.

Характеристиките на част от изследваните светодиодни лампи са:

LED G9 LAMP – с параметри: Цветна температура - Warm White 3000K Светлинен поток - 320 lm Електрическа мощност - 4W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 20,000 часа;	LED BULB E27 – с параметри: Цветна температура - Cool White 6000K Светлинен поток - 470lm Електрическа мощност - 7W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 20,000 часа;
LED BULB E27 – с параметри: Цветна температура - Warm White 2700K Светлинен поток - 470lm Електрическа мощност - 7W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 20,000 часа;	LED SPOTLIGHT GU10 – с параметри: Цветна температура - Nature White 4500K Светлинен поток - 350lm Електрическа мощност - 5W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 20,000 часа;

LED SPOTLIGHT GU10 – с параметри: Цветна температура - Warm White 3000K Светлинен поток - 350lm Електрическа мощност - 5W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 20,000 часа;	LED BULB E27 – с параметри: Цветна температура - Warm White 2700K Светлинен поток - 470lm Електрическа мощност - 7W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 15,000 часа;
LED SPOTLIGHT GU10 – с параметри: Цветна температура - Warm White 2700K Светлинен поток - 235lm Електрическа мощност - 4W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 15,000 часа;	LED SPOTLIGHT GU10 – с параметри: Цветна температура - Warm White 2700K Светлинен поток - 520lm Електрическа мощност - 6W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 50,000 часа;
LED SPOTLIGHT GU10 – с параметри: Цветна температура - Neutral White 4200K Светлинен поток - 550lm Електрическа мощност - 6W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 50,000 часа;	LED BULB E27 – с параметри: Цветна температура - Cool White 6000K Светлинен поток - 800lm Електрическа мощност - 8W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 50,000 часа;
LED BULB E27 – с параметри: Цветна температура - Warm White 2700K Светлинен поток - 760lm Електрическа мощност - 8W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 50,000 часа;	LED G9 – с параметри: Цветна температура - Neutral White 4200K Светлинен поток - 300lm Електрическа мощност - 3W Индекс на цветопредаване - Ra > 80 Експлоатационен срок - 50,000 часа;

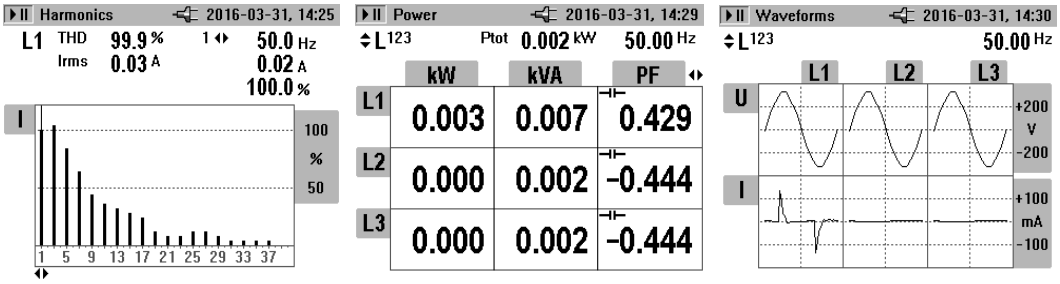
Фиг. 1. Снимки на част от изследваните светодиодни ретрофит лампи

На **фиг. 1** са показани снимки на част от изследваните светодиодни продукти, като умишлено не са показани фирмите производители на лампите, за да не се предизвика компрометиране на някоя търговска марка.

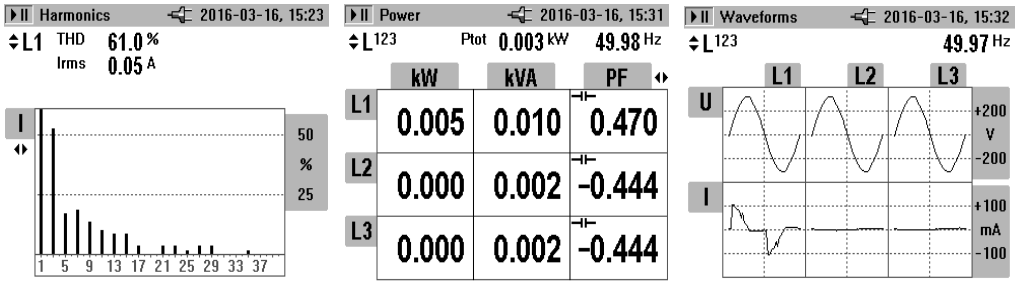
При провеждането на изследването са спазени изискванията на стандартите БДС EN 50160 и БДС EN 61000.

Използван е анализатор на качеството на електрическата енергия ANALYST 3Q, даващ възможност за измерване на всички параметри свързани с качеството на електрическата енергия. Измерването на хармоничните съставки на тока и напрежението става до 41 хармоник.

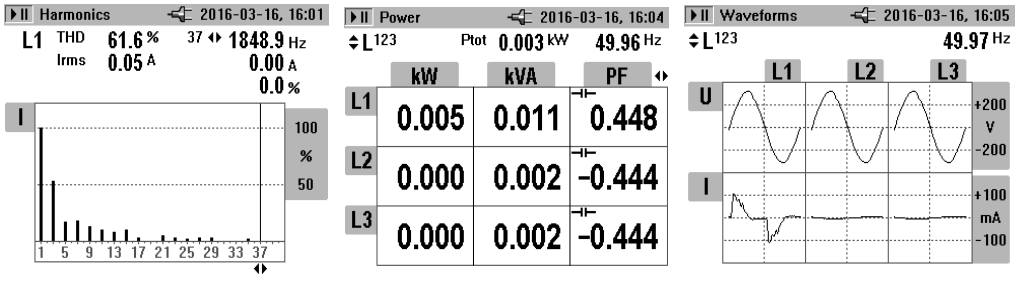
На **фиг. 2 до фиг. 9** са показани екрани от измерванията на различни видове светодиодни лампи. Показани са само по-значимите резултати на светодиодни лампи, които представляват интерес от гледната точка на „замърсяването“ на електрическата мрежа с висши хармоници.



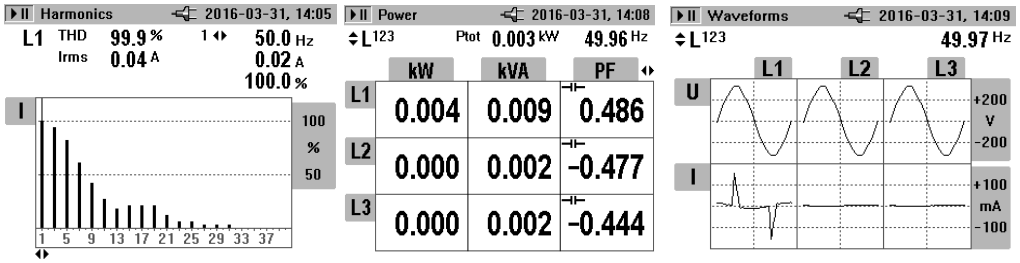
Фиг.2. Изследване на лампа LED G9, 4W, 3000K



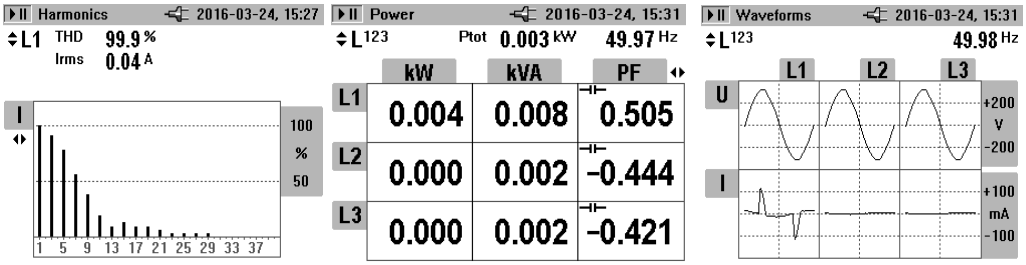
Фиг.3. Изследване на лампа LED BULB E27, 7W, 6000K



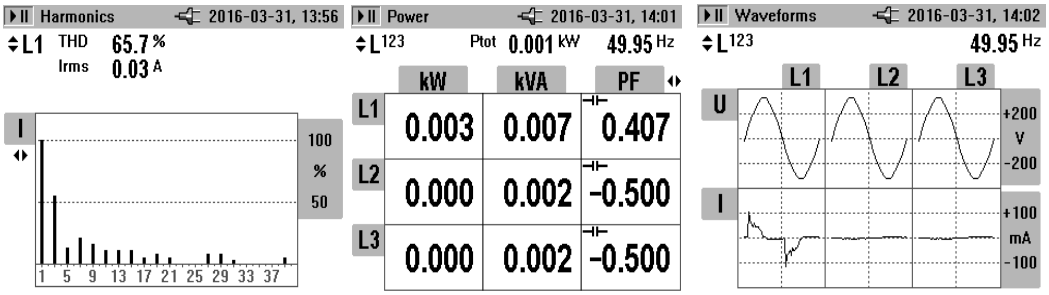
Фиг.4. Изследване на лампа LED BULB E27, 7W, 2700K



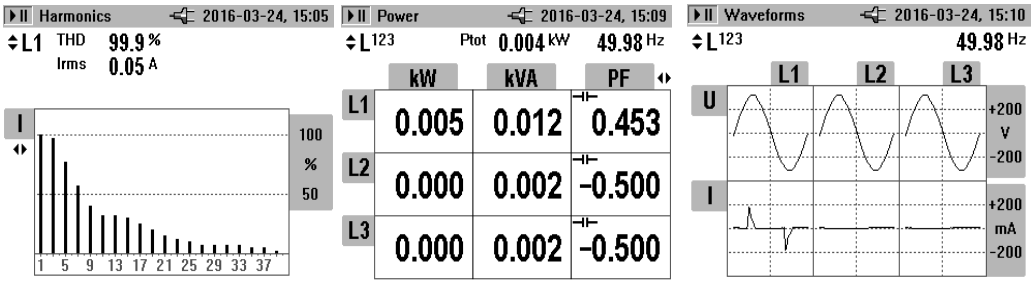
Фиг.5. Изследване на лампа LED SPOTLIGHT, 5W, 4500K



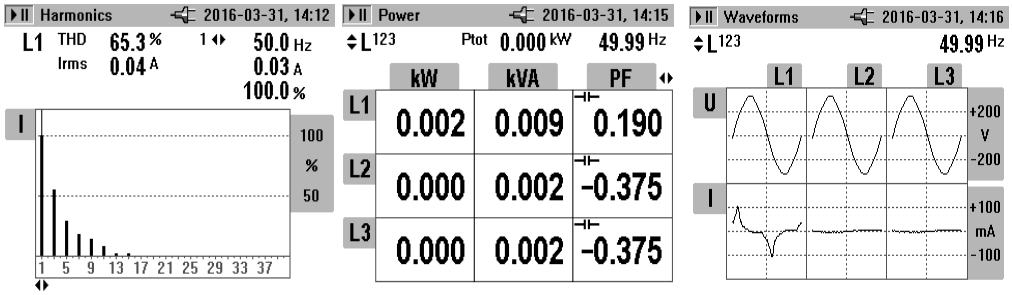
Фиг.6. Изследване на лампа LED SPOTLIGHT, 5W, 3000K



Фиг.7. Изследване на лампа LED SPOTLIGHT, 4W, 2700K



Фиг.8. Изследване на лампа LED SPOTLIGHT, 6W, 2700K



Фиг.9. Изследване на лампа LED G9, 3W, 4200K

ЗАКЛЮЧЕНИЕ

След проведените измервания и анализиране на получените резултати, могат да се направят следните изводи:

1. При нискобюджетните светодиодни лампи се наблюдава хармонично замърсяване в целия спектър (от 1 до 29 хармоник), което явно се дължи на по-нискокачествен захранващ модул. Общият показател THDI също е с много високи стойности.
2. При светодиодните продукти от по-висок клас хармоничните замърсявания са сведени само до 9-ти хармоник, като амплитудите на тока за 3, 5, 7 и 9

хармоник са много по-малки от амплитудата на основния хармоник. Показателя THDI има сравнително добра стойност.

3. Хармоничните замърсявания за напрежението са пренебрежимо малки за всички изследвани образци.
4. Проблемът, който евентуално може да се прояви след време, е че при много на брой светлинни източници, сумарният ток ще нарасне и тогава генерираните хармонични замърсявания ще започнат да оказват съществено влияние на захранващата мрежа.

ЛИТЕРАТУРА

[1] Shahriar Khan, "An Energy Saving Program for Bangladesh, for Reducing Load Shedding, and for Continuity of Power for IT Sector" – Proceedings of l1h International Conference on Computer and Information Technology, (ICCIT 2008) 25-27 December,2008, Khulna, Bangladesh.

[2] БДС EN 50160:2010. Характеристики на напрежението на електрическата енергия, доставяна от обществените електрически мрежи.

[3] БДС EN 61000-3-2:2014. Електромагнитна съвместимост (EMC). Част 3-2: Гранични стойности. Гранични стойности за излъчвания на хармонични съставящи на тока (входен ток на устройства/съоръжения ≤ 16 A за фаза).

За контакти:

маг. инж. Петя Петрова, докторант, Катедра "Електроснабдяване и електрообзавеждане", Русенски университет "Ангел Кънчев", e-mail: ppetrova@uni-ruse.bg

доц. д-р Орлин Петров, Катедра "Електроснабдяване и електрообзавеждане", Русенски университет "Ангел Кънчев", тел. 082/888 301, e-mail: opetrov@uni-ruse.bg

Математическа обосновка и схемотехническа реализация на апроксимация на триъгълен сигнал в синусоида

автор: инж. Димитър Йорданов
научен ръководител: гл. ас. д-р Снежинка Захариева

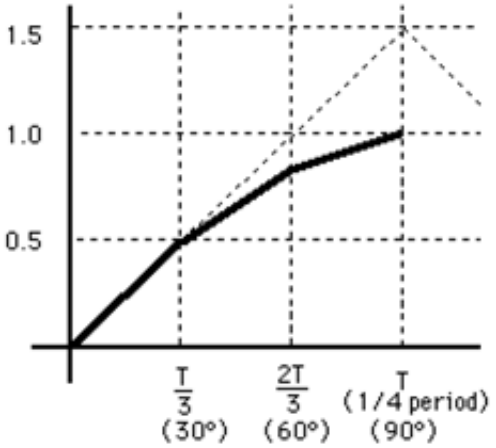
Mathematical explaining and schematic realization of approximation of triangle to sine wave: *In the practical exercise with the students usually is used variety of waveform, sine is one of them. The simplicity of schematic is the main purpose, so that we can use one signal to get two, for example to transform triangle wave to sine. There are many methods to transform triangle to sine wave, one of them is piecewise approximation. The aim of the report is to show mathematical explanation and practical realization of that method.*

Key words: *approximation, triangle wave, sine wave .*

ВЪВЕДЕНИЕ

Преобразуването на триъгълен сигнал в синусоидален в някои случаи може много да улесни схемното решение, като не е необходимо да се изгражда нова схема за реализация на конкретния генератор, а може да се преобразува съществуващ сигнал, в случая триъгълен в синусоидален.

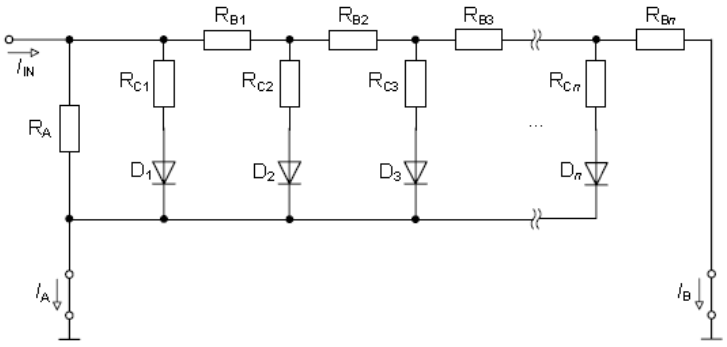
Един от методите за преобразуване на триъгълен сигнал в синусоидален е чрез частична линейна апроксимация, като на фиг.1 е показана графика илюстрираща процеса [3].



Фиг.1 Частичната линейна апроксимация

Точността на този вид апроксимация се определя от бройката на използваните отсечки. Математически този процес се описва с ред на Фурие и в зависимост от броя на членовете се определя точно до колко синусоидата се доближава до оригиналния триъгълен сигнал.

Схематично метода се изразява чрез използване на така наречена диодна матрица, чиято принципна схема е показана на фиг.2 [2].



Фиг.2 Принципна електрическа схема на диодна матрица

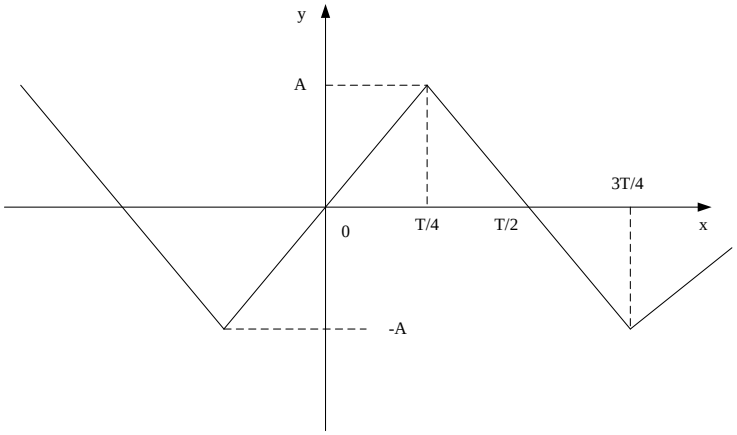
Всеки един диод създава точка на пречупване, като в зависимост от това колко точна трябва да е синусоидата се определя и броя на диодите. Диодната формираща схема става по-практична, когато съпротивленията са оразмерени към по-удобни стандартни стойности, и когато веригата на делителя на напрежение замества захранващия източник.

Когато съпротивленията във веригата са подходящо оразмерени диодите могат да се разглеждат в идеализиран модел, а веригата на делителя на напрежение да се използва като източник на точно напрежение. Съпротивленията в делителя на напрежение трябва да бъдат достатъчно малки, за да могат да се съпоставят със съпротивлението на диодните клонове, с оглед намаляване на тяхното взаимодействие [1].

ИЗЛОЖЕНИЕ

Математическа обосновка на апроксимация на триъгълен сигнал в синусоида

На фиг.3 е представена графика на триъгълния сигнал, който ще се разлага [3].



Фиг.3 Триъгълен сигнал

Математическата обосновка на процеса на апроксимация се заключава в разлагане в ред на Фурие:

$$f(x) = y = \begin{cases} \frac{4A}{T}x & x\epsilon[0, T/4] \\ -\frac{4T}{T}x + 2A & x\epsilon[T/4;\ 3T/4] \\ \frac{4A}{T}x - 4A & x\epsilon[3T/4;\ T] \end{cases} \quad (1)$$

където: y е периодична функция => y е нечетна

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos\frac{2\pi nx}{T} + b_n \sin\frac{2\pi nx}{T}$$

(2)

$$a_0 = \frac{2}{T}\int_0^T f(x)dx \qquad (3)$$

Косинусовите съставляващи се пресмятат с израза:

$$a_n = \frac{2}{T}\int_0^T f(x)\cos\frac{2\pi nx}{T}dx \qquad (4)$$

Синусовите съставляващи се пресмятат с израза:

$$b_n = \frac{2}{T}\int_0^T f(x)\sin\frac{2\pi nx}{T}dx \qquad (5)$$

От това, че f(x) е нечетна следва, че $a_n = 0$

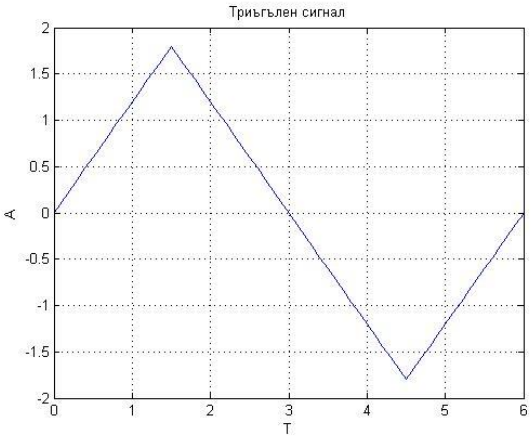
Изчисляване на коефициентите на реда на Фурие:

$$b_n = \frac{2}{T}\int_0^T f(x)\sin\frac{2\pi nx}{T}dx = \frac{2}{T}\left[\int_0^{T/4}\frac{4A}{T}x\sin\frac{2\pi nx}{T}\,dx + \int_{T/4}^{3T/4}\left(-\frac{4A}{T}x + 2A\right)\sin\frac{2\pi nx}{T}\,dx + \int_{3T/4}^{T}\left(\frac{4A}{T}x - 4A\right)\sin\frac{2\pi nx}{T}\,dx\right] = \frac{4A}{\pi^2 n^2}\left(\frac{\sin 2\pi n}{2} + \frac{\sin n\pi}{2} - \frac{\sin 3\pi n}{2}\right) \qquad (6)$$

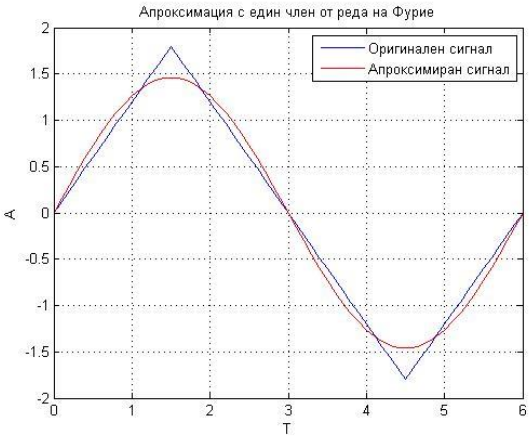
където n е номер в реда на Фурие.

$$f(x) = \frac{8A}{\pi^2}\sin\frac{2\pi x}{T} - \frac{8A}{\pi^2 3^2}\sin\frac{2\pi 3x}{T} + \frac{8A}{\pi^2 5^2}\sin\frac{2\pi 5x}{T} - \frac{8A}{\pi^2 7^2}\sin\frac{2\pi 7x}{T} + \cdots = \frac{8A}{\pi^2}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{(2n-1)^2}\sin\frac{2(2n-1)x}{T} \qquad (7)$$

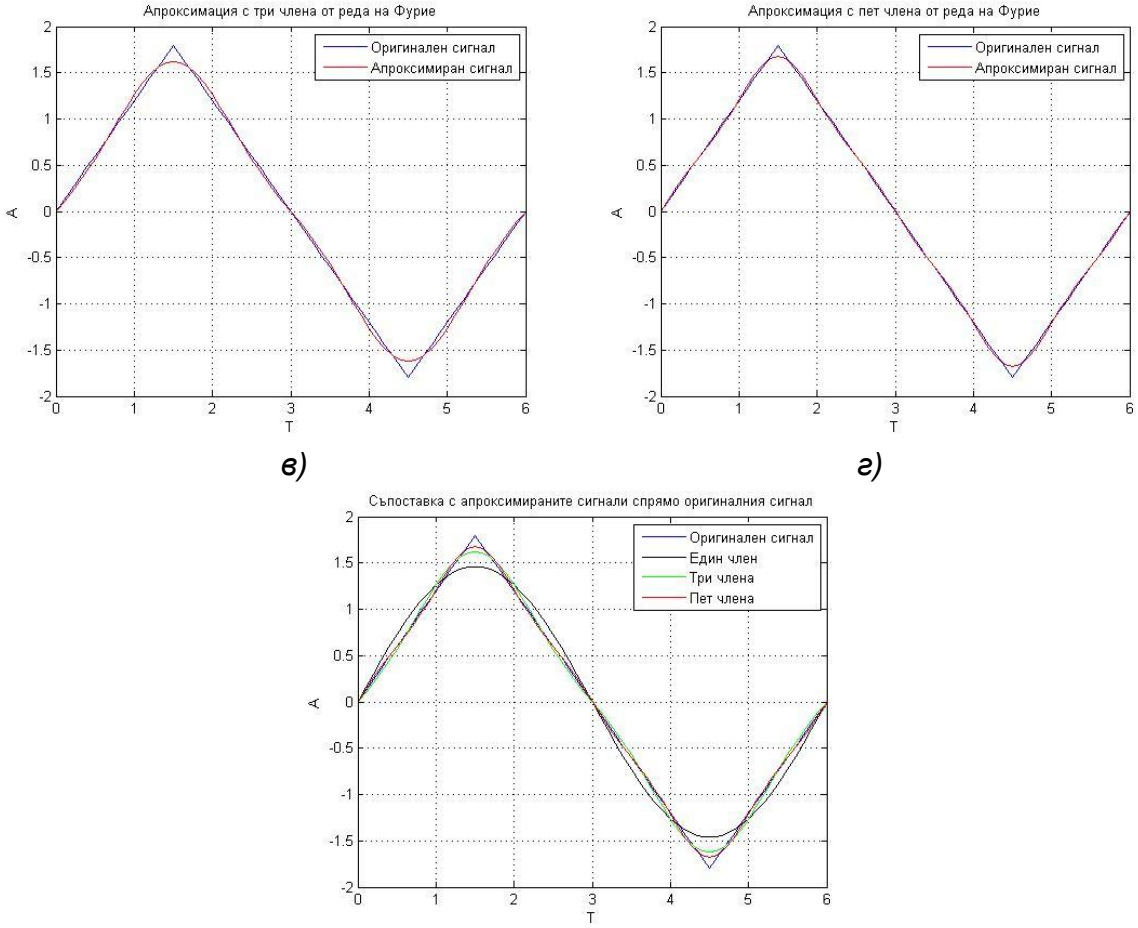
Поради факта че функцията е нечетна и с получените резултати от решаването на интеграла се оказва, че тя се описва само с нечетни членове. В конкретния случай са пресметнати и в последствие построени графики с един, три и пет члена на Фурие в програмна среда Matlab (фиг. 4 а), б), в), г) и д)). Номерацията е такава, защото конкретните членове отговарят на математическата подредба в реда на Фурие [5].



а)



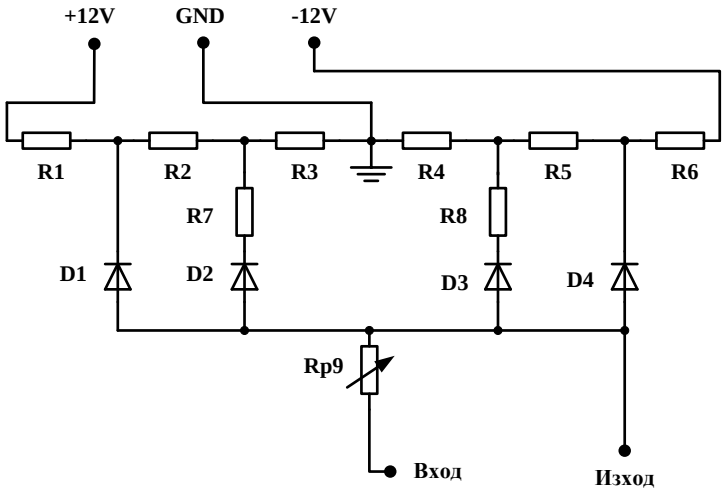
б)



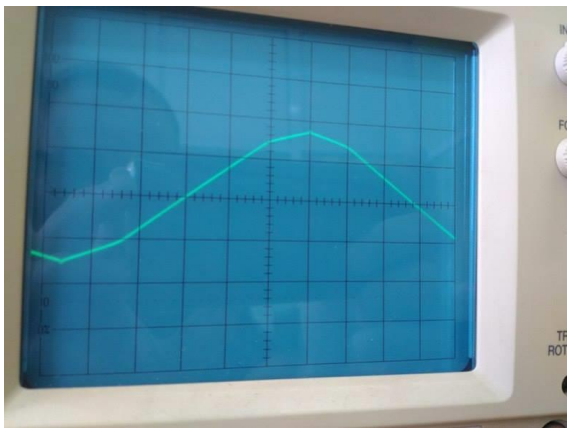
Фиг.4 Графики на броя на членовете върху апроксимацията на триъгълния сигнал

Схемотехническа реализация и практически резултати на апроксимация на триъгълен сигнал в синусоида.

Практически е реализирана схемата показана на фиг.4. Чрез потенциометъра Rp9 се определя до каква степен да бъде апроксимиран сигнала в определени граници, като на фиг.6 е показан фотос на апроксимирания синусоидален сигнал.



Фиг.5 Принципна електрическа схема на диодната матрица



Фиг.6 Експериментално получена апроксимирана синусоида

При сравнение между симулираната в програмна среда Matlab апроксимация и експериментално получената синусоида, може да се заключи, че фиг.3б се доближава най-много до практически получения резултат от фиг. 6.

ЗАКЛЮЧЕНИЕ

Метода на линейна частична апроксимация има няколко предимства като: проста схемотехническа реализация (елементи с ниска себестойност като диоди и резистори), прицизно настройване на апроксимацията чрез различен брой използвани диоди в схемата и потенциометър в изхода.

Разгледания метод може да бъде използван за нуждите на дисциплината: „Измервания в електрониката“, към катедра: „Електроника“.

Целта е студентите да се запознаят с конкретния метод и да оценят неговите предимства и недостатъци спрямо други методи за получаване на синусоидален сигнал от триъгълен.

ЛИТЕРАТУРА

[1] Gigov Hr. "Measurements in electronics", Varna
[2] Dimitrov V., St. Psederski, "Measurements in electronics", University of Ruse, Ruse, 2000.
[3] Osikovski B., I. Evstatiev, Y. Neikov, “Signals and systems”, 2002 University of Ruse
[4] http//www.electronics.dit.ie – 19.03.2017г.
[5] Signals and systems using Matlab - http://web.itu.edu.tr/hulyayalcin/Signal_Processing_Books/2011_Chapparro_Signals_and_Systems_with_Matlab.pdf - 01.03.2017г.

За контакти:

инж. Димитър Йорданов, магистър в Катедра “Електроника”, Русенски университет “Ангел Кънчев” yordanov_93@abv.bg

гл. ас. д-р Снежинка Захариева, Катедра “Електроника”, Русенски университет “Ангел Кънчев”, тел.: 082-888 382, e-mail: szaharieva@uni-ruse.bg

Разработване и изследване на понижаващ импулсен регулатор

автор: инж. Димитър Йорданов
научен ръководител: гл. ас. д-р Снежинка Захариева

Design and research of Step-Down Voltage Regulator: *Often when conducting practical exercises with students is using adjustable external power sources, which values of the supply voltages very likely differ from the nominal value specified for powering an electronic device.Developed is a lowering pulse generator for the needs of the educational process in the discipline "Power supplies". The aim of the report is to show how is designs that type of voltage regulators.*
Key words: *Step-Down Voltage Regulator, Design..*

ВЪВЕДЕНИЕ

DC/DC импулсните регулатори (известни още като превключващи регулатори) се появяват още през седемдесетте години на двадесети век. Те предлагат редица предимства пред обикновенните линейни регулатори, като най-важно от тях е високата им ефективност [3].

В наши дни има два начина да се подходи към проектирането на превключващи захранващи източници. Първият начин е посредством използване на елементи със стандартни стойности, които са препоръчани в документацията на фирмата производител на интегралната схема, чрез която се реализира регулатора. Вторият начин е когато са необходими нестандартни напрежения или токове, което налага преизчисляване на параметрите на елементите използвани в схемата.

Серията LM2576 представлява монолитна интегрална схема, която осигурява понижаване на изходното напрежение [2]. Този тип регулатори могат да бъдат натоварени с до 3A ток, като в изхода се получават фиксирани изходни напрежения от 1.23V, 3.3V, 5V, 9V, 12V, 15V. Предимствата на серията са, че изисква минимален брой външни елементи, прости са за използване и включват вътрешна балансирана и фиксирана честота на осцилатора. Стандартната серия от дросели, оптимизирана за използване с LM2576 е достъпна от различни производители, като тази особеност значително опростява проектирането.

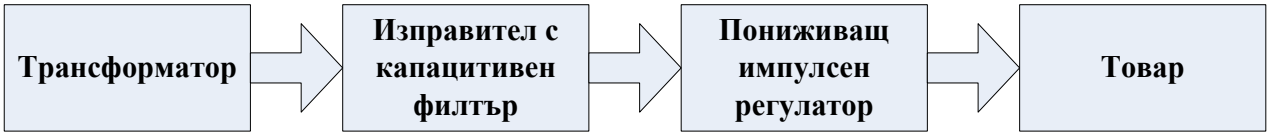
Понижаващите импулсни регулатори намират приложения в зарядни за всякакви батерии в диапазона от 1,23V ÷ 35V; високо ефективно преобразуване при приложение в автомобил [2].

Понижаващият импулсен регулатор ще бъде проектиран и разработен под формата на макет за нуждите на катедра: "Електроника", по дисциплината: "Токозахранващи устройства".

ИЗЛОЖЕНИЕ

Блокова и принципна схеми на понижаващ импулсен регулатор на напрежение

На фиг.1 е показана блоковата схема на понижаващия импулсен регулатор на напрежение.



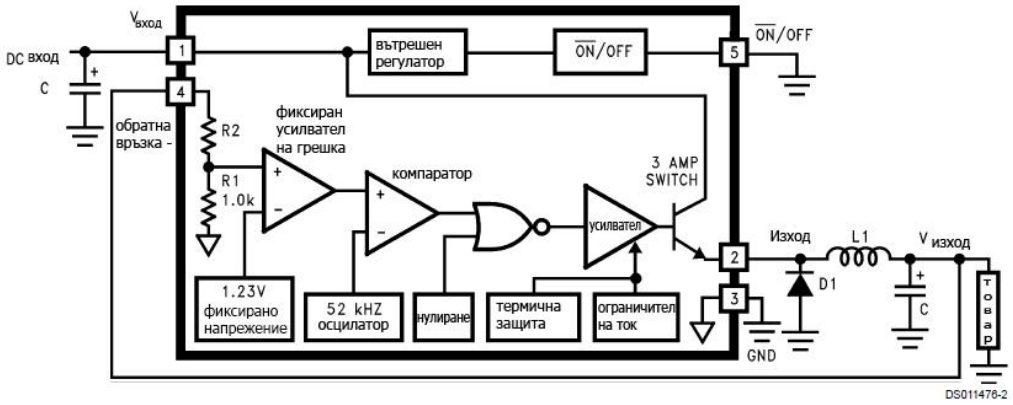
Фиг.1 Блокова схема на понижаващ импулсен регулатор

Тя се състои от блок трансформатор, чието основно предназначение е да преобразува параметрите на променливотоковата електрическа енергия - напрежение, честота, брой на фазите и да осигурява галванично разделяне на електрическите вериги.

Блок изправител с капацитивен филтър има за цел да преобразува променливотоковата енергия в постояннотокова, а чрез капацитивния филтър да се отстранят хармоничните съставляващи съпътстващи основния сигнал [1].

На фиг. 2 е показана структурната схема на LM2576 [2].

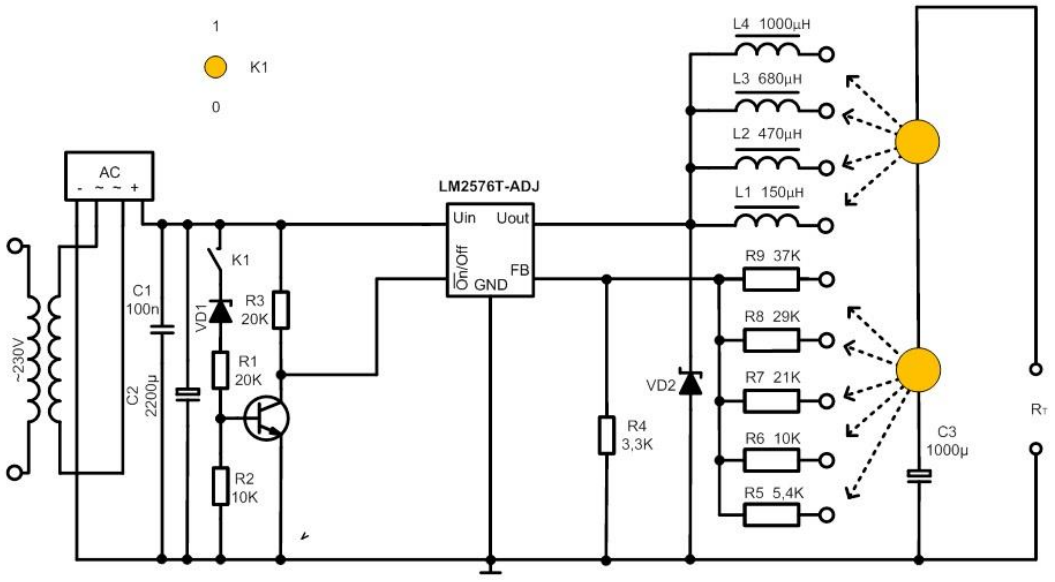
Както при всички токозахранващи устойства, проектирането на стабилизатора се явява много важна задача. Бързото превключване на тока, свързано с електрическата мрежа индуктира генерирано напрежение, което може да предизвика проблеми.



Фиг. 2 Структурна схема на понижаващ импулсен регулатор LM2576

На фиг.3 е показана принципна схема на понижаващ импулсен регулатор.

Максималната стойност на входното напрежение е 21V. Изходното напрежение може да бъде регулирано в границите от 3,3V до 15V, посредством галетен превключвател, който превключва резисторната матрица образувана от съпротивленията R4 - R5, R4 - R6, R4 - R7, R4 - R8, R4 - R9 (изчислени по зависимост 1 и 2). На база зависимост 3 и графика 4 е направен и подбора на индуктивностите за конкретните стойности на напреженията.



Фиг.3 Принципна електрическа схема на понижаващия импулсен регулатор

За да се получи фиксирано напрежение в изхода е необходимо [2]:

1. Оразмеряване на резисторите R1 и R2:

$$V_{OUT} = V_{REF}\left(1+\frac{R_2}{R_1}\right) \quad (1)$$

$$R_2 = R_1\left(\frac{V_{OUT}}{V_{REF}}-1\right) \quad (2)$$

където: V_{REF}=1,23V, R1 между 1k и 5k

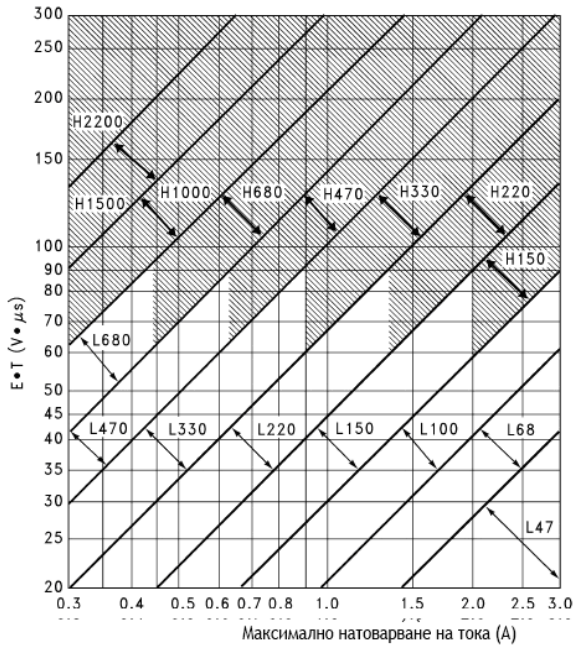
2. Избор на индуктивност (L1) [2]:

Избраната индуктивност трябва да бъде предназначен за работа с LM2576 с честота на превключване 52kHz и за ток 1,15 x Iтовар.

E.T (V.μs) от формулата следва:

$$E.T = (V_{IN}-V_{OUT})\frac{V_{OUT}}{V_{IN}}.\frac{1000}{F(kHz)}, V.\mu s \quad (3)$$

Получената стойност за E.T ще съвпадне с номера на E.T от вертикалната ос от фиг.4. От хоризонталната ос се избира максималното натоварване на тока. Определя се мястото на пресичане от стойността на тока и E.T и се записва номера на индуктивността.



Фиг.4 Определяне стойността на индуктивността L1

Пример:

Пресмятане E.T (V.μs)

$$E.T = (V_{IN}-V_{OUT})\frac{V_{OUT}}{V_{IN}}.\frac{1000}{F(kHz)} = E.T = (25-10)\frac{10}{25}.\frac{1000}{52} = 115, V.\mu s \quad (4)$$

E.T = 115 V.μs

Iтовар (Max) = 3A

Определяне на индуктивността = H150

Стойност на индуктора = 150μH

3. Избор на изходния кондензатор (Cout) [2]:

За осигуряване стабилна работа на регулатора е необходимо кондензаторът да отговаря на следните условия:

$$C_{OUT} \geq 13,300 \frac{V_{IN}(Max)}{V_{OUT}.L(\mu H)}, \mu F \quad (5)$$

Зависимост 5 дава стойности на кондензатора между 10μF и 2200μF, които ще задоволят изискванията към веригата за стабилна работа. Напрежението върху кондензатора трябва да е поне 1.5 пъти по-голям от изходното напрежение. За 10V регулатор, се препоръчва най-малко 15V или повече.

4. Диод на Шотки (D1) [2]:

Токът на улавящия диод трябва да бъде най-малко 1,2 пъти по-голям от максималния ток на натоварването. Също така, захранването трябва да издържа на постоянно отдадената мощност, накратко диода трябва да има текуща мощност равна на тока от интегралната схема. Обратното напрежение на диода, трябва да бъде най-малко 1,25 пъти от максималното входно напрежение.

Пример:

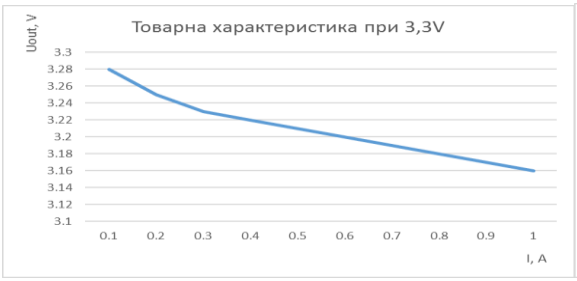
За ток 3A по препоръка на фирмата производител е посочено да се използва 30V, 31DQ03 Шотки диод, или аналог с подобни параметри.

5. Входен кондензатор (C_{IN}) [2]:

Необходим е алуминиев или танталов електролитен шунтиращ кондензатор, разположен в близост до регулатора за постигането на стабилна работа.

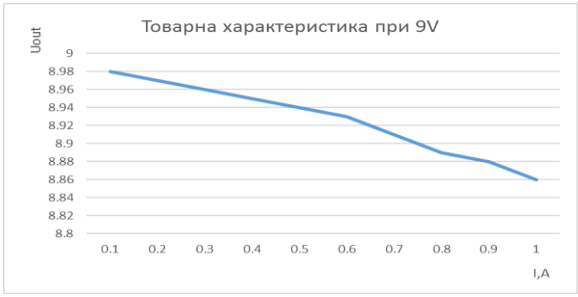
Резултати от проведени експериментални изследвания

Въз основа на проектирането и физическа реализация на импулсния понижаващ регулатор са снети изходните ток и напрежение и са построени товарни характеристики за изходните напрежения: 3,3, 5V, 9V, 12V и 15V, които са показани на фиг. 6а, б, в, г, д.

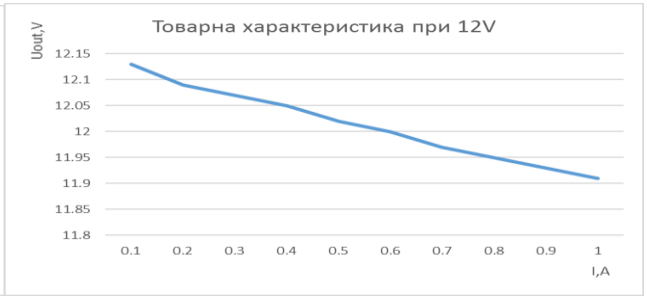


а)

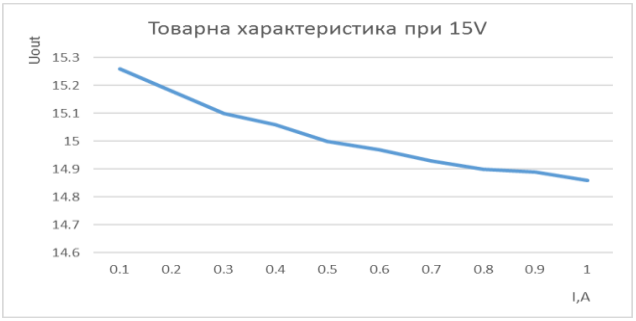
б)



в)



г)



д)

Фиг.6 Товарни характеристики на понижаващ импулсен регулатор

От получените товарни характеристики може да се констатира, че при промяна на товарния ток от 0,1A до 1A, най-малко изменение на постоянното напрежение е получено при 3,3V, а най-голямо при 15V.

ЗАКЛЮЧЕНИЕ

Разработеният понижаващ импулсен регулатор притежава добри изходни параметри, висока надеждност и ниска цена. Тези факти доказват приложимостта му както в лабораторни, така и в промишлени условия.

Разработеното устройство е лесно реализируемо, като поддръжката и ремонтът му са бързи и евтини, което е основно предимство на масовия пазар.

Разработеният макет, ще намери приложение в лабораторни условия по дисциплината „Токозахранващи устройства“ към катедра „Електроника“.

ЛИТЕРАТУРА

[1] Стефанов Н., „Токозахранващи устройства“, Техника, С., 2007г.
[2] https://www.onsemi.com/pub/Collaterual/SMPSRM-D.PDF - 14.03.2017г.
[3] Marty Brown, Power supply handbook – http://archieve.org/stream/Power_supply_Cookbook_2nd_Edition_By_Marty_Brown_Newnes_2001_278pp#page/n9/mode/2up, - 14.03.2017г.

За контакти:

инж. Димитър Йорданов, магистър в Катедра “Електроника”, Русенски университет “Ангел Кънчев” yordanov_93@abv.bg

гл. ас. д-р Снежинка Захариева, Катедра “Електроника”, Русенски университет “Ангел Кънчев”, тел.: 082-888 382, e-mail: szaharieva@uni-ruse.bg

Анализ на товаровите графици на електроенергийната система на България. Перспективи за развитие.

автор: Айхан Орхан Асан
научен ръководител: доц. д-р Вяра Русева

Analysis of the load profile of Bulgaria's electro energetic system. Development perspective.: *In the article an analysis of the structure of the production capacities in Bulgaria has been made. An overview of the percentage between the traditional electric energy and the one obtained through renewable energy sources in the countries of the Balkan peninsula is presented. The annual production and consumption of the electric energy for a period of 9 years has been analyzed. On the basis of these analyses are exposed the possible directions in which the electro energetic system of our country can develop.*

Key words: *electro energetic system, analysis, perspective.*

ВЪВЕДЕНИЕ

Електроенергетиката в България се промени през последното десетилетие както по отношение на структурата на отрасъла, така и по отношение на собствеността.

Производството на електрическа енергия в България започва в края на 19 век. През 1895 г. е изградена първата топлоелектрическа централа (ТЕЦ) „Перник“ с мощност 50 kW, а малко след това през 1900 г. първата водноелектрическа централа (ВЕЦ) „Панчарево“ с мощност 3000 kW. До средата на 20 век са изградени множество малки ТЕЦ и ВЕЦ с обща мощност 111 MW. През 1939 г. те произвеждат 266 хил. kWh електрическа енергия, т.е. по 42 kWh/жител [1]. От тях с най-голяма инсталирана мощност е ТЕЦ „Курило“ с мощност 15 MW.

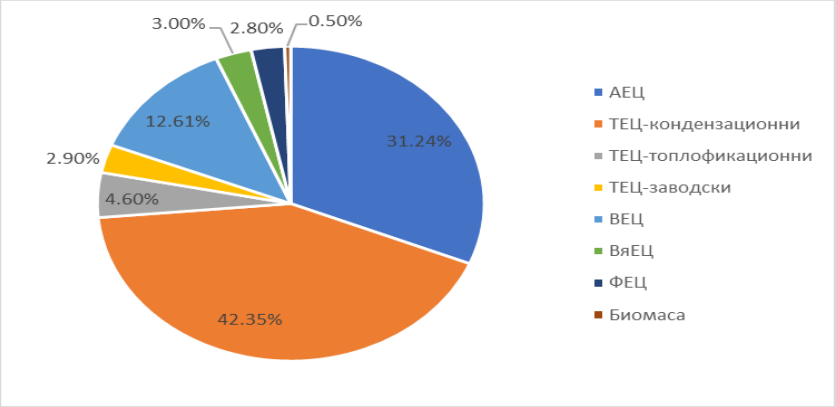
През 1982 г., т.е. 100 години по-късно в страната има в изправност 234 електроцентрали с общ капацитет 9 499 MW. От тях ТЕЦ-ове са с обща мощност 5 844 MW, ВЕЦ-ове са с 1 895 MW и вече е пусната в експлоатация и атомната ни централа (АЕЦ) – Козлодуй с мощност 1 760 MW.

В момента в структурата на производството на електрическа енергия доминират топлоелектрическите централи, които използват местни въглища. Това са централите в Марица изток и ТЕЦ „Бобов дол”. Общо от ТЕЦ се произвежда около 42 %, а от АЕЦ “Козлодуй” около 31 % от електрическата енергия в България. През последните няколко години бързо нарасна делът на вятърните и фотоволтаичните централи и към края на 2015 г. те произвеждат близо 3 % от електрическата енергия. При наличие на достатъчно валежи, съществуващите ВЕЦ осигуряват до 13 % от електрическата енергия (фиг. 1).

По отношение на собствеността, Законът за енергетиката и енергийната ефективност от 1997 г. позволи приватизация на електрическите централи с изключение на АЕЦ и структуроопределящите ВЕЦ.

В момента възникват проблеми при осигуряването на максималния товар на електроенергийната система поради ниските през зимата и много високите през лятото температури. Тъй като изграждането на нови енергийни мощности изисква време, се налага да се правят адекватни прогнози за увеличаването на производствените мощности.

Целта на работата е да се направи анализ на състоянието на електроенергийната система на България и да се анализират насоките за нейното развитие.



Фиг. 1. Процентно разпределение на произведената мощност по типове централи [2]

ИЗЛОЖЕНИЕ

Общата инсталирана мощност в електроенергийната система на България към 31.12.2015 г. е 12 790 MW, като разпределението по типове централи е показано в табл. 1 [2].

Таблица 1.
Инсталирани мощности и произведена електрическа енергия в България към края на 2015 г [2].

Видове електроцентрали	Произведена ел. енергия, GWh	Дял на произв. ел. енергия, %	Инсталирана мощност, MW	Дялна инсталираната мощност, %
АЕЦ	15 380	31,2	2 080	16,3
ТЕЦ – кондензационни	20 845	42,3	4 062	31,8
ТЕЦ – заводски	1 451	2,9	864	6,8
ТЕЦ- топлофикационни	2 277	4,6	780	6,1
ВЕЦ	6 213	12,6	3 198	25,0
Вятърни ЕЦ	1 468	3,0	701	5,5
Фотоволтаични ЕЦ	1 391	2,8	1 040	8,1
Биомаса	206	0,4	64	0,5
Общо	49 231	100,0	12 789	100,0

Като най-голяма инсталирана мощност имаме в ТЕЦ-кондензационни, следвани от ВЕЦ и АЕЦ. В общата мощност на електроенергийната система (ЕЕС) са включени фотоволтаични електроцентрали, заводски ТЕЦ, топлофикационни ТЕЦ, вятърни електроцентрали и централи работещи с биомаса.

С най-голям дял в произведената електрическа енергия отново са кондензационните ТЕЦ, а след тях е АЕЦ „Козлодуй". Макар и с по-малка инсталирана мощност от водноелектрическите централи, АЕЦ произвежда над два пъти повече електрическа енергия за страната. Това се дължи на факта, че атомната електроцентрала не зависи от климатичните промени. Тя се поддържа в технически изправно състояние и има възможността да произвежда електрическа енергия през цялата година на пълна мощност.

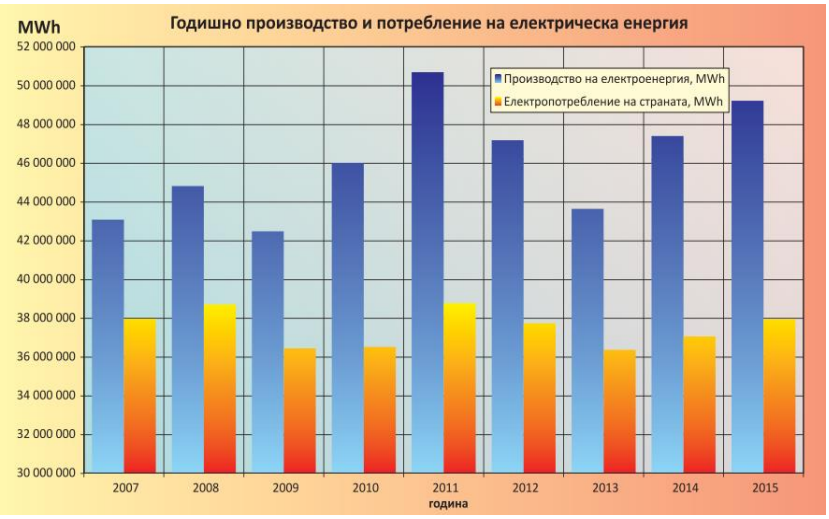
За сравнение в табл. 2 е показана произведената електрическа енергия от традиционни и възобновяеми енергийни източници в съседните на България страни.

Таблица 2.
Произведена електрическа енергия от традиционни и възобновяеми енергийни източници и внос-износ на електрическа енергия в страни от Балканския полуостров (месец юни 2016г.) [4].

2016г.	България	Румъния	Турция	Гърция
Общо произведена електрическа енергия, GWh	3 253	4 860	22 616	3 602
Невъзобновяеми източници, GWh	2 464 (~76%)	2 191 (~45%)	14 677 (~65%)	2 765 (~77%)
Възобновяеми източници, GWh	789 (~24%)	2 669 (~55%)	7 939 (~35%)	837 (~23%)
Внос на електрическа енергия, GWh	212	64	456	839
Износ на електрическа енергия, GWh	985	627	22	28
Потребление, GWh	2 463	4 258	23 050	4 413

От табл. 2 се вижда, че в съседните на България държави има значително по-голям добив на електрическа енергия от възобновяеми източници, като в Румъния тя достига над половината от общото производство. Това може да доведе до проблеми за нашата страна, тъй като през декември 2015г. в гр. Париж, България подписва споразумение, в което участват още 194 държави и се задължават да прекратят работата на всички електроцентрали, които използват въглища до 2030г. Всичко това ще доведе до значителен спад на производствените електрически мощности в страната ни.

Днес, България успешно търгува с електрическа енергия, като нейният износ е значително по-голям от вноса на електрическа енергия. Това показва, че страната ни има една добре развита електроенергетика, която успява да покрие нуждите ни.

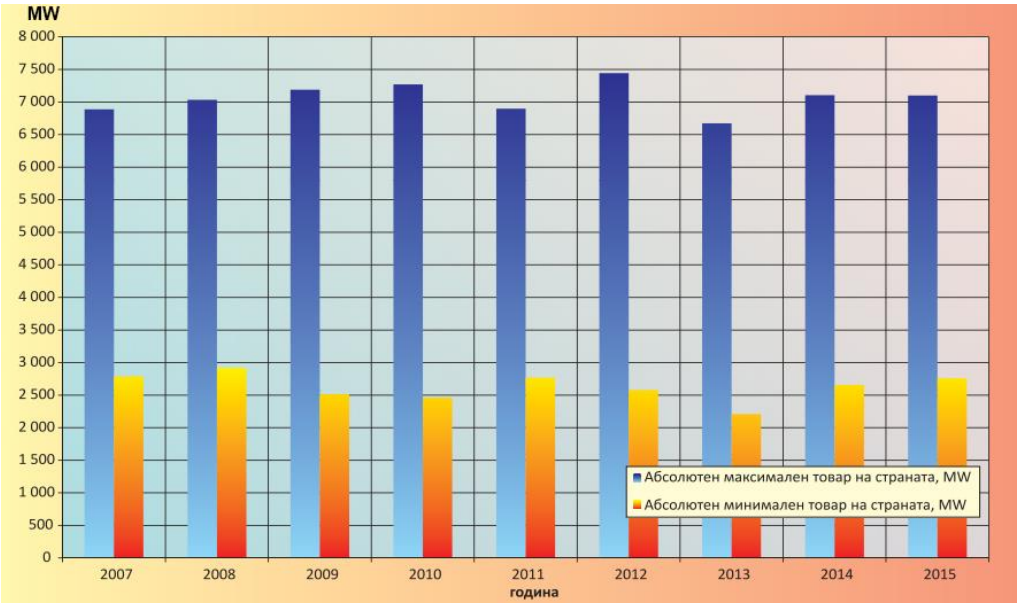


Фиг. 2. Годишно производство и потребление на електрическа енергия [3].

На фиг. 2 и фиг. 3 е разгледан девет годишен период от 2007г. до 2015г. за анализ на основните енергийни показатели на страната.

На фиг. 2 са показани абсолютният максимален и минимален товар. През 2013г. е отчетено най-ниското годишно електропотребление за разглеждания период. Това е един от показателите за икономическия застой на страната.

През 2012г. се отчита най-висока стойност на абсолютният максимален годишен товар. Това се дължи на ниските температури в деня, в който е регистриран този товар – 1 февруари, когато средната температура в страната е била -12,7^{o}C, което е с 13,4^{o}C под нормалната температура за този ден в годината. През 2017 г. имаше и по-ниски среднодневни температури на околната среда, което също доведе до високи стойности на максималните товари.



Фиг. 3. Абсолютен максимален и минимален товар на страната [3].

На фиг. 3 са представени годишното производство и потребление за разглеждания период. От нея става ясно, че през 2011г. се регистрира най-голямо годишно производство на електроенергия, като основна причина за това е рязкото нарастване на годишния износ на електроенергия (с 26%) спрямо 2010г., в резултат на възникнал по-траен недостиг в някои от съседните страни.

Развитие на електроенергийна система на България

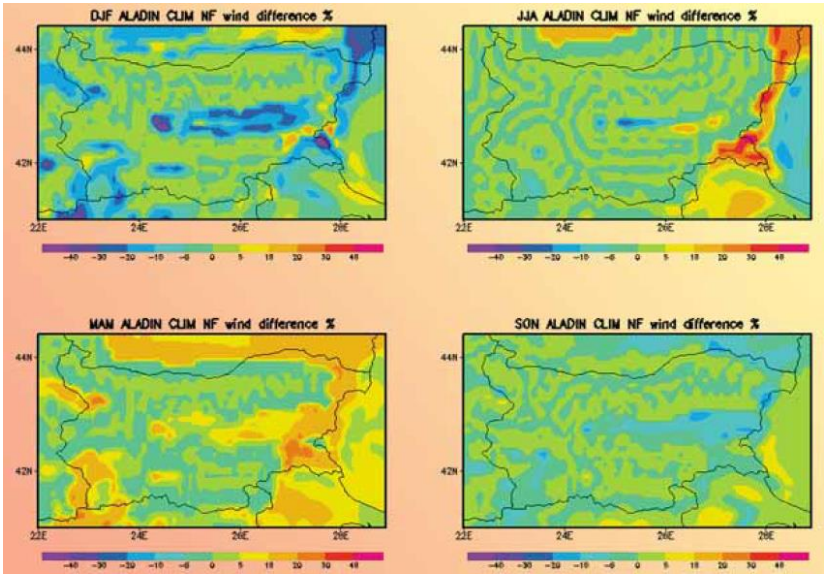
За задоволяване на бъдещото развитие на потреблението на електрическа енергия в страната и за заместване на изведените от експлоатация генериращи мощности, се налага необходимостта от изграждане на нови мощности. Насоките за развитието на електроенергетиката ни се разглежда в Енергийна стратегия на Република България до 2020 г. През последните години в България са разработени няколко стратегии за дългосрочно развитие на електроенергетиката. Недостатък е, че в тях липсва последователност, не се поставят достатъчно обосновани национални приоритети и не може достатъчно точно да се прогнозира развитието на индустрията, като най-голям енергиен потребител.

Анализ за развитие производството на електрическа енергия от възобновяеми източници

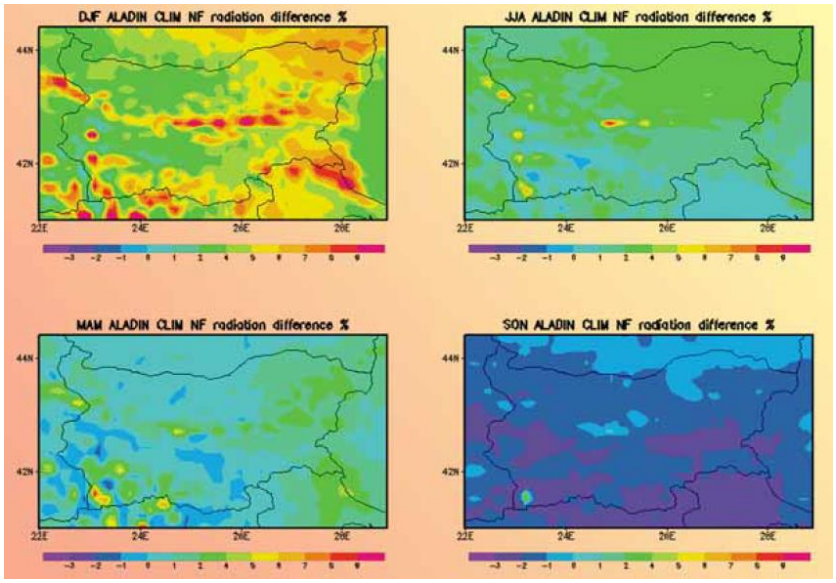
През последните години бяха изградени много вятърни и фотоволтаични централи. На фиг.4 са представени пространствени карти на очакваните промени (в проценти, %) на енергийния потенциал на вятъра до 2050г. по сезони. Изменението е в границите от -50% до +50%. Според направените прогнози става ясно, че най-голямо намаление на ветровия потенциал се очаква през зимата. Това е изразено най-добре в Централна и Югозападна България, както и в крайбрежната зона със стойности между 10 и 50%. Подобна тенденция се очаква и през есента, но с по-малки промени. През лятото очакваното изменение е от -20% до +50%, като най-голямото повишение се очаква да има в Югозападна България и крайбрежната зона с около от 30 до 50%.

При годишните изменения на ветровата енергия, най-голям ръст в енергийния потенциал може да се очаква в Югоизточна България до 14% и най-голям спад в централните части на страната с около 12%.

На фиг.5 са представени пространствени карти на очакваните промени (в проценти, %) в енергийния потенциал на слънчевата енергия до 2050г. по сезони. Изменението варира в границите от -4% до +10%.



Фиг. 4. Изменение в проценти за периода 2021 – 2050г. на енергийния потенциал на вятъра по сезони: зима (горе в ляво), пролет (долу в ляво), лято (горе в дясно), есен (долу в дясно) за територията на България [2].



Фиг. 5 Изменение в проценти за периода 2021 – 2050г. на енергийния потенциал на слънчевата радиация по сезони: зима (горе в ляво), пролет (долу в ляво), лято (горе в дясно), есен (долу в дясно) за територията на България [2].

През зимата промяната в потенциала на слънчевата енергия е положителна в цялата страна, като най-голямо увеличение на радиацията се наблюдава в Централна и Североизточна България (8-10%), както и в планинските райони. През лятото се очаква увеличение на радиацията както в Северна, така и в Южна България.

При годишните изменения на слънчевата радиация може да се очаква повишение в Североизточна България с 2 до 3,5% и на места в по-високите части на Стара планина и Пирин (до 6%). Тези оценки за разпределението на очакваните промени в енергийния потенциал на вятъра и слънчевата радиация вследствие на климатичните промени могат да послужат за правилно планиране на стратегии за развитие на ВЕИ за територията на България. В България има подходящи условия за изграждането на вятърни и фотоволтаични централи. Проблемът при тях е, че не може да се управлява работният им режим и те смущават устойчивата работа на

електроенергийната система. Не бива да се допуска изграждането на много такива нови мощности, докато не бъде решен сложният технически въпрос с акумулирането на произведената електрическа енергия. *По отношение на ВЕЦ* перспективно е изграждането на каскада „Горна Арда" и на каскада по река Места. Дискусионен е въпросът с изграждането на *нова мощност в АЕЦ*. Вложени са много средства в АЕЦ „Белене", но нейното строителство многократно е преразглеждано, липсват инфраструктура и присъединителни електропроводи и затова икономическата й ефективност не е достатъчно обоснована. На този етап по-перспективно е изграждането на още един блок в АЕЦ „Козлодуй".

По отношение на *преносната мрежа* се налага изграждане на някои нови електропроводи, главно за напрежение 110 kV, в районите с по-голямо икономическо развитие (Черноморското крайбрежие и София), както и в периферните райони на страната. Предстои изграждане на по още един електропровод 400 kV от подстанция „Марица-изток" до подстанция „Бургас" и от подстанция „Бургас" до подстанция „Варна". Сега протича, и е необходимо да продължи, обновяването на подстанциите чрез монтиране на съвременни защитни и комутационни апарати и цифрови релейни защити. Въздушните *разпределителни електрически мрежи*, особено тези за ниско напрежение, се нуждаят от непрекъсната поддръжка. Периодично се обновяват апаратите за защита и средствата за измерване. Необходимо е да се контролира натоварването по подстанции, трафопостове и участъци на мрежата, и при необходимост, да се проектират и изграждат нови елементи.

ЗАКЛЮЧЕНИЕ

От направения анализ на товаровите графици на България се вижда, че абсолютния максимален товар на електроенергийната система надхвърля 7000 MW. Проектирането и изграждането на производствени мощности отнема значително време и се влагат големи капитални вложения. Нуждата от нови мощности ще нарасне с подписването на споразумението за прекратяване на работата на всички електроцентрали, които използват въглища до 2030г.

За да не се окаже, че страната ни е принудена да закупува част необходимата ни електрическа енергия в статията са представени няколко възможности за развитието на електропроизводствените мощности, на преносната и разпределителната мрежи. Разгледани са пространствени карти на България за очакваните промени на енергийния потенциал на вятъра и слънчевата радиация до 2050г., които могат да се използват при проектирането и изграждането на електрически централи, произвеждащи електрическа енергия от ВЕИ.

ЛИТЕРАТУРА

[1] Манчев Б., И. Йотов, Т. Осиковски, Г. Денков, П. Петров, Д. Прокопиев. Електроенергетиката на България. Тангра ТанНакРа ИК, София, 2015, стр. 799
[2] Списание „Енергетика", брой м. ноември – декември, 2016г.
[3] Списание „Енергетика", брой м. януари – февруари, 2017г.
[4] http://www.entsoe.eu - European Network of Transmission System Operators for Electricity

За контакти:

Доц. д-р инж. Вяра Събова Русева, Катедра „Електроснабдяване и електрообзавеждане", Русенски университет „Ангел Кънчев", тел.: 0882 123 300, e-mail: vruseva@uni-ruse.bg

Айхан Орхан Асан, студент, Катедра „Електроснабдяване и електрообзавеждане", Русенски университет „Ангел Кънчев", тел.: 089 362 5272, e-mail: ayhan452@gmail.com

Електрически пътнически транспортни средства: технически характеристики и енергийна ефективност

автор: Радослав Ивов Иванов
научен ръководител: доц. д-р инж. Константин Коев

Electrical passenger transport vehicles: technical characteristics and energy efficiency. *Classifications and characteristics of electrical passenger transport vehicles are presented. Some technical advantages and disadvantages of the electrical vehicles are considered. The energy efficiency of the recent electrical vehicles is presented and analyzed.*

Key words: *electrical passenger transport vehicles, technical characteristics, energy efficiency.*

ВЪВЕДЕНИЕ

Транспортните средства, задвижвани чрез електрическа енергия, са особено актуални, поради основните си предимства - екологична безопасност и ниско ниво на шумова емисия [15].

Първи опити за създаване на електрически транспортни средства са правени в началните три десетилетия на XIX в. Тогава са разработени първите въртящи се електрически машини [8].

Електрическите транспортни средства се задвижват от електрическа енергия, която се преобразува в механична от тяговите двигатели или от неподвижни електромагнитни системи. Съвременното развитие на техниката позволява различните транспортни средства да се задвижват с електрическа енергия – железопътни релсови (влакове, трамваи, метро), автомобилни (пътнически и товарни, подемно-транспортни, строителни и селскостопански машини), някои верижни машини (военни, селскостопански), водни и въздушни транспортни средства [7].

Всички те се характеризират с различни конструктивни особености, технически параметри и ефективност на използване на консумираната енергия.

Целта на доклада е да се сравнят технически параметри на различни видове електрически пътнически транспортни средства и да се анализира енергийната им ефективност.

ИЗЛОЖЕНИЕ

Класификация на електрическите транспортни средства

Транспортните средства, задвижвани с електрическа енергия, са два вида, в зависимост от местоположението на захранващия източник – автономни и неавтономни. Първият вид транспортират източника на енергия, т.е. той е част от тях, а вторият вид – получават енергия от външен за тях източник. Основните представители на автономните електрически пътнически транспортни средства са леките автомобили (частни и за обществен транспорт - таксиметрови) и автобусите. Неавтономните електрически транспортни средства се движат в градовете и извън тях. Представители на първата група са метро (подземно градско релсово средство), тролейбуси, трамваи, а извънградски - релсови влакове (IEC – intercity express – междуградски експрес), включително и задвижвани с електромагнитни полета (MAGLEV (магнитна левитация над нерелсово трасе), Transrapid – магнитна левитация над единична релса).

Електротранспортните средства най-често се задвижват чрез въртящи се електрически машини или чрез взаимодействието на електромагнитни полета. Конструкцията и принципите на действие на тези задвижващи системи са представени в [2].

Електрическата енергия, захранваща транспортните средства, може да бъде с постоянни или с променливи параметри (ток, напрежение). Много често в транспортните средства (автономни и неавтономни) се използват уредби, чрез които електрическата енергия се преобразува в подходящия вид за задвижващата система. Автономните и неавтономните транспортни средства използват различни технологии и технически системи за преобразуване и производство на електрическа енергия, включително и от възобновяеми енергийни източници.

Пътната инфраструктура, използвана от електротранспортните средства, е показател по който те могат да бъдат класифицирани на релсови и безрелсови. са Трамваи, метро, междуградски влакове са представители на първата група. Втората група обхваща средствата, които използват пътната мрежа на класическия автомобилен транспорт (леки автомобили, автобуси, тролейбуси), и някои специални трасета (за задвижване с електромагнитни полета).

Електрическите транспортни средства могат да бъдат управлявани пряко от водач или непряко (без водач) - чрез съвременни електронни и комуникационни системи. Представители на втората група са леки таксиметрови автомобили в Сингапур и някои високоскоростни междуградски средства (MAGLEV) [11,13,16].

Технически характеристики на електрически пътнически транспортни средства

Факторите, които определят необходимата мощност за задвижването на електротранспортните средства, са: силите на съпротивление, които трябва да бъдат преодолявани по време на потегляне и на движение, механичните и електрическите загуби и скоростта на движение [1,10]. Електрическа енергия се използва не само за задвижване, а също и за осветление, сигнализация, климатизация, системи за навигация, управление и др. Следователно общата мощност на електротранспортните средства трябва да бъде по-голяма от необходимата за задвижването.

- Автономни електрически транспортни средства - леки автомобили (електромобили) и автобуси (електробуси)

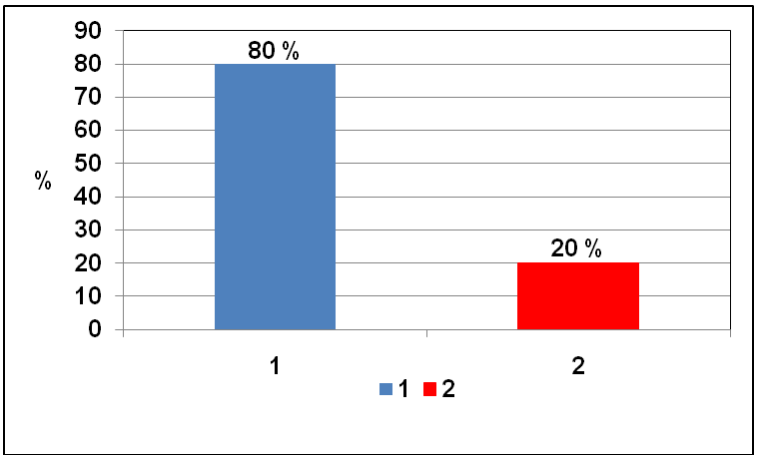
Характерни особености на тези транспортни средства са, че те не изискват специална пътна инфраструктура и се захранват от собствен източник на електрическа енергия, който е част от обзавеждането им. Основни недостатъци са ограничената им мощност и необходимост от изграждане на технически системи (електростанции) за зареждането им с електрическа енергия.

Мощността на автономните електротранспортни средства зависи от характеристиките на използваните източници на електрическа енергия (акумулатори, суперкондензатори, горивни клетки и др.). Някои по-важни характеристики са: енергийна плътност, kW/kg, електрически капацитет, Ah, големина на токовете и продължителност за зареждане и разреждане, брой цикли разряд-заряд, дълбочина на разряда, устойчивост на екстремни условия (високи и ниски температури и др.).

Енергийната плътност и електрическият капацитет на източниците определят максималната собствена маса на транспортните средства, масата на полезния товар, скоростта и продължителността на движение с едно зареждане. Съществени фактори при движението на автономните транспортни средства, които влияят върху разхода на електрическа енергия, са режимът на управление (субективното поведение на водача или електронните системи при управление без водач, които определят скоростта на движение), и променящите се пътни и атмосферни условия. Последните две условия не могат да бъдат управлявани. Следователно, за да се постигне най-малък разход на енергия (най-голяма енергийна ефективност) от електротранспортните средства, при конкретните условия на движение, е подходящо целенасочено да се въздейства (управление) върху режима на управление.

Електрическите транспортни средства, които използват пътна инфраструктура (шосета), усвояват средно около 80 % от консумираната електрическа енергия. Тази

стойност е 4 пъти по-голяма, в сравнение с транспортните средства, задвижвани от двигатели с вътрешно горене (ДВГ) - фиг.1. При тях енергията на горивото (бензин и дизел) се усвоява само около 20 %, защото останалата част се преобразува в неизползваема топлина [5].



Фиг.1. Общ коефициент на полезно действие (к.п.д.) на транспортни средства, които използват шосейната пътна мрежа: 1 – електрически; 2 – с двигатели с вътрешно горене.

Основните причини за по-голямата енергийна ефективност на електрическите транспортни средства са: голям коефициент на полезно действие (к.п.д.) на задвижващите електродвигатели - над 80%; енергия се консумира само при движение; задвижващите електродвигатели могат да преминат от двигателен в генераторен режим, при спиране и спускане по наклони. Произведената тогава електрическа енергия се връща в захранващия източник (рекуперация).

Важен показател за енергийната ефективност на електротранспортните средства е средната стойност на разхода на електрическа енергия за изминаване на 100 km, която за електромобилите обикновено е (10…23) kWh. Приблизително 20% от тази енергия не се използва ефективно (загуби) при зареждане на батериите [5].

Друга характеристика на електромобилите е времето за зареждане на акумулаторите. Производителите търсят непрекъснато възможности за намаляване на това време. Например литиево-йонни акумулатори с мощност (3…6) kW (230 V, 15 A) могат да бъдат напълно заредени за около (7…8) h при нормален режим на зареждане, и за (30…45) min - при бързо зареждане. Краткото време е особено важно за таксиметровите автомобили [6].

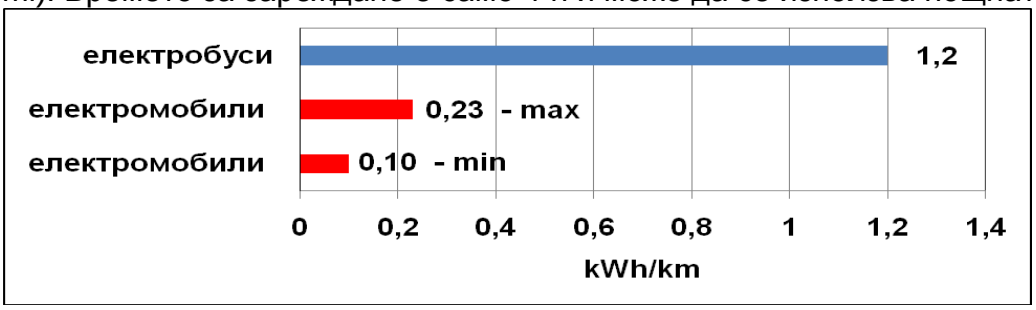
Електрическите автобуси се задвижват от електрически двигатели, захранвани от акумулатори или суперкондензатори, разположени в транспортното средство. Подобни решения се използват и в някои модели тролейбуси (захранвани от външна контактна мрежа), с цел спомагателен енергиен източник и за аварийни ситуации (при повреда в контактната мрежа).

Електробусите се използват почти само в градския транспорт, отколкото в извънградски линии. Основната причина е голямата им маса, която определя необходимостта от мощни електрически двигатели и акумулатори. В населените места скоростта на движение и дължината на маршрутите са ограничени. Тези условия позволяват, дори и при изискване за голяма мощност на транспортното средство (по-големи собствена маса и маса на полезния товар), да се използват електробуси, които да изминават определен маршрут с едно зареждане, при наличие на необходимата инфраструктура за зареждане с електрическа енергия.

Електробусите, също като електромобилите, могат да използват режим на рекуперация (при спиране или движение по наклонени участъци), за повишаване на енергийната ефективност. Средна стойност на разхода на електрическа енергия за изминаване на 1 km от електробусите е около 1,2 kWh. Тази стойност е 10 и повече пъти по-голяма от разхода при електромобилите – (0,10..0,23) kWh/km (фиг.2) [5].

Последно поколение електробуси на световния лидер BYD (Китай), се използват в Лондон (фиг.3). Те са двуетажни, с 54 седящи и 27 стоящи места (общо 81). Захранващите батерии са желязо-фосфатни,с мощност 345 kW, и с едно зареждане,

в градски условия, осигуряват изминаване на маршрут с дължина до 307,5 km (190 ml). Времето за зареждане е само 4 h и може да се използва нощната по-евтина електроенергия [4]. Средната стойност на разхода на електрическа енергия е 1,12 kWh/km.



Фиг.2. Специфичен разход на електрическа енергия на автономни електрически транспортни средства.

Електробусите, в зависимост от изградената техническа инфраструктура, при престой на спирки или в гараж, могат да зареждат акумулаторите си чрез пантографи от контактна система, разположена над транспортното средство, или по индуктивен начин. Ако се използват суперкондензатори вместо акумулатори, времето за зареждане с електрическа енергия е значително по-малко – **няколко min**. Това е важно предимство, но броят цикли заряд-разряд на кондензаторите е по-малък.

Фиг.3. Електробус BYD по улиците на Лондон.

Електробусите и електромобилите общо се характеризират с по-голяма скорост на маневриране и по-кратко време за ускорение, освен липса на вредни емисии и шум, в сравнение с транспортните средства с двигатели с вътрешно горене. Основен недостатък на електробусите е по-малката дължина на изминавания маршрут, в сравнение с автобусите с ДВГ [3].

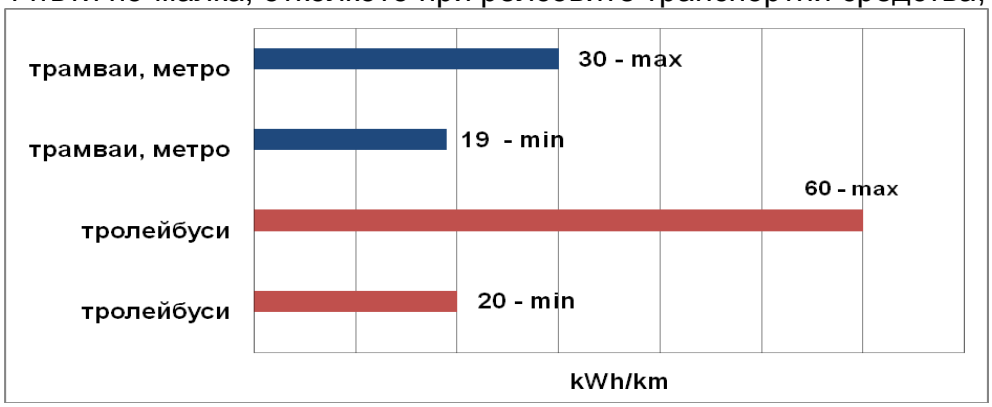
- Неавтономни електрически транспортни средства – релсови и безрелсови

Първата група са градски (метро, трамвай) и междуградски (ICE), а безрелсовите – градски (тролейбус) и извънградски (MAGLEV, Transrapid). Всички тези транспортни средства, за разлика от автономните, изискват специална пътна инфраструктура (с изключение на тролейбусите) и се захранват от външен източник на електрическа енергия – контактна мрежа (при релсовите транспортни средства), контактна релса (при метро) и системи за магнитна левитация (MAGLEV, Transrapid). Тези особености позволяват транспортните средства да бъдат достатъчно мощни и да транспортират голяма маса с висока скорост. Мощността на неавтономните електротранспортни средства се определя от мощността на външния захранващ източник, а тя зависи от характеристиките на транспортните средства и от условията на трасето и движението.

Основен недостатък е необходимостта от изграждане на сложна техническа инфраструктура за захранване с електрическа енергия.

Предимствата на неавтономните релсови транспортни средства, в сравнение с тези, които се движат по шосейната пътна мрежа (тролейбуси), са: по-малко съпротивление на търкаляне при движение на стоманените колела по релсите; по-добри аеродинамични характеристики на подвижния състав; по-малко препятствия (особено при метрото). По тези причини релсовите транспортни средства се характеризират с по-добра енергийна ефективност (фиг.4) и могат да се движат с по-високи скорости [12]. Сравнението между ресловите и безрелсовите извънградски неавтономни транспортни средства показва, че втората група се характеризират със сериозни предимства. Те са: липса на триене между транспортното средство и пътя; малки амплитуди на вибрации и шум – шумът е по-

малък с 30 %; малки радиуси на кривините на пътя – минималната стойност 75 m е 4 пъти по-малка, отколкото при релсовите транспортни средства; преодоляване на 10 % наклони на трасето при изкачване, което е 2,5 пъти по-голяма стойност, отколкото при релсовите [14].



Фиг.4. Специфичен разход на електрическа енергия на неавтономни електрически транспортни средства.

Принципът на движение на безрелсовите електротранспортни средства (MAGLEV, Transrapid), основан на взаимодействието между електромагнитни полета, е причина за отсъствието на триене между транспортното средство и пътя. Това е важно условие за движение с много високи скорости (над 400 km/h), при по-малки разходи за техническа експлоатация.

Фиг.5. Безрелсов влак MAGLEV в Китай.

Извънградските безрелсови транспортни средства, освен с безспорните си предимства, се характеризират и с недостатъци, които ограничават приложението им.

Основният проблем е много високата цена на инфраструктурата - 43,6 млн. щатски долара за 1 km двупътно трасе, включително транспортните средства и гарите. Пътният участък се намира в Шанхай (Китай) и е с дължина 30 km (фиг.5) [9]. Друг недостатък е, че само при големи скорости енергийната ефективност е по-голяма, в сравнение с релсовите транспортни средства. Сериозен проблем е големият разход на енергия за преодоляване съпротивлението на въздушната среда, което е определящ фактор при движение с много високи скорости. Мощността на задвижващата система P е правопропорционална на линейната скорост на движение v, повдигната на 3-та степен, т.е. $P \sim v^3$. Голямата мощност се осигурява от силни магнитни полета, чието влияние върху пътниците и техническите системи трябва да бъде ограничено или напълно елиминирано.

ЗАКЛЮЧЕНИЕ

Изследването на техническите параметри и енергийната ефективност на електрическите пътнически транспортни средства показва, че:

- безрелсовите транспортни средства (MAGLEV) са най-ефективни при много високи скорости, но разходите за изграждане на техническите системи и пътна инфраструктура са най-големи;
- релсовите транспортни средства (градски и междуградски) са по-ефективни от тези, които се движат по шосейната пътна мрежа, поради по-малкото триене при търкаляне на колелата, но разходите за изграждане на инфраструктурата са значителни;
- с най-малки енергийни разходи се характеризират електромобилите и електробусите, при ограничени мощност и дължина на изминатия път с едно зареждане на източника на енергия. Неговите характеристики са много важен

фактор при определянето на енергийната ефективност на тези транспортни средства.

ЛИТЕРАТУРА

[1] Българанов Л., Електрически транспорт, Технически университет–София,1991,250 с.
[2] Дановски, П. Анализ на технически параметри на тягови електрически двигатели. В: Сборник докалди на студенстка научна сесия на Русенски университет "Ангел Кънчев", Русе, 2015, 29-34 с., ISBN ISSN 1311-3321.
[3] Battery electric bus, https://en.wikipedia.org/wiki/Battery_electric_bus
[4] BYD, http://www.byd.com/news/news-325.html
[5] Electric car, https://en.wikipedia.org/wiki/Electric_car
[6] Electric vehicle battery, https://en.wikipedia.org/wiki/Electric_vehicle_battery
[7] Harrop, P. Anatomy of Electric Vehicles by Land, Water and Air, www.IDTechEx.com
[8]History of the electric vehicle, http://en.wikipedia.org/wiki/History_of_the_electric_vehicle
[9] How the maglev train move forward,https://www.quora.com/How-the-maglev-train-move-forward
[10] Husain, I. Electric and hybrid vehicles: design fundamentals. CRC Press,2003,270 pp.
[11] Incheon Airport Maglev, https://en.wikipedia.org/wiki/Incheon_Airport_Maglev,
[12] Kay, D. et al. Public transport, IEA ETSAP - Technology Brief T10 – January 2011, www.etsap.org
[13] Linimo, https://en.wikipedia.org/wiki/Linimo
[14] Liu, Z. et al. Maglev Trains Key Underlying Technologies. Springer-Verlag Berlin Heidelberg 2015, 215pp.
[15] New Energy and Fuel, http://newenergyandfuel.com/
[16] Singapore's self-driving cars can now be hailed with a smartphone, http://www.theverge.com/2016/9/22/13019688/singapore-self-driving-car-nutonomy-grab-ride-hail-test

За контакти:

Радослав Ивов Иванов, студент III курс, специалност „Електроенергетика и електрообзавеждане", Русенски университет "Ангел Кънчев", e-mail: rado1595@abv.bg

доц. д-р инж. Константин Георгиев Коев, катедра "Електроснабдяване и електрообзавеждане", Русенски университет "Ангел Кънчев", тел.: 082-888 201, e-mail: kkoev@uni-ruse.bg

Българска независима енергийна борса - развитие на електроенергийния пазар в България

автор: Кристиян Владимиров Николов
научен ръководител: доц. д-р Вяра Събова Русева

Independent Bulgarian energy exchange – development of electricity market in Bulgaria: *The price of electric power traded on Independent Bulgarian energy exchange IBEX is compared with other prices in markets like regulated market and free market. Also the price on IBEX is compared with other power exchanges like Nord Pool and EPEX Spot. It is shown how actually electrical energy is traded between participants and how it is physically purveyed.*

Key words: *Energy exchange, electric power price, market liberalization, power supply.*

ВЪВЕДЕНИЕ

Процесът по либерализиране на пазара на електрическа енергия в България започва през 2004 г. В действителност цената на електрическа енергия е пазарно понятие и трябва да носи известна печалба. Тя трябва да осигури разширеното възпроизводство на производствените и преносни мощности в електроенергийната система. Електроенергетиката е един от "естествените монополи". Затова във всички страни цената на електрическата енергия не се формира само от пазара, а косвено се регулира и от държавата, като се отчитат наличието на собствени енергийни източници, екологичното въздействие, социалните условия и др.

Към настоящия момент всеки потребител, производител и търговец може свободно да договаря цената на електрическа енергия и да избира своя доставчик [3]. За пълната либерализация на пазара, т. е. определяне цената по пазарен принцип се създава Българска независима енергийна борса (БНЕБ).

БНЕБ е създадена и оперира с платформата NORDPOOL, която се използва и от самата борса Nord Pool. Това е една от няколкото платформи за опериране на основни енергийни борси в Европа, като EPEXSPOT, GME, OMIE и целта на създаването им е постигане на общ електроенергиен пазар в Европейския съюз.

Предпоставките за избора на NORDPOOL като партньор са: това е най-големият борсов оператор в Европа, с най-голям опит – над 20 години и е доставчик с икономически най-изгодната оферта за опериране на пазара в България.

NORDPOOL е на-големият борсов оператор не само в Европа, но и в света, като за 2014 г., количеството на търгуваната от него електрическа енергия достига 501 TWh и има пазарен дял над 85%. На пазарите на NORDPOOL търгуват 370 компании (производители, доставчици, търговци, големи крайни потребители), а основните държави, в които оперира са Норвегия, Швеция, Финландия, Дания, Литва, Латвия и Естония. NORDPOOL е създадена с решение на Норвежкото правителство за дерегулация на пазара на електроенергия в Норвегия през 1991 г. [7,1].

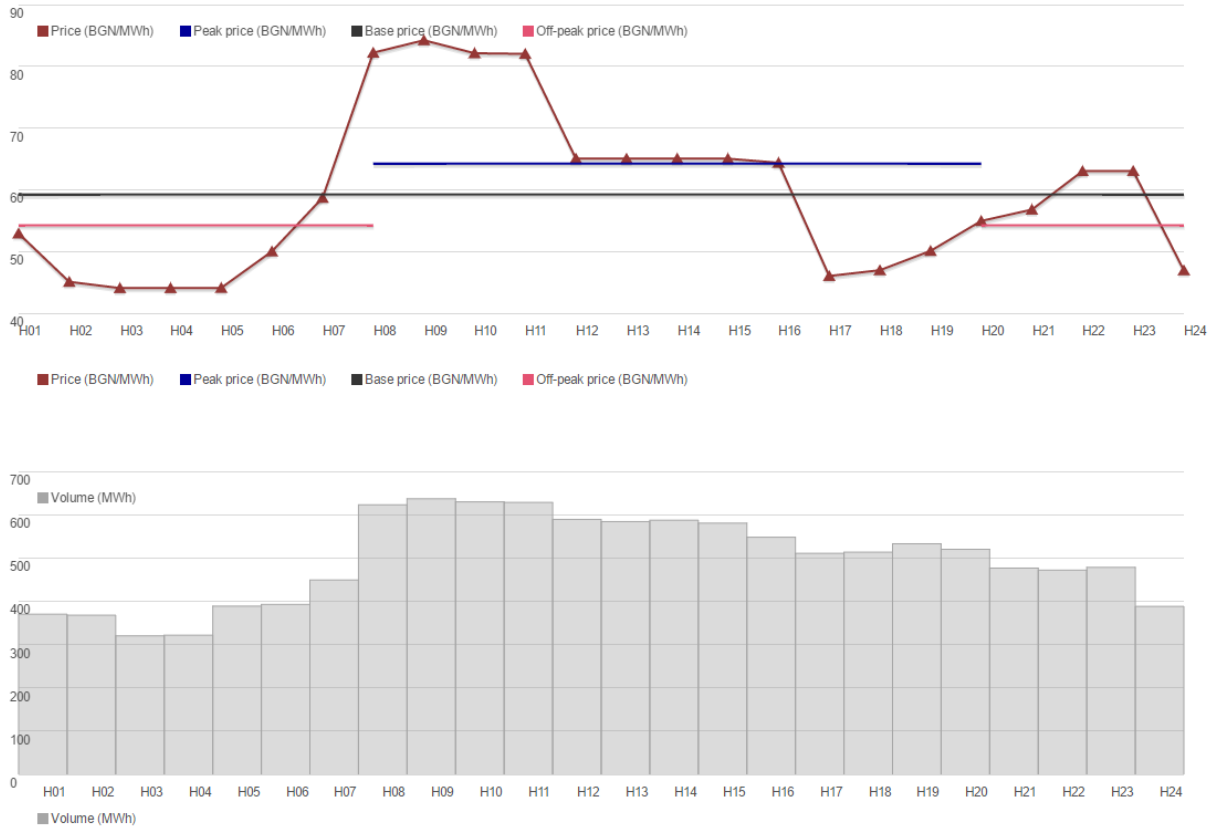
С оглед на партньорството на БНЕБ и NORDPOOL, и стремежът за постигане на общ пазар за свободно търгуване на електрическа енергия в Европа, целта на тази разработка е да се представи какви са развитието и перспективите на електроенергийния пазар в България, чрез създаване на БНЕБ.

ИЗЛОЖЕНИЕ

Българска независима енергийна борса започва своята дейност на 1 януари 2016 г. Както всяка друга борса, това е място, където се купува и/или продава електрическа енергия. Участници могат да бъдат всички производители, потребители и търговци, които изпълняват условията за участие на пазара на

електрическа енергия в страната [2]. Целта за създаването на БНЕБ е да се либерализира електроенергийният пазар, да се даде възможност на потребителите за свободен избор на доставчик на електроенергия, определяне цената на електрическата енергия по пазарен принцип, повишаване на ефективността, конкурентни цени и др.

Начинът на работа на борсата е представен на фиг. 1, където е показано изменението на цената на електрическата енергия в лв/MWh [6]. Това е търговията, която се осъществява за ден напред. Всички участници трябва да представят исканите от тях количества енергия по часово до 12:00 часа на предходния ден. За конкретния случай, графиката показана на фиг. 1 е снета на 04.04.17 г. и показва как изглеждат цените и обемите за 05.04.17 г.



Фиг. 1. Изменение на цената на електрическата енергия в зависимост от заявените количества за търсене и предлагане, за период от 24 часа за 05.04.17г.

В горната част на графиката е изобразена кривата на изменение на цената, а в долната част стълбовидното изменение на заявените търгувани количества за всеки час. Относно цената има и допълнителна информация като базова цена, цена при максимален товар и цена при минимален товар. Тези цени са различни за всяко денонощие.

От изменението на кривата на цената може да се установи, че нейната стойност е най-ниска, приблизително 44 лв/MWh, в периода с най-малко търсене, между часовете 1:00...5:00 означени на фиг. 1 като H01...H05. През този период търгуваните количества са малко над 300 MWh. С нарастване на количествата енергия до малко над 600 MWh в периода H07...H11 цената също нараства и тя достига своя максимум при стойност 84 лв/MWh. Забелязва се, че при двойно покачване на търсенето от 300 MWh до 600 MWh, цената също претърпява приблизително двойно увеличение от 44 лв/MWh до 84 лв/MWh. Тази зависимост не винаги е валидна и това може да се установи в часовете H17 и H18, където цената

спада до малко под 50 лв/MWh въпреки, че количествата енергия намаляват до малко над 500 MWh.

За да е пълноценен анализът на въздействието на БНЕБ върху пазара на електрическа енергия в работата е направено сравнение на цените формирани на борсата и на останалия пазар, също така и цените формирани на други основни борси, примерно NORDPOOL и EPEX Spot.

На фиг. 2 са представени цени на електрическата енергия в България според [8] съответно а) за индустрията и б) за домакинствата в периода юли – декември 2016 г.

Групи индустриални крайни потребители	Годишно потребление на електрическа енергия в хил. кВтч		Цени в лева / кВтч		
	Минимално	Максимално	Без всякакви данъци, такси и ДДС	Без ДДС и други възстановими данъци и такси	С включени всички данъци, такси и ДДС
			(Ниво 1)	(Ниво 2)	(Ниво 3)
Група - И1	<20		0.212	0.214	0.256
Група - И2	20	< 500	0.183	0.185	0.222
Група - И3	500	<2 000	0.152	0.154	0.185
Група - И4	2 000	<20 000	0.135	0.137	0.164
Група - И5	20 000	<70 000	0.120	0.122	0.146
Група - И6	70 000	≤150 000	0.110	0.112	0.135
Група - И7	> 150 000		0.111	0.113	0.135

Фиг. 2. а) Цени на електрическата енергия за индустрията за периода юли – декември 2016 г.

Групи домакинства крайни потребители	Годишно потребление на електрическа енергия в кВтч		Цени в лева / кВтч		
	Минимално	Максимално	Без всякакви данъци, такси и ДДС	Без ДДС	С включени всички данъци, такси и ДДС
			(Ниво 1)	(Ниво 2)	(Ниво 3)
Група - Д1	<1 000		0.158	0.158	0.189
Група - Д2	1 000	<2 500	0.155	0.155	0.186
Група - Д3	2 500	<5 000	0.153	0.153	0.183
Група - Д4	5 000	<15 000	0.153	0.153	0.183
Група - Д5	≥15 000		0.151	0.151	0.181

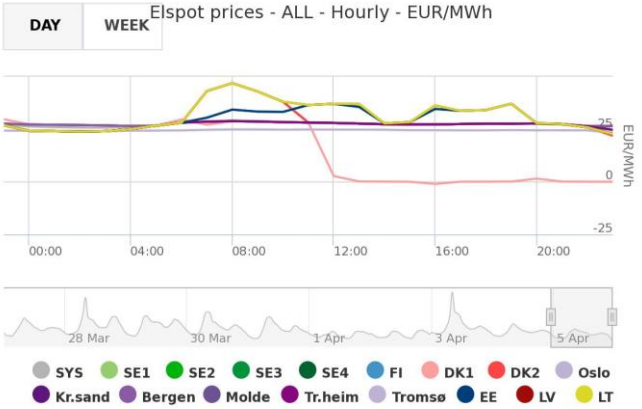
Фиг. 2. б) Цени на електрическата енергия за домакинствата за периода юли – декември 2016 г.

Цените на електрическата енергия варират в широки граници в зависимост от количеството потребена енергия, а също така и от типа на потребителя. Пример за това е потребител, който спада към група – И1 (от фиг. 2 а)) с годишно потребление на електрическа енергия по-малко от 20 хил. kWh. За него крайната цена на енергията е 0,256 лв/kWh, т.е. 256 лв/MWh. Цената на енергията значително намалява, ако потребителят спада към група – И7 с годишно потребление на електрическа енергия над 150 000 хил. kWh. За съответния потребител цената е 0,135 лева/kWh или 135 лв/MWh. По същия начин се тълкуват и цените на електрическата енергия за домакинствата показани на фиг. 2 б), като най-висока е цената 0,189 лв/kWh или 189 лв/MWh за група – Д1 с годишно потребление по-малко от 1000 kWh.

Цените на регулирания пазар и свободно договорените цени значително се различават от цените формирани вследствие търговията на БНЕБ. Най-ниската цена на електрическата енергия, която е определена на регулирания пазар е 135 лв/MWh с включени всички данъци, такси и ДДС и тя важи за потребител от група – И7. Дори при най-високата цена от търговията на БНЕБ, която е на 05.04.17 г. в 09:00 часа (приблизително 84 лв/MWh), разликата е голяма. Тази разлика значително се увеличава, ако се разгледа цената, която заплаща потребител на регулирания пазар от група – И1 – 256 лв/MWh от фиг. 2 а) и цената на борсата в

5:00 часа – 44 лв/MWh от фиг. 1. Разликата е приблизително 5,8 пъти. Именно това е най-силният аргумент за ползите от създаването на БНЕБ. Формирането на цена, която е в пъти по-ниска от цената на регулирания и свободния пазар.

Тъй като на БНЕБ могат да търгуват участници от целия Европейски съюз на фиг. 3 и фиг. 4 са представени цени на електрическата енергия за сравнение на борсите съответно NORDPOOL и EPEX Spot.

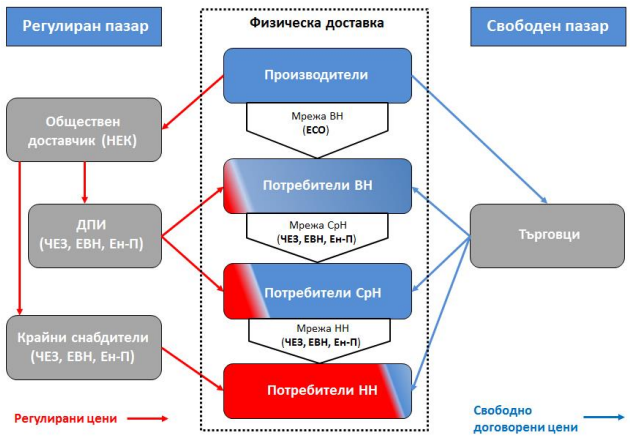


Фиг. 3. Цени на ел. енергия формирани на енергийна борса NORDPOOL за 24 часа

Фиг. 4. Цени на ел. енергия формирани на енергийна борса EPEX Spot за 24 часа

От графиката показана на фиг. 4 може да се констатира, че се търгуват огромни количества енергия (в GWh) на всеки час. Въпреки, че не са показани обемите на електрическата енергия на NORDPOOL, те са от същия порядък (GWh). Но и на двете борси цената варира (25...50) евро/MWh, което е приблизително (50...100) лв/MWh, т. е. цените на NORDPOOL, EPEX Spot и БНЕБ се изменят сравнително в еднакви граници.

Електрическата енергия е вид стока, но тя трудно се съхранява и по-особеното е, че се потребява тогава, когато се произвежда. Поради тази причина при договарянето, сключването на сделка между различните участници на пазара и въобще търговията с електрическа енергия е икономически процес, но тя трябва и физически да се достави от производителите до потребителите. Този процес е показан на фиг. 5 [4].



Фиг. 5. Процес на търговия и доставяне на електрическа енергия в България

При свободно избиране на доставчик и определяне на цената, договарянето е в следния ред:

производители ► търговци ► потребители ниско напрежение (НН).

Физическата доставка, се извършва по следния ред:

производители ► мрежа високо напрежение (ВН) ► мрежа средно напрежение (СН) ► мрежа НН ► потребители НН.

Пълната схема на пътя, по който се осъществяват сделките на свободния и регулирания пазар и физическата доставка са показани на фиг. 5.

За да е възможно услугите на БНЕБ да са лесно достъпни е необходимо електроенергийната инфраструктура (ЕЕИ) да отговаря на определени изисквания, тъй като участниците са голям брой. Изискванията, на които трябва да отговаря ЕЕИ са: качество на доставяната електрическата енергия, надеждност на

електрозахранването на потребителите при осигуряване на оптимален режим на работа на електроенергийната и електроснабдителната система.

ЗАКЛЮЧЕНИЕ

Предимствата на Българска независима енергийна борса се изразяват при формирането на цената на електрическата енергия. Тя се образува по пазарен механизъм според търсенето и предлагането, т. е. няма как да се спекулира с нея. Показано е, че цената на електрическата енергия е значително по-ниска на БНЕБ, в сравнение с другите разгледани пазари в България. Реално предимство на БНЕБ е, че всеки потребител има право да участва в нея, независимо от това дали е индустриален потребител, домакинство, производител и дали е с голяма или малка годишна консумация.

Като недостатък на БНЕБ и въобще на енергийните борси може да се посочи непостоянната цена на електрическата енергия във времето, но разликите в цените на пазарите са големи и в България това трудно би се нарекло недостатък.

ЛИТЕРАТУРА

[1] Въвеждане на борсов пазар в България, София 29.09.2015 г., материали от работна среща
[2] Закон за енергетиката, обн. ДВ, бр. 107 от 09.12.2003 г.
[3] Правила за търговия с електрическа енергия, обн. ДВ, бр. 66 от 26 Юли 2013 г.
[4] http://ateb.bg/ - Асоциация на търговците на електроенергия в България
[5] https://www.epexspot.com/en/ - Енергийна борса EPEX Spot
[6] http://www.ibex.bg/bg/ - Българска независима енергийна борса
[7] http://www.nordpoolspot.com/About-us/History/ - Енергийна борса Nord Pool
[8] http://www.nsi.bg/bg/content/ - Национален статистически институт

За контакти:

Доц. д-р инж. Вяра Събова Русева, катедра Електроснабдяване и електрообзавеждане, Русенски университет „Ангел Кънчев“, тел.: 0882 123 300 , e-mail: vruseva@uni-ruse.bg

Кристиян Владимиров Николов, студент, катедра Електроснабдяване и електрообзавеждане, Русенски университет „Ангел Кънчев“, тел.: 0886 236 746, e-mail: krisko.nikolow@gmail.com

Анализ на особеностите на водноелектрическата централа Кърджали

автор: Слави Ненов Желязков
научен ръководител: доц. д-р Вяра Русева

Analysis of the peculiarities of the hydroelectric power plant Kardzhali: *The main share of the production of electricity from renewable energy sources is provided by hydropower plants (HPP) in Bulgaria. They are characterized by some features: a long period of design and construction, large initial investments and easier operation and service. The work reviews the development of hydropower in Bulgaria and details the construction of Kardzhali HPP. On this basis, the main directions for the further development of hydropower in Bulgaria are outlined.*

Key words: *Hydropower plant, power generation, Kardjali Hydroelectric Power Plant.*

ВЪВЕДЕНИЕ

Във водноелектрическите централи (ВЕЦ) като възобновяем енергиен източник (ВЕИ) се използва водата в природата и засега те имат най-голям относителен дял в производството на електрическа енергия от ВЕИ.

Техните главни особености са: по-дълго проектиране и строителство, по-големи капитални вложения; непостоянство на разполагаемата мощност в зависимост от дебита и пада на водата; лесна и евтина експлоатация; бързо пускане; лесно и чувствително регулиране на работния режим. К.п.д. при ВЕЦ е около 90 %.

ВЕЦ не използват горива, не предизвикват емисии от парникови газове, не произвеждат токсични отпадъци сигурни и имат голяма дългосрочност. Съоръженията за собствени нужди във ВЕЦ са минимални и в тях няма съществени топлинни процеси. Често те работят в автономен режим, с автоматично управление и регулиране.

ВЕЦ са много важни за устойчивата работа на електроенергийната система. Чрез управление на тяхната мощност се покриват непрекъснатите изменения в товаровия график на потребителите и се осигурява поддържането на честотата в електроенергийната система.

България не е богата на водни енергийни източници, като средният годишен отток на един жител у нас е 2100 м^3. Затова е малък и технически използваемият хидроенергиен потенциал на страната – около 1200 kWh/жител. Към момента в България има 30 броя ВЕЦ и помпено-акумулиращи ВЕЦ (ПАВЕЦ), които са собственост на НЕК ЕАД с обща мощност 2713 kW. Има и ВЕЦ, които са частна собственост с мощност около 220 MW.

Целта на настоящата работа е да се анализира процентното участие на различните видове ВЕИ в произведената електрическа енергия от тях. В статията е направен анализ на състоянието на една от най-големите водноелектрически централи в България.

ИЗЛОЖЕНИЕ

Опазването на околната среда е проблем от световен мащаб, който не търпи отлагане. Вземат се редица мерки за намаляване на вредните емисии от парникови газове. Като един от най-големите замърсители и основен източник за глобалното затопляне се посочват топлоелектрическите централи (ТЕЦ).

Като екологична алтернатива на класическите ТЕЦ и ядрените електро-централи (АЕЦ) и като най-сериозен и реално приложим възобновяем източник са водните електроцентрали ВЕЦ. В България технически усвоимия хидроенергиен потенциал е 15 млрд. kWh. До сега само една трета от него е оползотворена. Към

края на 2015 година от ВЕЦ се произвеждат 12,6 % от произведената електрическа енергия в България.

Най-често ВЕЦ са разположени при язовири, за да използват по-високото ниво на водата (поради язовирната стена, която загражда реката). Това логично води до по-висок напор. Енергията, която може да бъде преобразувана от даден обем вода е правопропорционална на напора – тоест инсталация с по-висок напор използва по-малък обем вода, отколкото инсталация с по-нисък напор, за да се произведе едно и също количество енергия.

Няколко от най-големите ВЕЦ, построени под формата на каскади са по следните реки:

- **каскада Арда** е единствената система от големи язовири в България, изградена на едно поречие. В нея са включени язовир Кърджали и ВЕЦ Кърджали, язовир Студен кладенец и язовир Ивайловград с едноименни ВЕЦ. Инсталираната мощност на трите ВЕЦ е 290 MW, а средно годишното производство на електрическа енергия е 446 GWh [1];
- **каскада Белмекен-Сестримо-Чаира** е най-мащабният и сложен хидроенергиен комплекс в България. В нея са включени язовир Белмекен и ПАВЕЦ Белмекен, язовир Чаира с едноименния ПАВЕЦ, ВЕЦ Сестримо и ВЕЦ Момина клисура. Инсталираната мощност на каскадата е 1110MW, а средно годишното производство 1113 GWh
- **каскадата Баташки водносилов път** е един от големите хидро-енергийни обекти в България. В нея са включени язовир Голям Беглик и ВЕЦ Батак, язовир Широка поляна, язовир Батак и ВЕЦ Пещера, река Стара с ВЕЦ Алеко. Общата инсталирана мощност на каскадата Баташки водносилов път е 252MW, а средно годишното производство на електрическа енергия 467GWh.
- **каскада Доспат-Въча** е една от най-сложните хидравлични схеми. В нея се включват язовир Доспат, язовир Тешел и едноименния ВЕЦ, ВЕЦ Девин, язовир Цанков камък и едноименния ВЕЦ, язовир Въча и ПАВЕЦ Орфей, язовир Кричим с едноименния ВЕЦ и ВЕЦ Въча 1 и 2. Общата инсталирана мощност на каскадата е 403MW, а средно годишно производство на електроенергия 639GWh.
- **каска Рила** е първият голям хидроенергиен проект, реализиран в България. В нея са включени три язовира Малък Калин, Калин и Карагьол и електрическите централи ПАВЕЦ Калин, ВЕЦ Каменица, ВЕЦ Пастра и ВЕЦ Рила.
- и други.

Малките ВЕЦ са основно частна собственост. В категоризацията *малки ВЕЦ* спадат: микро ВЕЦ с мощност до 500 kW, мини ВЕЦ – от 500 до 200 kW и малки ВЕЦ – от 2000 до 10000 kW. Условно разделяне на малки и големи ВЕЦ е продиктувано от практически съображения. Малките ВЕЦ попадат в категория с по-малки изисквания относно сигурност, степен на автоматизация (с изключение на ВЕЦ без постоянен дежурен персонал), данъчни облекчения и квалификация на персонала.

У нас са изградени 49 малки ВЕЦ, от които 41 работят. Според проучване на Енергопроект е възможно строителство на нови 730 малки ВЕЦ с обща инсталирана мощност 212 MW и електропроизводство в средна по важност година 800 GWh (при средна часова използваемост 3500 часа).

Малки ВЕЦ могат да се изградят в съществуващи напоителни и водоснабдителни системи; подходящи са за отдалечени от електрическата мрежа потребители като хижи, животновъдни ферми, мандри, гранични застави и други. Могат да бъдат изцяло съоръжени с български машини, производство на заводите в Плевен, Видин и други предприятия. Не се нуждаят от големи инвестиции и са по

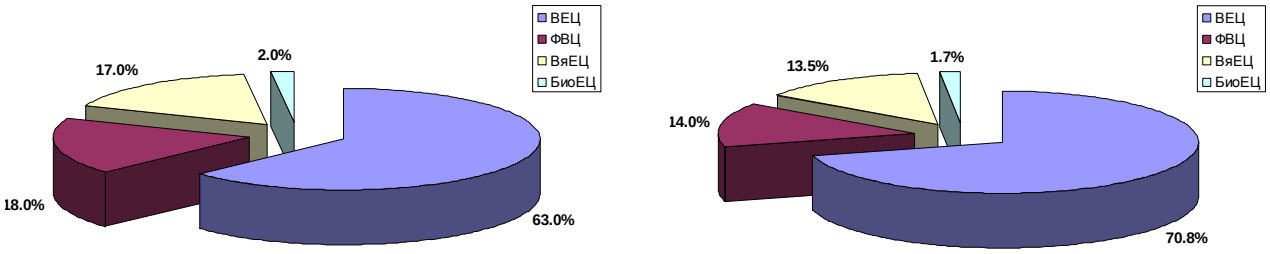
силите на отделна община, предприятие, дори и на индивидуален предприемач. Вписват се отлично в околната среда, без да нарушават екологичното равновесие.

В табл.1, съгласно данните от [3] е дадено брутното потребление на електрическа енергия от ВЕИ за пет годишен период. На фиг. 1 е представена структурата на годишното брутно прозиводство на енергия от ВЕИ за 2014 и 2015г.

Таблица 1

Брутното потребление на електрическа енергия от възобновяеми енергийни източници

Години	**2011**	**2012**	**2013**	**2014**	**2015**
Електрическа енергия, произведена от възобновяеми източници - дял от брутното потребление на електрическа енергия в **%**	12,9	16,1	18,9	18,9	19,1



Фиг.1. Структура на годишното брутно прозиводство на енергия от ВЕИ за 2014 и 2015г.

Оценката на прогнозният общ принос (изразен като инсталирана мощност и брутно производство на електрическа енергия) е представен в табл. 2 [4].

Таблица 2

Техно-логия	Години									
	2005		**2012**		**2015**		**2017**		**2020**	
	MW	GWh	MW	GWh	MW	GWh	MW	GWh	MW	GWh
ВЕЦ (включително ПАВЕЦ)	**2078**	**4336**	**2220**	**3441**	**2280**	**3534**	**2450**	**3798**	**2549**	**3951**

ВЕЦ Кърджали

Каскада ‘‘Арда‘‘ е с обем на трите язовира, които са включени към нея от 1,15 млрд. m^3 и е една от най- големите в Европа.

Хидровъзел Кърджали е първото стъпало на каскада Арда, изграден на 3 km над гр. Кърджали. Строителството му е изпълнено в периода 1957-1963 г., а укрепителните мероприятия за заздравяване на левия бряг - до 1976г. Първата турбина влиза в действие на 11.06.1963 година. Тогава тя е най-мощната водна турбина в България.

ВЕЦ „Кърджали“ има 2 основни изпускателя (ляв и десен), допълнителен тунелен изпускател и уред, наречен „светъл отвор“. Преливникът на стената е изграден от 4 шлюза [1].

Фиг.2. Язовирна стена на ВЕЦ Кърджали

Електроцентралата е под язовирна, надземна. В нея са монтирани четири турбини тип Франсис, с обща мощност 106,4 MW. Средногодишното и проектно производство е 165 GWh,а реализираното за експлоатационния период 116 GWh.

В табл. 3 са показани основните характеристики на ВЕЦ Кърджали, а на фиг. 2 е даден напречен разрез на язовирната й стена.

Таблица 3

Общ обем на язовира (**млн.m^3**)	Нетен напор (**m**)	Застроено водно количество (**m^3/sec**)	Инсталирана мощност **MW**	Средногодишно производство **(GWh)**	Годишно производство **(GWh)**
539,9	93	162	106	160	191

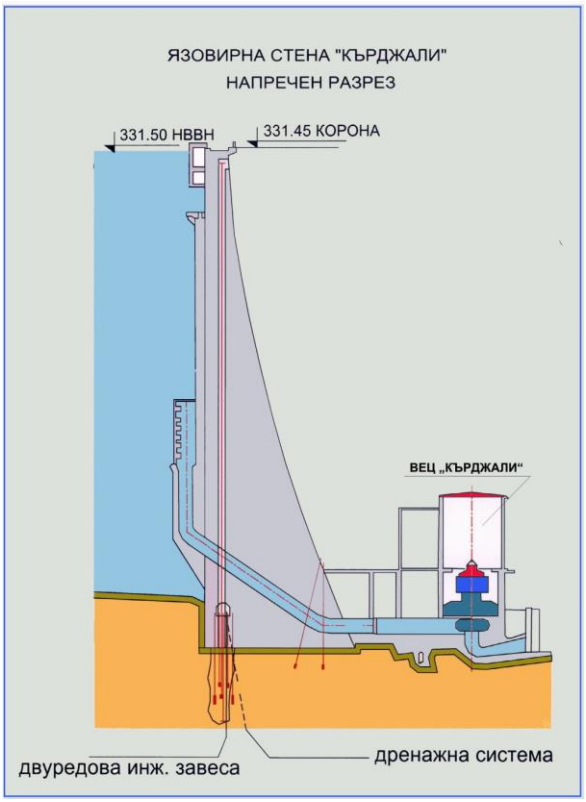
В периода от 2007г. до 2010г. във ВЕЦ „Кърджали” се проведе рехабилитация, обхващаща [2]:

1. Електрическа част

Обновяване на нови системи за управление и синхронизация, нови релейни защити, подменени са таблата за собствени нужди на ВЕЦ, монтирани са нови табла в командна зала, нови контролно-измервателни прибори, нова система за телеуправление и телесигнализация, пълна рехабилитация на закрита разпределително уредба 10,5kV и 20kV, както и частична рехабилитация на открита разпределителна уредба 110kV.

2. Турбинна част

- Монтирани са нови работни колела, нови турбинни регулатори, нови направляващи лопатки, нови бай-пасни клапани на дросел клапите, рехабилитирана е проточната част на турбините (нови облицовъчни пръстени на турбинни капаци и нови лагеруващи втулки с безмаслено смазване на направляващите апарати) и е направена рехабилитация на системите за техническо водоснабдяване.



Фиг. 2. Язовирна стена на ВЕЦ Кърджали

3. Архитектурно строителна част

Изършена е реконструкция на архитектурно-строителна част на командна зала, машинна зала, генераторни етажи, закритата разпределителна уредна, откритата разпределителна уредба и административни помещения и др.

От изброените дейности за рехабилитацията на ВЕЦ Кърджали се вижда, че тя е добре стопанисвана и експлоатитана.

Водноелектрическата централа ''Кърджали" е собственост на предприятие Водноелектрически централи. Това предприятие е със статут на клон на Националната електрическа компания и е с предмет на дейност производство на електроенергия и експлоатация и ремонт на ВЕЦ.

Предприятието Водноелектрически централи е резултат от сливането на клон Водноелектрически централи – група Родопи и предприятие Водноелектрически централи - група Рила [2]. Въвеждането на модерни технологии и рехабилитирането на обекти от предприятието Водноелектрически централи подобрява условията на работа във всички ВЕЦ в България и гарантира дългогодишната експлоатация на централите.

ЗАКЛЮЧЕНИЕ

След направения анализ на състоянието на хидроенергетиката в България и на ВЕЦ Кърджали може да каже, хидроенергийното развитие в страната е чист и печеливш процес, след възвръщане на първоначалната инвестиция. Рехабилитацията и качествената експлоатация на ВЕЦ Кърджали показват как трябва да се поддържат и експлоатират ВЕЦ в България.

Развитието на хидроенергетиката в България е от първостепенно значение и се нуждае от правителствена подкрепа в бъдеще.

ЛИТЕРАТУРА

[1] Манчев Б., И. Йотов, Т. Осиковски, Г. Денков, П. Петров, Д. Прокопиев. Електроенергетиката на България. Тангра ТанНакРа ИК, София, 2015, стр. 799
[2] Национална електрическа компания http://www.vec.nek.bg/
[3] Национален статистически институт http://www.nsi.bg/
[4] Списание ,,Диалог", ИНИ, Извънреден тематичен II, август 2012г.

За контакти:

Доц. д-р инж. Вяра Събова Русева, Катедра „Електроснабдяване и електрообзавеждане", Русенски университет „Ангел Кънчев", тел.: 0882 123 300, e-mail: vruseva@uni-ruse.bg

Слави Ненов Желязков, студент, Катедра „Електроснабдяване и електрообзавеждане", Русенски университет „Ангел Кънчев", тел.: 0884 133 662, e-mail: slavijelqzkov@gmail.com

Разработване на vu метър с микроконтролер

автор: Светослав Петров
научен ръководител: доц. д-р Цветелина Георгиева

Development a VU meter based on microcontroller: *In the paper is presented developed device VU meter based on a single microcontroller Arduino. The scheme of the VU meter was designed and tested in real condition. Arduino open software system is used for programming developing. The device allows to change the program code and to realize different tasks.*
Key words: *Arduino, VU meter.*

ВЪВЕДЕНИЕ

Volume unit (VU) meter или standard volume indicator (SVI) е устройство за измерване нивото на сигнала в аудио оборудването.

Оригиналният vu метър е пасивно електромеханично устройство, а именно 200μA DC амперметър. Работата на уреда се осъществява чрез медно-оксиден токоизправител, свързан като измервателен уред. Масата на стрелката предизвиква относително бавна реакция и интегрира сигнала с време на нарастване 300 ms.

С напредването на електрониката се появиха и познатитени микроконтролери. Във връзка с тази иновация сме предложили напълно приложима и изпитана в реални условия система за реализиране на измервателният уред VU метър. Съществуват множество схеми за изпълнение на уреда чрез различни интегрални схеми. Разликата между тях и изпълнението с микроконтролер е възможността за реално прилагане в управлението на звукови процеси и съвременното изпълнение. За постъпжане на входния сигнал към контролера се използва аналогов вход, което налага сигнала подаван към контролера да бъде постоянно токов, защото анологовите входове са постояннотокови.

Целта на статията е да се представи разработен VU метър базиран на едночипов микроконтролер.

ИЗЛОЖЕНИЕ

1. Разработване на системата

За реализирането на системата са изполвани Микроктролер Arduino и датчик - микрофон, на изхода на който е включен усилвател, поради това, че микрофона сам по себе си генерира твърде слаб сигнал, който е недостатъчен за работата на микроконтролера. Усилвателят е възможно да бъде както интегрален, реализиран с операционен усилвател на пример TL084, така и транзисторен, изпълнен в схема общ емитер. При транзисторният вариант използваме схема общ емитер, защото тя усилва сигнала, подаван на входа на усилвателя по 3-те показателя, а именно ток, напрежение, мощност.

Индикацията на сигнала се осъществява чрез LED матрица, реализирана със светодиоди. Анода на всеки от светодиодите е необходимо да се свърже към микроконтролера през резистор, който да ограничи пада на напрежение върху самия диод. Това се налага да се приложи, защото изходите на контролера осигуряват напрежение 5V(волта), а номиналното работно напрежение на светодиода е максимум 3V(волта).

1.1. Arduino Uno

Ардуино Uno е микроконтролерна развойна платка с ATmega328P AVR микроконтролер. Има 14 цифрови входно-изходни (I/O) порта, 6 аналогови входа, 16 MHz резонатор, четири светодиода (един потребителски, свързан на 13-ти цифров

I/O порт и три, които индикират работата на платката: ON, Tx и Rx), USB конектор, захранващ куплунг, бутон за рестартиране и ICSP конектор. Шест от цифровите I/O порта могат да се използват като PWM (ШИМ) изходи. Свързването с компютър се осъществява чрез USB кабел - USB A to USB B.

Uno може да се захранва през USB порта на компютъра или от външен източник, като превключването между различните начини за захранване става автоматично. Външният източник на захранване може да е AC-DCадаптер (7 до 12V) или батерия.

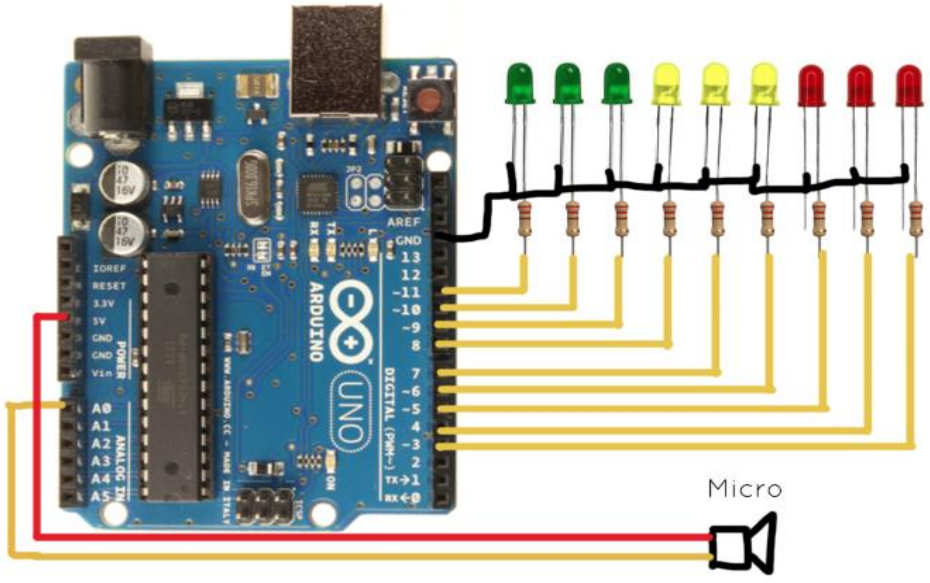
В Uno Rev.3 микроконтролера Atmega8U2, програмиран като USB-to-Serial адаптер, служещ за USB връзката, е сменен с Atmega16U2. След пина Arefca добавени два допълнителни пина за сигналите SDA и SCL (I2Cпротокола). Бутонът за рестартиране е преместен до USB конектора, а след пина reset има нов порт IOREF.

Техническите характеристики са следните:

- Микроконтролер: ATmega328P
- Работно напрежение: 5 V
- Захранващо напрежение (препоръчително): 7-12 V
- Цифрови I / O порта: 14 (от които 6 могат да са PWM изходи)
- Аналогови входове: 6
- Максимален ток на I / O порт: 40 mA
- Програмируема памет: 32 KB, от които 0.5 KB заети от буутлоудъра
- SRAM: 2 KB
- EEPROM: 1 KB
- Тактова честота: 16 MHz.

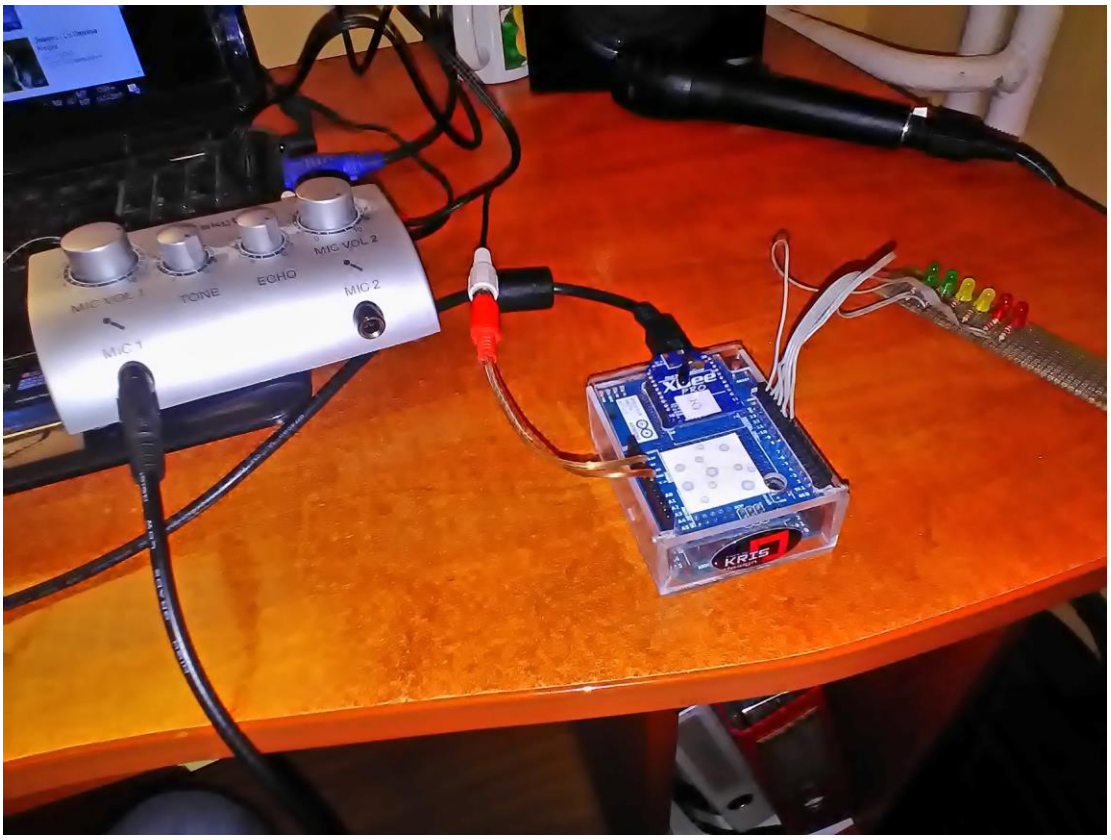
С помощта на Ардуино може много лесно да се навлезе в света на микроконтролерите. Програмирането му става с безплатния java базиран софтуер ArduinoIDE, който е изключително удобен и лесен за използване. Ардуино има голяма обществена подкрепа в цял свят и обширен набор от библиотеки и примери за използването на платформата.

На Фиг. 1 е представена блоковата схема на разработеното устройство.

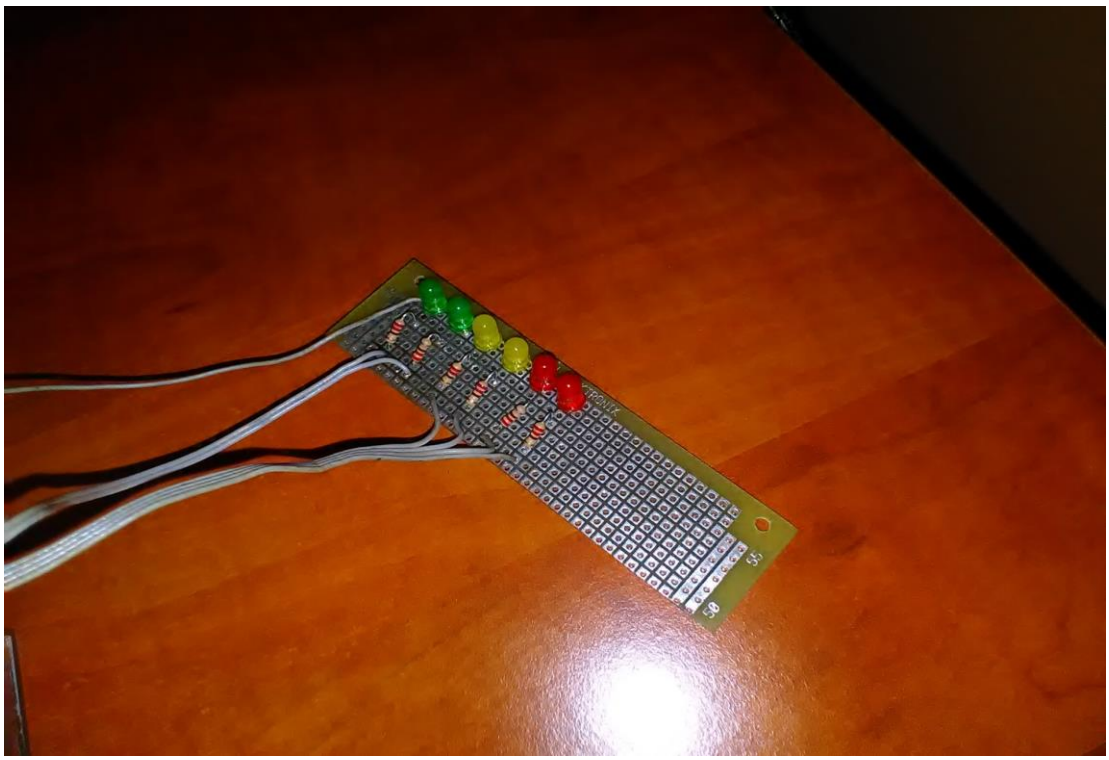


Фиг.1 Блокова схема на разработеното устройство.

На фиг. 2. е представено разработеното устройство, а на фиг. 3. - LED матрицата на VU метъра.



Фиг.2. Физически реализираното устройство – VU метър.



Фиг.3. LED матрицата на VU метъра.

Разработено е програмното осигуряване на VU метъра в средата на Ардуино. Представена е част от прогмания код за управление на устройството:

```
int val = 0;
void setup() {
pinMode(13, OUTPUT);
pinMode(12, OUTPUT);
pinMode(11, OUTPUT);
pinMode(10, OUTPUT);
pinMode(9, OUTPUT);
pinMode(8, OUTPUT);
}
void loop(){
val = analogRead(0);
if(analogRead(2) > val){
digitalWrite(13, HIGH);
} else{
digitalWrite(13, LOW);
}
```

ЗАКЛЮЧЕНИЕ

Проектиран е и е разработен vu метър базиран на микроконтролер. Разработено е програмното осигуряване на разработения уред в средата на Ардуино. Vu метърът е разработен и тестван в реална среда.

ЛИТЕРАТУРА

[1].https://www.arduino.cc
[2].https://www.arduino.cc/en/Main/ArduinoWirelessProtoShield
[3].http://www.digi.com/products/xbee-rf-solutions/modules/xbee-802-15-4

За контакти:

Светослав Петров, кадетра „Автоматика и Мехатроника“, Русенски университет “Ангел Кънчев”

доц. Цветелина Георгиева, Катедра „Автоматика и Мехатроника“, Русенски университет “Ангел Кънчев”, тел.: 082-888 668, e-mail: cgeorgieva@uni-ruse.bg

Разработване на графичен потребителски интерфейс за окачествяване на яйца базиран на система за компютърно зрение.

автор: Памела Железарова
научен ръководител: доц. д-р Цветелина Георгиева

Development of a graphical user interface for egg quality based on computer vision system. *The paper presents a developed graphical user interface for recognizing defective eggs in the MATLAB environment, based on computer vision. The interface is modular, which allows for the upgrade of the procedures and algorithms that are used. The accuracy of recognition for the four main qualitative groups of eggs was tested. Accuracy ranges is from 0.6 to 2.1%.*

Keywords: *Egg quality, MATLAB, Computer Vision*

УВОД

Съществуващите системи за сортиране на яйца използват различни по вид признаци за класификацията им като цвят, дефекти, размери и др. В тези системи за отделните качествени показатели се използват отделни сензори за тяхното определяне. За определяне на различни видове дефекти по яйцата се използва система със спектрофотометър [2, 3]. За определяне на размерите на яйцата се използва компютърно зрение [1]. Недостатък на съществуващите комерсиални системи е високата им цена, сложност на изпълнение и поддръжката им поради специфичното оборудване, което им е необходимо за правилното им функциониране.

Целта на статията е да се разработи графичен интерфейс, в който да са вградени процедури и алгоритми за определяне на дефектни яйца като се използва компютърно зрение и да се оцени точността на разпознаване.

ИЗЛОЖЕНИЕ

1. Видове дефекти по яйцата

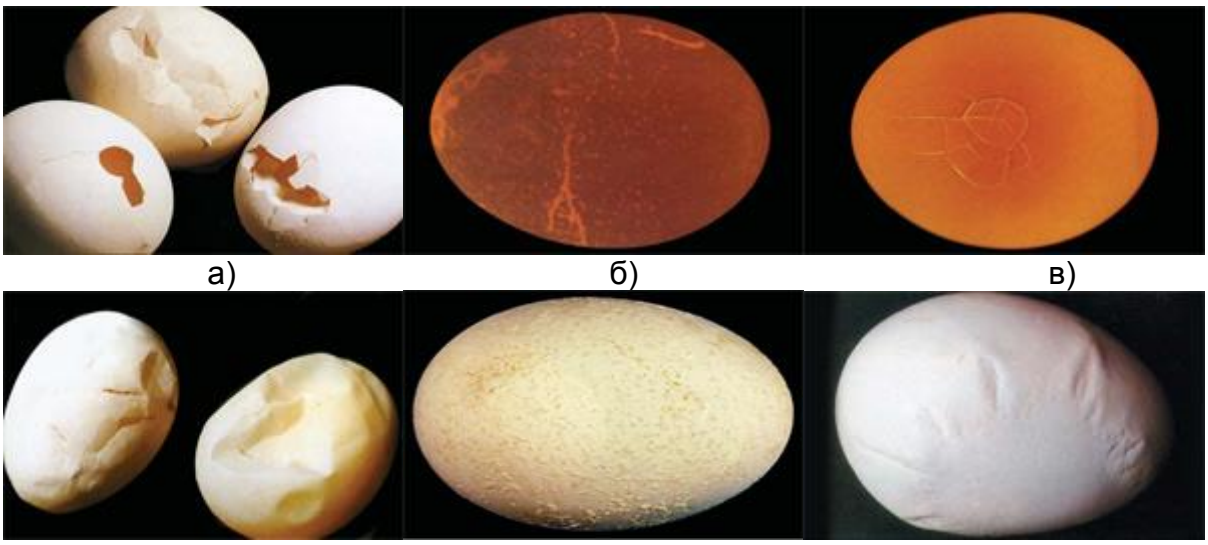
При определяне качеството на яйцата се обръща внимание на шест групи качествени показатели, характеризиращи състоянието на черупката: черупката, въздушната камера, белтъка, жълтъка, зародиша, вкуса и мириса на яйцата.най – често качеството на яйцата се определя посредством овоскопиране. Така могат да се установят: състоянието на белтъка, положението и подвижността на жълтъка, размерите на въздушната камера, цялостта на черупката и наличие на изменение в морфологичния и строеж, наличие на недостатъци по яйцата и др.

Черупката при всички категории яйца трябва да бъде с нормална структура и дебелина, здрава, чиста и неповредена.

В търговската мрежа могат да се реализират само яйца, при които цялостта на черупката не е нарушена. Пукнатите и счупени яйца трябва да се използват за преработка. Обръща се внимание и на чистотата на черупката, тъй като от нея до голяма степен зависи съхраняемостта на яйцата. За продажба могат да се предлагат само чисти или слабо замърсени яйца. Силно замърсените яйца не подлежат на продажба и съхранение, а трябва да се използват за преработка.

Често срещаните дефекти по яйца могат да бъдат следните видове:

- груби пукнатини (фиг. 1а) - отнася се до големи пукнатини и дупки, които обикновено водят до счупена мембрана на черупката. Честотата на грубите пукнатини се увеличава с възрастта на кокошката. Той варира от 1 до 5% от общото производство.



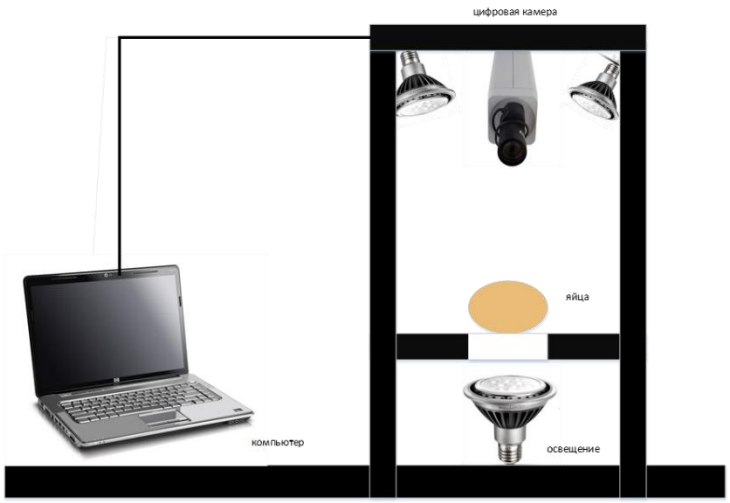
а) б) в)

г) д) е)

Фиг. 1. Дефекти по яйца

- много фини пукнатини (фиг. 1б), обикновено преминават надлъжно по дължината на корпуса.
- пукнатини с формата на звезда (фиг. 1в) – това са фини пукнатини, излъчващи навън от централната точка на удара.
- яйца без черупки или с много тънки черупки (фиг. 1г) - изглеждат непривлекателни и са много податливи на увреждане.
- яйца с груби черупки (фиг. 1д)- отнасят се до яйца с грубо оформени площи, често неравномерно разпределени върху черупката.
- плоски яйца - когато част от черупката е сплескана или нарязана. Често прилежащата част на черупката е набръчкана.

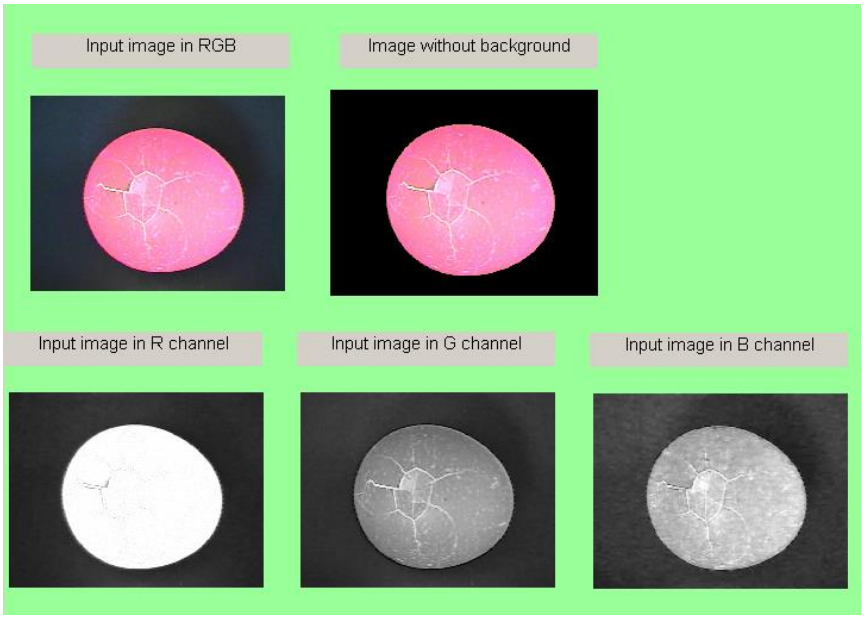
Поради това, че дефектите могат да бъдат оценени визуално се използва система за компютърно зрение (фиг. 2) за заснемане изображението на яйцата. Системата се състои от стенд с поставка за яйцата и монтирано осветление за осветяване на яйцето отгоре и отдолу; персонален компютър, в който се записва изображението, заснето с цветна цифрова камера. Изходното изображение е в RGB цветови модел с размери 640 x 480 пиксела.



Фиг. 2. Система за компютърно зрение

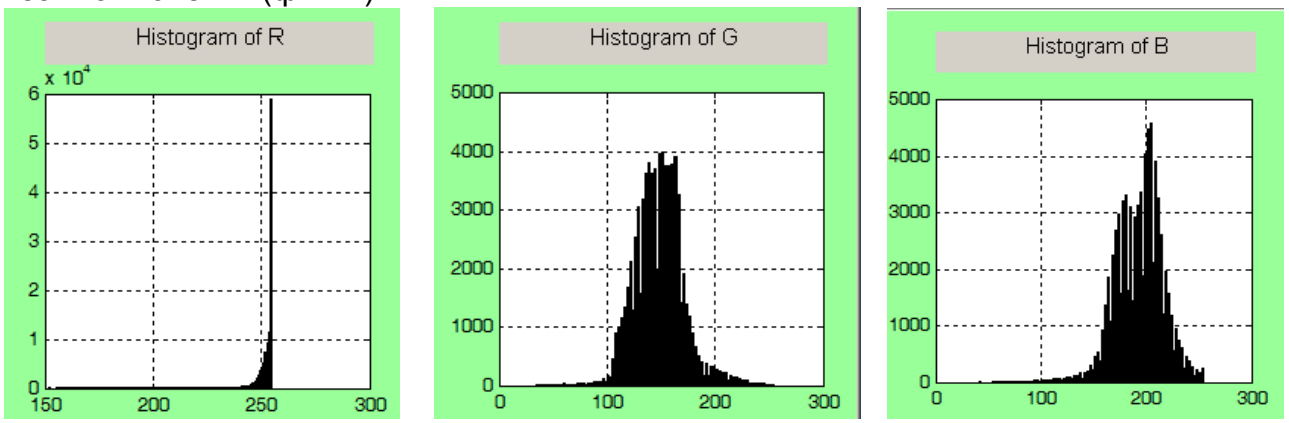
Основна стъпка е избор на информативна цветова компонента, която да се използва за откриване на дефектите по яйцата. За целта са използвани още три цветови модела – Lab, XYZ и HSV.

За разработването на интерфейса е използвана софтуерната платформа MATLAB. На фиг. 3. е представена част от графичния потребителски интерфейс, който е разработен, използвана за визуализация на изходното изображение на яйцето (в RGB модел), изображението на яйцето без фон (за да се обработват само пикселите от яйцето) и изображението на яйцето в трите компоненти от всеки цветови модел.



Фиг. 3. Графичен потребителски интерфейс за визуализация на изходното изображение, изображението без фона и трите компоненти на цветовите модели.

В интерфейса е вградена и възможност за визуализация на хистограмите на тези компоненти (фиг. 4).



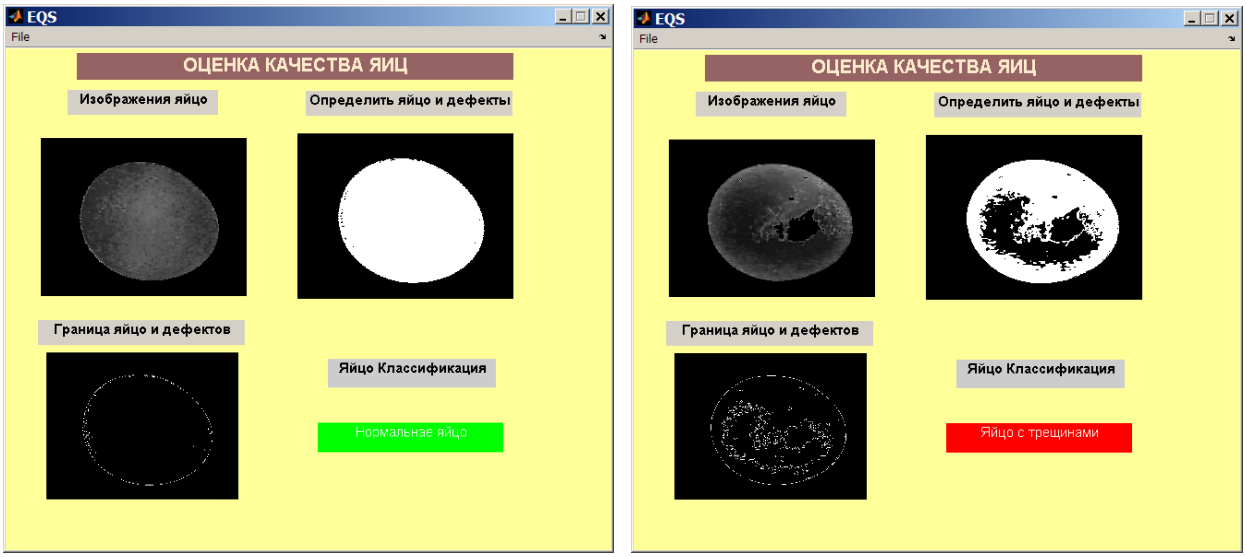
Фиг. 4. Визуализация на хистограмите на тези компоненти

Като информативна е оценена S компонентата от HSV цветовия модел. Алгоритъмът за разпознаване на дефектите по яйцата включва следните основни стъпки:

1. Преобразуване от RGB в HSV цветови модел на изходното изображение на яйцето.
2. Премахване на пикселите от фона на изображението чрез задаване на граници на H компонентата.
3. Преминаване към черно – бяло изображение чрез използване на вградена в MATLAB функция за определяне на прага на нивото на сивото.
4. Изобразяване на контурите в изображението на яйцето.

5. Оценяване на яйцето в един от двата възможни класа (с или без дефекти) като критерий за липса или наличие на дефекти е броя на контурите в изображението. При наличие на един контур – яйцето е без дефекти, при наличие на повече от един контур – яйцето е с дефекти.

Този алгоритъм и процедурите, които са използвани по отделните стъпки от него са вградени в разработения графичен потребителски интерфейс, който е показан на фиг. 5.



а) б)

Фиг. 5. Графичен потребителски интерфейс за разпознаване на дефекти по яйца. а) яйце без дефекти, б) яйце с дефекти

Разработеният графичен потребителски интерфейс е тестван със 120 яйца, по 30 броя от четирите класа s, m, l, xl. Резултатите от тестването са представени в табл. 1.

Яйцата са оценени от експерт и от разработения интерфейс. В последната колона на таблицата е представена грешката в проценти от неправилното разпознаване на яйцата.

Таблица 1 Резултатите от тестването на разработения интерфейс.

Размер на яйце	Експерт		Програма		Грешка	
	С дефект	Без дефект	С дефект	Без дефект	С дефект	Без дефект
S	13	17	15	15	0,6%	0,6%
M	14	16	16	14	0,6%	0,6%
L	15	15	12	18	0,9%	0,6%
XL	15	15	22	8	2,1%	2,1%

ЗАКЛЮЧЕНИЕ

В доклада е представен разработен графичен потребителски интерфейс за разпознаване на дефектни яйца в средата на MATLAB, базиран на компютърно зрение. Интерфейсът е модулно базиран, което позволява надграждане на

процедурите и алгоритмите, които се използват. Тествана е точността на разпознаване за четирите основни качествени групи яйца. Точността варира от 0,6 до 2,1%.

ЛИТЕРАТУРА

[1] Ibrahim R., Z. Mohd Zin, N. Nadzri, M.Z. Shamsudin, M.Z. Zainudin., Egg's Grade Classification and Dirt Inspection Using Image Processing Techniques, Proceedings of the World Congress on Engineering 2012 Vol II WCE 2012, July 4 - 6, 2012, London, U.K.
[2] Lunadei L., L. Ruiz-Garcia, L. Bodria, R. Guidetti, Automatic Identification of Defects on Eggshell Through a Multispectral Vision System, Food Bioprocess Technol, 2012 (5), 3042 – 3050
[3] SCHWAGELE F, POSER, R. and KROCKEL, L. (2001) Application of low-resolution NMR spectroscopy of intact eggs - Measurement of quality determining physical characteristics Fleischwirtschaft 81(10): 103-106.
[4] https://www.mathworks.com/

За контакти:

Памела Железарова, студент, Русенски университет „Ангел Кънчев", Факултет „Електротехника, електроника и автоматика", катедра „Автоматика и мехатроника", e-mail: paminka@mail.bg

доц. д-р инж. Цветелина Георгиева, Катедра "Автоматика и Мехатроника", Русенски университет "Ангел Кънчев",тел.:082–888 668;e-mail: cgeorgieva@uni-ruse.bg

Анализ на органолептична оценка на кисело мляко с добавка на пчелен мед

Автори: Диана Парапатиева, Мария Янева, Мирела Йорданова, Ели Костадинова
Научен ръководител: гл. ас. Златин Златев

Analysis of organoleptic assessment of yogurt with added honey. *Data from an organoleptic evaluation of the quality of yogurt with added honey are treated with the method "Correspondence analysis". Reported is the impact of tasters in evaluating the organoleptic characteristics of the tested products. It has been found that yogurt supplemented with 5% honey has better organoleptic characteristics compared to the control sample. The results confirm those mentioned in the available literature.*
Keywords: *Yogurt, Honey, Sensory scores, Correspondence analysis*

ВЪВЕДЕНИЕ

Данните от сензорния панел извършващ дегустационна оценка на киселото мляко могат да се разглеждат като тримерна матрица, съдържаща информация за оценяващия дегустатор, показателите за качество и пробите. За да се оценят точно изследваните млечни продукти чрез мненията на дегустаторите е добре да се разглеждат всички данни, отколкото да се осредняват. Основният начин за представяне на резултатите от дегустационната оценка е чрез диаграма в полярна координатна система за отделните показатели като вкус, текстура, цвят [2,6].

Нивото на достоверност на описанията на органолептичните характеристики на млечните продукти са от значение за точността в изследванията и бизнес решенията [7,9].

Функционалните храни са сред новите направления в науката за здравословно хранене. В последните години групата на функционалните храни, като продукти с определен благоприятен ефект върху човешкото здраве има все по-голям относителен дял в хранителната промишленост [1,3,4,9].

Напоследък се провеждат все повече изследвания за производство на българско кисело мляко с различни добавки. Целта е да се повишат органолептичните и лечебните свойства на млякото.

Проучването и приложението на натуралните суровини, тяхното оптимално количествено и качествено съчетаване, са от съществено значение за разработване на функционални продукти. Съществуват различни технологични методи за получаване на кисело мляко с добавка на пчелен мед [1,7].

Целта на доклада е да се направи анализ на данни от органолептична оценка на кисело мляко с добавка на пчелен мед.

ИЗЛОЖЕНИЕ

1. Материал и методи

Киселите млека са приготвени като е използван пчелен продукт – мед, закупен от търговската мрежа. Използвана е лиофилизирана закваска на производител от България (фирма „Лактина“ ООД) [8], съдържащи местни щамове млечно-кисели микроорганизми от групата на Streptococcus thermophilus и Lactobacillus delbrueckii ssp. Bulgaricus.

В органолептичния анализ участва сензорен панел от девет дегустатора, които не са разделяни по пол и възраст. Определените органолептични показатели са: Цвят, Външен вид, Вид на коагулума, Строеж при разрез, Консистенция при разбиване, Вкус и аромат, Остатъчен вкус.

Използван е метод „Анализ на съответствията“, наличен в програмният продукт Statistica. Този анализ е многомерен метод, даващ възможност за изследване на данни в табличен вид посредством графична интерпретация, а колоните в

таблицата могат да се представят като точки в пространство с малка размерност с последваща интерпретация, наречена „карта на съответствията“ [5].

2. Резултати и дискусия

В таблица 1 са посочени средните стойности на органолептичните показатели на кисело мляко с различно процентно съдържание на пчелен мед.

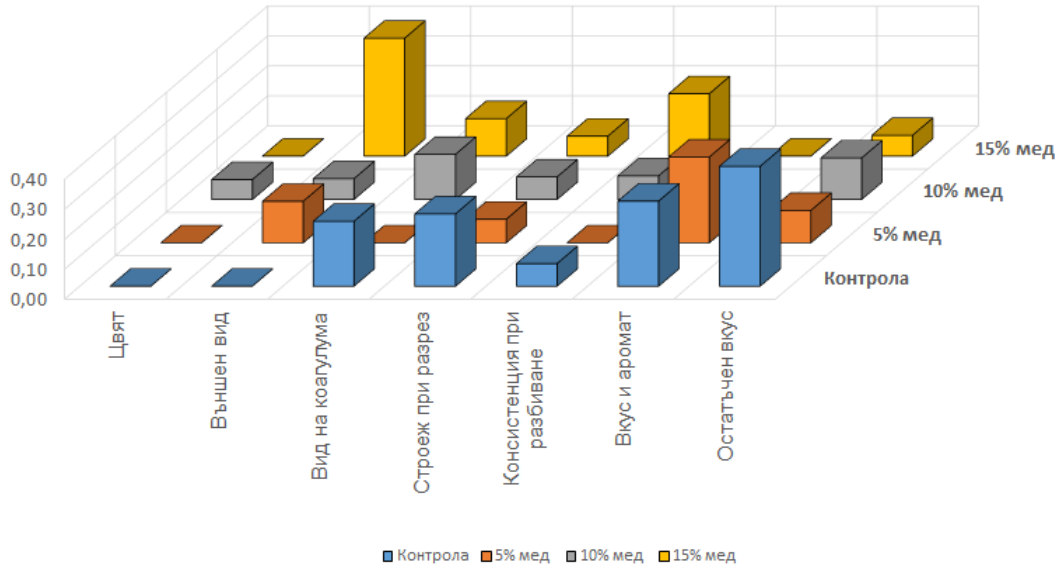
Таблица 1.

Резултати от органолептична оценка на кисело мляко с добавка на пчелен мед

Показател \ Проба	Контрола	5% мед	10% мед	15% мед
Цвят	9	9	8,67	9
Външен вид	9	8,33	8,33	7,33
Вид на коагулума	5,33	9	7,67	8
Строеж при разрез	6,33	7,33	7,67	8,67
Консистенция при разбиване	7,67	7	7,33	7,33
Вкус и аромат	7,33	5,33	7,67	9
Остатъчен вкус	3,33	5,33	8,33	8,33

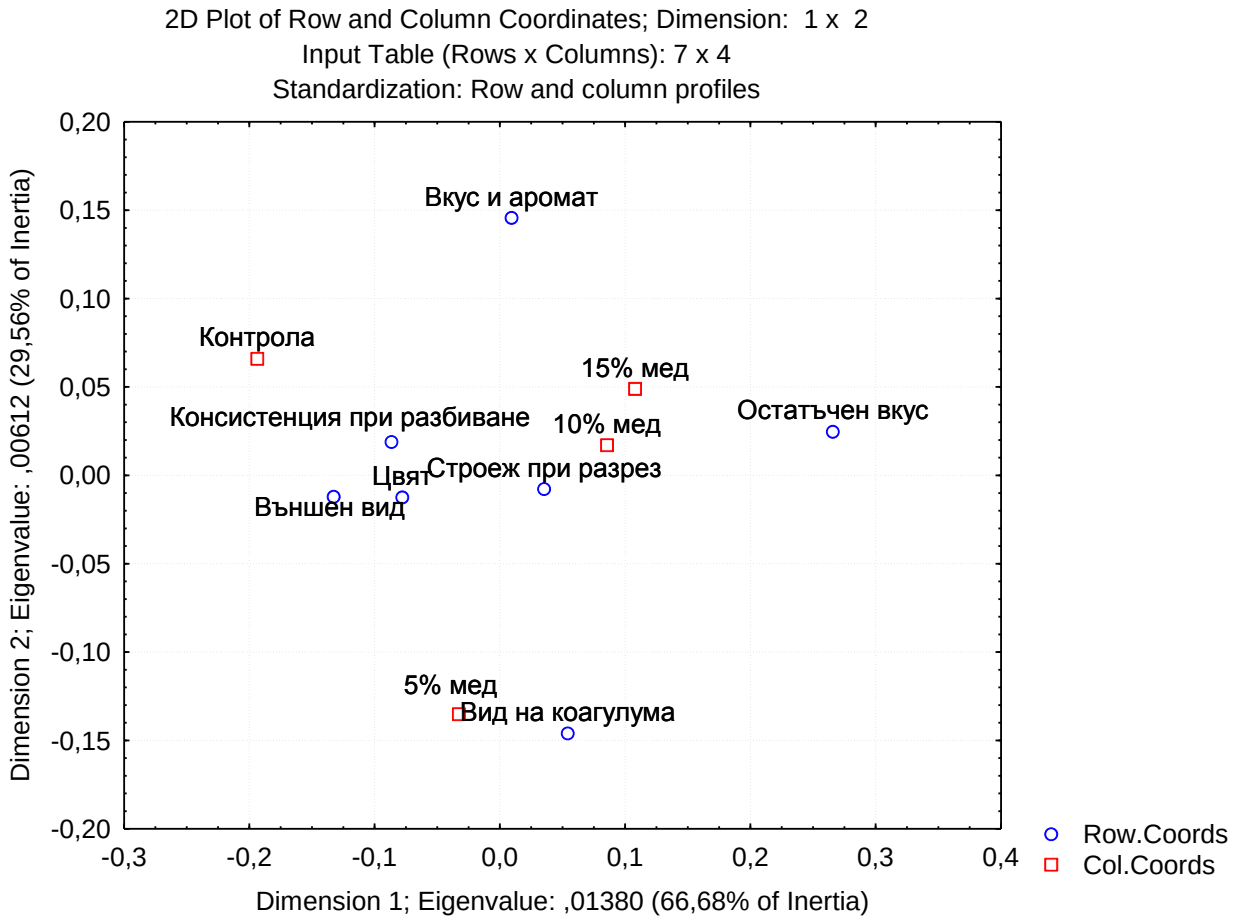
Анализът на данните от сензорния панел е направен като е отчетено отклонението на оценките от дегустаторите за отделните проби. Като критерий е използван коефициент на вариация.

На фигура 1 са представени в графичен вид резултатите за коефициент на вариация за кисело мляко с мед. От анализа на получените данни се установи, че с коефициент на вариация на мненията на дегустаторите, над 30% е контролната проба по показател „остатъчен вкус“ и киселото мляко с добавка на 15% мед по показател „външен вид“.



Фиг.1. Коефициент на вариация на деустационните оценки на кисело мляко с мед

На фигура 2 са представени резултати от анализа на данните по метод „Анализ на съответствията“. Използвана е средната стойност на данните. От анализът се установи, че контролната проба се различава в значителна степен по органолептични показатели от останалите проби, в които е вложено различно по процент количество пчелен мед. От графиката също така се наблюдава, че всички проби се различават в значителна степен по показател „остатъчен вкус“.



Фиг.2. Проверка на данни чрез метод „Анализ на съответствията“ по средни стойности”

ЗАКЛЮЧЕНИЕ

В доклада е представен анализ на органолептична оценка на кисело мляко с добавка на пчелен мед. За обработка на данните е използван метод „Анализ на съответствията, чрез който се подобрява визуализацията на резултатите и се улеснява обработката и анализа им.

С настоящия труд авторите считат, че кисело мляко с добавка на 5% пчелен мед води до подобряване на органолептичните показатели на полученият продукт, сравнен с контролната проба. По-високоите количества мед в киселото мляко, влошава структурата и външния му вид, което е неприемливо за потребителите.

Подобни резултати са получени от Bakr и Rashid [1,7], които посочват, че съдържанието на пчелен мед до 5% запазва физико-химичните и подобрява органолептичните характеристики на получения функционален продукт от кисело мляко.

ЛИТЕРАТУРА

[1] Bakr I., T. Mohamed, A. Tammam, F. Gazzar: Characteristics of Bioyoghurt Fortified With Fennel Honey, International Journal of Current Microbiology and Applied Sciences, vol. 4, No.3, 2015, pp.959-970

[2] Baycheva S., Application of devices of measurement of color in analysis of food products. Innovation and entrepreneurship – Applied scientific journal, Vol.4, No.4, 2016, ISSN 1314-9253, pp.43-59

[3] Gaazi B., S. Atanasov, P. Daskalov, Ts. Georgieva, V. Nedeva, Application of wireless sensor networks in management system of technological processes in precision agriculture, Proceedings of ICTTE 2014, ISSN 1314-9474, pp.1-6
[4] Georgieva Ts., N. Paskova, B. Gaazi, G. Todorov, P. Daskalov, Design of Wireless Sensor Network for Monitoring of Soil Quality Parameters, Agriculture and Agricultural Science Procedia, Vol. 10, 2016, pp.431-437
[5] Kazlacheva Z., J. Ilieva, M. Zhekova, P. Dineva, Fashion design on the base of connection between colors and lines, Applied Researches in Technics, Technologies and Education, Journal of the Faculty of Technics and Technologies, Trakia University, ARTTE Vol. 2, No. 1, 2014, ISSN 1314-8796, pp.54-64
[6] Mladenov, M., S. Penchev, M. Deyanov, Complex assessment of food products quality using analysis of visual images, spectrophotometric and hyperspectral characteristics. International Journal of Engineering and Innovative Technology (IJEIT), Vol. 4, Iss. 12, June 2015, ISSN: 2277-3754, pp.23-32
[7] Rashid A., Er.Thakur: Studies on Quality Parameters of Set Yoghurt Prepared By the Addition of Honey, International Journal of Scientific and Research Publications, Vol. 2, Iss.9, 2012, ISSN 2250-3153, pp.1-11 (2012)
[8] Starter cultures, http://lactina-ltd.com/eng/products-zakvaski.php (Accessed 03.12.2016)
[9] Vasilev M., I. Taneva, M. Velikova, R. Mihova, Interpreting sensory data of cheese "Krema" by Principal component analysis. ARTTE Vol. 4, No. 2, 2016, ISSN 1314-8796, pp.139-144

Благодарности: Работата по настоящия доклад е свързана с изследвания по проект **3.ФТТ/30.05.2016г**. „Безконтактни методи за оценка на основни качествени показатели на млечни продукти“.

За контакти:
Диана Парапатиева, студент, тел. 0894264945, e-mail: d.parapatieva@gmail.com, Тракийски университет, факултет „Техника и технологии“ – Ямбол, катедра „Електротехника, електроника и автоматика“
Мария Янева, студент, Тракийски университет, факултет „Техника и технологии“ – Ямбол, катедра „Електротехника, електроника и автоматика“
Мирела Йорданова, студент, Тракийски университет, факултет „Техника и технологии“ – Ямбол, катедра „Хранителни технологии“
Ели Костадинова, студент, Тракийски университет, факултет „Техника и технологии“ – Ямбол, катедра „Хранителни технологии“
гл. ас. д-р. инж. Златин Димитров Златев, Тракийски университет, факултет „Техника и технологии“ – Ямбол, катедра „Електротехника, електроника и автоматика“

Анализ на основни технически параметри на щангови пръскачки

Автори: Илия Ников, Стела Генчева, Мария Баева, Пламен Дучев
Научен ръководител: доц. д-р инж. Красимир Трендафилов

Analysis of main technical parameters of sprayers. *The report analyzes the two main technical parameters of sprayers - tank volume and flow rate of the pump. In self-propelled sprayer is analyzed and the power of the self-propelled chassis. The results show a linear relationship between the two main parameters in coupling and towed sprayers, while the self-propelled this relationship is nonlinear. It was found that there is no direct link between the work width of the tank capacity and pump flow in shed and self-propelled sprayers*

Keywords: *Sprayers, Reservoir, Pump flow rate, Work width*

ВЪВЕДЕНИЕ

Високо механизираното и автоматизирано селско стопанство може да прояви своите предимства само при условие на пълна степен на използване на наличната техника. Насищането му с машини изисква все повече да се прилагат нови по-съвършенни методи за организация и ръководство на производствените процеси [2,3,6].

Растително-защитните мероприятия играят важна роля за увеличаване на добивите и подобряване на качеството на получаваната растителна продукция. Механизираните технологии в растителната защита увеличават производителността на труда, снижават относителните разходи за извършване на операциите, подобряват условията на труда на работниците, подобряват качеството на работата и спомагат за намаляване на неблагоприятните въздействия върху околната среда [1,8].

Световна тенденция в земеделския сектор е нарастващият интерес към самоходните пръскачки. Все повече фермери откриват предимствата им при работата си с тях, а производителите на агромашини от своя страна провокират интереса на стопаните с периодични технически подобрения, които правят самоходната пръскачка незаменим, икономичен и високопроизводителен помощник за всяко стопанство [7].

На съвременното ниво на развитие на земеделската техника за растителна защита, освен самоходните, в България се използват прикачните и навесните пръскачки, като широко приложение намират тези от щангов тип [5].

Целта на доклада е да се направи анализ на основни технически параметри на щангови пръскачки.

ИЗЛОЖЕНИЕ

Щанговите пръскачки са главно навесни, прикачни и самоходни. На фигура 1 са представени в общ вид, по време на работа основните видове щангови пръскачки, които се използват в земеделската практика. Те имат резервоар, помпа, система за разпръскване на препаратите, рама, ходова част и механизъм за задвижване на работните органи. Резервоарът има филтър за пречистване на флуида. След като премине през филтъра, флуидът се подава от помпа чрез дозиране в разпръскващото устройство.

Дюзите са разположени по щангова тръба за разпространение на препарата на по-широка лента от площта. Разпръскващите устройства също се различават в зависимост от това дали са за полски или градински култури и в зависимост от начина им на действие, например центробежни, ротационни и инжекторни, като последните елиминират опасността от отклоняване на капките от вятър до определена скорост [4].

а) навесна б) прикачна в) самоходна

Фиг.1. Видове щангови пръскачки

3. Резултати и дискусия

От практическа гледна точка важни парамети на щанговите пръскачки са обема на резервоара и дебита на помпата. Направен е анализ на тези два основни параметъра на машините за растителна защита.

В таблица 1 са представени резултати от проучване в световната мрежа Интернет на предлаганите в България щангови пръскачки. Данните са за общо 60 броя пръскачки от трите основни типа – навесни, прикачни и самоходни.

Таблица 1.
Технически характеристики на щангови пръскачки

Самоходна			Прикачна		Навесна	
Обем на резервоар, l	**Дебит на помпа, l/min**	**Мощност на машина, hp**	**Обем на резервоар, l**	**Дебит на помпа, l/min**	**Обем на резервоар, l**	**Дебит на помпа, l/min**
3000	130	175	2800	150	250	110
4180	120	311	700	120	200	80
2200	220	145	200	40	200	100
2000	300	238	3000	165	200	60
3500	130	210	2400	265	220	80
3785	117	215	2500	250	400	27
3785	117	240	1500	70	400	30
4542	117	275	2700	180	600	120
4542	117	333	2500	160	600	85
4542	117	365	2000	120	600	100
3200	117	180	3200	160	660	100
4200	117	200	4000	250	800	105
5200	130	245	2200	170	800	99
2000	300	145	2200	170	800	114
2000	300	145	2200	170	800	130
2000	300	238	2500	194	400	50
2000	300	176	3000	194	1000	150
2000	240	145	2500	250	1000	114
2000	300	145	3000	150	1500	170
2000	300	145	2500	250	1600	180

Работната ширина на различните видове щангови пръскачки варира от 1,5 m до 36 m.

Нормалното налягане на хидравличните помпи е между 15 и 25 bar. Дебитът на помпите е между 27 и 700 l/min.

Видът на помпите са мембранни и бутално-мембранни.

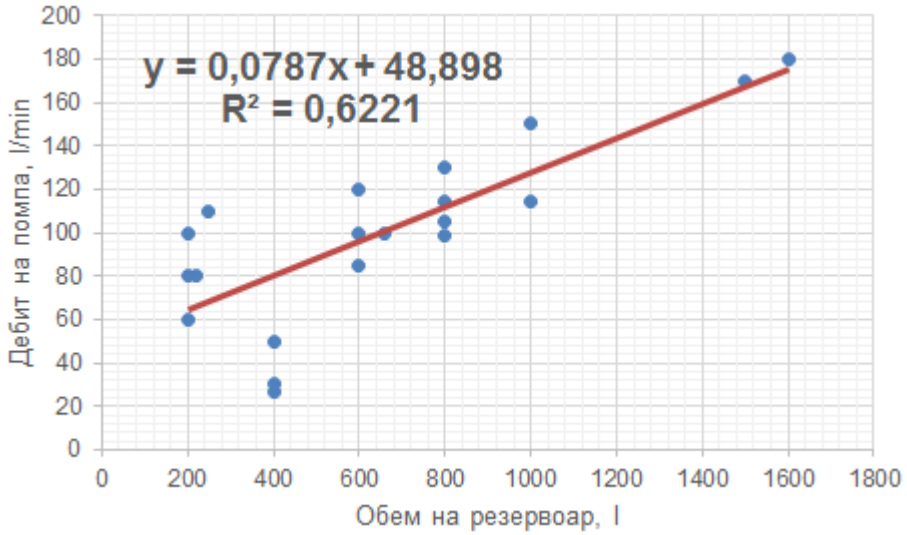
При всички модели се използват различни видове разпръсквачи (дюзи), като броят им достига до 32бр. на пръскачка. Разпръсквачите биват единични, двойни, тройни и четворни, както и керамични, месингови, конични и други видове.

Резервоарите за разтвора се изработват от различни материали, както и с различни обеми, спрямо работната ширина на пръскачката. Като материали за изработка на резервоарите се използват: полиетилен, резистентен полиетилен,

подсилен стъклопласт, полиестер, усилен полиетилен и др. Обемите на резервоарите варират между 200 и 6056 l.

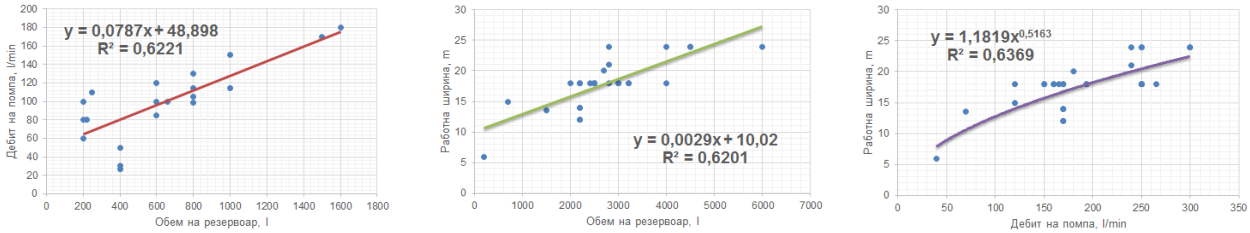
В зависимост от вида, марката и модела на пръскачките, мощността на тракторният агрегат варира между 45 и 365 hp.

На фигура 2 са представени резултати за обем на резервоара и дебита на помпата за навесните пръскачки. Наблюдава се линейна зависимост между тези два показателя. Направена е проверка за връзка между работната ширина на пръскачка, обема на резервоара и дебита на помпата, но при тази проверка се установи, че няма пряка връзка между тези технически параметри, тъй като коефициентът на корелация е R=0,01-0,02.



Фиг.2. Обем на резервоар и дебит на помпата за навесни пръскачки

На фигура 3 са представени резултати за обем на резервоара, работната ширина и дебита на помпата за прикачни пръскачки. Връзката между обема на резервоара и дебита на помпата, както и тази с работната ширина е линейна, докато при дебита на помпата и работната ширина тя е нелинейна.



а) Обем на резервоар и дебит на помпа

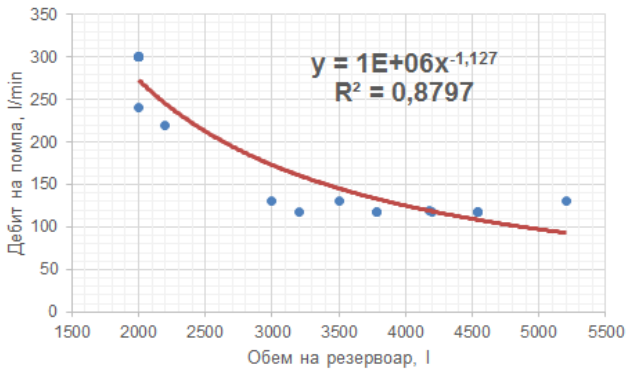
б) Обем на резервоар и работна ширина

в) Дебит на помпа и работна ширина

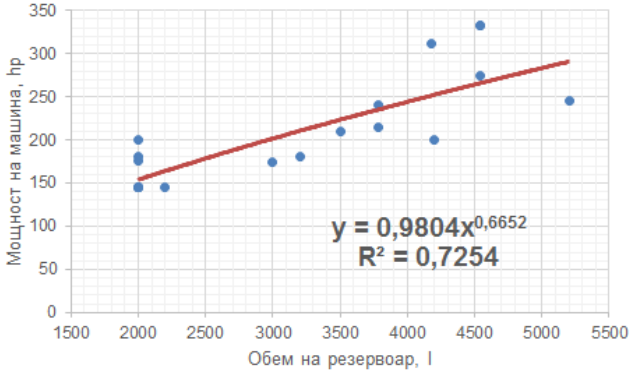
Фиг.3. Връзка между технически параметри на прикачни пръскачки

На фигура 4 са представени резултати за обем на резервоара и дебита на помпата за самоходни пръскачки. Наблюдава се нелинейна зависимост между тези технически параметри на пръскачките.

Направена е проверка за връзка между работната ширина на пръскачка, обема на резервоара и дебита на помпата, но при тази проверка се установи, че няма пряка връзка между тези технически параметри, тъй като коефициентът на корелация е R=0,002-0,01.



а) Обем на резервоар и дебит на помпата



б) Обем на резервоар и мощност на машина

Фиг.4. Връзка между технически параметри на самоходни пръскачки

При самоходните пръскачки, поради наличието на самоходно шаси е направен анализ на връзката между обем на резервоара и мощност на машината. Наблюдава се нелинейна зависимост между тези два технически параметъра на машините.

ЗАКЛЮЧЕНИЕ

С настоящия труд авторите считат, че:

- ✓ Освен самоходните, в България се използват прикачните и навесните пръскачки, като широко приложение намират тези от щангов тип;
- ✓ При навесните и прикачните пръскачки се наблюдава линейна зависимост между обема на резервоара и дебит на помпата, докато при самоходните тази зависимост е нелинейна;
- ✓ При навесните и самоходните пръскачки няма пряка връзка между работната ширина и обема на резервоара и дебита на помпата.

ЛИТЕРАТУРА

[1] Dragoev D., N. Stratiev, Justifying technology for growing wheat, XXV International Conference "Management and Quality" for young scientists, Collection of scientific works, Yambol, 11-12.05.2016, ISSN 978-619-160-679- 5, pp.24-31
[2] Gaazi B., S. Atanasov, P. Daskalov, Ts. Georgieva, V. Nedeva, Application of wireless sensor networks in management system of technological processes in precision agriculture, Proceedings of ICTTE 2014, ISSN 1314-9474, pp.1-6
[3] Georgieva Ts., N. Paskova, B. Gaazi, G. Todorov, P. Daskalov, Design of Wireless Sensor Network for Monitoring of Soil Quality Parameters, Agriculture and Agricultural Science Procedia, Vol. 10, 2016, pp.431-437
[4] Importing attached inventory, http://agrobio.elmedia.net/bg/ (accessed 03.04.2017) (in Bulgarian)
[5] Kehayov D., G. Komitov, P. Penchev, Optimize of Machine-Tractor Fleet for Plant Protection in Agrotreyd Ltd. – village Okop Yambol mu, Proceedings of University of Ruse, vol.54, No. 1.1, 2015, pp.131-136
[6] Nedeva V., Z. Zlatev, S. Atanasov, Advanced information technologies in precision farming, ISTC, Agricultural machinery XXI, vol.5(142), 20-21.06.2013, Varna, Bulgaria, ISSN: 1310-3946, pp.8-11
[7] Self-propelled sprayers - machines that each farm must have, http://www.agrocompass.bg, (accessed 11.04.2017) (in Bulgarian)
[8] Tasev G., K. Krastev, Exploration of mathematical model for optimization of frequency of diagnosis of the elements of machines, Proceedings of The 11th International

Conference, Reliability and statistics in transportation and communication, Latvia, 2011, ISBN 978-9984-818-34-4, pp.115-119

Благодарности: Работата по настоящия доклад е свързана с изследвания по проект **5.ОУП/27.05.2016** „Подобряване на инфраструктурата за направление „Машинно инженерство“ и „Общо инженерство“ на Факултет „Техника и технологии“ и Аграрен факултет при ТрУ“

За контакти:

Илия Георгиев Ников, студент, Тракийски Университет – Стара Загора, Аграрен факултет, катедра „Растениевъдство“, тел. 0894329510, e-mail: Ilyo_16@abv.bg

Стела Генчева, студент, Тракийски университет, факултет „Техника и технологии“ – Ямбол, катедра „Машинно инженерство“.

Мария Баева, студент, Тракийски университет, факултет „Техника и технологии“ – Ямбол, катедра „Електротехника, електроника и автоматика“

Пламен Дучев, студент, Американски университет, спец. Компютърни науки, p2duchev@abv.bg

доц. д-р инж. Красимир Трендафилов, Тракийски университет, факултет „Техника и технологии“ – Ямбол, катедра „Машинно инженерство“.

Наблюдение на времето за усвояване на поливната вода при индетерминантни доматени насаждения на база колорометрични измервания на листата

автор: Светослав Атанасов
научен ръководител: проф. Пламен Даскалов

Survey of irrigation water uptake time at indeterminate tomato plants based on colorimetric measurements of the leaves: *In the form of a sequence of actions, a methodology has been proposed for measuring the time for irrigation of irrigated water from greenhouse tomato plants. On the basis of a purely scientific observation, prior to the measurements themselves and during the experiment, it is hypothesized that under the particular environmental conditions in which the experiment is carried out and in this tomato variety, the water moves to the top of a plant high 1 m in 1 h . On the basis of the same pure physical observation it was found that the dried leaves darkened, and after the pollen they became lighter-green, which was proved by the measurements with a colorimeter. It has also been noticed that watered plants notice bleaching of the leaves of the leaves, become bright, stand out, enlarge.*

Key words: *greenhouse tomato plants, water uptake time.*

ВЪВЕДЕНИЕ

Нуждата от подобно изследване възникна във връзка с провеждано дисертационно изследване, което се занимава с намиране на интелигентен начин за определяне връзката между влажността и температурата на почвата и цвета на листата на оранжерийни доматени насаждения. Всичко това се прави с оглед оптимално управление на напояването. Другата причина за възникване на изследването, обект на тази статия, е относителната липса на информация по темата. Използваният инструментариум (колориметър и уред за измерване на параметри на околната среда) е описан в [1]. Калибрирането на сензора за почвена влага е обект на друго изследване и доклад [2]. Според автора на тази статия, изследването на времето на усвояване може да бъде направено по два начина – по морфологични признаци – деформиране на листата вследствие стреса на засушаване (обект на бъдещо изследване) и по методиката описана в изложението на тази статия. Целта е да се получи един вид „преходна характеристика", в която са се улови колко време след поливка растението реагира, променяйки цвета на листата си до върха.

ИЗЛОЖЕНИЕ

При това изследване се разчита на способа на *научното наблюдение*. Според съществуващата традиция при наблюдението се извършва научно-познавателна дейност, която е както практическа, така и логическа. При *непосредственото наблюдение* обектът се описва, а свойствата му се възприемат непосредствено от сетивния орган. *Опосредстваното наблюдени*е се извършва чрез уреди, един вид усилватели на сетивния орган, които се поставят между наблюдавания обект и наблюдателя [3]. В това изследване, обект на настоящата статия, е използвана комбинация от *непосредствено* и *опосредствано наблюдение*.

Сортът, обект на изследване, е луксозен хибрид холандски домати наречен „Амати" („Amati"). Семената на изследваните растения са засадени в края на юни, а разсада – в края на юли. Експериментите са проведени в лабораторни условия, максимално близки до оранжерийните върху едно от засадените растения.

Характерно за този хибриден сорт домати е, че те са устойчиви на болести като тютюнево мозаечен вирус (Tm), вертицилум (V), нематода (N), фузариум (F1,2) и листна плесен (St). Поради тази причина доматите са предпочитани от земеделските производители. Доматите „Амати" са със средно едър плод (тегло на един домат е

около 180 – 220 гр.), много приятни на вкус, кръгли и ярко червени на цвят. Подходящи са за консумация в сурово състояние и за преработка. От „Амати“ може да бъде приготвена лютеница, доматено пюре, доматени сокове, кетчуп, различни видове консерви и др. [4]

Този сорт домати е подходящ за отглеждане, както в оранжерии, така и на открито. „Амати“ е индетерминантен (високорастящ) хибрид, който има отворен хабитус и поради това има възможност за дълъг период на плодоносене. [5]

Датите на проведените експерименти и измервания, дните след засаждането и височината са надземната част на растението са описани в Табл. 1:

Таблица 1. *Информация за експериментите*

Дата на експеримента	Дни след засаждане	Височина на растението
11 Септември 2016	около 42	около 90 cm
18 Септември 2016	≈ 49 дни	≈ 120 cm

През първия ден на изследването (11.09.2016) са взети RGB цветови проби веднъж непосредствено преди поливка и десет пъти след поливка през половин час.

При провеждането на всяко измерване от горната половина на растението са взимани на случаен принцип по девет RGB стойности (или деветдесет случайни RGB стойности) за цялото изследване след поливка, които са усреднени за всеки час на взимане на пробите.

Пробите са взимани хаотично, на случаен принцип от различни листа при отделните измервания. Един набор от измервания отнема от 5 до 7 min. Измерванията са в диапазона 70-90 cm височина на растението (горната му част).

Поливката при всички експерименти е еднократна и обилна, без да бъдат „удавени“ растенията.

В това конкретно изследване не е взет под внимание конкретният тип почва като влияещ фактор, понеже това не е акцентът тук. Прецизиране на изследване, включващо и калибриране на сензор според конкретния тип почва е направено в друго изследване [2].

В този конкретен ден, преди поливка липсва слънце, което да задейства силно фотосинтезата и растението да "засмуче" почвената влага с помощта също и на изпаряването. Преди да бъдат напоени растенията не са не са поливани 3-4 дни.

Климатичните условия при провеждането на експеримента на 11.09.2016 са описани в Табл. 2:

Таблица 2. *Климатични условия във времето при първия експеримент*

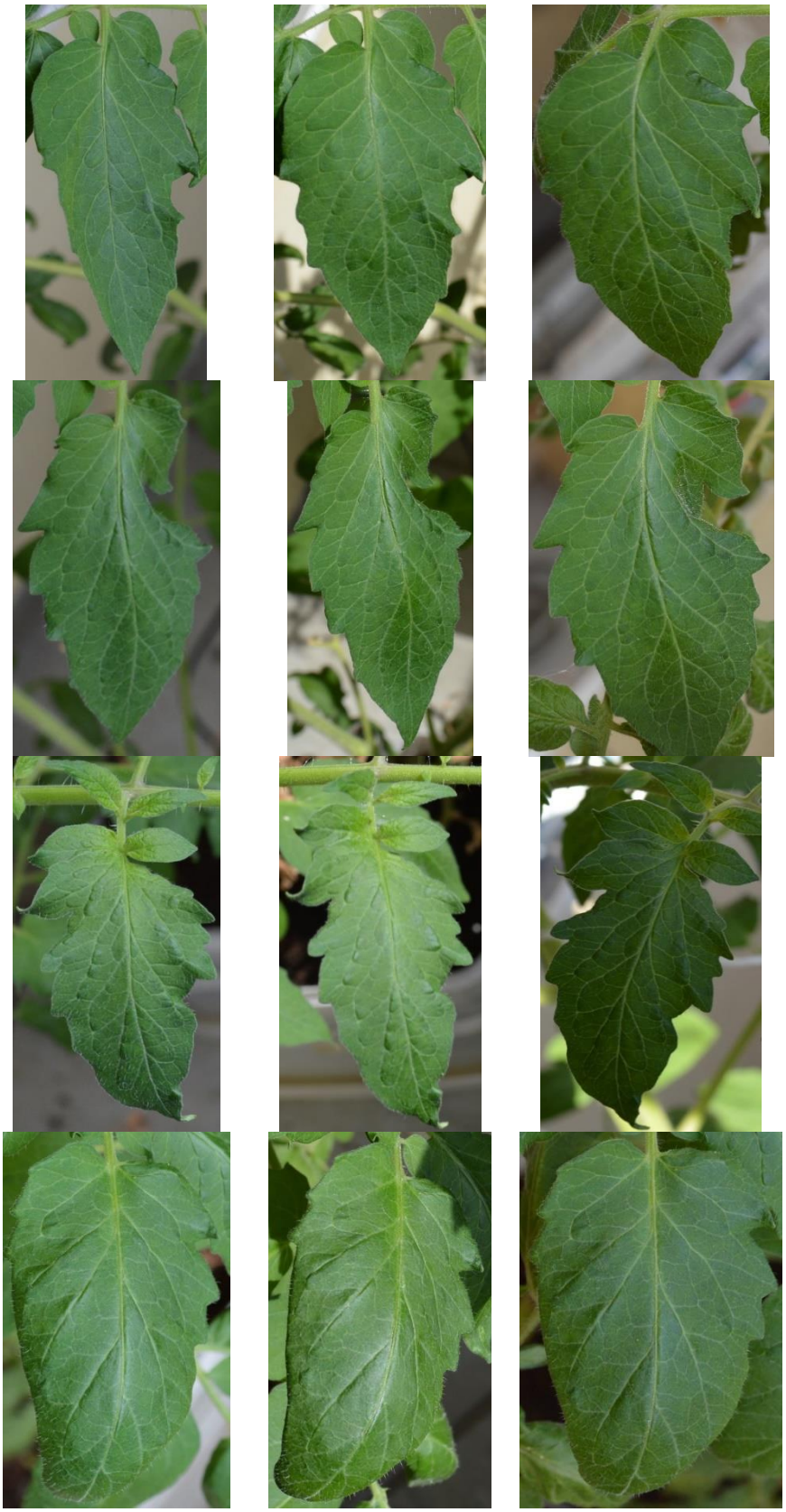
	Условия	**Осветеност,** kLux	**Температура въздух,** °C	**Влажност въздух,** %	**Почвена влажност,** m^3/m^3
Преди поливка	Облачно	4,9	26,5	51,8	0,256
2 h след поливка	Слънчево и топло	40,3	33	40,7	0,295
5 h след поливка					0,293

На набора от снимки (Фиг. 1), на всеки ред, е представено едно и също листо непосредствено преди поливка, два часа след поливка и пет часа след поливка.

Тук си струва да се отбележи нещо забелязано при измервания, а именно че час и половина след поливка се забелязва *изравняване* в показанията (*уравновесяване* на отчитаните RGB стойности), докато при другите измервания те варират от големи до малки.

От чисто научното наблюдение се забеляза че при този, както и последващите експерименти, няколко часа след поливка жилките на листата избеляват, стават

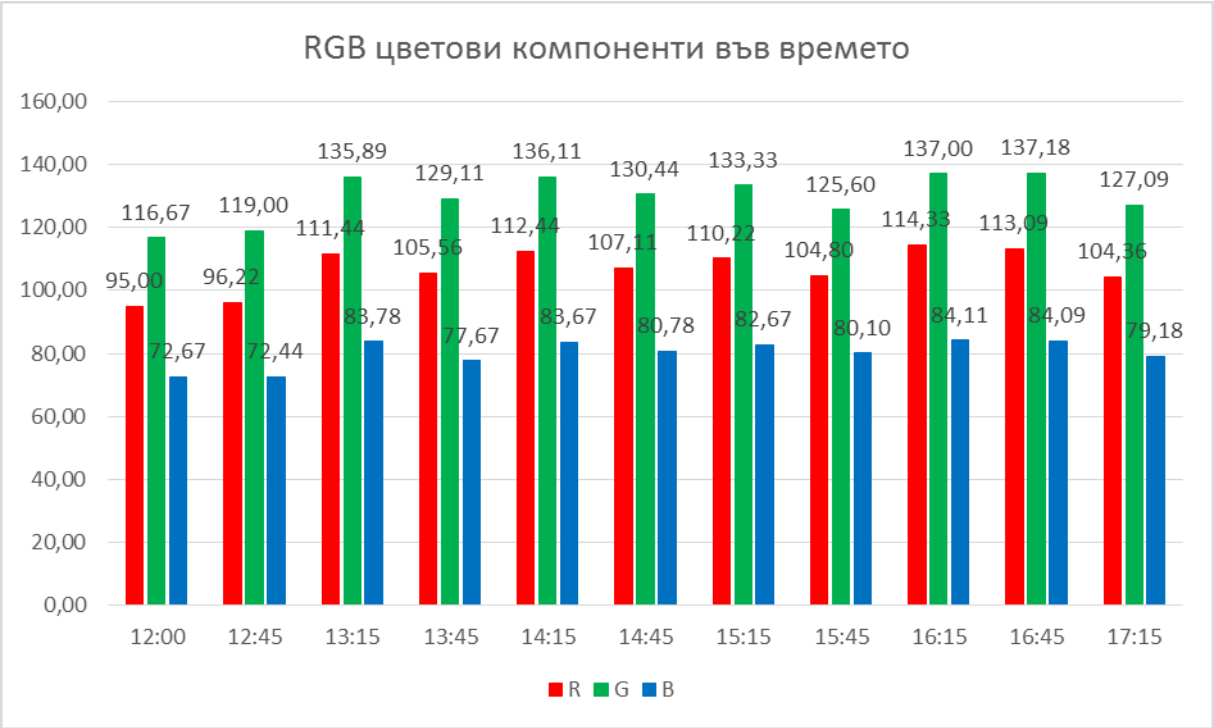
светли, изпъкват, уголемяват се (т.е. видимо е че проводящата тъкан се напълва с течност). Това се установява няколко часа след поливка, с невъоръжено око.



а) б) в)

Фиг. 1. Снимки на изследвани листа във времето: а) Преди поливка, б) 2 часа след поливка, в) 5 часа след поливка. На всеки ред е едно и също листо.

Използвайки колориметъра и измерването на цвета, с което може да бъде отчетено достигането на усвоената влага до върха на растението, се получава следващата фигура (Фиг. 2) във вид на диаграма:



Фиг. 2. Изменение на RGB във времето преди и след поливка, първи експеримент

Както е видно на диаграмата, между 30 и 60 min след поливка (в 12:15 h е била тя), цветът на листата в изследваната горна част на растението (около върха) се променя. На нея е представено изменението на RGB цветовите компоненти във времето по време и след поливка, като са визуализирани графично и цифрово средните стойности получени при всяко измерване.

На база горната диаграма се достигна до извода, че през втория ден от изследването трябва да бъде увеличена резолюцията (честотата) на измервания през 15 мин след първия половин час.

През втория ден на изследването (18.09.2016) са взети RGB цветови проби веднъж непосредствено преди поливка и е увеличена резолюцията на измерванията след поливка - 30, 45, 60 и 75 min след нея (в 14:00 h е била тя).

При провеждането на всяко измерване са взимани на случаен принцип от горната половина на растението по девет RGB стойности (или седемдесет и две случайни RGB стойности) за цялото изследване след поливка, които са усреднени за всеки час на взимане на пробите.

Един набор от измервания отнема 5-8 min. Измерванията са в диапазона 100-120 cm височина на растението. Забелязва се, че крайните листа на върха на всяка „клонка“ са завяхнали.

Преди да бъдат напоени растенията не са не са поливани няколко дни.

Климатичните условия при провеждането на експеримента на 18.09.2016 са:

Таблица 3. *Климатични условия във времето при втория експеримент*

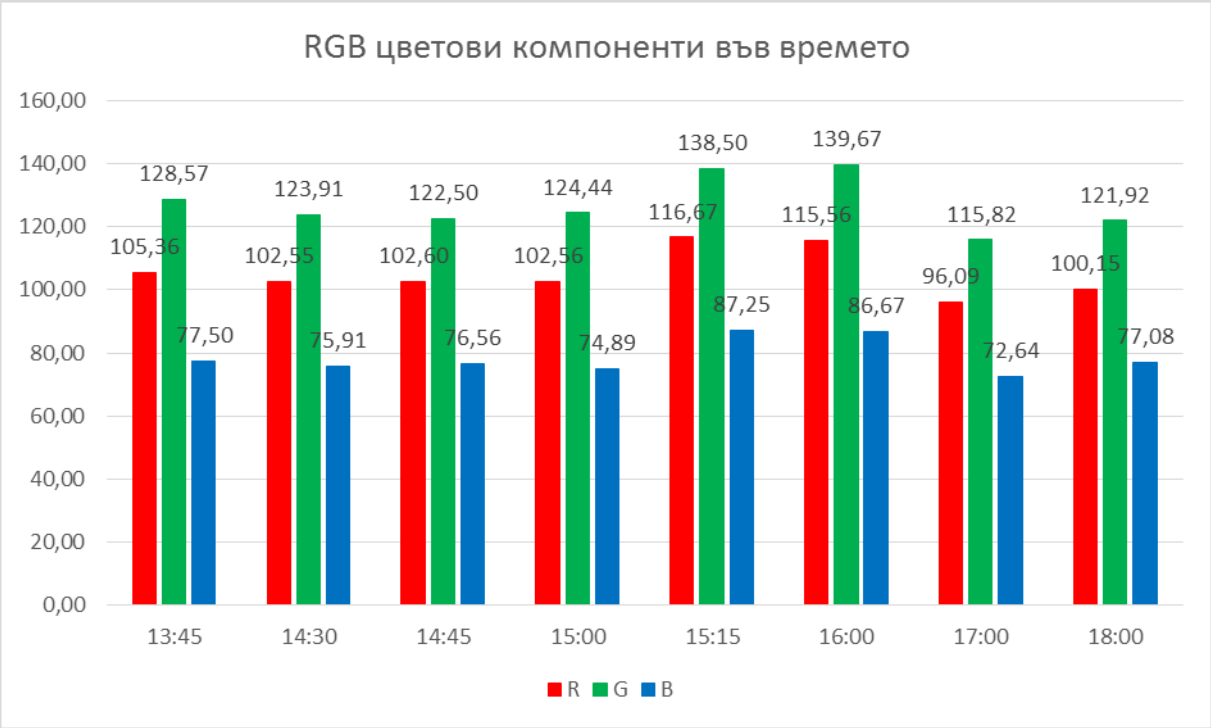
	Условия	**Осветеност,** kLux	**Температура въздух,** °C	**Влажност въздух,** %	**Почвена влажност,** m^3/m^3	**Температура почва,** °C
Преди поливка	Слънчево, горещо	42,4	34,5	36,7	0,271	24,8
1,5 h след поливка	Много горещо	57,3	36,3	32	0,308	25,2
2 h след поливка	Непоносима жега	32,4	36,07	37,9	0,306	27,24
3 h след поливка			36,97	31,49	0,306	28,10
4 h след поливка			34,17	32,79	0,304	28,57

Час и половина след поливка листата изсветляват и жилките изпъкват и се изпълват.

При тези климатични и почвени условия и при този сорт може да бъде изказана хипотезата, че водата се усвоява до върха на растението за 1 h, ако то е високо около 100 cm, а ако е около 120 cm - за 1,25 h до 1,5 h.

Наблюдава се, че тези листа които не са изложени на пряка слънчева светлина са по-тъмни. Също тези които са по-близо до стъблото са по-светли от тези в края на клонката с листа.

При измерванията проведени 2 h и 3 h след поливка се появява *изравняване* и *уравновесяване* на измерваните RGB стойности.



Фиг. 3. Изменение на RGB във времето преди и след поливка, втори експеримент

От графиката се вижда, че при втория експеримент между 60 и 75 min след поливка цвета се променя. Тук обаче височината на растението е около 120 cm надземна част. Затова при следващото измерване ще цвета ще бъде измерван на различни височини под върха.

ЗАКЛЮЧЕНИЕ

Изказаната хипотеза, че при този сорт домати и при тези климатични условия поливната вода се усвоява за 1 h ако растението е високо 100 cm и за 1,25 h до 1,5 h ако растението е високо 120 cm, е частично доказана дотук и предстои да бъде потвърдена при следващите изследвания и измервания на цвета на листата.

В последващите измервания цветът ще бъде изследван на различни височини от растението, с цел повишаване резолюцията и по-прецизно установяване по кое време докъде се е просмукала влагата по продължението на самото растение. В досегашните изследвания [1] цветът е бил измерван само във най-горната и най-долната част на растението.

Освен на различни височини е установена нужда и да се увеличи честотата на измерванията – те да бъдат през 15 min след първия половин час.

ЛИТЕРАТУРА

[1] Atanasov, S. S., P. I. Daskalov, and V. I. Nedeva, An Intelligent Approach of Determining Relationship between Tomato Leaves Color and Soil Moisture and Temperature, Bulgarian Journal of Agricultural Science, vol. 22, no. 6, 2016, pp. 1027-1035, SCOPUS, www.scopus.com.

[2] Атанасов, С., Калибриране на FDR сензор за специфична почва при измерване на почвена влажност. Научни трудове на Русенския университет, 2015, том 54, серия 3.1, 217-221.

[3] Ковачев, В. Научно наблюдение (физико-методологичен анализ), София, 2001, ISBN 954-607-479-9.

[4] http://www.agrogradina.bg/Домати-Амати

[5] http://zemedelie-bg.com

За контакти:

Светослав Атанасов, докторант, Катедра "Автоматика и мехатроника", Русенски университет "Ангел Кънчев", e-mail: s_s_atanasov@abv.bg

Проф. д-р инж. Пламен Даскалов, Катедра "Автоматика и мехатроника", Русенски университет "Ангел Кънчев", тел.: 082 888 377, e-mail: daskalov@uni-ruse.bg

Разработване на симулатор на светофарна уредба с програмируеми логически контролери.

Автор: Георги Тодоров
Научен ръководител: доц. д-р Цветелина Георгиева

Development of a traffic light simulator with programmable logic controllers. *Developed traffic light simulator with programmable logic controllers is presented in the paper. For the purpose is used easySoft CoDeSys software platform. This software allow to simulate the traffic ligths without real controller connected to the computer, modify and upgrade of developed simulator.*
Keywords: *Programmable Logic Controller, easySoft CoDeSys, traffic ligths*

УВОД

Непрекъснатото нарастване на обема на движението на различните видове транспорт налага проучване на основните параметри и закономерности, с цел правилната му организация и управление.

С наредба за регулиране на движението по пътищата със светлинни сигнали се определят видовете светлинни сигнали, които се използват за регулиране движението на пътните превозни средства и на пешеходците по пътищата, отворени за обществено ползване, както и условията, редът, местоположението, начинът за поставяне и изискванията към пътните светофари, които подават тези сигнали. Светлинните сигнали се подават от пътни светофари. Пътният светофар се състои от една или повече отделно обособени светофарни секции, всяка от които излъчва светлина с определен цвят и посока.

Пътни светофари се поставят, както следва:

- в населените места – съгласно проект за организация на движението, разработен въз основа на генералния план за организация на движението;
- извън границите на населените места – в съответствие с проекта за организацията на движението по пътя.

В зависимост от предназначението си пътните светофари са за регулирането на движението на:

- пътните превозни средства на кръстовищата, пешеходните пътеки, стеснени и други участъци от пътя;
- пътните превозни средства по отделна пътна лента;
- трамваите;
- пешеходците;
- пътните превозни средства на железопътен прелез.

Поради това, че светофарните уредби са различни по вид и предназначение и всяко кръстовище има своята специфика е необходимо да се разработи симулатор на светофарна уредба.

Целта на доклада е да се разработи симулатор на светофарна уредба базиран на програмируем логически контролер.

ИЗЛОЖЕНИЕ

1. Изисквания към техническите средства, използвани за регулиране на движението със светлинни сигнали

Светофарните уредби и техническите средства, използвани за тяхното изграждане, трябва да отговарят на изискванията на БДС 13261

"Системи телеавтоматични и автоматизирани за управление на пътното движение. Технически изисквания. Видове и основни параметри. Технически

изисквания" и на БДС 16102 "Светофари, пътни знаци и маркировка. Свето - технически изисквания".

Пътните светофари, използвани за регулиране на движението по пътищата, трябва да отговаря на следните изисквания:

1. всяка секция на пътния светофар има самостоятелен източник на светлина, независим от източниците на останалите секции;

2. светещите полета на пътния светофар са равномерно осветени;

3. източниците на светлина, използвани в пътните светофари, са с повишена надеждност и трайност;

4. всяка светофарна секция има сенник (козирка), чиято конструкция позволява подобрена видимост на сигнала от участниците в движението, за които той е предназначен, и ограничава видимостта му за участниците в движението, за които не се отнася;

5. конструкцията на светофарните секции е такава да може на ограничава възможността за получаване на "фантом ефект".

Устройството, което управлява смяната на светлинните сигнали на светофарите (контролера), трябва да отговаря на следните условия:

1. да осигурява възможност за регулиране продължителността на светофарния цикъл и на основните и спомагателните тактове през 1s;

2. да има защита срещу едновременното включване на зелена светлина с червена и/или жълта светлина от един светофар;

3. да осигурява защита срещу подаване на сигнал от една светофарна уредба, с които се разрешава едновременното преминаване на превозни средства в конфликтните направления;

4. да осигурява защита срещу подаване на сигнал, който разрешава преминаване в дадено направление, при отсъствие на сигнал, който забранява преминаването на пътни превозни средства в конфликтните му направления;

5. да осигурява контрол за правилната работа на светофарните секции, с които се подават сигналите с червена светлина;

6. да осигурява автоматично изпълнение на преходните интервали при ръчно превключване на светлинните сигнали;

7. да има защита срещу нарушаване последователността на подаване на светлинните сигнали;

8. да има защита срещу блокиране работата на светофарната уредба, в резултат на което продължителността на светофарния цикъл става по – голяма от 150s;

9. при възникване на неизправност, която застрашава безопасността на движение, да осигурява автоматично преминаване на светофарната уредба в режим на работа „жълта мигаща светлина".

При работа на светофарната уредба в режим на ръчно управление операторът определя продължителността на сигналите, с които се разрешава и забранява преминаването през регулираното място (основните тактове). Продължителността на преходните сигнали между основните тактове се задава предварително и се изпълнява автоматично.

При работата на светофарната уредба в режим на автоматично управление продължителността на светофарния цикъл и на подаваните светлинни сигнали, моментът на тяхната смяна, както и продължителността на преходните интервали:

а) могат да бъдат определени предварително – твърдо програмно управление;

б) могат да се определят в процеса на работа на светофарната уредба в съответствие с параметрите на транспортните и пешеходните потоци, чието движение се регулира – гъвкаво управление.

2. Избор на програмируем логически контролер и софтуерна среда за симулация и управление на светофарна уредба

Контролерът е гъвкава микропроцесорна система, позволяваща реализация на различни негови конфигурации в съответствие с потребителските нужди при висока надеждност и експлоатационни качества. Той е предназначен за регулиране на уличното движение при различни по организация и сложност кръстовища. Неговата модулност, ремонтно пригодност чрез инженерен пулт, компактност, удължения експлоатационен живот на ел. лампите в светлинните секции, също функционалните му и схемни решения позволяват чрез специфично програмно осигуряване и управление, да бъдат изпълнявани широк кръг от технически задания.

Избран е компактен логически програмируем контролер easyControl [6], който притежава функционален дизайн както за управление на машини, така и за системи и се характерезира със следното:

- гъвкави интерфейси CANopen или easyNet - комбинирания интерфейс CAN позволява да се избере собствена мрежова структура;
- лесни актуализации – слотът за модула памет прави актуализациите на програмите или вградените програми (фърмуера) лесно и достъпно от потребителите;
- вграден Ethernet – Ethernet интерфейсът дава възможност за лесно интегриране на EASY Control. Това опростява програмирането и съединенията, например на системи за визуализация чрез OPC.;
- удобна работа – като единствен компактен програмируем логически контролер с вграден и дистанционен дисплей EASY Control дава възможност за проста работа и визуализация.

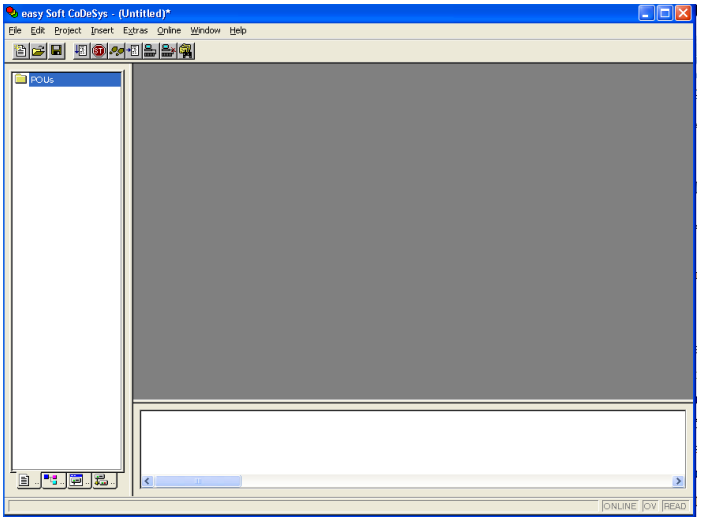
На фиг. 1 е показан лицевият панел на програмируем контролер от серията EASY Control.

Фиг. 1. Лицев панел на програмируем контролер (ПК) от серията EASY Control.

EasyControl се програмира с програмния продукт easySoft-CoDeSys в съответствие с IEC 61131-3. EasySoft-CoDeSys е система за програмиране, основана на CoDeSys 3S за промишлени PLC. Мощните технически възможности, лесната работа и широкото използване на този софтуер в компонентите за автоматизация на различни производители са гаранция за успех.

При необходимост от графичен език за програмиране, например схема на функционален блок, многостъпална схема, схема на последователни функции, или текстово програмиране – списък с инструкции или структуриран текст е целесъобразно да се използва easySoft-CoDeSys за програмиране. Има възможност

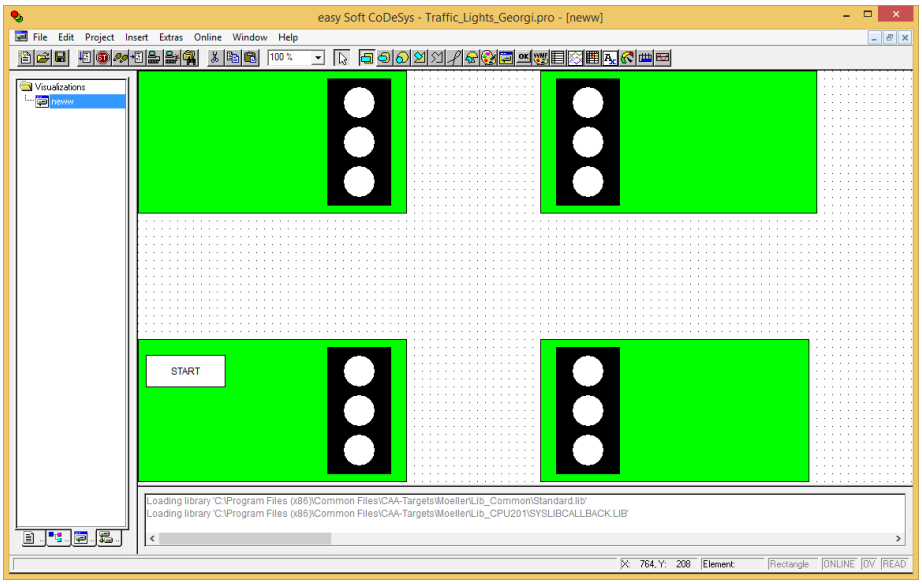
да се разработи симулатор на конкретна задача, без да се налага свързване на контролер. За тази цел easySoft-CoDeSys предлага няколко функции за програмна симулация. Не се налага да се използва различен операторски интерфейс, тъй като манипулациите са еднакви, както при работа онлайн със свързания контролер.
На фиг. 2. е показан основният прозорец на програмното средство easySoft-CoDeSys.



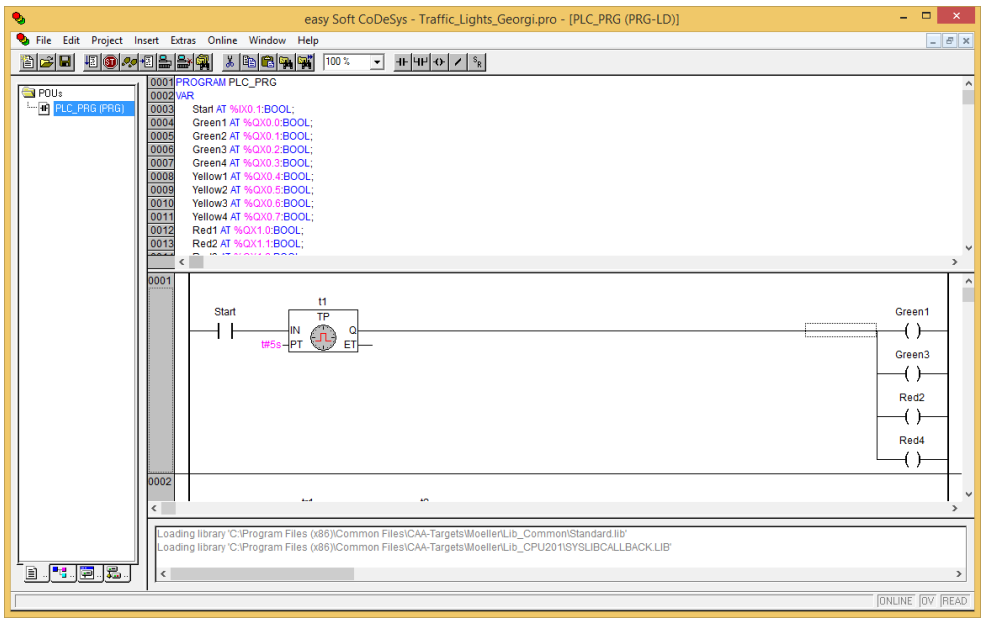
Фиг. 2. Основен прозорец на easySoft-CoDeSys

В долната лява част на прозореца са разположени четири бутона: POUs (програмируеми организационни единици), Data type (тип данни), Visualizations (визуализации) и Resources (ресурси). В долният ляв прозорец (message window) се съдържа всички съобщения от предшестващите компилации или сравнения. При двойно щракване с мишката върху даденото съобщение (грешка) в програмата се маркира реда в който се съдържа грешката.

Разработеният симулатор на светофарна уредба е представен на фиг. 3, а разработената програма на фиг. 4.



Фиг. 3. Разработен симулатор на светофарна уредба



Фиг. 4. Разработена програма на светофарна уредба

ЗАКЛЮЧЕНИЕ

В доклада е представен разработен симулатор на светофарна уредба. За програмна среда е използвана easySoft-CoDeSys, която позволява симулация без наличие на реален контролер, модифициране и надграждане на разработения симулатор с цел тестване на различни варианти на светофарните уредби.

ЛИТЕРАТУРА

[1] Даскалов П. Компютърни системи за управление (Ръководство за лабораторни упражнения), Русе, Русенски университет „Ангел Кънчев", 2006.
[2] www.moeller.bg

За контакти:

Георги Тодоров, студент, Русенски университет „Ангел Кънчев", Факултет „Електротехника, електроника и автоматика", катедра „Автоматика и мехатроника", e-mail: gochko55@abv.bg

доц. д-р инж. Цветелина Георгиева, Катедра "Автоматика и Мехатроника", Русенски университет "Ангел Кънчев",тел.:082–888 668;e-mail: cgeorgieva@uni-ruse.bg

ИЗСЛЕДВАНЕ НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ТЕМПЕРАТУРАТА В СУШИЛНЯ

автор: Георги Петров
научни ръководители: доц. д-р Донка Иванова, гл. ас. д-р Николай Вълов

Research of temperature control system in drill: *In this paper is presented regulation of the temperature and velocity of the incoming airflow in the dryer. For this purpose, various regulators are being studied which will regulate the drying agent parameters and select a regulator that satisfies a defined drying process quality.*

Key words: *Drying, setting of temperature controller.*

ВЪВЕДЕНИЕ

Сушенето на земеделска продукция е използвано преди стотици години по нашите територии. Използваните методи са се базирали на естествените енергоизточници - слънчевите лъчи. Основен недостатък на този метод е голямата продължителност, а от там също така зависимостта от атмосферни условия. Този метод е неприложим и от гледна точка на съвременните изисквания за хигиена на процеса. За производството на по-големи количества сушени плодове и зеленчуци са пригодени сушилни, използващи дърва за загряване на продуктите и от там принудителното им изсушаване. Скъсявано е времето на процеса, но много често готовата продукция е имала твърди примеси и неприятен мирис. За качеството на готовата продукция от съществено значение е контролирането на параметрите на сушилния агент по време на самия сушилен процес.

Промишлените сушилни имат висока производителност, осигуряват постоянни, предварително зададени, параметри на сушилния процес и добро качество на продукцията.

Основният проблем при промишлените сушилни е, че имат високи енергийни разходи. Това определя нуждата от управление на сушилния процес, така че да се постигнат възможно най-ниски енергийни разходи за протичането му. Сушенето, като типичен топло и масообменен процес, е процес, който позволява управлението на параметрите на сушилния агент постъпващ в сушилната камера [1]. Целта на управлението на параметрите на обдухващия поток постъпващ в камерата, е да се постигне по-добро бързодействие и енергопотребление на процеса, при текущите стойности на параметрите на атмосферния въздух и запазване на хранителните качества на суровините е особено актуално.

ИЗЛОЖЕНИЕ

ТЕХНИЧЕСКА ЕКИПИРОВКА НА ЕКСЕРИМЕНТАЛНАТА СУШИЛНЯ

Основни процеси, протичащи при процеса сушене, са свързани с отделянето на водата от вътрешността (сърцевината) на изсушаваните материали към повърхността, след което тези водни капчици се откъсват от потока на сушилния агент към атмосферата. Определящи фактори за сушенето са: температурата и скоростта на сушилния агент и второстепенни продължителността на процеса във времето и влагосъдържанието на сушилния агент. Основното количество енергия в сушилния процес е необходимо за загряването на сушилния агент. От друга страна, необходимата енергия е различна през отделните фази, през които протича сушилния процес. Поради тези причини е наложително да се изготви адекватна система за измерване и управление на посочените фактори. Използваната електронагревателна пещ в значителна степен наподобява масово използваните

индустриални сушилни камери. Обемът на сушилната камера, с която реализиран проекта е 0.5m^3, фиг.1.

Фиг.1.Експериментална сушилна камера

Камерата е с двойно дъно, като във въздушните междини са монтирани горен и долен нагревател, всеки от които е с мощност 1000W. Подбраната мощност е достатъчна за загряване на сушилия агент до 400℃, но при сушенето на плодове и зеленчуци е недопустимо загряване над 100℃ [1]. Тази по-висока инсталирана мощност на нагревателите способства за повишената динамика при установяване на зададена температура на агента, особено в началните фази, когато като правило имаме по-голяма температурна разлика между околната температура и нужната температура на сушилния агент.

За циркулация на въздуха в камерата се използва осев вентилатор с електрическа мощност 180W. За прецизно регулиране на скоростта на въздушния агент се използва честотен преобразувател за захранваване на вентилатора.

Съществуващите промишлени сушилни са проектирани и конструирани, така че да не допускат съществени изменения и настройки на предварително зададените параметри - температура и скорост на сушилния агент. С цел намаляване на енергийните разходи е необходимо регулиране на всички параметри, влияещи на сушилния процес и то в широки граници, при различните плодове и зеленчуци.

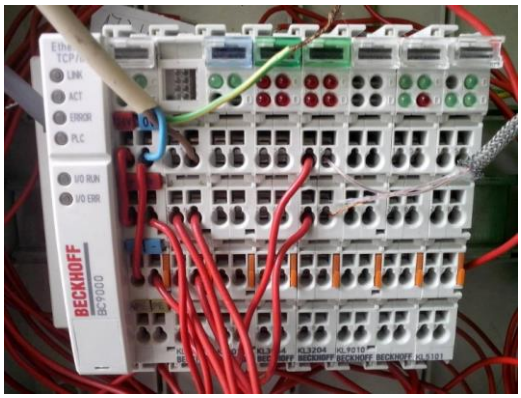
Граничните стойности, в които се променят указаните параметри, са: температура θ - 28÷90℃; относителната влажност на въздуха φ - 15÷99%; скорост на въздуха v - 0.5÷1.5m/s.

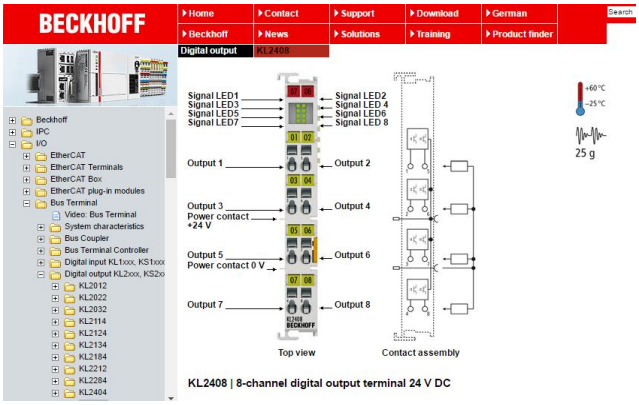
За управлението на температурта в сушилнята избираме PLC–контролер на производителя "BECKHOFF"[2], фиг.2.

Загряването на въздуха в сушилнята в сушилнята камера се осъществява посредством двата нагревателя с мощност 1000W всеки. Комутацията им към електрическата мрежа е реализирана през синхронно токов ключ (SSR-реле) - CELDUC SC942160 [3]. Синхронно токовият ключ служи, като изпълнителен механизъм в системата.

ЕКСЕРИМЕНТАЛНО СНЕМАНЕ НА ПРЕХОДНАТА ХАРАКТЕРИСТИКА НА ОБЕКТА

Преходната характеристика представлява реакцията на обекта във функция от времето при подаване на стъпално въздействие на входа му. Преди подаване на стъпално въздействие обектът трябва да бъде приведен в равновесно състояние, при което изходът му да е стабилизиран в дадена работна точка. При прилагане на стъпалното въздействие, след протичане на преходния процес, изходът му се установява в ново равновесно състояние.



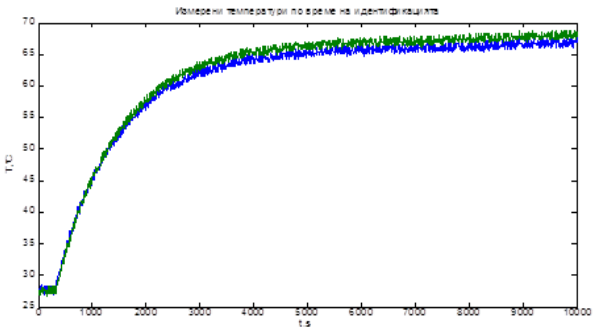


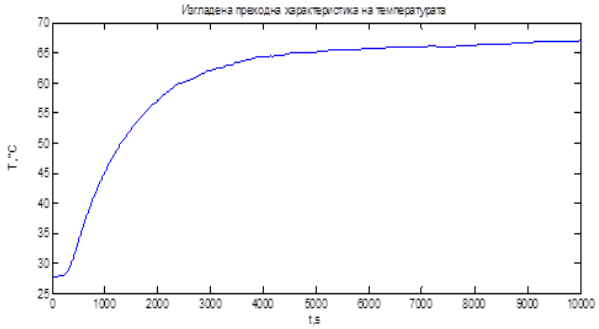
а) б)

Фиг.2. PLC контролер BC9000 на BECKHOFF и разширителен модул KL2408

За тези обекти теоретично установяването на изходната величина трае безкрайно дълго време. Но в практиката се счита, че преходния процес е приключил, когато вече не се регистрира изменение на изходната величина.

Най-често за намиране на параметрите на обекта, се извършва идентификация на обекта който ще се управлява на основата на експериментално снетата му преходна функция, фиг.3. Идентификация на обекта се извършва, чрез използването на System Identification Tool от програмата MATLAB. Определят се параметрите на обекта, апроксимиран с апериодично звено от първи ред със закъснение.





а) б)

Фиг.3 Експериментално снети и изгладена преходни характеристики на температурата в сушилната камера

Параметрите на обекта получени след идентификацията са:

$$W(s) = \frac{k_0 e^{-\tau_0 s}}{T_0 s + 1} \qquad (1)$$

$k_0 = 1.58$ – коефициент на пропорционалност на обекта

$\tau_0 = 180s$ – чисто закъснение

T_0=1389.36s – времеконстанта на интегриране

След идентификацията избираме регулатор и определяме параметрите му съгласно методиката 0 на Циглер-Никълс. Коефициентът на пропорционалност k_p за регулатора при П-закон е:

$$k_p = \frac{T_0}{k_0 \tau_0} = \frac{1389.36}{1.58 \times 180} = 4.88 \qquad (2)$$

Изчислените параметри на регулатора при ПИ-закон са:

$$k_p = \frac{0.9T_0}{k_0 \tau_0} = \frac{0.9 \times 1389.36}{1.58 \times 180} = 4.4 \qquad (3)$$

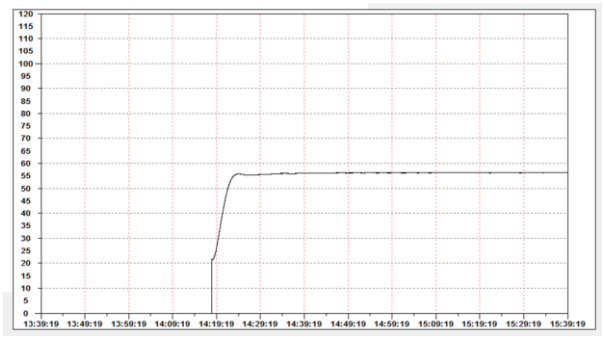
$$T_I = 3.3\tau_0 = 3.3 \times 180 = 594s \qquad (4)$$

$T = 1s$

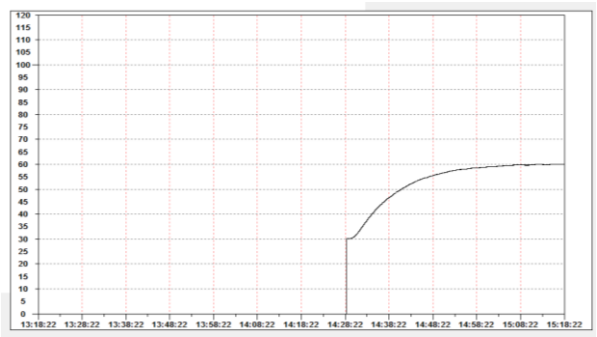
На фиг.4а е показана експериментално снетата преходна характеристика по задание θ=60℃ на системата с П-регулатор. Очевидно е, че има грешка в установен

режим и времето за установяване е 10 минути. Грешката може да бъде компенсирана, чрез увеличение на коефициента k_p.

Преходна характеристика на системата с ПИ-регулатор е представена на фиг.4б. При тази конфигурация на системата, грешката в установен режим е 0 и преходния процес е апериодичен, но времето за установяване е 30 минути.



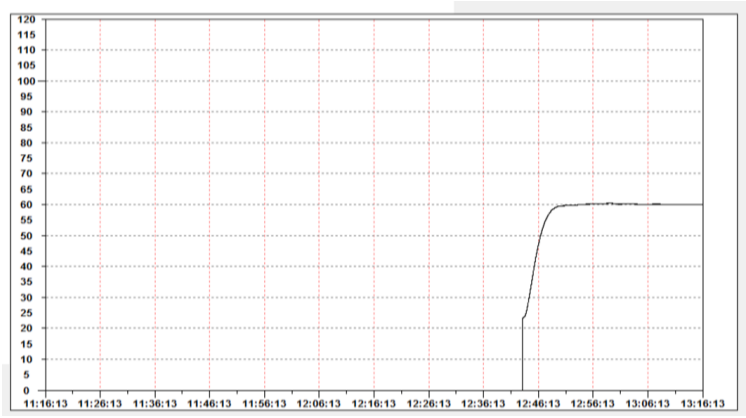
а)П-закон



б)ПИ-закон

Фиг.4 Преходни характеристики с различни регулатори

След допълнителна настройка на параметрите на регулатора, избираме *Ti*=300s и се реализира преходният процес показан на фиг.5. Температурата се установява за 5 минути и няма статична грешка в установен режим.



Фиг.5 Преходен процес след допълнителната настройка на ПИ-регулатора

ЗАКЛЮЧЕНИЕ

Желана температура от 60℃ при системата с П-регулатор, ясно се вижда от преходната характеристика, че не се установява. За това по-подходящо е използването на ПИ-регулатор в системата. Настойката на ПИ-регулатора е адекватна за скорост на сушилния агент 1.5m/s, но ако се работи с различна, се налага отново корекция на параметрите на регулатора.

ЛИТЕРАТУРА

[1] Абтишев, Д. З., Дипломен проект-"Регулатор на температура в експериментална сушилня". Русенски университет "Ангел Кънчев", 2015.
[2] https://www.beckhoff.com/
[3] https://vikiwat.com

За контакти:

Георги Илиев Петров, катедра "Автоматика и мехатроника", Русенски университет "Ангел Кънчев", e-mail: joropetroov@abv.bg

доц. д-р Донка Иванова, Русенски университет "Ангел Кънчев", Катедра „Компютърни системи и технологии", тел.: 082-888 266, e-mail: divanova@uni-ruse.bg.

Комбинирано захранване с електрическа и топлинна енергии на промишлено предприятие

автор: Богдан Йорданов
научни ръководители: проф. д- р.инж. Иван Палов, доц. д-р инж. Кирил Сираков

Combined power supply with electric and thermal energy to an industrial plant: *The possibility of a combined power supply to an industrial plant with thermal and electrical energy was studied. Four options are considered to provide the energies needed for an average production plant. Consideration has been given to the consumption and characteristics of four variants for the production and / or delivery of the respective energy carriers. An assessment has been made of the four options based on the heat and electricity consumed by the plant.A base option is selected and the others are compared. Data on energy consumption and costs are presented for each option. After the calculations made, the most appropriate of them is recommended.It has been found that the most cost-effective and environmentally friendly option is the one with the application of a cogeneration plant.*

Key words: *Cogeneration systems, Water heaters, Electric power system, Heat power plants.*

ВЪВЕДЕНИЕ

Проблемите, свързани с производството на топлинна и електрическа енергии през последните десетилетия, постоянно нарастват. Основни фактори за това са: опазването на околната среда – намаляване на отделяните вредни емисии, развитието на алтернативните източници на енергия, максимално оползотворяване на енергоносителите, повишаване на цените за топлинна и електрическа енергии, и др.

В доклада се разглеждат четири варианта за осигуряване на нужните енергии за средно производствено предприятие. Първият от тях е комбинираното производство на топлинна и електрическа енергии от когенератор. Според [10] когенераторите са се наложили като най-енергийно ефективен метод за усвояване на енергията от първоизточника, било то изкопаеми горива, биомаса или др. Лесно приложими са за централни отоплителни системи на сгради, болници и заводи [1,2]. При втори и трети вариант за производство на топлинна енергия се използва водогреен котел, а електрическата енергия се доставя от електроенергийната система (ЕЕС). При четвърти вариант топлинната и електрическата енергии се доставят от топлоелектрическа централа (ТЕЦ), а електрическата енергия се доставя от ЕЕС. Този вариант е приет за базов и спрямо него се определят технико-икономическите параметри.

Целта на доклада е да се определят основните технико-икономически параметри и да се предложи икономически целесъобразен вариант за комбинирано захранване с топлинна и електрическа енергии на промишлено предприятие.

ИЗЛОЖЕНИЕ

При първият вариант за производство на топлинна и електрическа енергии се използва когенератор. За изчисляване на необходимата мощност на съответния когенератор могат да се използват различни методи. В [1] е синтезирана методика за ефективен избор по технически условия. Правилният избор на мощността е много важен за техническата и икономическа ефективност от инсталирането на когенератор и неговото използване. Тъй като често се случва вече инсталирани когенераторни системи да не са правилно подбрани и заради това те не се използват пълноценно. Заради това е от първостепенна важност първоначалните проучвания на обекта да се извършват от квалифицирани специалисти в съответните области [1,2].

На фиг.1. е показан общ вид на модулен когенератор.

Фиг.1. Общ вид на когенераторен модул

След направено проучване, са сравнени параметрите [3,5,6,11] на основните характеристики за различни видове когенератори. За изследваното предприятие е избран когенератор тип: „Vitobloc 200–EM-30/660". Основните характеристики на този когенератор са:

Вид гориво	Отдавана активна електрическа енергия, kW	Отдавана топлинна енергия, kW	Консумация на гориво	Коефициент на полезно действие
Природен газ/биогаз	530	698	1395 kW	0,88

За определяне на инсталационните и експлоатационните разходи на когенератора са използвани усреднени данни от литературни източници. В табл.1. са представени стойностите за инсталационните разходи [4], и тези за поддръжка и експлоатация на различни типове когенератори.

Таблица 1.

Разходи за когенератори използващи различни двигатели

Двигател	Инсталационни разходи	Разходи за експлоатация и поддръжка
Бутален	$1 000 до $1 800 за kW	$0,010 до $0,015 за kWh
Газотурбинен	$800 до $1 500 за kW	$0,005 до $0,008 за kWh
Микротурбинен	$1 000 до $2 000 за kW	$0,010 до $0,015 за kWh

При втори вариант за производството на топлинна енергия се използва водогреен котел на природен газ, а електрическата енергия се закупува от ЕЕС. За този вариант е нужно да се избере водогреен котел и нужната му горелка. След направено проучване, са сравнени параметрите [7,8,9,12] на основните характеристики за различни видове котли. За изследваното предприятие е избран водогреен котел тип: „UNITHERM - YA465". Основните характеристики на този котел са:

Вид гориво	Отдавана топлинна енергия, kW	Цена за котел, лв.	Цена за горелка, лв.
Природен газ	540	6 512	6 033

За нужната горелка също е направено проучване, сравнени са параметрите [7,8,9,12] на основните характеристики за различни видове горелки. За изследваното предприятие е избрана горелка за водогреен котел тип: „TWIN 70/2-E 213". Основните характеристики на тази горелка са:

Вид гориво	Отдавана топлинна енергия, kW	Консумация на гориво
Природен газ	543	74,4 m^3/h

При трети (А) вариант за производството на топлинна енергия се използва водогреен котел на дървесен чипс, а електрическата енергия се закупува от ЕЕС. За този вариант е нужно да се избере водогреен котел и нужната му горелка. След направено проучване, са сравнени параметрите [7,8,9,12] на основните характеристики за различни видове котли. За изследваното предприятие е избран водогреен котел тип: „Centrometal - EKO-CKS 500". Основните характеристики на този котел са:

Вид гориво	Отдавана топлинна енергия, kW	Цена за котел, лв.	Цена за горелка, лв.
Дървесен чипс	500	109 000	13 943

За нужната горелка също е направено проучване, сравнени са параметрите [7,8,9,12] на основните характеристики за различни видове горелки. За изследваното предприятие е избрана горелка за водогреен котел тип: „Pasian BP- BP 550". Основните характеристики на тази горелка са:

Вид гориво	Отдавана топлинна енергия, kW	Консумация на гориво
Дървесен чипс	550	50 kg/h

При трети (Б) вариант за производството на топлинна енергия се използва водогреен котел на пелети, а електрическата енергия се закупува от ЕЕС. За този вариант е нужно да се избере водогреен котел и нужната му горелка. След направено проучване, са сравнени параметрите [7,8,9,12] на основните характеристики за различни видове котли. За изследваното предприятие е избран водогреен котел тип: „ThermoStahl - MCL BIO 450". Основните характеристики на този котел са:

Вид гориво	Отдавана топлинна енергия, kW	Цена за котел, лв.	Цена за горелка, лв.
Пелети	522	49 000	13 943

За нужната горелка също е направено проучване, сравнени са параметрите [7,8,9,12] на основните характеристики за различни видове горелки. За изследваното предприятие е избрана горелка за водогреен котел тип: „Pasian BP- BP 550". Основните характеристики на тази горелка са:

Вид гориво	Отдавана топлинна енергия, kW	Консумация на гориво
Пелети	550	50 kg/h

Четвърти вариант е когато предприятието да закупува нужната топлинна и електрическа енергии от ТЕЦ и ЕЕС.

Производственото предприятие работи на трисменен режим, непрекъснато в продължение на 330 дни през годината. Топлинният и електрическият му товарови графици са постоянни. Средната консумация на топлинна енергия е 450 kwh, а на електрическа енергия е 350 kwh.

Базисни цени за различните видове горива, както и емисионните фактори за тях към 01.2017г. са представени в табл. 2.

На базата на горните данни са направени изчисления за технико-икономическите параметри за четирите варианта. Конкретните стойности за съответните параметри са представени в табл. 3.1. и табл. 3.2.

Таблица .2.

Данни за енергоносителите

Вид гориво	Цена	Емисионни фактори
		t/MWh
Дървесен чипс	110,00 лв./t	0,043
Електрическа енергия	137,56 лв./MWh	0,819
Пара от ТЕЦ	81,41 лв./MWh	0,29
Пелети	280,00 лв./t	0,043
Природен газ	50,58 лв./MWh	0,202

Таблица 3.1.

Резултати 1 изчисления за предложените варианти за захранване на малко предприятие

№ Вар.	Видове източници на енергия	Консумация	Общ разход на енергия	КПД	Разход на гориво/енергия	Общ годишен разход за енергия	Разход за енергия
		MWh/год	MWh/год		MWh/год	хил. лв./год	хил. лв./год
1.	Електрическа енергия от когенератор	2 772	6 336	0,88	7 200	400,170	364,170
	Топлинна енергия от когенератор	3 564					
2.	Електрическа енергия от мрежата	2 772	6 336	-	2 772	614,724	381,316
	Топлинна енергия от газов котел	3 564		0,78	4 569		231,108
3.А	Ел.енергия от мрежата	2 772	6 336	-	2 772	644,454	381,316
	Топлина енергия от котел на пелети	3 564		0,72	8 800		207,413
3.Б	Ел.енергия от мрежата	2 772	6 336	-	2 772	914,678	381,316
	Топлина енергия от котел на дървесен чипс	3 564		0,75	8 448		506,843
4.	Електрическа енергия от мрежата	2 772	6 336	-	2 772	671,461	381,316
	Топлинна енергия от ТЕЦ	3 564		-	3 564		290,145

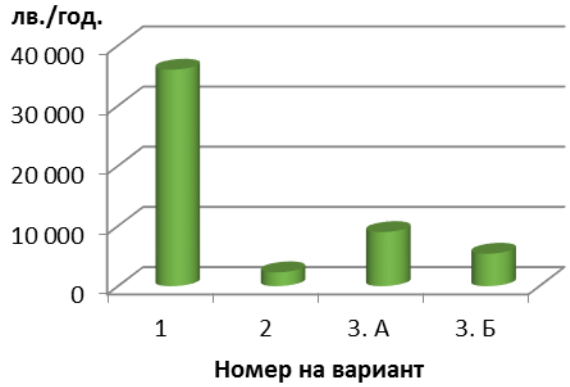
Таблица 3.2.

Резултати 2 изчисления за предложените варианти за захранване на малко предприятие

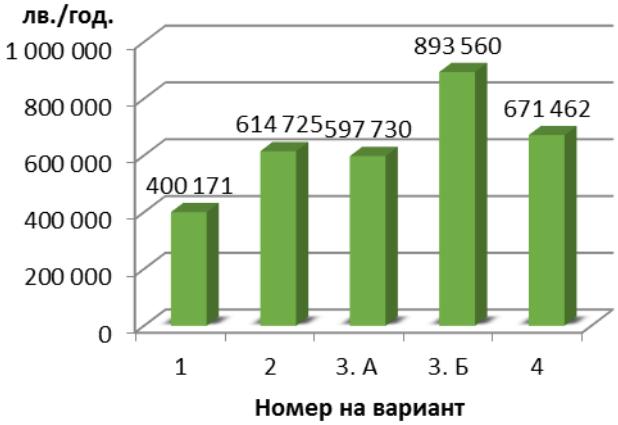
№ Вар.	**Видове източници на енергия**	**Годишни експлоата-ционни разходи**	**Обща специ-фична цена**	**Икономия спрямо базовия вариант**	**Намаление на разходите за енергия спрямо базовия вариант**	**Необходими инвестиции**	**Въглеродни емисии**	**Срок на откупуване**
			лв./MWh	лв.		Лв.	t/год.	год
1.	Електрическа енергия от когенератор Топлинна енергия от когенератор	36 000	63,16	271 290,90	40,40%	1 862 264	1 454	6,86
2.	Електрическа енергия от мрежата Топлинна енергия от газов котел	2 300	97,02	56 736,94	8,45%	12 547	3 193	0,22
3.А	Ел.енергия от мрежата Топлина енергия от котел на дървесен чипс	9 000	101,71	73 731,48	10,98%	122 943	2 649	1,67
3.Б	Ел.енергия от мрежата Топлина енергия от котел на пелети	5 400	144,36	-222 098,56	-33,08%	62 943	2 634	-
4.	Електрическа енергия от мрежата Топлинна енергия от ТЕЦ	- -	105,98	-	0,00%	-	 3 304	-

На фиг.2. са показани годишните експлоатационни разходи. От графиката може да се констатира, че при използване на когенератор (вариант 1), има най-висок дял на разходите. Докато при използване на котел на газ (вариант 2) те са най-ниски.

На фиг.3. е представен общият годишен разход за енергии. От графиката се установява, че при когенераторна уредба, тези разходи са най-малки в сравнение с останалите варианти – 400 хил. лв. Вариантът (3.Б.) с употреба на котел на пелети е най-скъп и възлиза на 893 хил. лв. Това прави този вариант практически неприложим. При останалите варианти за доставяне на енергии резултатите са сравнително близки по стойност на годишните разходи за енергии.



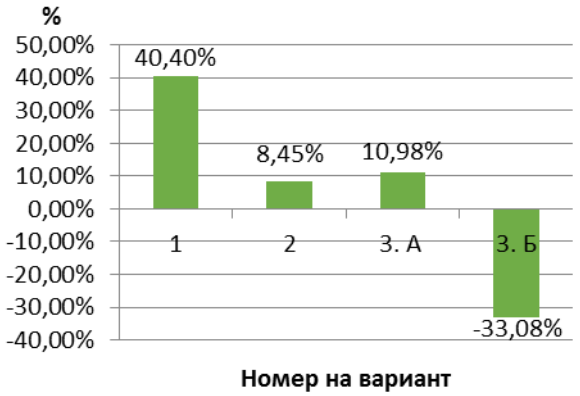
Фиг.2. Годишни експлоатационни разходи



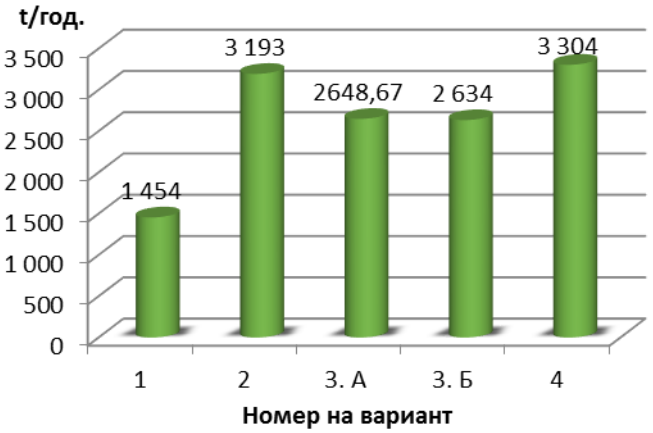
Фиг.3. Общ годишен разход за енергии

На фиг. 4. е посочено процентното намаляване на разходите за енергии спрямо базовия вариант - 4, закупуването на топлинна енергия от ТЕЦ и електрическа енергия от ЕЕС. Могат да се констатират следните резултати. При използване на когенератор, ще има около 40% намаляване на разходите за топлинна и електрическа енергии, докато при варианта 3.Б. с използване на котел на пелети има дори отрицателна стойност. Това е така, тъй като този вариант е с по-високи разходи от базовия. Варианти 2. и 3.А. са близки по стойност и намаляването на разходите за енергии са в границите на (8…10)%.

На фиг.5. са представени количествата на отделяните въглеродни емисии при производството на определеното количество енергии за всеки от вариантите. От графиката се установява, че при вариант 1. - с когенератор, отделените вредни емисии в атмосферата са най-малки – 1 454 t/год. Отделяните вредни емисии при варианти 3.А. и 3.Б. са около 2 600 t/год, а при варианти 2 и 4 те са малко над 3 000 t/год.



Фиг.4. Намаление на разходите за енергии спрямо базовия вариант

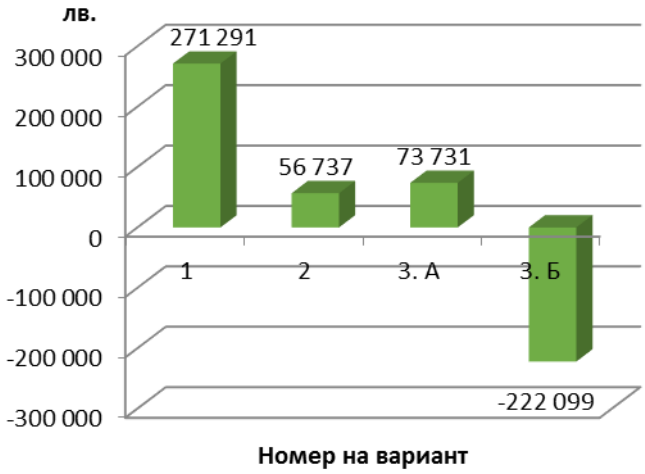


Фиг.5. Въглеродни емисии

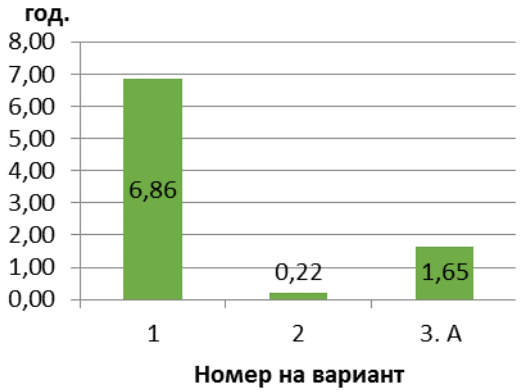
На фиг.6. е показана икономията на средства за енергия спрямо базовия вариант. Може да се констатира, че при първи вариант спестените средства са над 271 хил. лв./год. При вариант 3.Б. има повишение на разходите спрямо базовия вариант и заради това се получава отрицателна стойност в графиката. При варианти 2 и 3.а. икономията е около (55…74) хил. лв./год.

На фиг.7. е представен срока на откупуване на икономически целесъобразните варианти за доставяне на топлинна и електрическа енергии за производственото предприятие. При използване на когенератор (вариант 1), той би бил около 7 години,

а ако се приложи котел на газ – вариант 2. срокът спада на под една година. При вариант 3.А. той е около 2 години. Вариант 3.Б. не се разглежда тъй като той е нерентабилен.



Фиг. 6. Икономия спрямо базов вариант



Фиг. 7. Срок на откупуване

ЗАКЛЮЧЕНИЕ

1. Установени са възможните варианти за комбинирано захранване с топлинна и електрическа енергии на разглежданото производство, а именно чрез: когенаратор; топлинна енергия от котел на газ + електрическа енергия от електроенергийната система (ЕЕС); топлинна енергия от котел на пелети + електрическа енергия от ЕЕС; топлинна енергия от котел на дървесен чипс + електрическа енергия от ЕЕС; топлинна енергия от ТЕЦ + електрическа енергия от ЕЕС.

2. Определени са годишните експлоатационни разходи за всеки вариант. Тези разходи при употреба на котел на газ са около 2,3 хил. лв.

3. Установени са общите годишни разходи при внедряването на отделните варианти. Най-големи разходи се получават при вариант 3.Б. – 893 хил.лв. При захранване с употреба на варианти 2, 3А. и 4. общият годишен разход е сравнително еднакъв и е в рамките на (597…671) хил.лв. Най-ниски са общите годишни разходи при прилагането на когенераторна уредба – 400 хил. лв.

4. Разходите за енергия в проценти, спрямо възприетия за базов вариант номер 4, показват, че при използването на когенератор икономиите могат да достигнат до 40%. При вариант 2. и 3.А. икономиите са (8…11)%. За вариант 3.Б. се получава повишаване на разходите с 33 % спрямо базовия.

5. Въглеродните емисии при вариант едно са близо два пъти по-ниски от колкото при останалите варианти и възлизат на 1454t/год.

6. Комбинираното производство на топлинна и електрическа енергии от когенератор е икономически ефективно и е свързано с отделянето на най-малко въглеродни емисии. Недостатък на този вариант са големите инвестиционни разходи и сравнително големия срок на откупуване.

ЛИТЕРАТУРА

[1] Русева В., К. Сираков, Ст. Стефанов, Ив. Палов, Методика за избор мощността на когенератор // Енергиен форум, Доклади, том 1, секция I, Топло – ядрена енергетика, газо и топлоснабдяване, секция IV Екология, възобновяеми източници на енергия, Варна, 2005, с. 404-407.

[2] Сираков К., В. Русева, Ст. Стефанов, Ив. Палов, Структура на електроенергийните връзки и режими на работа на когенераторна инсталация // Научни трудове на Русенски университет "Ангел Кънчев", т.41, с.3.1. Русе, 2004, с. 25-29.

[3] http://www.bosch-industrial.co.uk/files/BOSCH_CHP_Brochure_UK.pdf
[4] http://www.claverton-energy.com/38-hhv-caterpillar-bio-gas-engine-fitted-to-long-reach-sewage-works.html
[5] http://www.turboden.eu/en/products/products-chp.php
[6] http://www.evinoxenergy.co.uk/Sites/Evinox/library/files/CHP%20Data%20Sheet%202551128B.pdf
[7] http://www.izotermstil.com/bg/%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82-TWIN-E-TWIN-2-E-88.html
[8] http://www.izotermstil.com/files/1239743970_file_113_324.pdf
[9]http://www.thermodesigntotal.com/bg/p/607.%D0%9F%D0%B5%D0%BB%D0%B5%D1%82%D0%BD%D0%B0-%D0%B3%D0%BE%D1%80
%D0%B5%D0%BB%D0%BA%D0%B0-Pasian-BP
[10] https://en.wikipedia.org/wiki/Cogeneration
[11] https://energy.gov/sites/prod/files/2016/09/f33/CHP-Recip%20Engines.pdf
[12] http://www.thermodesigntotal.com/files/Instrukcii_sunM50_M70.pdf

За контакти:

Богдан Боянов Йорданов, Русенски Университет „Ангел Кънчев", специалност „Електроенергетика и електрообзавеждане", магистър, e-mail: bogi.y.93@gmail.com

Синтез на наблюдател на състоянието за управление на топлинен обект

автор: Владислав Толев
научни ръководители: доц. д-р Донка Иванова, гл. ас. д-р Николай Вълов

Design of a full-state observer control of the heat object*: Design of a full-state observer control of the heat object is presented in the paper. Observer is designed using the software packages for computer aided control system design - MATLAB® and Simulink.*

Key words: *full-state observer, heat object, control*

ВЪВЕДЕНИЕ

Използването на наблюдател на състоянието е приложимо за решаването на широк спектър от проблеми, като се започне от химическата и биотехнологическата промишленост до автоматизацията, автоматичния контрол, навигация, мехатроника и др.

Методите за анализ и синтез на системи за управление в пространство на състоянията намират широко приложение в практиката поради следните причини:

- Описанието в пространство на състоянията позволява задълбочено вникване в системата и нейните параметри в сравнение с класическите честотни методи. Най-общо казано честотните методи целят да определят входно-изходните променливи на системата, а при описание в пространство на състоянията също така се обръща внимание и на вътрешните променливи на системата;
- Желаната динамика на системата може лесно да се реализира чрез определяне на съответните полюси на системата;
- Голямо предимство е приложението при системи, където трябва да се управлява повече от една входна и една изходна величина;
- Синтезът на наблюдател на състоянието е наложително когато не всички променливи са пряко измерими;
- Приложими са както при линейни, така и при нелинейни системи и при системи променящи параметрите си във времето;

ИЗЛОЖЕНИЕ

Целта на настоящата статия е да се синтезира наблюдател на състоянието в система за автоматично управление на топлинен обект.

1. Описание на топлинния обект:

Обектът за упрвление е отопляемо помещение, с изходна променлива температурата в помещението, и управляващо въздействие – мощността на топлинния източник [1].

Предавателната функция на обекта е :

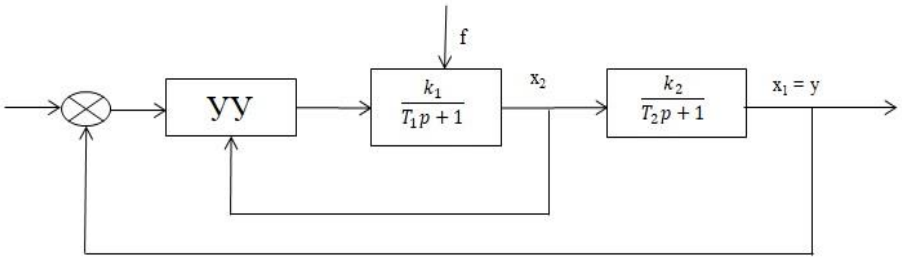
$$W(p) = \frac{k_1.k_2}{(T_1 p+1)(T_2 p+1)} \quad (1)$$

където k_1 и T_1 са параметри на отопляемото помещение,
k_2 и T_2 – параметри на термопреобразувателя.

Управляващото въздействие е ограничено по стойност

$$|u(t)| \leq U_m \quad (2)$$

Структурната схема на системата е представена на фиг. 2.1



Фиг. 2.1 Структурна схема на системата

Описанието на обекта с въведени променливи на състоянието x_1, x_2 :

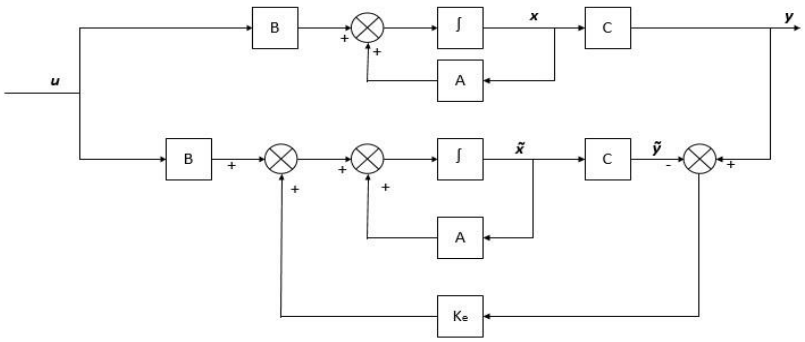
$$\frac{x_1}{dt} = \frac{k_2 x_2 - x_1}{T_2} \quad (3)$$

$$\frac{x_2}{dt} = \frac{k_1 u - x_2}{1} \quad (4)$$

Числените стойности на параметрите на топлинния обект са:
k_1 = 0.009 ˚C/W, k_2 = 1, T_1 = 700.2 s, T_2 = 30 s, U_m = 2400 W ;

2. Синтез на наблюдател на състоянието за топлинен обект

Основни изисквания при управление на топлинни обекти са икономичност по отношение на разхода на енергия и топлинен комфорт. За намаляване на разхода на енергия е необходимо да се следва определен денонощен температурен график за отопляване на помещението, в съответствие с които да се променя задаващото въздействие на системата. Понижаването на температурата в определени часове на денонощието води до икономия на енергия, но изисква, за да се поддържа определен топлинен комфорт, бързото му загряване при промяна на заданието. Управлението само по минимум на разхода на енергия води по увеличаване на продължителността на преходния процес. В съответствие с това е реализиран синтез на оптимално по бързодействие управление и синтез на оптимално по разход на енергия управление. Синтезираното упрваляващо устройство може да се приложи, ако се сумират всички променливи на състоянието. За повечето обекти променливите на състоянието или част от тях са недостъпни за измерване. В този случай се налага синтезирането на наблюдател на състоянието, при който се получават приблизителни, вместо самите променливи. Наблюдателят на състоянието е практически копие на обекта за управление – има същите входни въздействия и се описва с почти същите диференциални уравнения. Сравнява управляемата величина y с прогнозираната управляема величина y_1 [1, 2, 3]. Структурната схема е представена на фиг. 2.2.



Фиг. 2.2 Структурна схема на наблюдател на състоянията

Векторът на състоянието на една динамична система, включващ всички променливи на състоянието, съдържа достатъчното количество информация, което

позволява да бъде предсказвано поведението на системата, ако е известен нейният математически модел. В частност, отделни компоненти на вектора на състоянието могат да бъдат измеряеми, но в общия случай тези променливи са неизмеряеми. Използването на динамична система наричана наблюдател, която на базата на изходния сигнал **y(t)** и управляващото въздействие **u(t)** генерира оценката **x̃(t)** на вектора на състоянието **x(t)**, решава този проблем. Това позволява векторът на състоянието на наблюдателя **x̃(t)** да се използва за формиране на управляващото въздействие във вид на линейна обратна връзка по състояние **u(t)=-K x̃(t)**. Наблюдателят е динамична система, подчиняваща се на две принципни изисквания:

- При еднакви начални условия на обекта и наблюдателя, векторът на състоянието на наблюдателя трябва да е равен на вектора на състоянието на обекта с определена точност.
- При различни начални условия за обекта и наблюдателя, след определено време (времето на преходния процес на наблюдателя), първото условие също така трябва да е изпълнено.

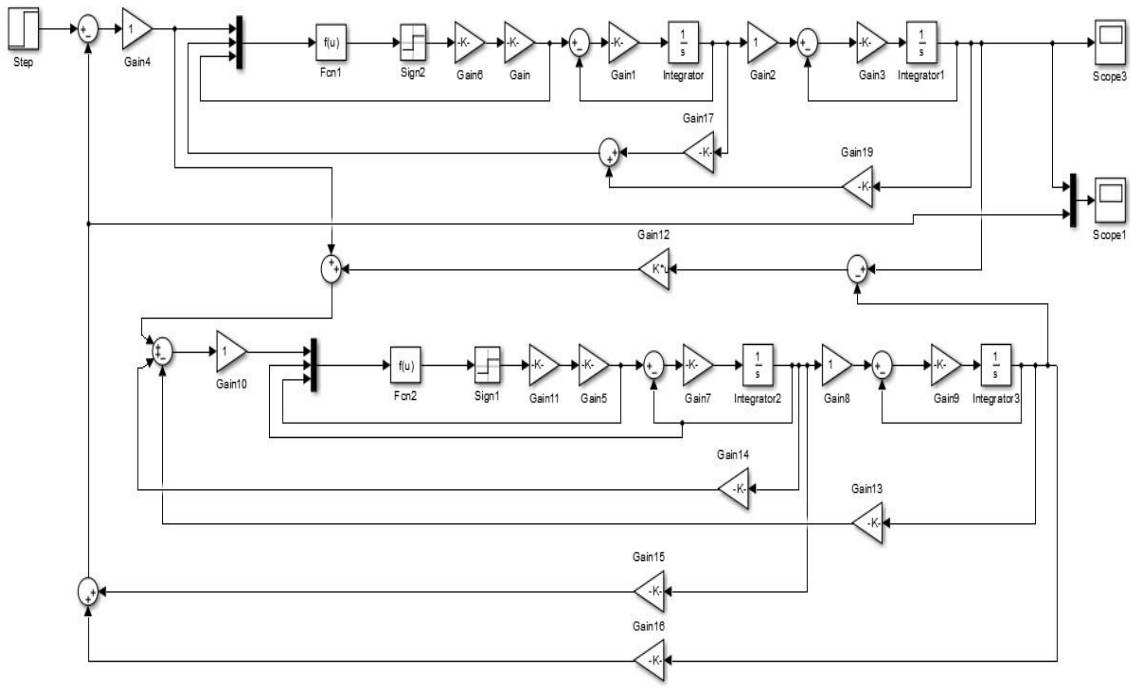
Нека описанието на линейната система, представляваща обект на управление, да има следния вид в пространството на състоянията:

$$\dot{x} = Au + Bu \quad (5)$$

$$y = Cu + Du \quad (6)$$

От тук следва да се изведат матриците на състоянието:

$$A = \begin{bmatrix} 0 & \cdot & 1 & 0 & \cdot & 0 \\ 0 & \cdot & 0 & 1 & \cdot & 0 \\ 0 & \cdot & 0 & 0 & \cdot & 0 \\ 0 & \cdot & 0 & 0 & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -a_n & \cdot & -a_{n-1} & -a_{n-2} & \cdot & -a_l \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ . \\ 1 \end{bmatrix}, \quad C=[1\ 0\ .\ .\ 0],\ D=b_0.$$



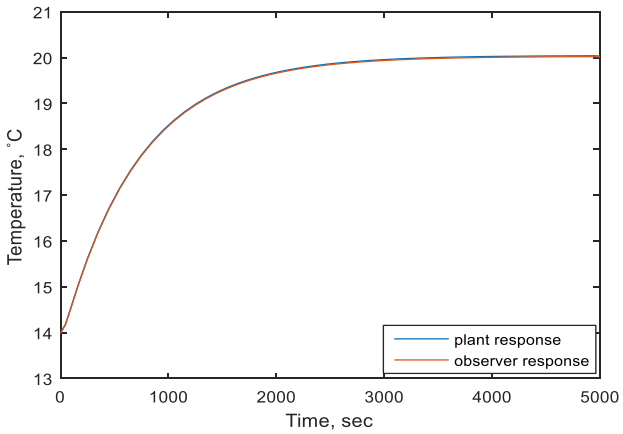
Фиг. 2.3 Simulink модел на системата

За да може да се проектира наблюдател на състоянието системата трябва да отговаря на следните условия:

- Управляемост - свойство, свързано с възможността за привеждане на обекта за управление от едно установено състояние в друго установено състояние с помощта

на управляващите въздействия. Необходимо и достатъчно условие за управляемост по състояние на линейната стационарна система е матрицата:
Q=$\begin{bmatrix} B & AB & A^2B & \ldots\ldots\ldots A^{n-1}B \end{bmatrix}$ да има ранг n, като n е размерност на вектора на състоянието.
-Наблюдаемост – свойство, свързано с възможността за намиране на вектора на състоянието по данни за вектора на изхода. Необходимо и достатъчно условие за наблюдаемост на линейна стационарна система е матрицата:
S=$\begin{bmatrix} C^T & A^TC^T & (A^T)^2C^T & \ldots\ldots & (A^T)^{n-1}C^T \end{bmatrix}$ да има ранг n.

За представяне на получния наблюдател на състоянията ще се използва Simulink. На фиг. 2.3 е представен Simulink модел на системата за управление на топлинен обект с наблюдател на състоянието. На фиг. 2.4 са показани изходната променлива на системата за автоматично управление на топлинен обект и изходната величина на наблюдателя на състоянието. Очевидно е, че двата преходни процеса съвпадат.



Фиг. 2.4 Сравнение между изходните реакции на топлинния обект и наблюдателя на състоянието

ЗАКЛЮЧЕНИЕ

Понякога променливите в една система не са достъпни за измерване или е прекалено скъпо да се измерват. Проектираният наблюдател на състоянието, представен в статията, дава възможност всички променливи в една система да бъдат известни и наблюдавани.

ЛИТЕРАТУРА

[1] Попова М., Д. Иванова, Н. Нойков. Оптимално по разход на електрическа енергия управление на толинен обект. Научни трудове, РУ „Ангел Кънчев“, т. 39, серия 3, 2001, с. 134-138
[2] Garipov, E. Optimization methods for improvement tuning of PID controllers, Proceeding of Int. Conf. Automatics & Informatics, Sofia, 2001, pp. A-119-A-122
[3] Попова, М., Н. Нойков. Математическо описание на топлинни процеси на базата на електротоплинната аналогия. Научни трудове, РУ „Ангел Кънчев“, т. 37, серия 3, 1999, с. 223-226.

За контакти:

Владислав Толев, Катедра “Автоматика и Мехатроника“, Русенски университет “Ангел Кънчев“, e-mail: crosh@mail.bg
доц. д-р Донка Иванова, Катедра „Автоматика и мехатроника“, Русенски университет “Ангел Кънчев“, тел.: 082-888 266, e-mail: divanova@uni-ruse.bg

Изкуствени невронни мрежи за класификация на видове чай, базирана на VIS/NIR спектрален анализ

автор: Марияна Сестримска
научен ръководител: доц. д-р Таня Титова

Artificial Neural Networks for Classification of Tea Types based on VIS / NIR Spectrum Analysis*: In the present paper presents two types of artificial neural networks adapted to recognize the samples with different ingredients. The study is based on VIS / NIR spectroscopy, measurement of color and pH.Experimental database is pre-processed by the methods principal components analysis and stepwise linear discriminant analysis in order to reduce the dimensionality of the output feature space and extract the most valuable of informative perspective characteristics of tea samples.*

Key words: *VIS/NIR spectral analysis, principle component analysis, artificial neural network, Self-organizing maps, tea.*

ВЪВЕДЕНИЕ

Чаят е напитка, която се получава чрез запарване на различни видове билки, изсушени цветове или плодове на различни растения. Той е сред най-консумираните напитки в световен мащаб. В редица страни като Китай, Япония, Русия, Турция, Великобритания, Германия и др. има установени дългогодишни традиции в отглеждането и консумацията на чай.

Качествата на чая се обуславят от голямо съдържание на различни органични съединения като полифеноли, алкалоиди, флавоноиди, кофеин и др. Биохимичният му състав включва аминокиселини, въглехидрати и протеини. Листата на чаеното растение съдържат множество витамини като вит. С, Е, В1, В6, каротин, фолиева киселина, а също така и минералите манган, калий, флуориди др. Ароматните качества на напитката се дължат на присъствието на множество летливи органични съединения, чието съдържание зависи от вида, сорта, съставките, начина на отглеждане и начина на приготвяне на чаената напитка.

Целта на настоящата публикация е да се представи методика за подготовка на експериментална база данни, редукция на високо-размерното признаково пространство, както и селекция на най-информативни окачествяващи фактори. В последствие са синтезирани два типа невронни класификатори, който различават видове билков чай, с различни съставки.

ИЗЛОЖЕНИЕ

I. Невронен класификатор за билков чай с различни съставки и произход.

В изследването са използвани 200 проби от седем различни вида билков чай, закупени от търговската мрежа. Пробите са предварително селектирани в седем групи, всяка от които получава идентификационен код (етикет). Разпределението на чаените проби по групи, както и етикета на всяка от групите са представени в таблица 1.

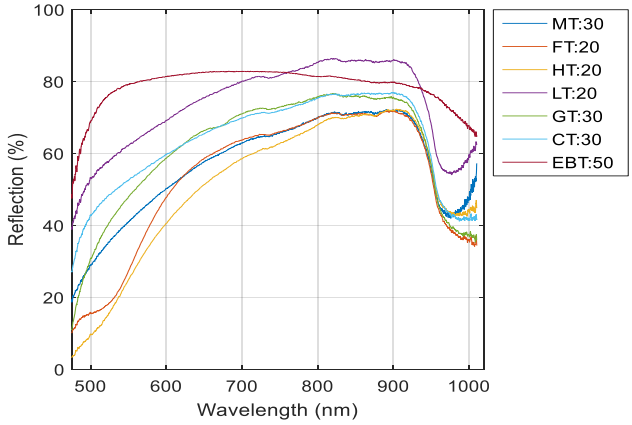
Таблица 1. Групиране на 200 проби чай

Група1	MT:30	30 проби чай мента от 3 различни марки
Група 2	FT:20	20 проби плодов чай
Група 3	HT:20	20 проби билков чай
Група 4	LT:20	20 проби чай липа
Група 5	GT:30	30 проби зелен чай от 3 различни марки
Група 6	CT:30	30 проби чай лайка от 3 различни марки
Група 7	EBT:50	50 проби чай *English Breakfast* от 5 различни марки

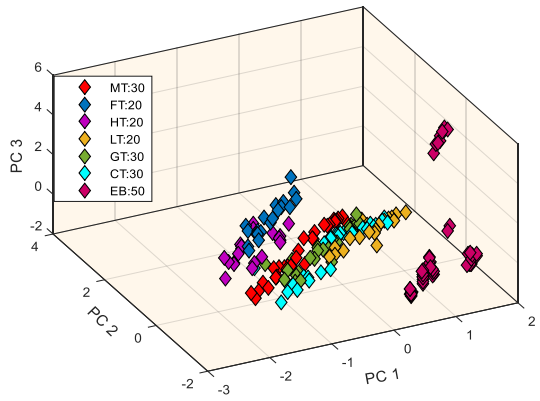
Чаените пакетчета (2-3g) от всеки вид са запарени със загрята до 100°C дестилирана вода за време от 3 до 5 минути. Така приготвените проби са охладени до стайна температура 22-23°C, налети са в 20 милилитрови стъклени затворени епруветки и са подготвени за последваща обработка. Всички проби чай са получени и съхранявани при еднакви условия.

За всички седем вида чай са снети спектралните характеристики на дифузно отражение в *VIS/NIR* диапазона на електромагнитния спектър на светлината от 450nm до 1010nm. Всяка от пробите е поставена в стъклено петри с диаметър 9cm и височина 1cm, като изследваната течност изпълва 2/3 от обема на петрито. Светлинният източник на спектрофотометъра (*FO-THLS-3100*) е позициониран на 15cm от петрито, а фиброоптичната сонда е поставена под ъгъл 45° на височина 10cm. За всяка проба са снети по 5 спектрални характеристики на отражение, като при последваща обработка резултатите са усреднени [6,7,8].

На фиг. 1. са представени усреднени спектрални характеристики на дифузно отражение за седемте различни вида чай. Паралелно със кривите на отражение са измерени характеристиките на цвета (*L*, a*, b*, c*, h**) и *pH* на чаените проби.



Фиг. 1. Усреднени спектрални характеристики на дифузно отражение за седем вида билков чай



Фиг. 2. Проекция на експерименталните данни във факторното пространство, генерирано от първите три главни компонента

В резултат на проведените измервания е получена експериментална база данни, която има следния матричен вид $X_{(200\times207)}$. Стълбовете на матрицата X, представляват 207 експериментални признака, характеризиращи чаените проби. Първите седем признакови вектора са: *L*, a*, b*, c*, h**, λ_{dom}, pH. Останалите 200 стълба на експерименталната матрица представляват спектралните характеристики на дифузно отражение, изгладени по *метода на плъзгащото средно*. Редовете на матрицата X, представляват 200 проведени наблюдения, съответстващи на различните видове чай.

Експерименталният набор от данни матрица е подложен на анализ по метода на главните компоненти (PCA), с цел редуциране на изходното признаково пространство. На фиг. 2. е визуализирано разположението на експерименталните данни във ново полученото факторно пространство. Очертават се (с известно припокриване) седем клъстера, съответстващи на седемте различни групи чай.

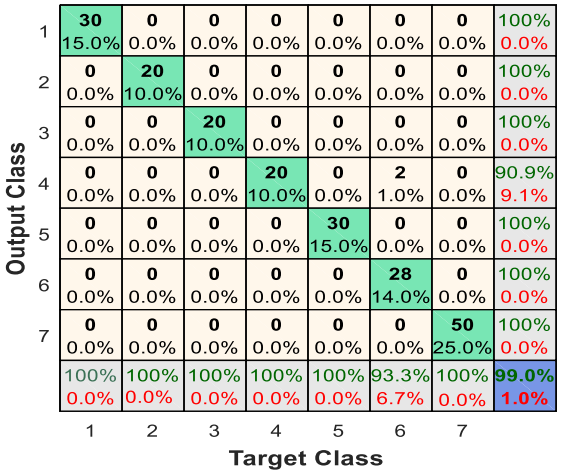
Десетте първи собствени вектора (главни компонента), отразяват общо 99,90% от вариацията на изходните експериментални данни. Точно по тази причина те са избрани за 10 входни вектора на изкуствена невронна мрежа.

В настоящата разработка за класификация на чаените проби е използвана еднопосочна (*feed forward*) невронна мрежа с метод на обучение - обратно разпространение на грешката (*BackPropagation*), изпълнена в програмната среда на софтуерния пакет MATLAB. BackPropagation – алгоритъма има за цел минимизиране на средно-квадратичната грешка на изхода на мрежата, което се осъществява с помощта на градиентна процедура [1].

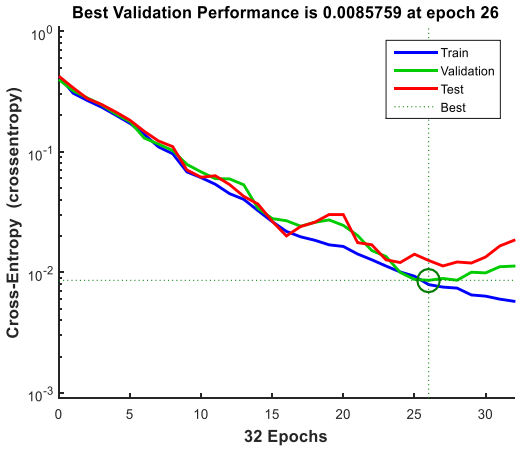
Изкуствената невронна мрежа има трислойна структура, състояща се от един входен, един междинен (скрит) и един изходен слой, с обратно разпространение на грешката. Като активиращи функции в скрития и изходния мрежови слой са използвани съответно *тангенс-сигмоидална* и *Softmax* функции. Броят на входните неврони на мрежата е равен на първите десет най-информативни главни компонента, получени от PCA-анализа на изходните експериментални данни. Първите десет главни компонента са предварително нормирани.

На фиг. 3. е представена обобщена таблица на грешките (*Confusion matrix*), която отразява точността на работа на невронния класификатор. За обучаващата извадка (с обем 140 проби), една проба от клъстер 6 е погрешно разпозната, като принадлежаща на клъстер 4, т.е. една проба от чай лайка е диагностицирана от класификатора като липов чай. При тестовата извадка (с обем 30 проби) отново една проба от клъстер 6 е погрешно разпозната, като принадлежаща на клъстер 4. При процеса валидиране е постигната 100% точност (или 0% грешка).

На фиг. 4. е представено изменението на средно-квадратичната грешка при обучение, тест и валидиране на невронната мрежа. Тестовата и валидиращата крива имат сходен вид, с намаляващ характер на изменение. Не се наблюдава преобучение на мрежата.



Фиг. 3. Таблица на грешките



Фиг.4. Изменение на средно-квадратичната грешка за процесите на обучение, тест и валидиране на невронната мрежа

II. Самоорганизираща се невронна мрежа на Кохонен (*Self-organizing map*) за многофакторна класификация на чай тип „английска закуска" (*English Breakfast*) с различен географски произход на съставките

В настоящото изследване е предложена методология за обучение на самоорганизираща се изкуствена невронна мрежа, за многофакторна класификация на чай тип „английска закуска" от пет различни търговски марки. Експерименталното изследване на чаените проби е базирано на спектрален анализ във видимата и близката инфрачервена област на електромагнитния спектър на светлината

(*VIS/NIR spectral analysis*). Паралелно със спектралните характеристики са снети и характеристиките за цвят и pH на чая.

Експерименталните данни са анализирани по метода стъпков линеен дискриминантен анализ, с цел да се редуцира размерността на изходното признаково пространство и да се извлекат най-ценните, от информативна гледна точка, характеристики на чаените проби.

Табл. 2. Групиране, съставки и произход на изследваните чаени проби

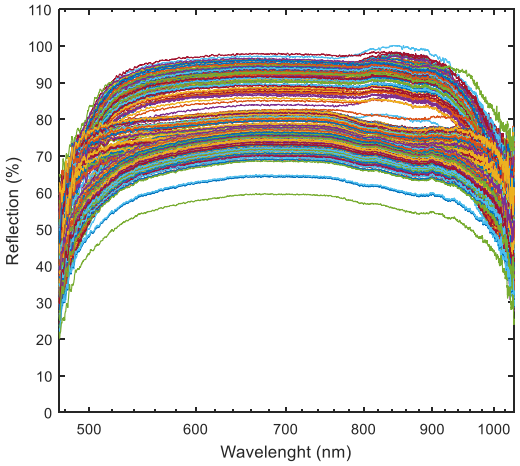
Търговска марка	**Етикет (код)**	**Брой проби**	**Съставки и произход**
Ahmad English Breakfast	English Breakfast 1	57	Индийски Асам, цейлонски чай, кенийски робуста чай.
Tetley English Breakfast	English Breakfast 2	65	Микс от цейлонски и индонезийски чай; листа от черен чай
Twining English Breakfast	English Breakfast 3	70	Кехлибарен чай микс от Асам, Шри Ланка и Кения
Dilmah English Breakfast	English Breakfast 4	100	100% чист цейлонски чай (Шри Ланка)
Tazo English Breakfast	English Breakfast 5	60	Три вида чаени листа от Асам, Южна Индия и Шри Ланка

Използвани са 352 проби чай „английска закуска“ (*English Breakfast*) от пет различни марки, закупени от търговската мрежа. Пробите са предварително селектирани в пет клъстерни групи, всяка от които получава идентификационен код (етикет). Разпределението на чаените проби по групи, етикета на всяка от групите и информация за съставките и произхода на изследвания чай, са представени в таблица 2.

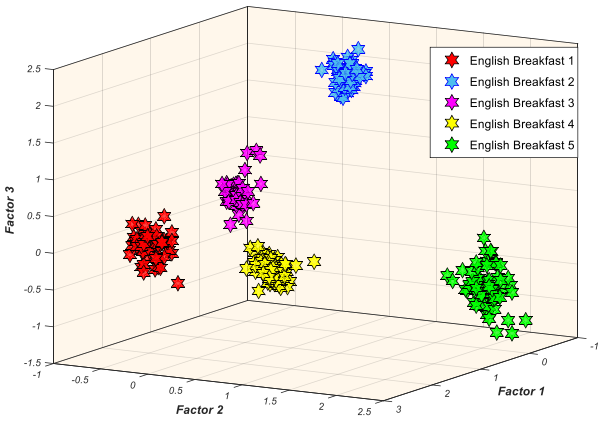
Линейният дискриминантен анализ е статистически подход, разработен от Фишер, който се използва за обработка на данни. При LDA – алгоритъма се изследва случайна величина или случайна извадка от експериментални данни. Методът намира линейна зависимост между променливите или трансформира оригиналните променливи (фактори) в нови, произтичащи от линейно независими комбинации. Дискриминацията се осъществява чрез увеличаване на разликите между класовете, като по този начин вероятността за погрешна класификация е сведена до минимум [2,9].

Самоорганизиращите се невронни мрежи или т.нар. мрежи на Кохонен (Self-organizing maps-SOM) са безсупервайзорни (unsupervised learning) системи („без учител“), които представляват възможност за представяне на многомерно входно пространство, в 2-D факторно пространство, наречено самоорганизираща се карта (SOM). Мрежите на Кохонен имат двуслойна структура, в която първият (входния) слой съдържа толкова неврони, колкото са признаковите елементи на изследвания обект, а изходния (втория) слой е свързан с всеки неврон от входния слой. Броят на невроните в изходния слой се определя от оператора [1,9].

На фиг. 5. са представени 352 спектрални характеристики на дифузно отражение, снети в диапазона 470-1010nm на електромагнитното лъчение.

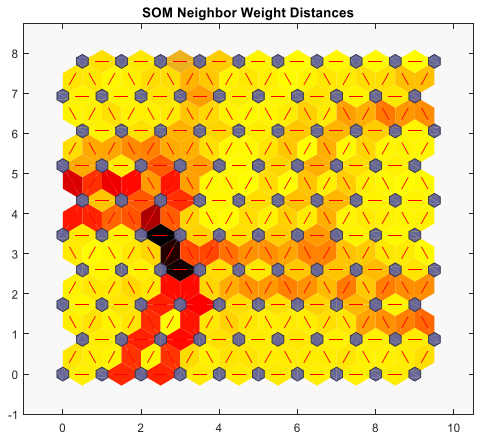


Фиг. 5. Спектрални характеристики на дифузно отражение за 352 проби чай тип „английска закуска"

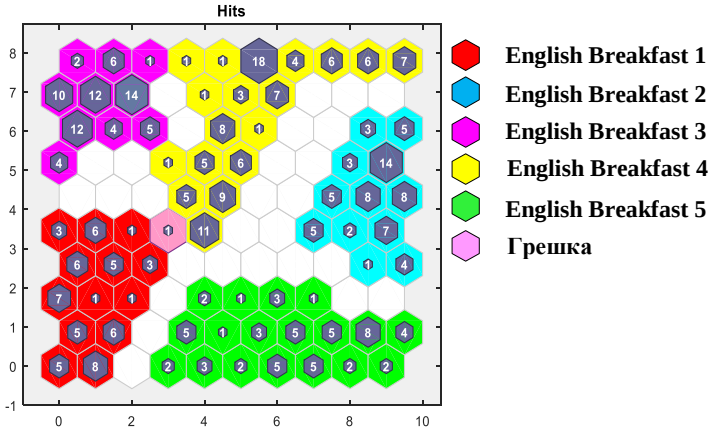


Фиг. 6. Визуална интерпретация на разположението на изследваните проби, според първите три канонични променливи (фактора) на линейния

Спектралните характеристики, заедно със стойностите за pH и цвят образуват експерименталната база данни (признаковото пространство), за която е проведен стъпков дискриминантен анализ, който разделя изследваните проби на пет клъстерни групи, съответстващи на петте различни марки чай *English Breakfast*. На фиг.6. е представена проекцията на чаените проби във факторното пространство, генерирано от LDA. След дискриминантния анализ първите четири фактора са нормирани и подадени като входни вектори на самоорганизираща се невронна мрежа на Кохонен.



Фиг. 7. Унифицирана матрица на разстоянията: U - matrix



Фиг. 8. Двумерна шестоъгълна карта на Кохонен с размери 10×10 неврона

Мрежата на Кохонен представлява двуизмерна шестоъгълна самоорганизираща се карта с размери 10×10 неврона. Шестоъгълният модел е избран по подразбиране в програмният пакет MATLAB. Всеки възел от решетката представлява прототип, точка проектирана в рамките на признаковото пространство, определено от експерименталните данни. Невроните се конкурират да интерпретират максимално точно опитните стойности, като неврон „победител" е този, за който модела се доближава най-точно до стойностите на входния вектор [3].

На фиг. 7. е представена т.нар. унифицирана матрица на разстоянията, която е определена от невронната мрежа, след процеса на обучение. U-матрицата отразява връзките (разстоянията) между невроните на мрежата. Сивите шестоъгълници представляват невроните на мрежата, а червените линии са връзките между тях (фиг. 7). Различните разстояния между невроните са отразени като връзките между тях са оцветени в различни цветови нюанси. Светлите тонове отговарят на близки разстояния (т.е. тесни връзки между невроните), а тъмните цветове означават далечни разстояния. Благодарение на тази методика е възможно да се определят границите на клъстерите, дефинирани от самоорганизиращата се невронна мрежа.

На фиг. 8. е представен изходния слой на самоорганизиращата се невронна мрежа. Той представлява двумерна шестоъгълна карта с размери 10×10. От фигурата се вижда, че невронната мрежа разделя изследваните проби на 5 ясно обособени клъстерни групи. Тъмните шестоъгълници представляват невроните „победители". Тяхната площ е пропорционална на броя проби силно свързани с този елемент. Звената с ниска плътност се приемат за граници на клъстерните групи.

В проведеното изследване самоорганизиращата се невронна мрежа на Кохонен класифицира анализираните чаени проби в пет клъстера, според търговската марка на чая. Една единствена проба е погрешно идентифицирана от мрежата като част от клъстер 4, вместо от клъстер 5 (на фиг. 5.25. погрешно разпознатата проба е оцветено в светло-розово), т.е. постигната е точност на работа на мрежата от 99,72% (грешка 0,28%).

ЗАКЛЮЧЕНИЕ

В настоящата публикация е представена методика за синтез на два типа изкуствени невронни мрежи, обучени да класифицират различни видове чай. Експерименталното изследване е основано на снемане на спектралните характеристики на дифузно отражение във VIS/NIR диапазона на електромагнитния спектър. Паралелно със спектралните криви са измерени цветовите десктиптори и pH на чаените проби.

Експерименталния набор от данни е подложен на предварителна статистическа обработка, с цел редуциране на високо-размерното признаковото пространство и извличане на най-ценната информация, съдържаща се в експерименталния набор от данни.

Полученият висок процент на точност потвърждава успешната реализация на поставената класификационна задача. Предложената методология би могла да се приложи за идентификация на чаени проби с различни съставки, географски произход и степен на качество.

ЛИТЕРАТУРА

[1] Дамянов, Ч. Неразрушаващо разпознаване на качеството в системите за автоматично сортиране на хранителни продукти, Академично издателство на УХТ – Пловдив, 2006.

[2] Вындев, Д. Записки по приложна статистика. Част II, СУ „Св. Климент Охридски", София, 2003.

[3] Bieroza, M., A. Baker, J. Bridgeman. Exploratory analysis of excitation-emission matrix fluorescence spectra with self-organizing maps as a basis for determination of organic matter removal efficiency at water treatment works, Journal of Geophysical Research, 2009.

[4] Cabrita, M., J. Aires-De-Sousa, M. Gomes Da- Silva, F. Rei, A. Costa Freitas. Multivariate statistical approaches for wine classification based on low molecular weight phenolic compounds, Australian Journal of Grape and Wine Research, 138–146, 2012.

[5] Dong-Kyun, K., J. Kwang-Seuk, Ch. Kwang- Hyeon, L. Geung-Hwan, J. Gea-Jae, K. Hyun- Woo. Patterning zooplankton communities in accordance with annual climatic conditions in a regulated river system (Nakdong River, South Korea), International Review of Hydrobiology, 2012.
[6] Draganova Ts., Modeling of spectral data characteristics of healthy and fusarium diseased corn kernels, Agricultural science and technology, 2010, Impact Factor : 0.255, No 2(2), pp. 90 – 95, ISSN 1313-8820
[7] Gang L., H. Yang, Discrimination of different brands of Nescafé coffee using VIS-NIR spectroscopy and comparative study, International Conference on Agricultural and Biosystems Engineering, 2011
[8] He Y., X. Li, X. Deng, Discrimination of varieties of tea using near infrared spectroscopy by principal component analysis and BP-model, Journal of Food Engineering, 1238–1242, 2009
[9] Maeda, M., N. Shige, H. Miyajima. Learning model in relaxation algorithm influenced by Self-Organizing Maps for image, 2008.

За контакти:

Доц. д-р Таня Титова, Катедра "Автоматика, информационна и управляваща техника", Университет по хранителни технологии – гр. Пловдив, e-mail: t_titova@abv.bg

д-р инж. Марияна Сестримска, Катедра "Автоматика, информационна и управляваща техника", Университет по хранителни технологии – гр. Пловдив, e-mail: mariana_brusova@abv.bg

Система за известяване на времето

автори: Момчил Букреев и Красимир Николов
научен ръководител: доц. д-р Ирена Вълова

System for weather forecast: *This paper represents the necessity of internet users to get weather forecasts by mail. It includes the some existing systems that are similar to the currently presented. The reader of this paper will see the main parts of development of the system, used tools and the user interface (UI) of the site.*

Key words: *OpenWeatherMap API, Nodemailer, CronJob.*

ВЪВЕДЕНИЕ

В днешно време все повече интернет потребители стават част от бързо разрастващата се cloud общност в интернет пространството. Бурното развитие на cloud технологиите предоставя на потребителите бърз и лесен достъп до огромен брой услуги, което допринася за преминаването към изцяло cloud computing-а. Този доклад е насочен към разрешаване на проблем, свързан с ежедневието на всеки потребител, или по-точно - известяване на всеки интернет потребител за текущата прогноза за времето. В доклада е представена разработката на приложение за известяване на времето.

СЪЩЕСТВУВАЩИ СИСТЕМИ

Съществуват различни системи за следене на времето в реално време, като те показват текущото време за даден регион, времето за определен период (почасов, дневен, седмичен, месечен). В информацията за времето влизат следните по-важни показатели:

- Температура на въздуха;
- Влажност на въздуха;
- Атмосферно налягане;
- Скорост на вятъра;
- Вероятност за валежи;
- Часове на изгрев и залез.

Примери за такива системи са:
https://www.yahoo.com/news/weather
http://www.dailymail.co.uk/home/weather/index.html
https://openweathermap.org/
https://www.gismeteo.ru/

ИЗЛОЖЕНИЕ

1. ОСНОВНИ ПОНЯТИЯ

1.1. **Уеб услуга** - представлява софтуерна система, която предоставя комуникация между взаимносъвместими компютърни системи по компютърни мрежи, според определението на консорциума W3C. На практика това означава стандартни интерфейси между приложенията. Тези стандарти се основават на технологии, които са общи за всички платформи мрежов софтуер, каквито са например XML и HTTP. [2]

1.2. **WEB API** е приложно-програмен интерфейс, предназначен за уеб сървър или уеб браузър. Концепцията за API е като архитектура, която е свързана с предоставянето на програмни интерфейси към група от услуги към различни приложения, обслужвайки различни видове потребители. Когато се използва в контекста на уеб програмиране, едно API е дефинирано като група от HTTP извикващи съобщения, заедно с

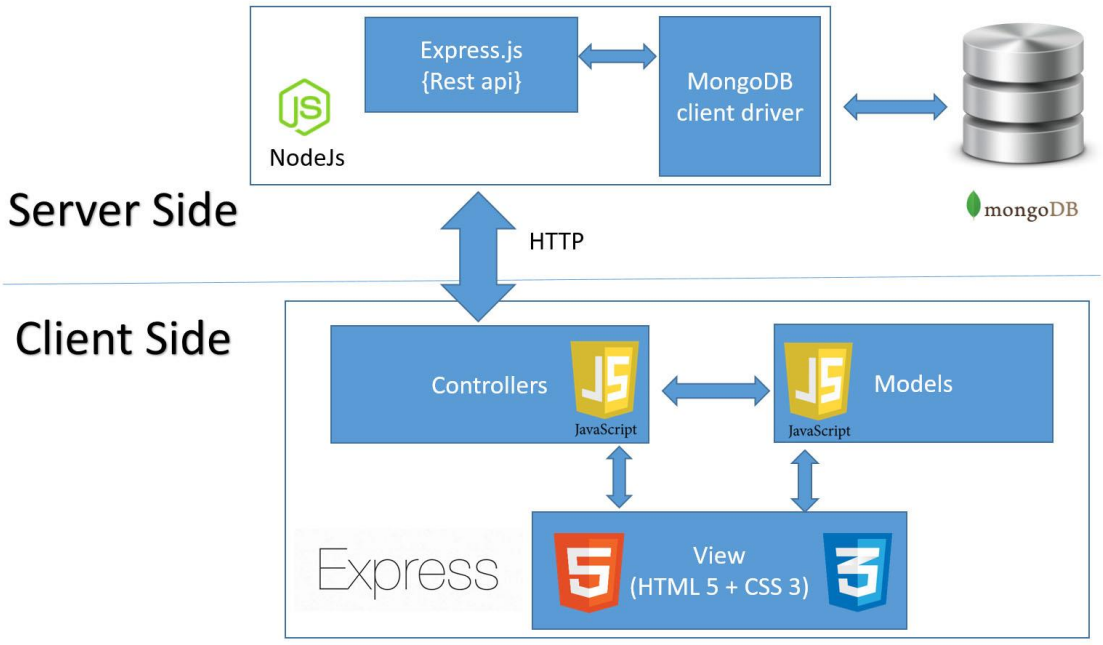
дефиниция на структурата на отговарящите съобщения, което обикновено е при Extensible Markup Language (XML) или Java Script Object Notation (JSON) формат. [4]

1.3. **JSON** - или JavaScript Object Notation, е текстово базиран отворен стандарт създаден за човешки четим обмен на данни. Произлиза от скриптовия език JavaScript, за да представя прости структури от данни и асоциативни масиви, наречени обекти. Въпреки своята връзка с JavaScript, това е езиково независима спецификация, с анализатори, които могат да преобразуват много други езици в JSON. [3]

1.4. **Облачна технология** - модел, който прави възможен мрежовия достъп до споделени ресурси като интернет мрежи, сървъри, хранилища за масиви от данни и софтуерни приложения с мининално участие или управление от доставчика на услугата. С навлизането на този технологичен бизнес модел потребителите могат да достъпват тежки по отношение на разхода на ресурс приложения чрез леки преносими устройства като мобилни телефони, лаптопи и PDA устройства. Облачните технологии преместват изчислителната мощ и информацията от десктоп компютрите и преносимите устройства в мега мощни дата центрове което намалява разходите и формира нов по-гъвкав подход за правене на бизнес. [1]

2. ОПИСАНИЕ НА ПРЕДЛАГАНОТО РЕШЕНИЕ

- **Архитектура (фиг. 1)**



Фиг. 1 Архитектура на claud базирано приложение

Приложението е реализирано чрез използването на NodeJs в комбинация с Express JS и нерелационната база от данни – mongoDB. Клиентската част е трислойна от тип MVC. За визуализиране на необходимата информация са използвани познатите HTML5, CSS3 и JavaScript.

- **Разработване**
  - ❖ **Избор на БД** - при избора на подходяща база от данни са взети под внимание следните ключови показатели:
    - ✓ Няма нужда от релации (необходимост от една таблица - колекция)
    - ✓ Скорост и достъп до данните

За целта е избрана mongoDB за БД. В приложението е създадена база от данни

с име "weather", в която има само една колекция (users) като в нея се пазят email-а и града, използвани за известяване.

- **Използвани API-та и модули**
  - ✓ Openweather-api - безплатен сървис за получаване на информация относно текущото време в даден регион по зададен град.

Формиране на примерна заявка:

api.openweathermap.org/data/2.5/weather?q=Shuzenji&units=metric&lang=en&mode=json&APPID=d41724ec2a07e1b5516db613299351c1

Отговор на примерната заявка:

Получаваме следният примерен JSON:

{"coord":{"lon":139,"lat":35},
"sys":{"country":"JP","sunrise":1369769524,"sunset":1369821049},
"weather":[{"id":804,"main":"clouds","description":"overcast clouds","icon":"04n"}],

"main":{"temp":289.5,"humidity":89,"pressure":1013,"temp_min":287.04,"temp_max":292.04},
"wind":{"speed":7.31,"deg":187.002},
"rain":{"3h":0},
"clouds":{"all":92},
"dt":1369824698,
"id":1851632,
"name":"Shuzenji",
"cod":200}

- **Nodemailer** - модул за Node.js приложения, който ни позволява да изпращаме email-и по лесен начин. Единственото, което Nodemailer изисква е въвеждането на email. Примерен отговор при успешно изпращане на email:

{"name":"nodemailer","hostname":"M-Bukrev","pid":8332,"level":30,"component":"smtp-connection","sid":"F0lm30ct1wI","tnx":"network","localAddress":"192.168.43.234","localPort":50870,"remoteAddress":"74.125.195.109","remotePort":465,"msg":"Secure connection established to 74.125.195.109:465","time":"2017-03-28T13:51:01.138Z","v":0}

{"name":"nodemailer","hostname":"M-Bukrev","pid":8332,"level":30,"component":"smtp-connection","sid":"F0lm30ct1wI","tnx":"smtp","username":"weathernowis@gmail.com","action":"authenticated","method":"PLAIN","msg":"User \"weathernowis@gmail.com\" authenticated","time":"2017-03-28T13:51:01.990Z","v":0}

{"name":"nodemailer","hostname":"M-Bukrev","pid":8332,"level":30,"component":"smtp-transport","tnx":"send","messageId":"<5552fd61-50d8-58cc-c558-d19c87b19e65@M-Bukrev>","msg":"Sending message <5552fd61-50d8-58cc-c558-d19c87b19e65@M-Bukrev> to <edew@dir.bg>","time":"2017-03-28T13:51:01.992Z","v":0}

{"name":"nodemailer","hostname":"M-Bukrev","pid":8332,"level":30,"component":"smtp-connection","sid":"F0lm30ct1wI","tnx":"message","inByteCount":1328,"outByteCount":1331,"msg":"<1331 bytes encoded mime message (source size 1328 bytes)>","time":"2017-03-28T13:51:02.660Z","v":0}

Message sent successfully!

Server responded with "250 2.0.0 OK 1490709063 g13sm3705297wmd.28 - gsmtp"

{"name":"nodemailer","hostname":"M-Bukrev","pid":8332,"level":30,"component":"smtp-connection","sid":"F0lm30ct1wI","tnx":"network","msg":"Connection closed","time":"2017-03-28T13:51:04.153Z","v":0}

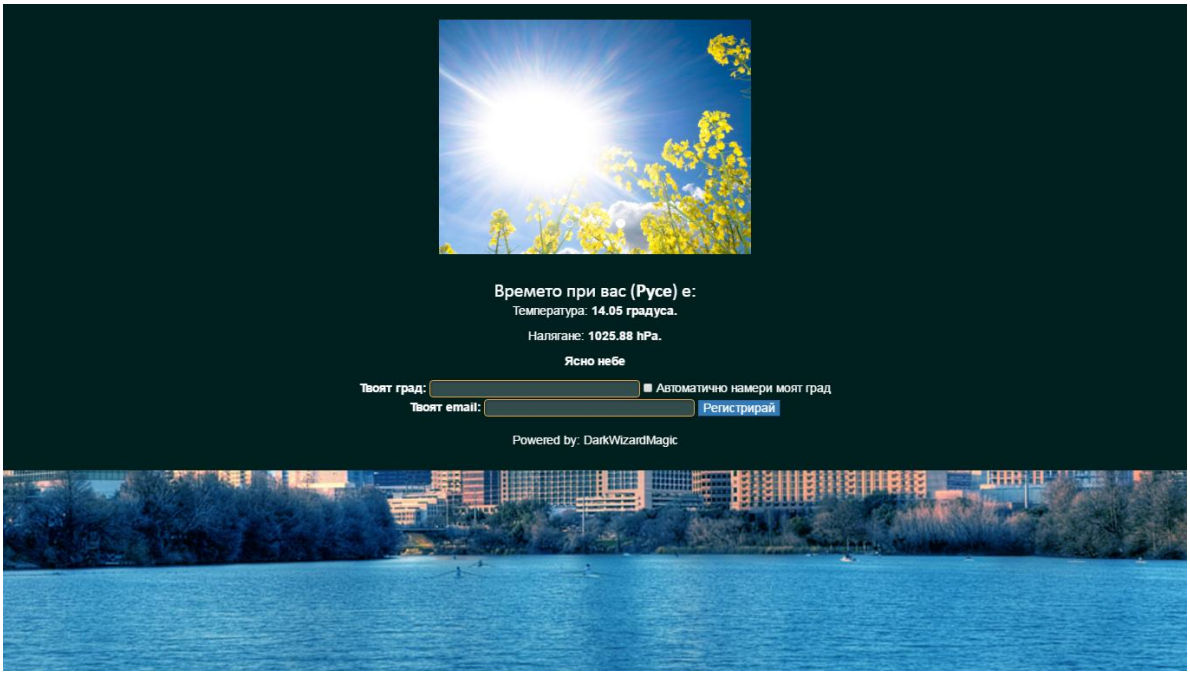
- **Cron** - модул за задаване и изпълняване на планирани задачи. Чрез него, през определен период от време се изпращат email-и до всички абонирани потребители.

3. ОПИСАНИЕ НА ПОТРЕИБИТЕЛСКИЯ ИНТЕРФЕЙС

Външният облик на приложението е изграден чрез HTML5 и CSS3 в комбинация с познатият от всички Bootstrap Framework. Това ни дава възможност да използваме приложението на устройства с различна разделителна способност.

Приложението разполага с два основни потребителски екрана. Първият екран предоставя следните възможности на потрбителя (фиг. 2):

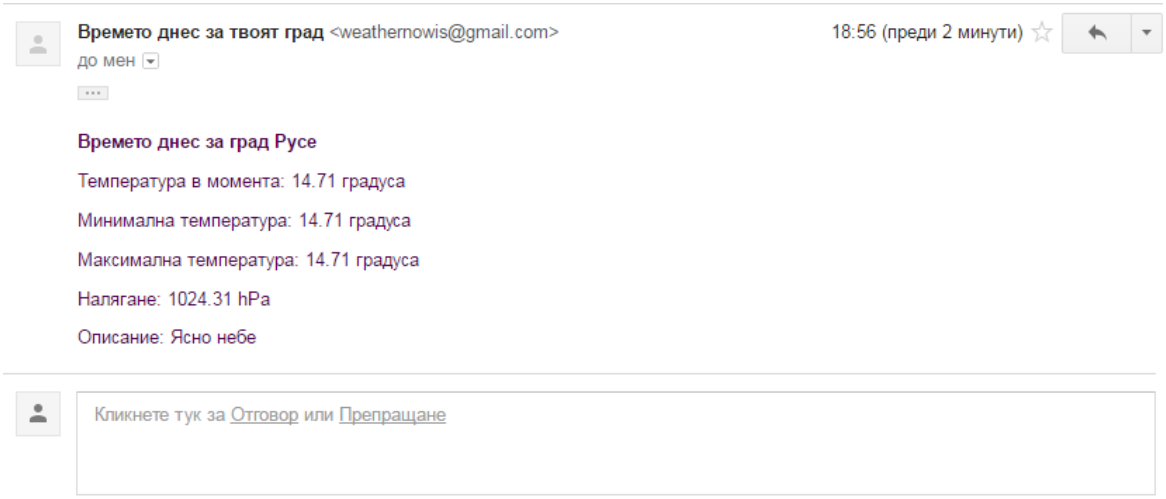
- следене на времето, въз основа на засичане на текущото местоположение на устройството;
- форма за попълване, чрез която потребителят може да се абонира за известяване всеки ден. Определянето на града може да стане чрез ръчно въвеждане или автоматично, чрез избор на отметката "Автоматично намери моят град";



Фиг. 2 Начален екран на приложението

След попълване и изпращане на данните от формата за регистрация, потребителят се известява за успешно абониране.

През определен интервал от време Cron модулът изпълнява задачата да претърси съответната БД и да вземе абонираните мейли с отговарящите им градове. След това се изпълнява заявка към Openweather api и се препраща отговор като email на потребителя в показания на фиг. 3 формат:



Фиг. 3 Формат на известяващите електронни съобщения към потребителите

ЗАКЛЮЧЕНИЕ

Направеното приложение бе тествано на различни устройства като успешно се справи с всички резолюции.

Като бъдещо развитие може да се добавят следните функционалности:

- Известяване чрез SMS;
- Възможност за прогнозиране за няколко дни;
- Промяна на езика на приложението.

ЛИТЕРАТУРА

[1] Писков, И., Облачни технологични модели – видове облаци, февруари, 2012 http://blog.icn.bg/novini-ot-icn-bg/oblachni-tehnologii-modeli/
[2] Уикипедия, 24 октомври 2015. https://bg.wikipedia.org/wiki/Уеб_услуга
[3] Уикипедия, 23 януари 2017. https://bg.wikipedia.org/wiki/JSON
[4] Уикипедия , 14 декември 2016. https://bg.wikipedia.org/wiki/Приложно-програмен_интерфейс

За контакти:

инж. Красимир Николов, Русенски университет "Ангел Кънчев", Специалност "Компютърни системи и технологии", GSM: 0883-562-304, e-mail: kr.nikolow@abv.bg

инж. Момчил Букреев, Русенски университет "Ангел Кънчев", Специалност "Компютърни системи и технологии", GSM: 0897-042-967, e-mail: edew@dir.bg

доц. д-р Ирена Вълова, Русенски университет "Ангел Кънчев", Катедра „Компютърни системи и технологии", тел.: 082-888 685, e-mail: irena@ecs.ru.acad.bg

Уеб базиран текстов редактор

автор: Баръш Юмеров
научен ръководител: гл. ас. д-р Йордан Калмуков

Web text editor: *This paper presents online system for storing, editing and deleting user files which are accessible from everywhere, explains cloud computing and discusses the benefits of using cloud technologies.*

Key words: *cloud, cloud computing, storing, JavaScript, REST*

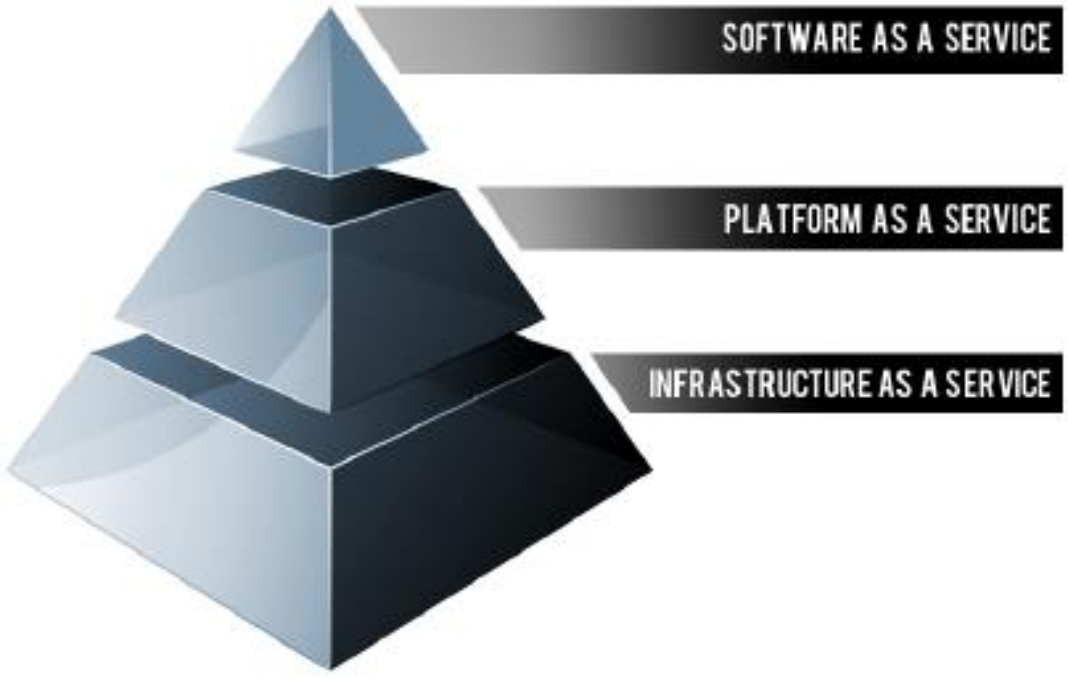
ВЪВЕДЕНИЕ

"Изчисления в облак" е предоставянето на компютърни (изчислителни) услуги, а не на продукт. Изчислителните облаци дават възможност на предприятия, публични администрации и граждани, използвайки мрежи като интернет, да получат достъп до техните данни и софтуер, инсталирани на компютри, разположени другаде.

С развитието на технологиите и интернет, информацията в днешно време е леснодостъпна и неограничена. Тук обаче възниква основният проблем с обема от данни. Достъпа до информация не представлява затруднение, но именно нейното съхранение изисква ресурси.

Cloud computing може да се дефинира като нов стил в компютинга, при който динамично мащабируеми и много често виртуализирани ресурси се предоставят под формата на услуги в интернет. Чрез тази технология става възможно потребителите да използват различни устройства (PC, лаптопи, смартфони, и други) за достъп до програми, място за съхранение и платформи за разработка на приложения в интернет,чрез услуги предоставяни от облака. Основни предимства: икономии на средства, лесно динамично мащабиране и висока достъпност.

ВИДОВЕ ОБЛАЧНИ РЕШЕНИЯ



Фиг. 1 Видове облачни решения

Различни облачни решения се предлагат на клиентите за използване като услуга и повечето от тях попадат в една или няколко от следните категории:

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Именно ориентацията към услуги прави облачните технологии толкова привлекателни и мощни като решения в ИТ индустрията напоследък. Компютърните ресурси се отдават под наем, което дава възможност клиентите да не са ангажирани със закупуване на хардуерни или софтуерни ресурси за своя бизнес.

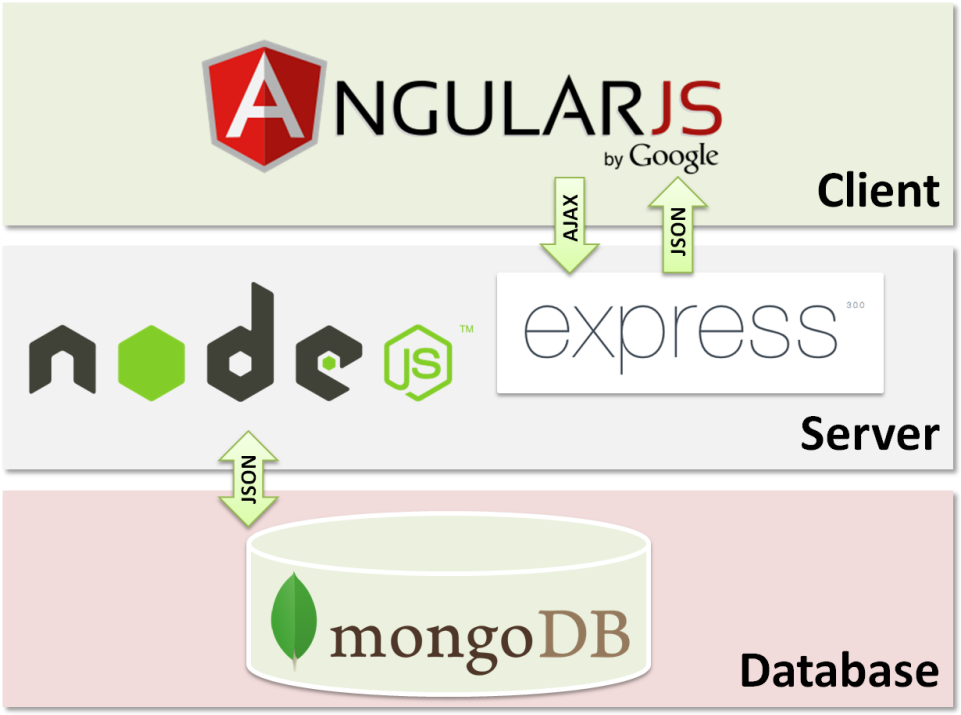
Софтуер като услуга

SaaS е софтуер, който е достъпен за крайния потребител чрез Интернет. За разлика от традиционните пакети с приложения, които потребителите инсталират на компютрите или сървърите си, фирмата доставчик притежава софтуера и го предоставя на потребителите, като съхранява в системата си техните данни. Потребителят плаща само месечна такса за използването му [5]. С тази услуга не е необходимо закупуването на допълнителен хардуер или инфраструктура за работата на софтуера. Моделът спестява на потребителите пари за консултантски услуги, свързани с инсталиране на софтуера. Ако крайният потребител не намира услугата за полезна, може да се откаже от нея по всяко време, без да загуби нищо.

Моделът SaaS има предимства пред алтернативното закупуване на софтуер. С него не е необходимо продуктът да се инсталира на всеки компютър поотделно, с което се спестява време и пари, съответно за закупуване на лицензи. Обновленията се извършват централизирано и компанията винаги разполага с последната версия без това да и струва никакви усилия и средства на фирмата-потребител.

Фиг. 2 SaaS

MEAN STACK



Фиг. 3 MEAN stack

За направата на на уеб базирания текстов редактор е избрано MEAN stack. Той представлява колекция от JavaScript базирани технологии - MongoDB, Express.js, AngularJS, and Node.js. От клиентската част до сървъра и базата от данни се използва само JavaScript [3].

- **Node.js** е мулти-платформена среда за изпълнение на сървърни и мрежови приложения с отворен код. Приложенията се пишат на JavaScript и могат да се изпълняват в Node.js среда под OS X, Microsoft Windows, Linux и IBM [2].
- **Express** е фреимуорк за **Node.js**, който е създаден за улеснение и ускорение работата на програмистите за създаване на уеб и мобилни приложения [4].
- **MongoDB** е система за обработване на бази данни от документи, разработена от 10gen. Тя е от рода на нерелационните бази от данни (NoSQL). Вместо да съхранява информация в таблици, както е при традиционните релационни бази от данни, MongoDB съхранява структурираната информация в JSON формат с динамични схеми. Това прави интегрирането на информацията в определени приложения доста по-лесно и по-бързо.
- **Angular** е TypeScript базирана платформа за създаване на front-end на уеб приложения. Разработен е от Angular Team в Google, които са и разработили AngularJS

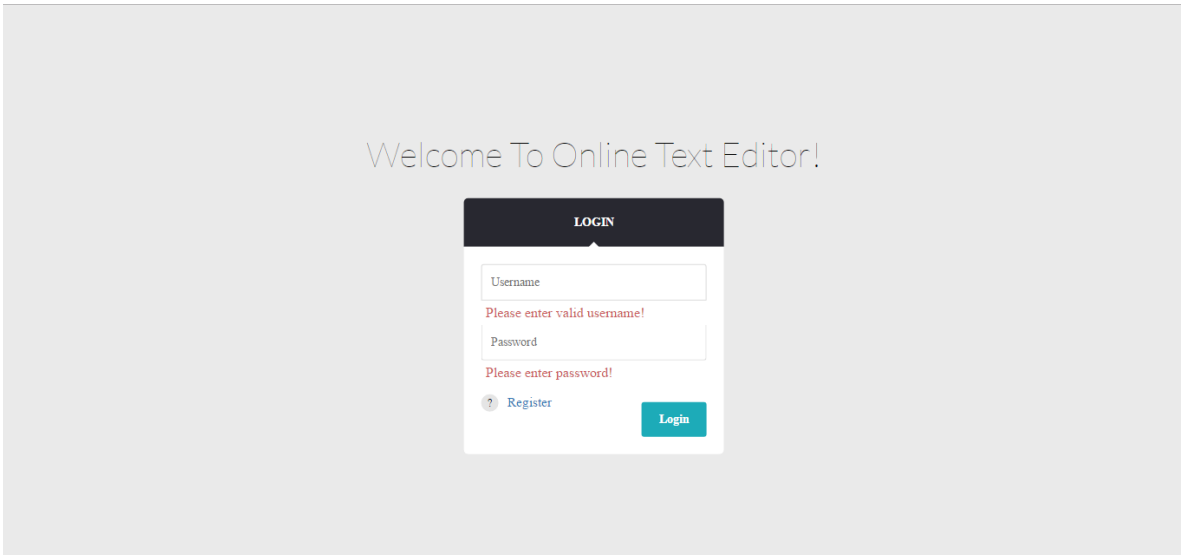
ОПИСАНИЕ И СНИМКИ ОТ РАБОТАТА ПРИЛОЖЕНИЕТО

Направеното приложение е разделено на две части – сървър и клиент. За сървърната част се използва NodeJS (Express), който посреща заявки от клиентската част, а клиентската част е написана на Angular 2.

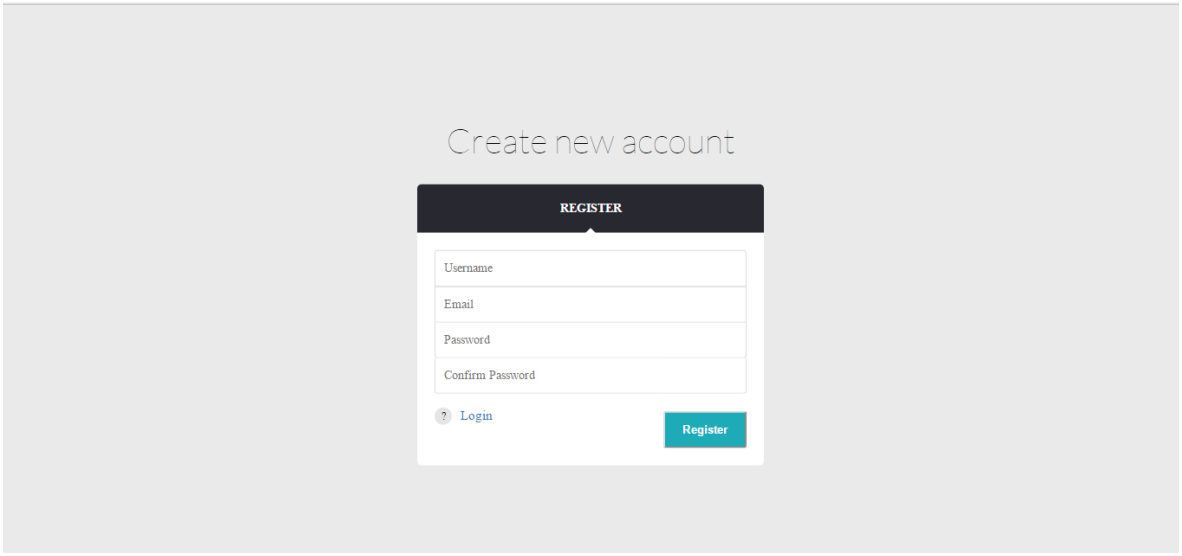
В сървърната част са дефинирани контролери, които посрещат заявките и модели, които осъществяват връзката с базата от данни (MongoDB). Структурата на БД е много опростена. В нея има два документа – Users и Files. В Users се пазят

полетата за потребителите, а във Files - за потребителските файлове. За всеки един документ в Express са създадени модели за по-лесен достъп до самите данни в базата.

Всеки потребител преди да започне работа с приложението трябва да се впише със своя потребителски акаунт (фиг. 4) чрез въвеждане на име и парола. Ако няма такъв може да си създаде чрез попълване на регистрационна форма (фиг. 5).



Фиг. 4 Форма за вписване



Фиг. 5 Форма за регистрация на нов потребител

Клиентсата част представлява SPA (Single Page Application), т.е. всичките нужни за рендиране данни (HTML, CSS и JavaScript) се изтеглят при първото зареждане на приложението, след което динамично се сменят страниците без реално презареждане.

За отделните блокове на страниците са създавани различни TypeScript компоненти, които накрая се обединяват и създават цели страници, така самото развиване, поддръжка и тестване на приложението става по-лесно и бързо.

За управление на достъпа на потребителите се използва JWT. JSON Web Token представлява ключ който се генерира от сървъра и се дава на потребителя. С него потребителят удостоверява самоличността си. Ключът е криптиран и съдържа данни за вписания потребител. След успешна автентикация потребителят при всяка заявка

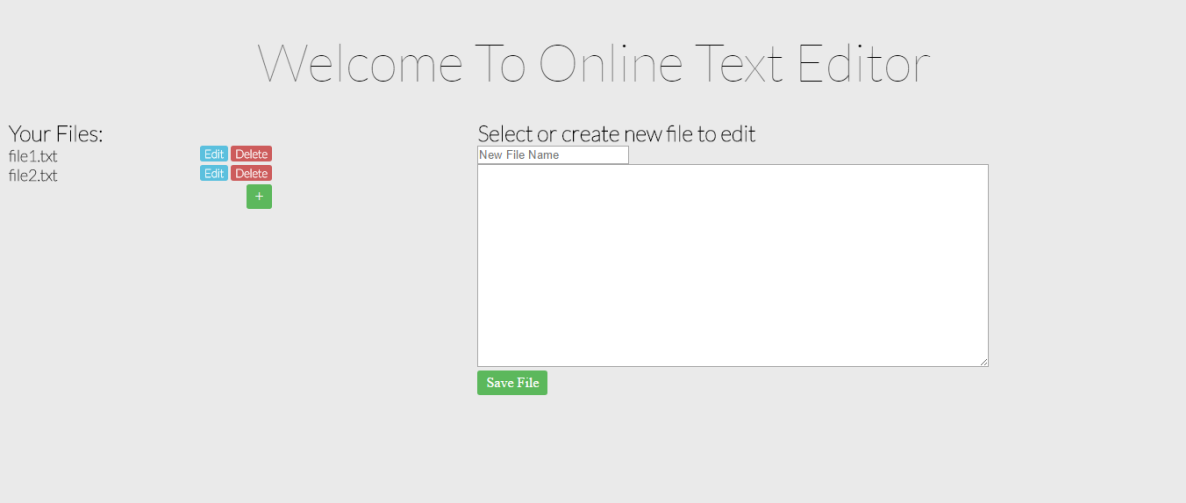
към сървъра изпраща този ключ с който казва „кой" е. Така се избягва при изпращане на потребителско име и парола към сървъра при всяка заявка. За по-голяма сигурност от хакерски атаки полученият от сървъра „ключ" вместо да се запазва като куки в браузъра, той се пази в LocalStorage на браузъра, понеже някои браузъри изпращат всички кукита при всяка заявка, което може да доведе до слаби места за „атаки".

Преди каквото и да е записване на информация в базата, тя се валидира от сървъра. Ако валидацията на всички данни мине успешно чак тогава се предприема записването им в базата от данни. При успешно регистриране на нов потребител, неговата парола се хешира и се пази в базата в хеширан вид. Пример за записан потребител в базата от данни:


```
{
        "_id" : ObjectId("58daba4ce2c09e050cdbec4e"),
        "username" : "barish",
        "email" : "barish@example.com",
        "password":"$2a$10$maWuq4jA3mfVkY2RUKLLxOM2JGEZ/v2sRS95Ii9AknJfYD04XGaMG",
        "__v" : 0
}
```


След успешно вписване потребителят се препраща към потребителска страница (фиг. 6). Примерен JSON отговор от сървъра при успешно вписване:


```
{
        "token":
        "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImJhcmlzaCIsIl9pZCI6IjU4ZDE5Y2VkYmZjMWU2MmQzY2Q1ODhmMiIsImlhdCI6MTQ5NDM1MTg4MSwiZXhwIjoxNDk0MzUzNjgxfQ.LfcOqCJMwEbQIjLRDshhROVqnCDyglKIj8N_LZE3g3Y",
        "username": "barish"
}
```

Фиг. 6 Потребителска страница

В ляво се намират файловете на вписания потребител. Всеки файл може да бъде редактиран или изтрит, съответно като се натисне на съответния ред на файла edit/delete. Като се натисне Edit съдържанието на файла се зарежда динамично във текстовото поле и чрез натискане на бутона Save file се запазват промените. За създаване на нов файл потребителят трябва да натисне зеления бутон (+) в ляво след което трябва да въведе име и текст на новия файл и отново чрез натискане на Save file файлът се записва. Всичките заявки към сървъра са асинхронни и промените в потребителския интерфейс са динамични.

Пр: След успешно създаване на нов файл той се добавя при останалите файлове в лявата част без презареждане на цялата страница.

ЗАКЛЮЧЕНИЕ

Настоящето приложение е подходящо за употреба в ежедневието, както и в бизнес среда с цел съхраняване на текстови файлове. Приложение от същият характер за съхраняване на текстови данни е OneDrive – където могат да се съхраняват текстови документи, таблици и презентации.

Възможностите за доразвиване на продукта са насочени в две насоки:

- От софтуерна където възнамеряваме да се добавят компилатори на различни езици и така да се превърне в интегрирана среда .
- От страна на продукта да се добавят възможности за споделяне на файлове между потребители.

ЛИТЕРАТУРА

[1] И. Вълова, Учебни материали по Облачни технологии, 2017
[2] https://nodejs.org/en/about, 13.04.2017
[3] https://www.sitepoint.com/introduction-mean-stack, Jay Raj 17.04.2014. An Introduction to the MEAN Stack
[4] https://expressjs.com/, 13.04.2017 - Web Applications
[5] http://cio.bg/2620_modelat_softuer_kato_usluga__vaprosi_i_otgovori, 14.06.2016 - Моделът "софтуер като услуга" – въпроси и отговори

За контакти:

Баръш Юмеров, Русенски университет "Ангел Кънчев", Специалност "Компютърни системи и технологии", e-mail: barish.yumerov@gmail.com.

гл.ас. д-р Йордан Калмуков, Русенски университет "Ангел Кънчев", Катедра „Компютърни системи и технологии", тел.: 082-888 827, e-mail: jkalmukov@gmail.com.

Проектиране и разработване на облачно-базирано приложение за управление на смарт устройства

автори: Павел Златаров, Мирослав Маринов
научен ръководител: доц. д-р Ирена Вълова

Design and Development of a cloud-based smart device control application: *The paper describes the design and implementation of a cloud-based application for controlling smart home devices. The aim of the project is to lay the foundation for the creation of a universal, vendor-independent solution capable of controlling smart devices from different manufacturers using a single dashboard.*
Key words: *Cloud, Smart device, Networking, Web services*

ВЪВЕДЕНИЕ

Забързаното ежедневие на повечето хора в днешно време налага намирането на най-бързите възможни решения за ефективно решаване на ежедневните проблеми и задачи. Масовото навлизане и поевтиняване на компютърната техника вече играе важна роля в улесняването на ежедневието на потребителите (използващите компютри и мобилни устройства отдавна имат възможност да комуникират отдалечено и да извършват различни дейности, отнемащи по-малко време онлайн), но концепцията за отдалечено управление на устройства за домашна автоматика е позната на масовия потребител сравнително отскоро. Въпреки това, различни типове smart устройства (лампи, електрически ключове, контакти, различни видове сензори, smart ключалки и дори електроуреди) набират все по-голяма скорост и намират място във все повече домове. Централизираното и отдалечено управление на такива устройства, обаче, не винаги е възможно, поради налагането на различни ограничения – хардуерни, софтуерни, ограничения на домашните мрежи, ограничения, наложени от производителя, и др. Приложението, описано в този доклад, има за цел да постави основите на платформа, която цели да премахне повечето от тези ограничения и да позволи отдалечено управление на устройствата без забавяне.

ЧЕСТО СРЕЩАНИ ПРОТОКОЛИ И СТАНДАРТИ

Тъй като повечето смарт устройства имат за цел запазване на ниска цена и работа във вече съществуващи домашни мрежи, повечето от тях поддържат до определена степен най-често срещаните комуникационни стандарти и протоколи. Често се срещат smart устройства, поддържащи:

- Bluetooth
- Wi-Fi
- ZigBee
- Комуникационни протоколи по 2.4GHz честотни ленти
- Ethernet
- Серийни портове
- Други

Протоколите, по които могат да бъдат управлявани устройствата включват:

- HTTP
- TCP/UDP
- Текстово базирани протоколи
- Двоични протоколи
- Други

КОНТРОЛ НА SMART HOME УСТРОЙСТВА В РЕАЛНО ВРЕМЕ

Постигането на максимална ефективност и осигуряване на удобство за потребителя налага предвиждане на възможност за управление на smart

устройствата чрез приложението от всяка точка на света, както и осигуряване на навременно изпращане на командите. Протоколи като HTTP не са подходящи за тази цел, тъй като всяка заявка или команда изисква изграждането на нова връзка и размяната на голямо количество заглавни данни (headers) – това увеличава значително времето за предаването на команди и отговори между smart устройството и управляващото го клиентско приложение. Употребата на TCP/UDP в „чист“ вид пък налага разработката на собствени механизми за определени задачи, като например криптиране на предаваните данни и запазване на състоянието на системата между отделните заявки.

TCP, UDP и други протоколи често изискват и конфигуриране на мрежата, в която се намира smart устройството, което затруднява процеса по инсталация. Ако такава конфигурация не се направи, управлението е възможно само ако устройството и потребителят се намират в същата мрежа – контролът от външни мрежи не е възможен. Тъй като в повечето домашни и малки корпоративни мрежи често има защитни стени (firewall) или NAT устройства, в повечето случаи се налага използването на подходи като port forwarding или port triggering за преодоляването им и осигуряване на свързаност към външни мрежи.

WebSocket протоколът позволява две отдалечени компютърни системи да комуникират помежду си в реално време. Макар че WebSocket масово се използва от уеб приложения заедно с HTTP, поддържа се от всички модерни браузъри и уеб сървъри, той може да се прилага при всякакви видове приложения. WebSocket комуникацията започва подобно на HTTP, чрез изпращане на заглавни съобщения (headers) в текстов формат [1]. След установяване на връзка двете приложения се превключват в двоичен режим, като е възможна двупосочна комуникация. За по-нататъшни съобщения се използва вече съществуващата връзка, което елиминира необходимостта от създаване на нова и намалява забавянията. Съобщенията могат да бъдат както в текстов, така и в двоичен формат, което позволява и прехвърлянето на файлове, ако е необходимо.

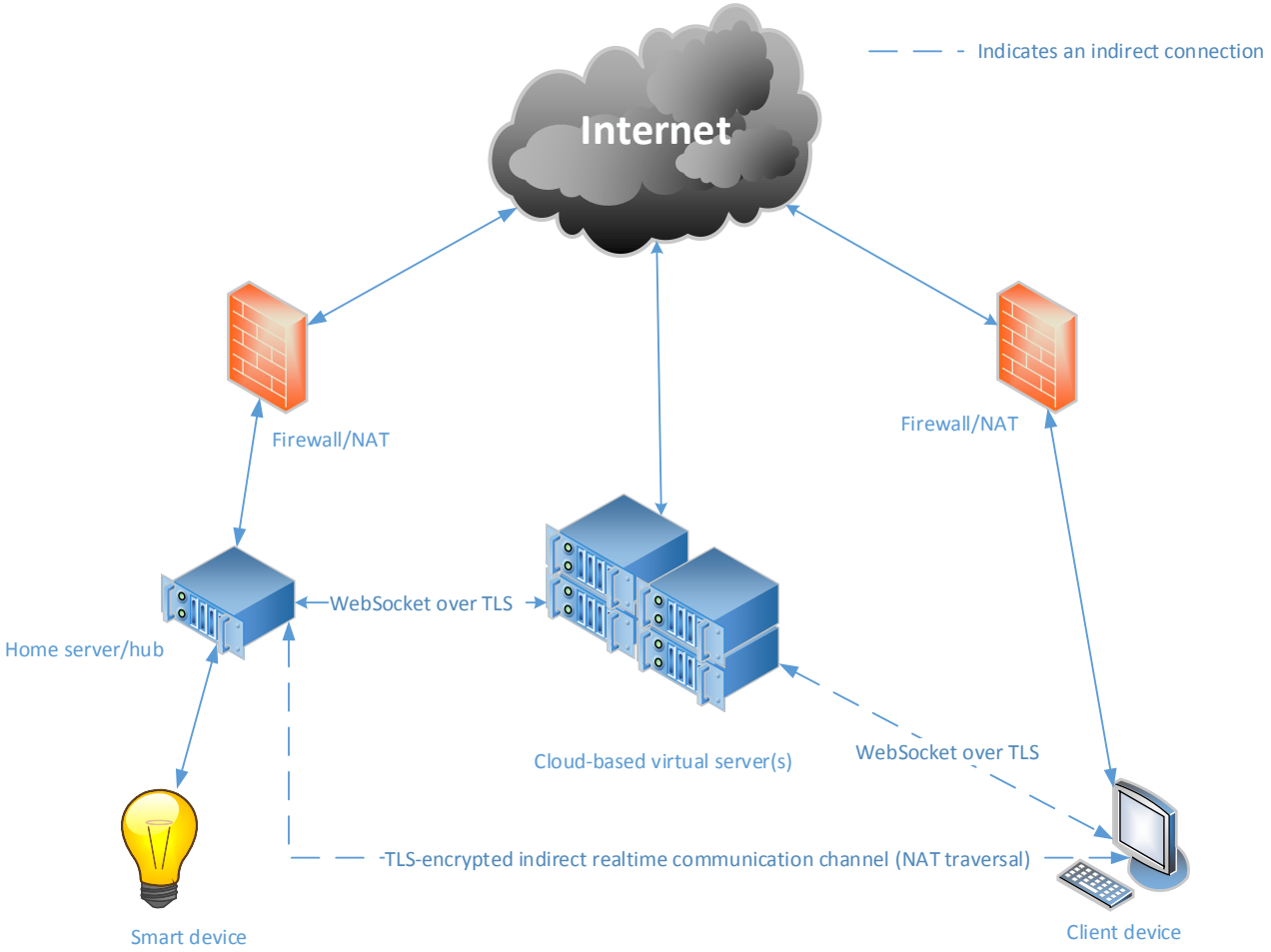
При наличието на централен сървър, двете крайни устройства могат да го използват за препредаване на WebSocket съобщения, което позволява създаването на псевдо-директен комуникационен канал, без необходимост от преконфигуриране на мрежите. Освен това, WebSocket използва същите портове като HTTP и HTTPS, което го прави съвместим с повечето съвременни мрежови конфигурации.

ПРОЕКТИРАНЕ

Предложеното приложение е съставено от три модула, използващи WebSocket протокола за връзка помежду си:

- **Централен сървър** – физическа или виртуална машина, разположена в публичен облачен център за данни (public cloud datacenter). Този компонент се грижи за идентификацията на потребителите и разпределянето на заявките между клиентите и посредниците (hub).
- **Посредник (hub)** – програма или хардуерно устройство, намиращо се в дома на потребителя. Грижи се за приемането на командите от сървъра и транслирането им към разбираем от конкретното смарт устройство формат, независимо от начина му на свързване към мрежата. При хардуерната реализация, посредникът може да поддържа повече от един комуникационен стандарт.
- **Клиент** – уеб приложение, позволяващо на потребителя да управлява своите смарт устройства от всяка точка на света, стига да е налична свързаност с Интернет

Мрежовата архитектура на приложението е показана на Фиг. 7.

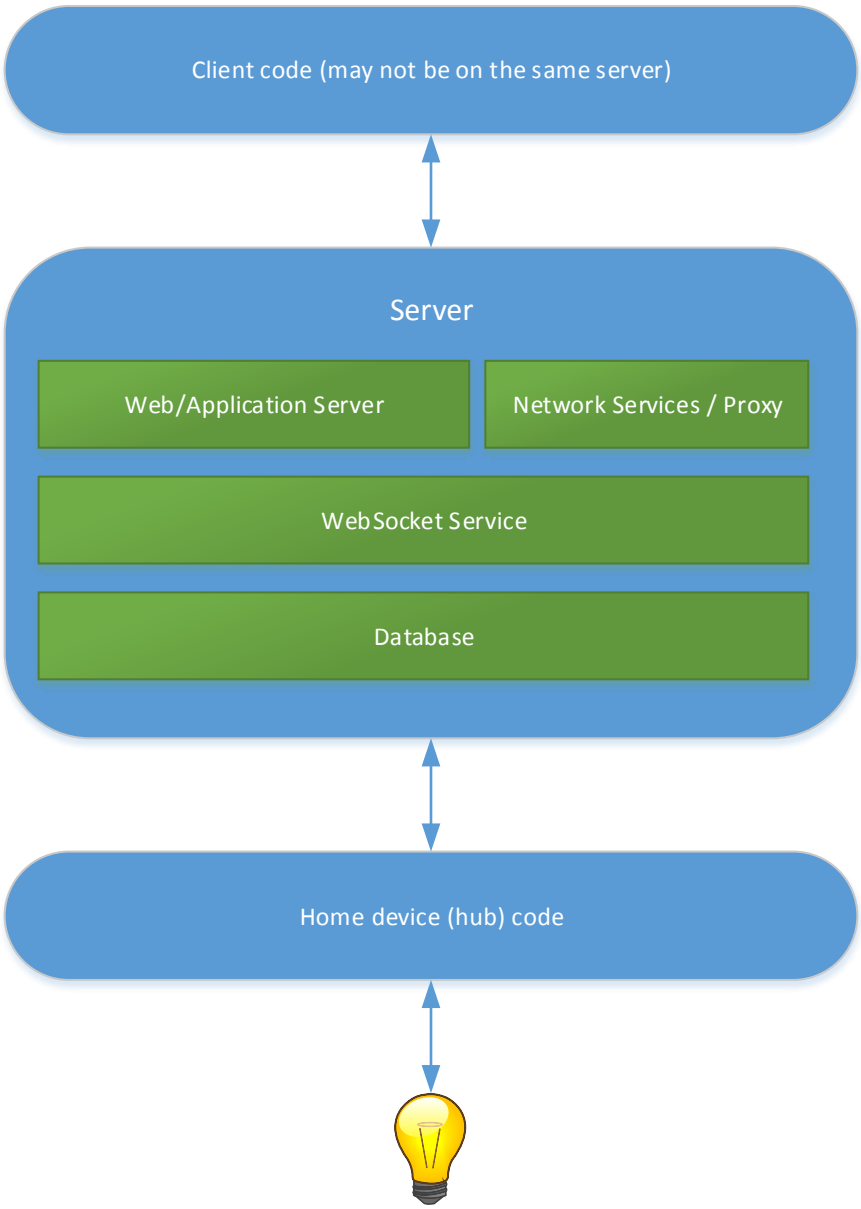


Фиг. 7 Схема на мрежовата архитектура на приложението

Клиентското приложение и посредникът използват WebSocket протокола, за да комуникират със сървъра, намиращ се в публичен център за данни. Играейки ролята на посредник, сървърът създава псевдо-директен комуникационен канал, което позволява употреба на приложението без необходимост от преконфигурация на NAT и firewall устройства, ако такива има налични в мрежите (NAT hole-punching). Смарт устройството и посредникът трябва да се намират в една и съща мрежа и подмрежа, но биха могли да се намират в различна мрежа от тази на клиента, стига и двете мрежи да са свързани с Интернет. За правилната работа на системата, функцията IGMP Snooping, поддържана от някои рутери и от OpenWRT, трябва да бъде изключена. Не на последно място, криптирането на връзката между отделните модули се осигурява чрез задължителното използване на TLS (Transport Layer Security) с RSA с 2048-битов ключ.

СОФТУЕРНА РЕАЛИЗАЦИЯ

На Фиг. 8 е показана опростена диаграма на софтуерната архитектура на приложението.



Фиг. 8 Диаграма на софтуерната архитектура

Използваните технологии включват:

- Клиентско приложение – HTML5 и JavaScript. Това позволява използването на приложението от което и да е съвременно мобилно устройство или компютър.
- Сървър – реализиран чрез езика PHP, Laravel framework и библиотеката Ratchet, позволяваща поддръжка на WebSocket. Данните за идентификация на потребителя се пазят в БД, управлявана от СУБД MySQL. Модулът е мултиплатформен.
- Посредник - написан чрез използването на Mono/.NET Framework и езика C#. Както другите два модула, посредникът е мултиплатформен и може да се изпълнява както под Windows, така и под Linux и macOS. Възможно е и интегрирането му в хардуерно устройство, например Raspberry Pi, за създаване на цялостно plug-and-play решение.

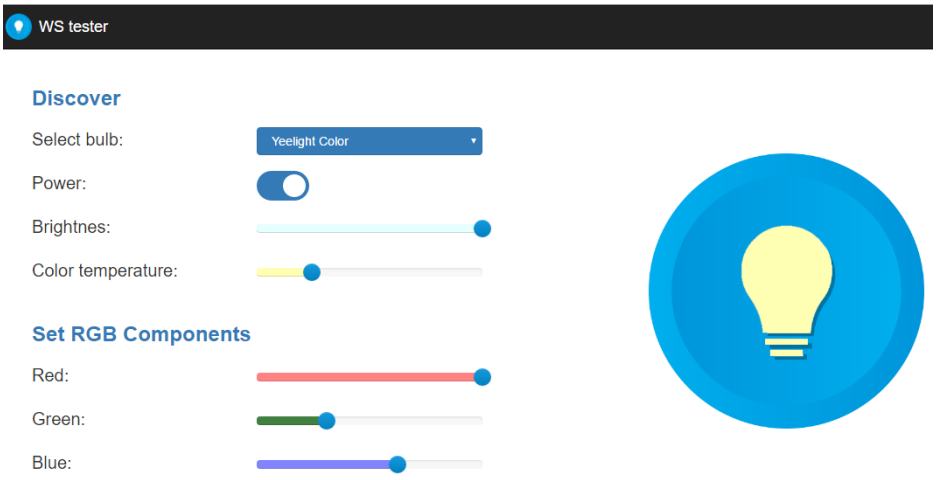
Програмният интерфейс (API) на приложението се отличава с това, че работи по WebSocket протокола, вместо да предоставя REST или SOAP уеб услуга. Поради това, единствената входна точка е адресът на WebSocket услугата. Съобщенията, обменяни между компонентите, са в JSON формат. Възможно е дадено съобщение

да съдържа в себе си друго такова, като поведението на приложението зависи от дадената команда. WebSocket входната точка изисква задължително TLS криптиране, което прави обмяната на съобщения между компонентите сигурна. Посредникът и клиентът се идентифицират пред сървъра чрез API ключ. Модул, който не притежава правилният ключ, не може да комуникира по WebSocket канала и връзката бива автоматично разпадната от сървъра при неуспешна идентификация. На Фиг. 9 са показани примерни съобщения.


```
{
   "action": "notifySubscribers",
   "id": 586,
   "secret": "insert-your-own",
   "content": "{\"event\":\"command\",\"requestId\":1,\"command\":\"discover\"}"
}
{
   "action": "commandResponse",
   "toCommand": "discover",
   "requestId": 1,
   "data": [],
   "error": 200,
   "bulbId": null,
   "message": "OK"
}
```


Фиг. 9 Примерни съобщения между модулите

Графичният потребителски интерфейс, реализиран чрез HTML5 и Javascript, е показан на Фиг. 10.



Фиг. 10 Графичен потребителски интерфейс

Към момента се поддържат всички Wi-Fi устройства от серията Yeelight на Xiaomi Corporation. Приложението може да управлява smart лампи с бяла светлина, RGB лампи, LED ленти, настолни лампи и др., поддържащи режим за разработчици, описан в сайта на производителя [5].

ЗАКЛЮЧЕНИЕ

Приложението беше подложено на множество тестове и от обобщените резултати може да се заключи, че работи точно, бързо и е лесно за употреба от потребителите. Извадка на резултати от направените тестове е представена в следващата таблица.

	Включване	**Изключване**	**Яркост**	**Температура**	**RGB компоненти**
Време за реакция	< 1 секунда	< 1 секунда	< 1 секунда	< 1 секунда	< 1 секунда

Създаденият продукт може да се прилага както във все по-широко навлизащата домашната автоматика, така и (с модификации) за индустриални приложения. Приложим е навсякъде, където е нужно сравнително навременно (но не с точност по-малка от няколко секунди, в зависимост от мрежата) и защитено предаване на команди към отдалечени устройства и използване на резултата от тях. Използването на приложение-посредник осигурява и бъдещата съвместимост на системата и с други смарт устройства – не само такива за осветление.

ЛИТЕРАТУРА

[1] Fette, Ian. "The websocket protocol." (2011), https://tools.ietf.org/html/rfc6455
[2] Furukawa, Y. "Web-based control application using WebSocket." ICALEPCS2011 (2011): 673-675.
[3] Pimentel, Victoria, and Bradford G. Nickerson. "Communicating and displaying real-time data with websocket." IEEE Internet Computing 16.4 (2012): 45-53.
[4] Surie, Dipak, Olivier Laguionie, and Thomas Pederson. "Wireless sensor networking of everyday objects in a smart home environment." Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008. International Conference on. IEEE, 2008.
[5] Yeelight WiFi Light Inter-Operation Specification, Yeelight, 2015 http://yeelight.com/download/Yeelight_Inter-Operation_Spec.pdf

За контакти:

инж. Павел Златаров, катедра „Компютърни системи и технологии“, Русенски университет „Ангел Кънчев“, e-mail pavel.zlatarov.bg@ieee.org

инж. Мирослав Маринов, катедра „Компютърни системи и технологии“, Русенски университет „Ангел Кънчев“, тел. 0889183880, e-mail miro42@abv.bg

доц. д-р инж. Ирена Вълова, катедра „Компютърни системи и технологии“, Русенски университет „Ангел Кънчев“, e-mail irena@ecs.uni-ruse.bg

Design and implementation of a pattern repository for protein cross motif search

author: Miroslav Marinov
supervisor: phd Irena Valova

Abstract: Finding most significant protein motifs in secondary structures of proteins. *This paper gives a new software for storing protein data and searching into it for most interesting protein motifs.*
Key words: *Protein, Motif, Secondary Structure, Cross Compare method, Pattern repository (PR).*

ABSTRACT

Proteins are complex biological structures and the fundamental brick for all organic life. Proteins can be studied at different levels of complexity. At the most basic levels, proteins are threads of amino acids. At the secondary level, proteins can be seen as cluster of repeating structures or **motifs**, such as helices and strands with a complex but identifiable spatial arrangement. In literature, protein is usually analyzed at the primary levels through topological approaches. However, we believe that new interesting insights can be achieved studying proteins at the secondary level using a geometrical approach and pattern repository. We exploited parallel methods, and advanced implementation and programming techniques to develop our **Cross Compare method**, which managed to retrieve and distinguish with very good precision thousands of interesting motifs.

INTRODUCTION

Biological chemistry is organized around chemical element carbon (C). It is element of the living matter. Carbon has the ability to form stable covalent bonds with other bulk elements such as hydrogen (H), oxygen (O), nitrogen (N) and carbon itself. A protein is a polymer which consist one or more chains (polypeptides) of amino acids. There are only 20 different amino acids that can naturally occur in proteins. Amino acids are called residues. They are part of a (poly-) peptide. [0]

Proteins are large and complex polymers and their structure is described at several levels of abstraction:

- **The primary structure** – represents the sequence of all amino acids in polypeptide chain;
- **The secondary structure** - represents secondary structure elements in protein;
- **The tertiary structure** - represents the overall 3D shape of a single polypeptide chain, the atom comprising and position. This structure completely identifies proteins which are made up of only one polypeptide chain.
- **The quaternary structure** – represents proteins which are made up of more than one polypeptide chain which are also called protein subunits. [0]

Different protein structures are illustrated on Fig. 1.

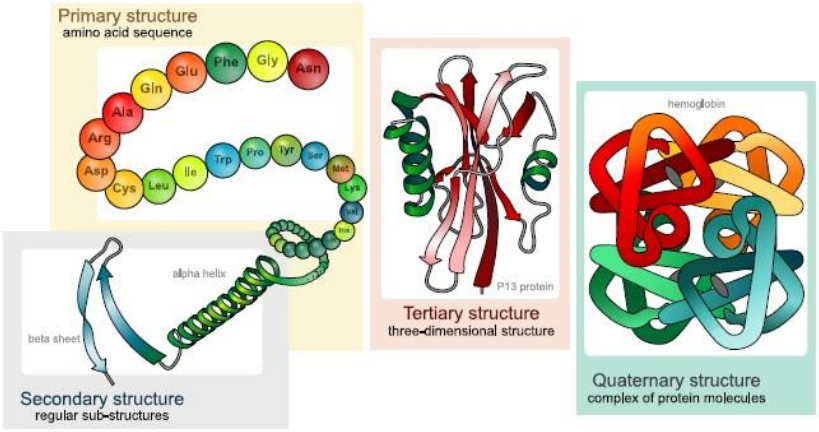


Fig. 1 Protein structures [1]

Secondary structure element is a small segment of the protein chain. It can be identified as a recurring pattern among a multitude of proteins. Each secondary structure element is made of multiple residues shaped in 3D structure of protein. The first two to be discovered, and the most commonly recurring secondary structure elements, are the α-helix and the β-sheet as described by Pauling [0, 0].

Protein folding is the subject of a number of physical and chemical constraints. It is not a random process. Some recurring folding patterns have been identified at the secondary structure level of the protein. They are small groups of secondary structure elements which are called super-secondary structures or structural motifs. Since special biological functions are deemed to be tightly connected with these 3D structures, motif pattern searching and discovery has become an important field in the bioinformatics domain [0].

STATE OF THE ART

So far known variety of methods and algorithms for recognition of a common motif in different proteins. In one of them, subscribed in papers [0][0], we check for uniformity pattern that is observed in primary protein with a motif that is found in another protein. In our case, we collect the proteins compares and store them into databases. Then extract results from database, examine them and analyze the possible reasons that could potentially be very good and common motifs.

CROSS MOTIF SEARCH

Loading files pairs of proteins, there are several options:

- proteins already be inserted into the database;
- one of the proteins is inserted into the database, and the other is not;
- both proteins are not inserted into the database.

In all three instances, it is considered a simple rule that if there is information about protein, it is not loaded again. However, there is no any information about the comparison between the two proteins, then if there is information for both protein is charged only this comparison between them. For effective cross motif search, there must be enough information for proteins. This means that in addition to information about source protein and it search proteins should provide information about comparisons between all search proteins or part of them.

CROSS COMPARE METHOD

The method consists finding a pattern with two important conditions:

- based on source protein can be found motif in search protein that corresponds to the pattern of other search proteins;

- finding a similar pattern to check whether it complies with the motifs that are loaded into the database for these specific proteins.

Where there is sufficient information, the cross compare method began to examine the basis of source protein all search proteins for which there is information in the database. The method continues with a comparison of all search proteins with one another. There are three options at this point:

- to have no information in the database for comparison between source protein and search proteins;
- to have information about the comparison, but there are no common motifs between source protein and search proteins;
- to have information for comparison and to have common motifs between search proteins based on the source protein.

The idea of the method is considered in the example shown on Fig. 2.

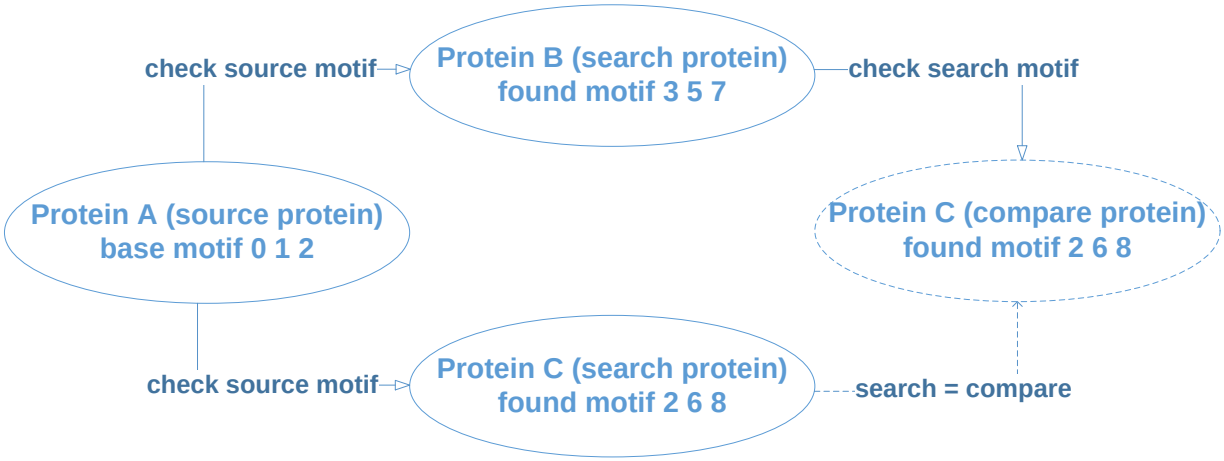


Fig. 2 Example of cross compare method

Explore the motif "0 1 2" source protein A as we begin to search the search proteins B and C. In the case under consideration, we find that there is a match with the subject motif respectively motif "3 5 7" in protein B and motif 2 6 8 in protein C. We continue to explore motifs, as search protein C of source protein A was examined compare protein C for search protein B. The last step is to verify findings motif in search protein B with discoveries motif in compare protein C in the existing information in the database for comparison between protein B and protein C. If the test is successful we pay particular attention to the motif "0 1 2" of source protein A, because there are likely to be found in other proteins.

IMPLEMETATION

ARCHITECTURE

The program is implemented through the C ++ programming language, QT framework and MySQL server. The architecture is illustrated on Fig. 3.

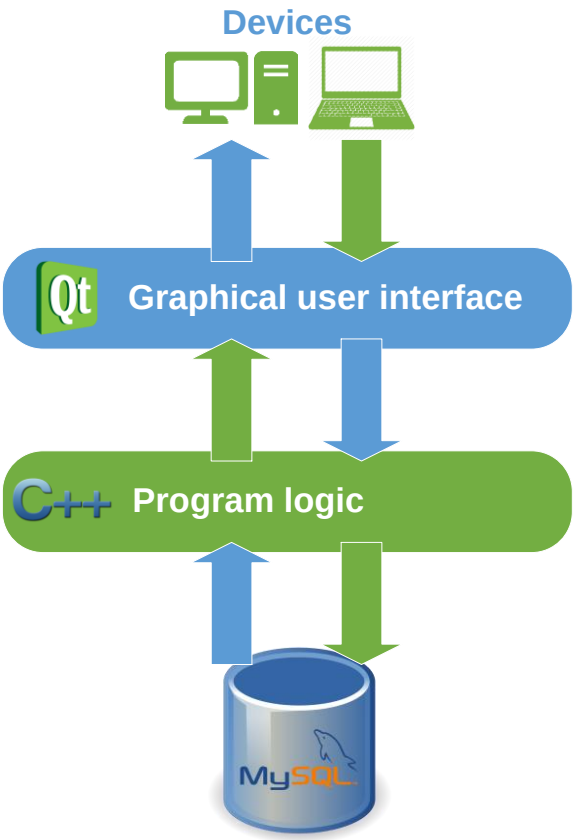


Fig. 3 Architecture of application

PROTEIN INFORMATION

Thanks to several tables ensures the preservation of all relevant information about each protein. They keep the name of the protein, all of the motifs of the loaded file, its secondary structure, together with the coordinates, and the points that form the individual chains of the protein. Once all this information is available, starting with the preservation of the result of the comparison between source and search protein.

PROTEINS COMPARISON

The other tables in the database are to keep the information from the comparison of proteins. They keep the proteins compare result, which include all protein chains with hits, number of these hits, motifs, that appear in the comparison, and coordinates of points on the peaks of comparing between proteins. Furthermore, the results of the comparison between protein here is the table which stores the expression for calculating the percentage of matching. It is necessary to be able to keep this expression, which operates in particular database, to update current information and when we load new data into the database to calculate it with the same expression. Different databases can work with different expression and this requires each database to have table to keep it for correct calculating of matching percentage.

RESULTS

Upon completion of cross compare method generated results are subject to different treatment by the user. The program allows filtering of results in different ways to separate the most remarkable motifs among them. There are additional options to generate files depending on user preferences and depending on how the results are created.

To get maximum insight from the work of the program will make a test with the following several conditions:

- The maximum number of files that will load in the database will be approximately 478;
- The maximum number of databases will be 4;
- Will divide files into 4 parts ranging from 120 and reach 478;
- Each of the four parts will be loaded into one databases;
- The name of each database depends of loaded files in it, i. e. database names are: 120_files, 240_files, 360_files and 478_files;
- We will examine each database separately charged with her own files;
- The test will be made by "Add source protein motifs".

The results are shown on Fig. 4 (only one base protein) and on Fig. 5 (global search for each protein into database).

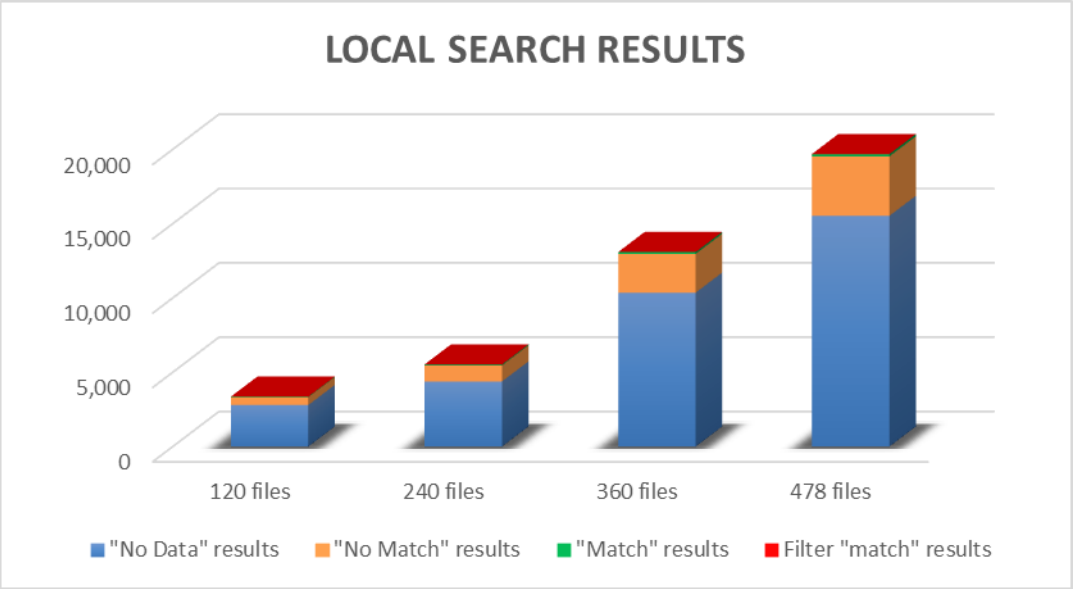


Fig. 4 Local search final results

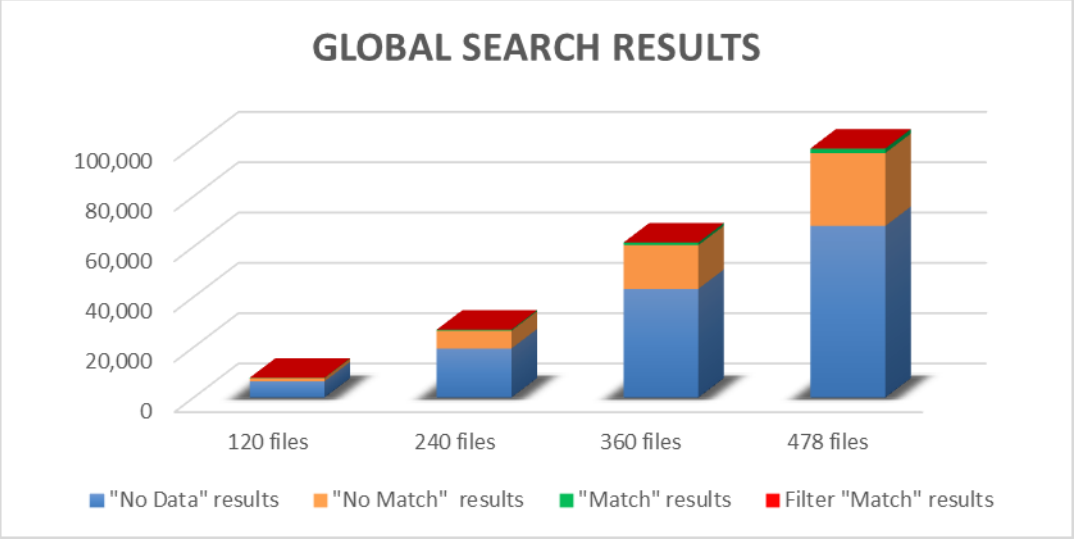


Fig. 5 Global search final results

Note that these tests are made with random data about proteins and comparisons between them.

CONCLUSION

From the results we can say that the number of files does not really matter in the study of proteins. Rather interest is working with files in which each protein inserted into the database has comparisons with everyone else in it. Only then is possible to use the best power of the application and to distinguish the most remarkable motifs.

From the results we can conclude that the method is effective. Provides a new way to study proteins. Through this method carefully you can explore many different motifs, among them will excel those with the most notable features. It is they must be studied in depth and from them to seek answers for uniformity of structures in different proteins.

The method shrinking circle of best possible motifs, studying preliminary results for proteins. Thus we can focus biologists who motifs to look for and exactly which proteins are found to be able to more effectively focus resources to deal with the study of common structures in proteins.

BIBLIOGRAPHY

[1] Cantoni, V., Ferrati, M., Musci, M., Nugrahaningsih, N., Structural motif identification and retrieval: a geometrical approach, Department of Electrical, Computer and Biomedical Engineering, Pavia, Italy, 2014.

[2] Ferrati, M., Musci, M., Geometrical motif search in proteins: parallel approach, Department of Engineering, Pavia, Italy, 2014.

[3] Pauling, L., Corey, R., and Branson, The anatomy and taxonomy of protein structure, National Academy of Sciences of the United States of America, 1951.

CONTACTS:

Miroslav Boianov Marinov, RU "Angel Kanchev", Faculty of EEA, Specialty "Computer systemc and technologies", course I, Master degree, e-mail: miro42@abv.bg

Irena Valova, Department of "Computer systemc and technologies" Faculty of EEA, RU "Angel Kanchev", e-mail: Irena@ecs.ru.acad.bg

Анализ на два вида мрежови атаки и методи за предпазване от тях

автор: инж. Калоян Петров
научен ръководител: доц. Пламен Захариев

Analysis of two types of network attacks and methods to prevent them: *Basic switch security does not stop malicious attacks. Security is a layered process that is essentially never complete. The more aware the team of networking professionals within an organization are regarding security attacks and the dangers they pose, the better. Defending a telecommunication network against attacks requires vigilance and education.*

Key words: *Switch, Ports, Port-security, Vulnerabilities, Attackers, Prevention, Mac address, CAM table, Yersinia, DTP, Network Threats, Man-in-the-Middle.*

ВЪВЕДЕНИЕ

Изграждането на сигурност в дадена мрежа е критичен фактор, на който трябва да се обърне сериозно внимание. Кабелните и безжичните компютърни мрежи са от съществено значение за ежедневните ни дейности. Индивидуалните организации зависят по същия начин от техните мрежи и компютри. Неправомерното проникване в мрежите може да доведе до прекъсване на комуникацията и до загуба на данни. Мрежовата атака може да бъде опустошителна и да доведе до кражба на важна информация и загуба на време и пари.

Нарушителите могат да получат достъп до мрежата през софтуерна уязвимост, хардуерна атака или чрез „разбиване" на потребителско име и парола на упълномощен потребител. Нарушителите, който получават достъп чрез модифицирането на софтуер или използването на софтуерна уязвимост се наричат „хакери".

След като хакерът получи достъп до мрежата могат да възникнат четири вида заплахи:

- **Кражба на информация**
- **Загуба на информация и манипулация**
- **Кражба на самоличност**
- **Отказ на услуги**

Мрежовите атаки могат да бъдат класифицирани в три основни вида:

- **Разузнавателна атака –** този тип атака открива и проследява системите, услугите и слабостите на една мрежа
- **Атака за получаване на достъп –** неоторизирана манипулация на информация, системен достъп или използване на привилегии
- **Отказ на услугата-** прекъсване или повреждане на мрежите, системите или услугите

1. Препълване на MAC таблицата на комутатор

MAC таблицата на комутатора съдържа MAC адресите асоциирани с всеки физически порт, както и асоциирания VLAN на порта. Когато рамка пристигне на порта на комутатор MAC адреса на източника се записва в MAC таблицата. Ако MAC адреса вече е записан тогава комутатора проверява дали присъства MAC адреса на желаната дестинация, за която е предназначена рамката. В случай че присъства комутатора изпраща рамката на желания порт, но ако MAC адреса на желаната дестинация е неизвестен тогава комутатора изпраща рамка на всеки свой порт (Broadcast) с изключение на този от който е получил рамката. Ако устройството, за което е предназначена рамката е асоциирано с някой от портовете на комутатора то връща отговор със своя MAC адрес . По този начин комутатора научава за него.

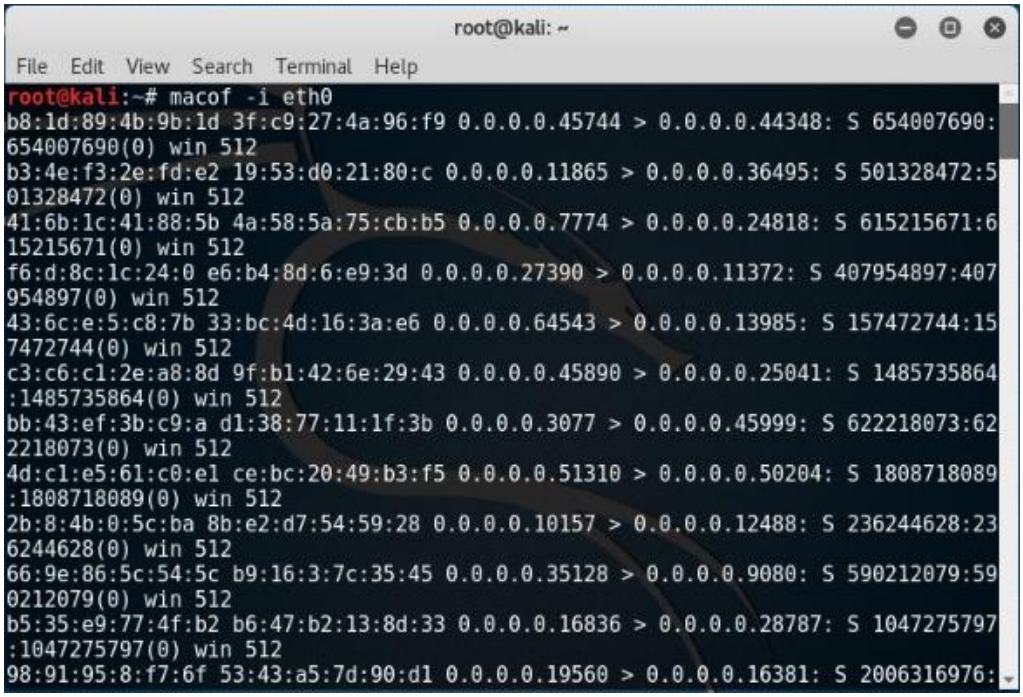
Останалите устройства в мрежата отхвърлят рамката. Защото не е предназначена за тях.

Препълването на Mac таблицата се осъществява чрез използването на фалшиви, неизвестни адреси за комутатора. Когато на даден порт на комутатора се прикачи хакер, който ще го „атакува" той използва тези фалшиви адреси за генерирането на заявки към комутатора докато Mac таблицата се запълни с тях и измести валидните записи. По този начин устройството се запълва само с фалшиви записи. Когато това се случи комутатора, който е "интелигентно устройство" започва да работи като своя предшественик HUB-а (тоест всяка получена рамка на даден порт се изпраща на всички останали). Опасността от това е, че рамката от оторизирания трафик ще бъде получена на порта, на който хакера се е прикачил, като по този начин може да анализира трафика на устройствата в мрежата.

2. Осъществяване на атаката

Осъществяването на този тип атака се извършва сравнително лесно, ако приемем идеалните условия – Man-in-the-Middle. За целта е необходимо да разполагаме с машина (компютър) на който да е инсталиран или стартиран чрез Live CD операционна система Kali Linux. Необходим е и обаче физически достъп до устройството, което ще се атакува в случая това е Cisco Switch серия 29xx.

След като сме се свързали към Fa0/1 интерфейсът на комутатора за да препълним MAC адресната таблица е необходимо изпълнението само на една команда – "**macof –i eth0**". Изпълнението на тази команда генерира фалшиви Mac адреси с които се подават заявки на съответния интерфейс на който сме свързани. Фигура номер 1 представлява резултата от въвеждането на командата.



Фиг. 1 Резултат от въвеждането на командата „macof –i eth0"

Резултатите от фигура 1 представляват генерирането фалшиви Mac адреси на източници и получатели към комутатора. По този начин Mac или CAM таблицата на комутатора се запълва, както става ясно от следващите две фигури, на който са илюстрирани резултатите в MAC адресния брояч на комутатора преди и след изпълнение на препълващата атака.

```
Switch#show mac address-table count

Mac Entries for Vlan 1:
-------------------------
Dynamic Address Count   : 3
Static  Address Count   : 0
Total Mac Addresses     : 3

Total Mac Address Space Available: 8044
```

Фиг. 2 Резултат в Mac адресния брояч преди изпълнението на командата „macof –i eth0"

```
Switch#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count   : 7992
Static  Address Count   : 0
Total Mac Addresses     : 7992

Total Mac Address Space Available: 48
```

Фиг. 3 Резултат в Mac адресния брояч след изпълнението на командата „macof –i eth0"

След като Mac адресната таблица е препълнена комутатора е препълнена мрежовия сегмент в който работи комутатора не се различава от "споделена преносна среда" използваща HUB. Тогава злонамерения потребител има възможност да анализира трафика в мрежовия сегмент.

3. Предпазване от препълване на Mac адресната таблица

Един от начините да избегнем препълването на Mac таблицата от неоторизиран злонамерен потребител е конфигурирането на *port-security.* За целта е необходимо режима на работа на порта да е статичен (Trunk или Access), след това да се конфигурира *port-security* на Mac адреса било то статичен, динамичен или динамичен „лепкав" (фигура 4).

```
Switch(config-if)#switchport port-security ?
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
```

статичен

Динамичен „лепкав"

Фиг. 4 Възможно опции за конфигуриране на port-security

Също така е възможно да се зададе максимален брой на Mac адресите, който могат да се научат от съответния порт чрез въвеждането на командата "switchport port-security maximum" и след това въвеждане на съответния максимален брой Mac адреси (могат да варират от 1 до 132 на порт). Освен това добра практика е да се изключват неизползваните портове на комутатора. Третия ред от възможните опции е "violation". С него се оказва какво да бъде предприетото действие при нарушение на правилата (по подразбиране порта се изключва).

4. VLAN Hopping атака

Мрежата с множествен достъп Ethernet поддържа различни режими на работа между мрежовите устройства от тип точка-точка. Комутаторите на Cisco използват

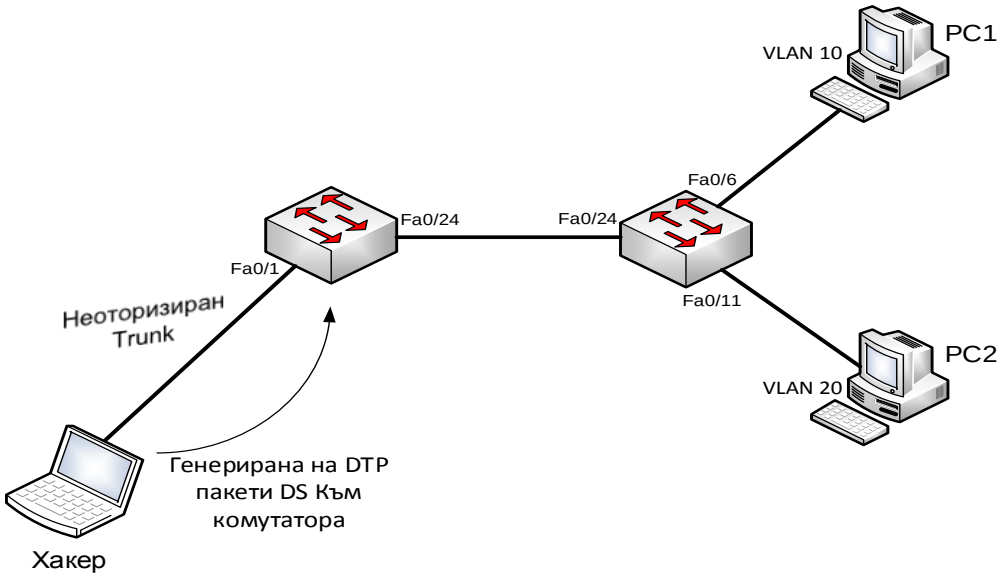
функция наречена „договаряне" на режима, която се поддържа от Dynamic Trunking Protocol (DTP). Протоколът е разработка на Cisco и по подразбиране е активен на Cisco Catalyst 2960 и Catalyst 3560 комутатори. Комутатори от други фирми не поддържат DTP протокола. Два са режимите на връзките, който могат да бъдат договорени или статично зададени. Режим за пренасяне на маркиран трафик (Access), или режим на пренасяне на немаркиран трафик (Trunk). Интерфейсът на комутатор може да бъде поставен в режим на договаряне на Trunk. DTP управлява Trunk договарянето само ако порта на съседното устройство е конфигуриран в режим да поддържа DTP. Порта разполага с четири режима на работа, като два от тях са статични (Static Trunk, Static Access), а останалите са динамични управляващи се от DTP, който служат за договаряне на връзката (Trunk или Access). На представената таблица 1 са илюстрирани различните режими на порта и договарянето на връзките между тях.

Таблица 1 Режими на работа на портовете и договаряне на връзките между тях

	Dynamic Auto	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

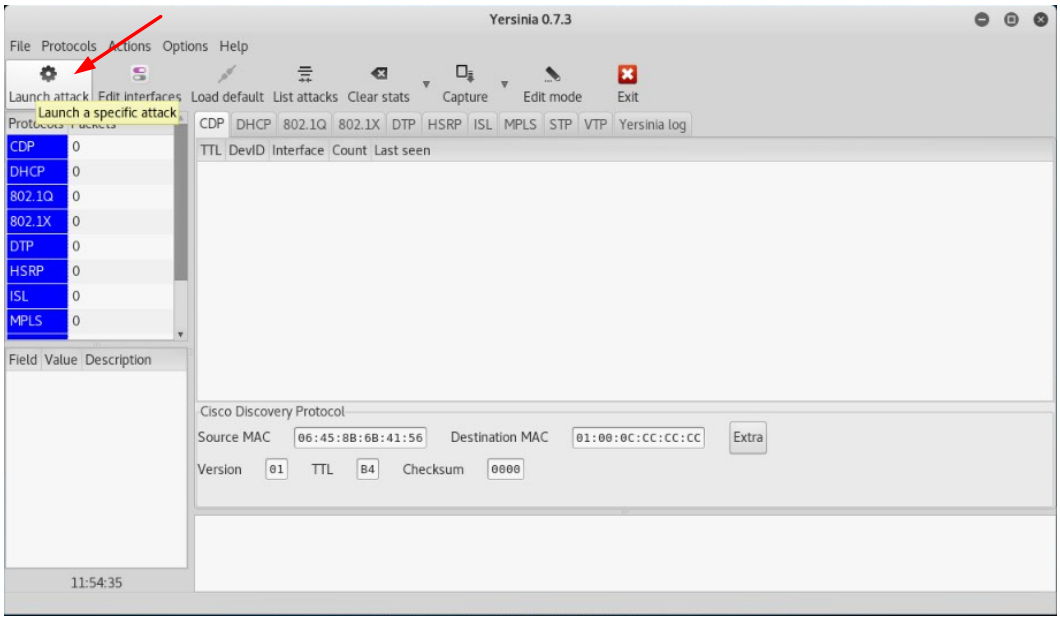
5. Осъществяване на DTP атака

Именно договарянето между връзките отваря вратичка за пробив в сигурността. Да си представим, че на някой от портовете на Switch-а, който работи в динамичен режим се прикача хакер с лаптоп фиг.5. Когато хакерът осъществява този тип атака той използва слабостта на устройството, която е режима на порта по подразбиране а именно Dynamic Auto. По този начин той конфигурира системата, която в илюстрирания случай е лаптоп да представя себе си като Switch генерирайки DTP пакети емулирайки стандарта 802Q. Така се мами комутатор (Switch) и "той си мисли", че друг комутатор се опитва да формира Trunk връзка. Когато това се случи хакера получава достъп до всички позволени vlan мрежи на Trunk връзката.



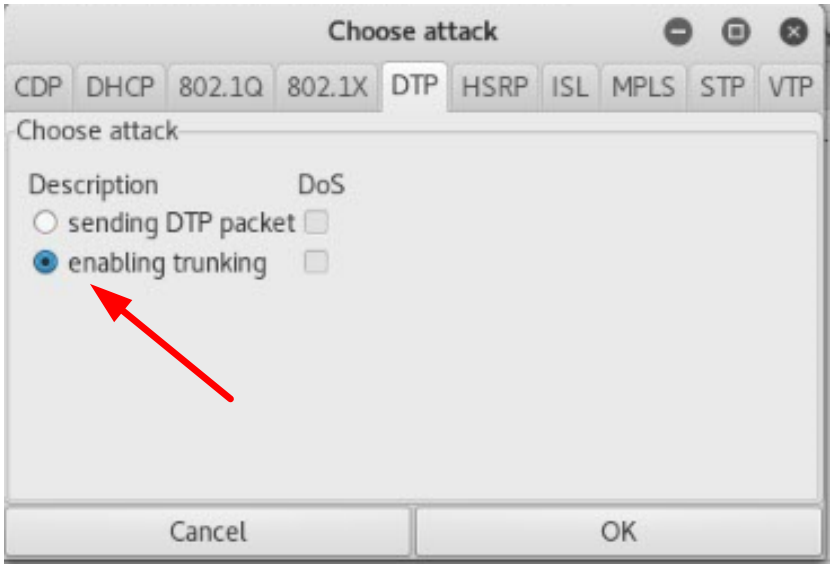
Фиг. 5 Топология на мрежата, върху която се осъществява атаката

След като е стартиран Kali Linux на хакерската машина DTP атаката може да се осъществи със софтуера "Yersinia" илюстриран на (фиг.6), който се използва за осъществяване на атаки в каналния слой от OSI модела.



Фиг. 6 Yersinia

От горния ляв ъгъл се избира стартиране на специфична атака. След избирането на бутона се отваря прозорец с набор от атаки. От там се избира DTP атака. След като е избрана атаката, която ще се осъществява в случая DTP в под менюто „описание" избираме "Enable Trunking", което позволява емулирането на DTP пакети (Dynamic Desirable) – Фигура 7.



Фиг. 7 Избиране на атака с емулиране на пакети Dynamic Desirable

Заради същността на DTP, атакувания комутатор на фигура 5 „инстинктивно" сформира Trunk връзка на порта, на който е свързана хакерската машина. След горно извършените действия атаката е осъществена и хакерската машина генерира DTP пакети и сформира неоторизираната Trunk връзка. На следващите две фигури са илюстрирани Trunk връзките на комутатора преди и след извършване на атаката.

```
Switch#show interfaces tru

Port        Mode             Encapsulation  Status        Native vlan
Fa0/13      on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/13      1,10,20

Port        Vlans allowed and active in management domain
Fa0/13      1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,10,20
Switch#
```

Фиг. 8 Trunk Връзките на комутатора преди извършването на DTP атаката

```
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       auto             802.1q         trunking      1
Fa0/13      on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/13      1,10,20

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20
Fa0/13      1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20
Fa0/13      1,10,20
```

Фиг. 9 Trunk Връзките на комутатора след извършването на DTP атаката

Когато това се случи за мрежата става много опасно, защото могат да се извършват Man-IN-the-middle атаки, който могат да бъдат критични и скъпо струващи на дадена организация.

6. Предпазване от DTP атака

- Изчистване на всички TRUNK портове който не се използват.

- Добра практика е всички портове да се конфигурират в неизползваем VLAN.
- Изключване на всички неизползваеми портове.
- Конфигуриране на портовете в статичен режим на достъп(Static Access).
- Основния Native VLAN да бъде неизползван от други VLAN мрежи.
- Основния Native VLAN да бъде различен от VLAN1 !
- На портовете, който се изисква Trunk да се изключи договарянето (изпращането на DTP пакетите)

ЗАКЛЮЧЕНИЕ

Осъществяването на демонстрираните атаки е само първата стъпка към проникването в дадена мрежа. Веднъж успешно изпълнени те отварят нови врати към пробиви в сигурността, който могат да бъдат фатални. Научната статия има за цел да се направят тестове на сигурността в дадена мрежа чрез извършване на атаките. По този начин се разбира къде са слабостите на мрежата, с цел да се предприеме съответната защита. Една мрежа никога не е напълно защитена, затова мрежовите администратори трябва да са добре запознати с видовете заплахи и имплементирането на методи за сигурност.

ЛИТЕРАТУРА

[1] Andrew Lockhart. NETWORK SECURITY HACKS.
[2] CCNA Routing and Switching: Routing and Switching Essentials.
[3] CCNA Routing and Switching: Introduction to Networks

За контакти:

Калоян Петров, Русенски университет „Ангел Кънчев", специалност „Интернет и мултимедийни комуникации", e-mail: kaloqnpetroff@gmail.com

доц. Пламен Захариев, Русенски университет „Ангел Кънчев", Катедра „Телекомуникации", e-mail: pzahariev@uni-ruse.bg

Анализ на характеристиките и възможностите на Cicret гривна

автор: Мартина Прахова
научен ръководител: гл.ас. д-р Григор Михайлов

Analysis of characteristics and possibilities of Cicret Bracelet: *The Cicret Bracelet can project a touchscreen onto your arm, making it possible for you to easily access and work your apps without having to take out your phone. The bracelet uses a Pico projector to project your phone's screen onto your arm, and it's equipped with eight proximity sensors which makes it possible for the bracelet to detect the finger position whilst you control the device. With the Cicret Bracelet, you can make your skin your new touchscreen. Read your mails, play your favourite games, answer your calls, check the weather, etc. Do whatever you want on your arm. The device will allow users to send and receive emails, browse the web and play games. It will also be possible for users to pair it with an existing smartphone, answer incoming phone calls and activate the speakerphone functionality on their smartphone.*

Key words: *Cloud technology, Mobile device, Pico project Technology.*

ВЪВЕДЕНИЕ

Cicret гривната е като таблет, но върху кожата. Потребителите носят тънка пластмасова лента на китката и просто поклащат ръката си, за да активират Android touchscreen повърхност на ръката си.

Четиричленен екип от Франция е измислил идеята за гривна, която да може да превърне ръката на притежателя си в екран на мобилен телефон, използвайки пико проектор. Оборудвана с масив от осем сензора за близост, които определят позицията на пръста на потребителя, гривната може да бъде използвана за провеждане на телефонни обаждания, писане на имейли, сърфиране в мрежата, игри, както и за гледане на филми [1,4]. Гривната съдържа микро USB порт и акселерометър, като поддържа bluetooth и wi-fi технологиите.

Развитието на Cicret е базирано на облачна технология, като се състои от две части. Първата е приложение, а втората е самата гривна. Приложението Cicret е единственото интуитивно, сигурно и свободно решение за тези, които искат да чатят, използват и обменят данни, като в същото време няма никакъв шанс да бъдат проследени. Приложението не изисква никакви лични данни, използва AES-256 стандарт за шифриране и RSA алгоритъм за шифриране на данни, при който се използват различни ключове за шифриране и дешифриране [4].

Гривната е водоустойчива и приложенията за нея са обширни – тя може да прави всичко, което един телефон или таблет могат, но без нуждата от твърд екран.

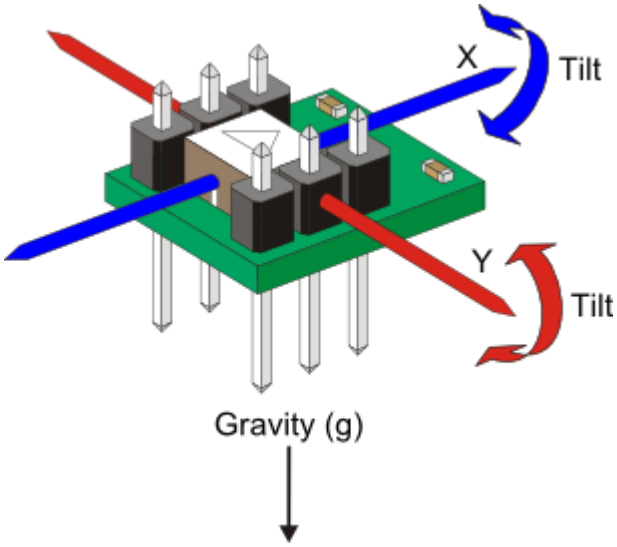
I. КОМПОНЕНТИ НА CICRET ГРИВНАТА

Cicret гривната съдържа USB порт и акселерометър, както и поддържа bluetooth и wi-fi, но не разполага със собствена SIM карта, като това означава, че технологията трябва да се използва в комбинация с мобилен телефон. Гривната съдържа също и акселерометър, който при поклащане на ръката на потребителя я активира и при повторно поклащане я поставя в спящ режим. На Фиг. 1 е изобразена структурата на гривната [3] и тя се състои от следните компоненти:

- Акселерометър - електромеханично устройство, което измерва вибрации или сила на ускорение. Акселерометрите се използват в таблети и цифрови камери, така че изображенията на екрана винаги да се показват изправени; използват се при дроновете за стабилизиране при полет. При мобилните телефони екранът се върти автоматично, за да се приспособи към изгледа на потребителя. При тази гривна, когато е разклатена два пъти се активира и когато се разклати отново се поставя в спящ режим.

Фиг. 1 Структура и компоненти на гривната

Двуостният акселерометър (фиг.2) е чувствителен спрямо гравитационното земно притегляне, което му позволява да отчита наклон, вибрация и движение. Сензорът осигурява два независими резултата, обозначени на фигурата като X и Y. Оста X измерва наклон напред или назад, а Y измерва наклон настрани [5].

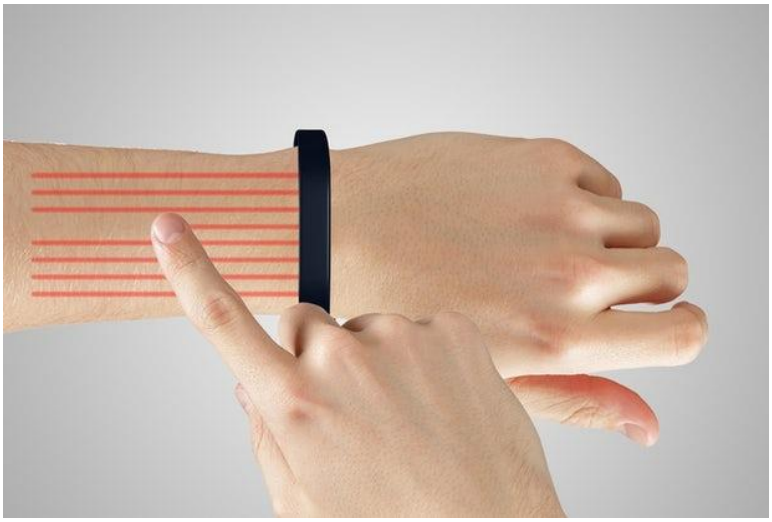


Фиг. 2 Двуосен акселерометър

- Карта памет- използват се за съхранение на цифрова информация. Cicret гривната работи с 16 и 32 GB карти.
- Процесор;
- Вибратор – дава известия на потребителя;
- Микро USB порт – използва се, за да осигури свързаност, посредством USB кабел (фиг. 3) за обмен на данни между дадена система и гривната, както и за зареждане на батерията.
- Батерия – осигурява приблизително 8 часа работа;

Фиг. 3 Микро USB кабел

- Сензори за близост – сензори, способни да улавят присъствието на близки обекти без да се осъществява физически контакт (фиг.4) [1, 6]. Пико проектора проектира интерфейса върху ръката и когато поставим пръстът си върху този интерфейс, един от осемте широкообхватни сензора за близост спира и така сензорът изпраща информацията до процесора в гривната.



Фиг. 4 Сензори за близост

- Пико проектор – включва миниатюрни хардуер и софтуер, които могат да проектират цифрови изображения върху всяка близка повърхност.
- Bluetooth – когато не е налична wi-fi връзка, гривната и телефонът могат да бъдат свързани посредством Bluetooth; също може да се използва и за обмен на данни с други устройства.
- Wi-Fi компонент – позволява връзка между смартфона и гривната, докато има интернет свързаност, налична и за двете устройства.
- LED – показва известия, както и работата на даден процес.
- Бутон – бутон за включване и изключване на гривната.

Концепцията Cicret се състои от две части – гривна и приложение. За да използваме гривната трябва да изтеглим и инсталираме приложението Cicret App, като то не изисква достъп до каквато и да било лична информация.

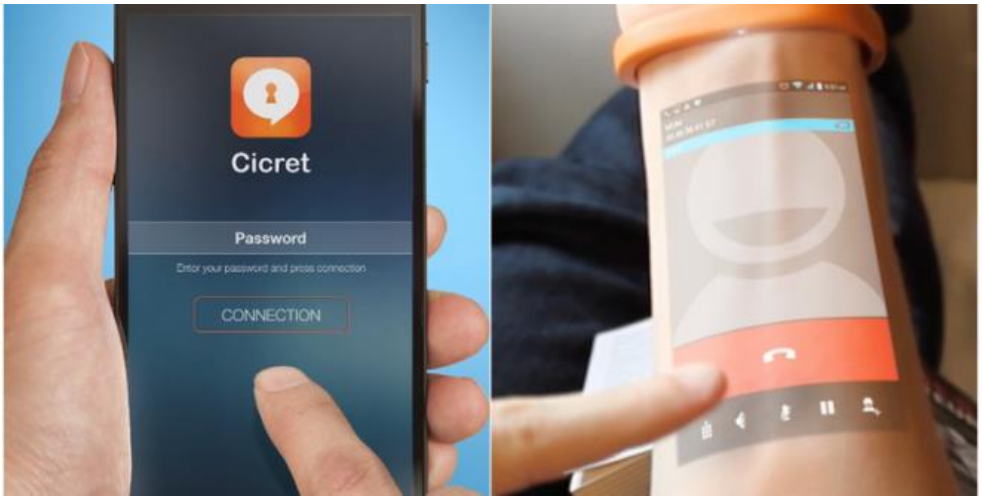
II. ПРИНЦИП НА РАБОТА

Както беше обяснено по-горе гривната използва пико проектор, за да визуализира телефонния екран върху ръката на потребителя, разполагайки с осем сензора (фиг. 5) [1], които дават възможност на гривната да улови позицията на пръста, като след това изпраща информацията до процесора в гривната.

Фиг. 5 Пико проектора и масива от 8 сензора с които е оборудвана гривната

Cicret работи с версия на Android, като може да бъде свързана с мобилен телефон чрез Bluetooth. Потребителите ще могат използват Wi-Fi за връзка, гривната също така има и micro USB порт. Компанията има и приложение – Cicret App, програма за сигурност, която осигурява анонимност и опции за криптиране за мобилните устройства. Cicret гривната, заедно с приложението (фиг.6) [1] ни позволяват достъп до почти всички приложения на телефона без нуждата от това да държим устройството постоянно в ръцете си.

Приложението предоставя анонимност и пълен контрол над всякаква информация, която споделяме, дори и след като сме я споделили, все още можем да я изтрием или коригираме. Приложението не изисква никакви лични данни, използва AES-256 стандарт за шифриране и RSA алгоритъм за шифриране на данни[4].



Фиг. 6 Приложението Cicret и интерфейса на гривната

ЗАКЛЮЧЕНИЕ

Cicret гривната все още е във фаза прототип, но се очаква в близките месеци да бъде пусната на пазара [1], като възможностите на този продукт са вълнуващи.

Гривната ще позволява достъп до почти всички приложения на мобилното устройство, без нуждата да го държим в ръцете си постоянно. Гривната е водоустойчива и може да се използва както с мобилен телефон, така и самостоятелно. Недостатък е ниският живот на батерията. Cicret гривната е една впечатляваща технология, която ще революционира начина, по който използваме приложенията, като използваме своята собствена кожа и превръщайки я в новият ни touchscreen.

ЛИТЕРАТУРА

[1] https://cicret.com
[2]http://www.dailymail.co.uk/sciencetech/article-2871401/The-bracelet-turns-ARM-touchscreen-Cicret-projects-emails-videos-games-skin.html
[3] https://vulcanpost.com/
[4] http://www.techtimes.com/
[5] http://fusion94.org
[6] http://newatlas.com/cicret-bracelet

За контакти:

Мартина Прахова, Специалност „Интернет и мултимедийни системи“, магистър, email: m.prahova8@abv.bg

гл. ас. д-р Григор Михайлов, Катедра “Телекомуникации”, Русенски университет “Ангел Кънчев”, тел.: +359 82 888 836, e-mail: gmihaylov@uni-ruse.bg

Роботи в сферата на изкуствения интелект

автор: Денислав Денчев
научен ръководител: гл. ас. д-р инж. Веселка Тодорова

Robots in the field of artificial intelligence-*In this report, I briefly look at "Artificial Intelligence," how it works, where it is used, what it serves, and why it is so useful. Robotics is a branch of AI, which is composed of Electrical Engineering, Mechanical Engineering, and Computer Science for designing, construction, and application of robots. The robots have* ***mechanical construction****, form, or shape designed to accomplish a particular task.*

Key words: *artificial intelect , intelect , robots*

ВЪВЕДЕНИЕ

Изкуственият интелект е наука за концепциите, които позволяват на компютрите да правят неща, които за хората изглеждат разумни. Изкуственият интелект има способност да анализира обкръжаващата го среда и да предприема действия, които увеличават възможността за постигане на определени цели. Изучаването на възможностите за създаване на такива устройства, наричани интелигенти агенти, е предмет на обособен дял от информатиката.

По друг начин казано, изкуственият интелект е наука за концепциите, методите и средствата за създаване на интелигентни компютърни програми и изследване на естествения интелект чрез компютърни системи.

Теорията на изкуствения интелект се основава на хипотезата, че основно човешко качество като интелигентността, може да бъде толкова точно описано, че да бъде симулирано от машина. Подобни разсъждения, свързани с въпросите за природата на разума и научното високомерие, могат да бъдат открити в митологията, художествената литература и философията още от Древността. В миналото обект на оптимистични или критични спекулации, днес изкуственият интелект е важен елемент на информационните технологии, използван за разрешаване на някои от най-трудните задачи в областта на информатиката [1].

Изследванията в областта на изкуствения интелект са силно специализирани, обособени в няколко подобласти, които често не успяват да взаимодействат ефективно. Тези направления възникват около определени институции, работата на отделни изследователи, решаването на конкретни задачи и често ги разделят различия в подхода към изграждането на изкуствен интелект, както и използването на напълно различни технически средства. Общи за повечето подобласти на изследванията на изкуствения интелект са задачи като възможността за разсъждение, обучение, планиране, общуване, възприемане, както и способността за движение и манипулиране на обекти.

I. АНАЛИЗ ВЪРХУ ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

Къде се използва изкуствен интелект?

Все повече банки въвеждат системи за изкуствен интелект при „игрите“ на борсата и управление на собствеността. Невронни мрежи се използват широко при разпознаване на текст и глас, медицинска диагностика, както и в националната сигурност. Автоматизиран онлайн асистент, осигуряващ обслужване на клиенти на уебстраница – едно от най-примитивните приложения на изкуствения интелект.

Приложенията на изкуствения интелект

Техниките на изкуствения интелект са твърде общи и твърде много, за да бъдат изброени. Наскоро, когато дадена техника достигне до масово потребление, тя вече не спада към изкуствения интелект; този феномен се описва като AI ефект.

Конкурси и награди в сферата на изкуствения интелект

Съществуват редица състезания и награди, които насърчават изследователската дейност в сферата на изкуствения интелект. Главните теми, които се насърчават са: обща машинна интелигентност, комуникативно поведение, извличане на данни, роботизирани коли, роботизиран футбол и други игри [2].

Факти свързани с изкуствения интелект

1. Независимо дали става въпрос за Google Now, Siri или Cortana, гласът по подразбиране е от женски пол. Няма конкретна причина това да е така, но за избора влияят няколко фактора. Според специалистите женският глас звучи по-успокояващо и по-малко заплашително от мъжкия. Освен това, върху AI работят предимно мъже и е нормално те да възприемат женския глас за по-атрактивен.
2. Екип учени са разработили робот, който може да се самопоправи при повреда, дори и след като загуби два от шестте си крака. За да разбере какъв точно му е проблемът, след регистрирането на такъв, роботът анализира с помощта на алгоритъм всички грешки и изчислява какво не е наред и как да се възстанови сам.
3. Интересен феномен в изкуствения интелект е суперкомпютърът SGI Altix, наречен Nautilus. Оказва се, че до известна степен, Nautilus може да предсказва бъдещето. Той е предвидил Арабската пролет. Нужната му информация, Nautilus събрал от над 100 милиона новинарски статии от всички краища на света, датиращи още от 1945 година.
4. Първата статия, написана от изкуствен интелект, се появи във вестник The Los Angeles Times. Тя се отнасяше до земетресение със степен 5 по скалата на Рихтер, регистрирано в Калифорния. Компютърът разчел данните от сеизмографа и основавайки се на тях съставил анонса. Разбира се все още сме далеч от написването на книга или сценарий за филм, но технологията се развива.
5. През 1997 година компютърът Deep Blue на IBM победи тогавашния световен шампион по шах Гари Каспаров. През 2011 година пък, IBM Watson участва в телевизионната игра Jeopardy и спечели. През тази година суперкомпютърът Claudico се яви на покер турнир в Питсбърг и макар че не победи, игра достойно.
6. Има една поговорка според, която компютрите са толкова умни, колкото лицето, което ги използва. Въпреки това, изкуствения интелект може да се самообучава. Например, Google разработиха система за изкуствен интелект, която се научи сама да играе Atari 2600 игри. След това, тя победи някои от най-добрите играчи в света. Друг пример е робот разработен от армията на САЩ, който се научи да готви от клипове в YouTube [3].

II. ПРИЛОЖЕНИЕ НА РОБОТИТЕ

В началото роботите са се използвали само и единствено в сферата на производството. Самата дума „робот“ идва от чешката дума „робота“, което в превод означава „тежък труд“, „робство“. С течение на времето роботът се развива дотолкова, че да може да се управлява безжично чрез wi-fi, оборудва се със софтуери за глас, жироскоп, глобална система за позициониране и безброй сензори

като например за топлина, за мощност, за ултразвук, за химически вещества или за радиация. Днес роботите са по-мощни и по-функционални, извършват задачи, които преди дори и не бихме си представили като например:

- **Помощници.** В една болница в Чикаго робот фармацевт за секунди намира, приготвя и предоставя на хората лекарства с помощта на механичните си ръце. Пощенските служби разполагат с много роботи, които сортират, вдигат и подреждат пакети и колети. Подобна на змия роботизирана ръка може да прониква в затворени пространства, като например в самолетните крила, за извършването на необходими прегледи и поправки.
- **Другари.** Пациентите в един дом за стари хора в Япония се радват на едно симпатично пухкаво тюленче робот. То може да отговаря на ласките им, защото има сензори за допир, светлина, звук, температура и дори може да реагира на начина, по който го държат. Тюленчето робот имитира поведението на живите тюленчета, като издава звуци, мига с очи и движи плавниците си. Някои хора смятат, че то удовлетворява човешката потребност от другарство и има терапевтичен ефект.
- **В медицината.** Робот с три ръце се е надвесил над пациента, а на няколко метра встрани хирургът наблюдава триизмерен образ на сърцето на пациента през визьора на огромна конзола. Той управлява ръцете на робота, докато извършва операция за възстановяване на увредена сърдечна клапа. Този метод е минимално инвазивен благодарение на прецизните движения на робота, вследствие на което оперативната травма е по–малка, кръвозагубата е по–малка и възстановяването на пациентите е по–бързо.
- **В домакинството.** С натискането на един бутон кръглият робот с плосък корпус започва да смуче праха от пода. Роботът почиства откритите пространства, извършвайки спираловидни движения, почиствайки покрай стените, като постепенно „научава“ разположението на предметите в стаята. Той разпознава и заобикаля стълбите. Накрая автоматично спира и се връща на първоначална позиция за презареждане. Вече над два милиона такива прахосмукачки роботи са в употреба.
- **В космоса.** Мобилният робот „Спирит“ с шест колела изследва повърхността на Марс. Към роботизираната му ръка са прикрепени специални прибори, благодарение на които роботът анализира състава на почвата и скалите. Той е оборудван с камери, с помощта на които до Земята вече бяха изпратени над 88500 изображения на Марс, включително снимки на терена, кратерите, облаците, прашните бури и залезите на планетата. Освен „Спирит“ има и други мобилни роботи, които в момента изследват Марс.
- **Спасителни акции.** Под димящите и изключително горещи развалини на двете сгради на Световния търговски център в САЩ седемнайсет робота с размера на баскетболна топка са търсели оцелелите. Оттогава насам различните модели роботи са усъвършенствани допълнително.
- **Подводни дейности.** Учените използват автономни подводни апарати, за да изследват дълбините на океана. Тези апарати са безпилотни и са със собствено захранване. Други приложения на роботите под водата са: търсене и спасяване на оцелели при злополуки, поддръжка на телефонни кабели, проследяване на китове и разминиране на океанското дъно [4].

III. ROBOTBASE

Роботът /тя/ ще ви събуди сутрин, ще включи осветлението, ще ви приготви кафе, ще ви помогне с избора на тоалет и ще ви повика такси. А когато вече сте на работното си място, ще влезе в ролята на квалифициран личен асистент. Тя също така е невероятен фотограф, обучен охранител, страхотен събеседник и още много, много неща.

Тя е разработка на американския стартъп Robotbase и е първият в света персонален робот с изкуствен интелект, който може да упражнява различни роли. От Robotbase твърдят, че изкуственият интелект, който притежава, е един от най-напредналите в момента. Тя не само чува, но и разбира какво ѝ говорите, може да да разпознава лица и предмети, да чете настроения и емоции, да се свързва с различни устройства и приложения. И тъй като непрекъснато се самообучава, с всеки изминал ден става все по-умна.

Проектът бе показан по време на технологичното изложение CES в Лас Вегас миналата седмица. В момента събира финансиране в платформата Kikstarter като целта за набиране на 50 хиляди долара капитал вече е постигната. Плановете са роботът да дебютира в края на тази година на цена под 1 500 долара.

ЗАКЛЮЧЕНИЕ

Изкуственият интелект може да съществува във всичко – от смартфона ни, през търсачката на Google, до автономните автомобили и др. Нека да погледнем още по-напред във времето, в ерата на роботиката, където дори вече ще сме свидетели на автомобили без шофьори, а скоро ще се открият и автономните ресторанти, но пък ще се закрият много професии. Обобщено тенденцията е следната: ускорява се темпът, с който се формира обществото. Когато дойде ерата на роботите, ще имаме спешна нужда от регулации. Светът ще се промени, когато започнат да остават гладни хора, заради безработица и тогава ще има бунтове и размирици.

ЛИТЕРАТУРА

[1] Veselka Stoyanova, Zhaneta Tasheva, Research of the characteristics of a steganography algorithm based on lsb method of embedding information in images, *Publication: Trans MotAuto15*. Available from: https://www.researchgate.net/publication/304579312_Trans_MotAuto15, accessed Mar 30, 2017

[2]http://cio.bg/1960_izkustven_intelekt__osnovni_koncepcii_i_prilozhenie_v_otbranitelnata_tehnika

[3] http://smartnews.bg

[4] https://wol.jw.org/bg/wol/d/r46/lp-bl/102008326

За контакти:

Серж. Денислав Пламенов Денчев , Катедра „Компютърни системи и технологии", НВУ „Васил Левски", факултет „А, ПВО и КИС", тел.: 0893725515, e-mail: Denintos@gmail.com

гл. ас. д-р инж. Веселка Тодорова, НВУ „Васил Левски", тел.:0888065638, e-mail: veselka_tr@abv.bg

Компютърна и мрежова сигурност

автор: К-т Серж. Денислав Денчев
научен ръководител: гл. ас. д-р инж. Веселка Тодорова

Computer and network security: *In this report it is analyzed what computer and network security are, what they represent, where they are used, what their purpose and frequent use are.*
Keywords: *computer security, information security, network security*

ВЪВЕДЕНИЕ

Компютърна сигурност е клон на информационната сигурност с приложение в компютрите и компютърните мрежи. Основна цел на компютърната сигурност е защита на информацията и хардуера от кражба, повреждане или от природни бедствия, като същевременно на законните потребители се осигурява достъп до тях и ползотворна работа.

Терминът сигурност на компютърната система обхваща процесите и механизмите, чрез които важната и чувствителна информация бива защитавана от неправомерен достъп, изменение или унищожаване, което би могло да бъде следствие, както от действията на лица с недостоверен произход, така и вследствие на случайни събития. Сравнени с останалите компютърни технологии, стратегиите и методите, които се използват в сферата на компютърната сигурност са твърде различни, главно заради особения характер на дейността – предотвратяване на нежелано компютърно действие, вместо осигуряване на точно определен, желан начин на действие на системата.

Мрежовата сигурност се състои от разпоредби и вътрешно-организационни политики, възприети и прилагани от мрежови администратор с цел превенция и наблюдение на неоторизиран достъп, злоупотреба, модификация или предизвикване на отказ на услуга на компютърна мрежа и ресурси, които са мрежово достъпни[2]. Мрежовата сигурност включва оторизацията на достъп до данни в мрежата, които са контролирани от мрежови администратор. Потребителите използват или имат приписано ID (*идентификация*) и парола, или друг тип автентизираща информация, която им позволява достъп към информация или програми, които са от тяхното ниво на упълномощеност. Мрежовата сигурност покрива разнообразие от компютърни мрежи, както публични, така и частни, които са използвани за ежедневни действия и дейности като транзакции и комуникация между бизнеси, правителствени институции и агенции, и отделните домашни потребители в мрежата. Тя е насочена към това, което се подразбира от наименованието, а именно гарантиране на сигурността на дадена мрежа, както и защита и наблюдение на операциите, които са извършвани в нея. Най-честият и прост начин за защита на мрежовите ресурси е чрез задаване на уникално потребителско име и парола за потребителите.

АНАЛИЗ НА ЗАПЛАХИ И АТАКИ КЪМ КОМПЮТЪРНИТЕ МРЕЖИ

Компютърните системи и мрежи - базата на съвременните информационни системи - са едни от най-високотехнологичните продукти на човешката материална култура. Но те не са безотказни. Даже да няма враждебни действия срещу тях, надеждното им функциониране не е неограничено. За да се поддържа то на необходимото ниво, още при проектирането им се предвиждат специални апаратни, програмни и програмно-технически средства. В нея компютърната и мрежовата сигурност се разглеждат като способност за противодействие срещу неразрешен достъп до данни и ресурси на автоматизираните информационни системи (АИС) и мрежи. За разлика от всички други машини, създадени от хората, компютрите не

преобразуват енергия от един вид в друг, а данни в информация. Именно тя е най-ценният компонент в тях. По данни на ФБР на САЩ всеки път, когато е "пробита" компютърната защита на голяма компания, тя губи средно 700 000 долара, а банките губят по 8 000 долара в секунда от сривове и откази на компютрите [3]. Измамите с кредитни карти предизвикват загуби около 5 милиарда долара годишно [4]. Съвременните информационни инфраструктури съдържат две основни съставни части - изчислително-комуникационна и управленческа [3]. Една от най-важните задачи на управленческата инфраструктура е организирането и съпровождането на системата за сигурност. Тази система трябва да осигури ефикасна защита срещу несанкциониран достъп до устройствата и ресурсите на компютърните системи и мрежи.

Проблемите, свързани със защитата на компютърната информация, довеждат до появата на нова научна и практическа дисциплина - информационна сигурност (ИС). Специалистите в тази област трябва да умеят да разработват, реализират и експлоатират системите за осигуряването на информационна сигурност (СИС). Тези системи поддържат цялостността, пригодността, конфиденциалността и достъпността на информацията и осигуряват физическа (на технически средства, свързочни линии, отдалечени компютри) и логическа (на данни, операционни системи, приложни програми) защита на информационните ресурси. Ръководителите на малки и големи фирми все още подценяват мерките за защитата на своите компютри и данни.

1. Заплахи и атаки към компютърните мрежи

1.1 Общи въпроси на компютърната сигурност

Сигурността е свойство на една система да противостои на външни или вътрешни дестабилизиращи фактори, които могат да доведат до нейното нежелателно състояние или поведение. Това важи и за сигурността на информационните системи.

Целта на всяка информационна система е предоставяне на пълна, достоверна и своевременна информация. Тази информация е уязвима, както поради случайни, така и поради злонамерени дестабилизиращи фактори (заплахи), което налага да се вземат мерки за нейната защита.

Съвсем формално погледнато ценността на компютърната информация зависи от това колко струва времето на потребителя при въвеждането на данни в компютъра, колко данни са съхранени и от това колко дълго би продължило възстановяването на тези данни, ако те се загубят. Разходите за възстановяване на данните при тяхната загуба или поради попадането им в чужди ръце може многократно да надхвърлят стойността на компютъра. Потребителите трябва да защитят своите компютърни данни и от механични повреди, и от стихийни бедствия. В края на краищата все едно е дали твърдият диск ще бъде унищожен от компютърен вирус, или същата "услуга" ще му бъде оказана от наводнение, или мълния. Статистиката показва, че най-големият брой инциденти със загуби на потребителска информация са или случайни, или причина за тях са самите потребители. Всеки ръководител трябва да определи ценността на данните за неговата организация или фирма - лични данни за персонала, информация за заплатите, номера на банкови сметки, изследователски и развойни продукти, финансови отчети, медицински картони, делова кореспонденция и др. За съжаление подобни данни често се оставят напълно незащитени. Проблемите стават по-сложни при работа в мрежа.

Под защита на информацията трябва да се разбира постоянно използване на средства и методи, прилагани с цел:

а) защита на конфиденциалността (тайната) - да не се допуска разкриването на информация от неоторизирани лица;

б) защита на цялостността - да не се допуска неоторизирана преднамерена или случайна модификация на информацията;

в) защита на достъпността - да не се допуска отказ на информация или ресурс.

Обект на защитата е структурен компонент на информационната система, в който има информация, подлежаща на защита. Такива обекти са компютрите (работни станции на потребители и администратори на системи, локално използвани персонални компютри, периферни устройства), мрежови средства (модеми, апаратура за предаване на данни, рутери, мрежови сървъри, комуникационни канали) и помещенията.

Компютърните системи и мрежи са техническата база на информационните системи. Компютърната и мрежова сигурност е свойство на компютърните системи и мрежи да противодействат на опитите за несанкциониран достъп до обработваната и съхраняваната информация, водещи до деструктивни действия и получаване на лъжлива информация.

Тя се гради върху следните концепции:

- идентификация - потребителите използват компютърните приложения чрез потребителски идентификатор (ID);
- автентификация - доказване на самоличността на потребителя;
- оторизация - присвояване на права за достъп на всеки потребител (например за запис, четене или изпълнение на файл);
- контрол на достъпа - присвояване на права за достъп до мрежови ресурси и предпазване на ресурсите чрез лимитиран достъп (кой, как, кога и при какви условия има достъп);
- конфиденциалност - защита на данните (чрез контрол на достъпа и криптиране);
- цялостност на данните (интегритет) - откриване на несанкционирана модификация на данните, обикновено при предаване на съобщението;
- доказване на източника на данните;
- управление на отказ от услуги (DoS) - предотвратяване препълването на лентата на пропускане на канала или блокирането на достъпа;

Има три главни аспекта на сигурността на компютърните системи и мрежи – уязвими места, заплахи и противодействие.

1.2 Класификация на заплахите и атаките за компютърните системи и мрежите

Уязвимото място е слабост в компютърната информационна система и в мерките за нейната сигурност, която може да доведе до компрометиране сигурността на системата. Под уязвимо място се разбира всяка точка на компютърните и комуникационните системи и на системата за тяхната защита, където те са слабо защитени срещу заплахи и атаки, свързани с тяхната сигурност. Уязвимите места в една система зависят от конкретната й реализация. Заплаха е човек, обект, събитие, процес или явление, които могат да нанесат вреда на компютърните системи и мрежи.

Примери за заплахи [3]:

- използване на известен способ за достъп до системата с цел извършване на забранени действия;
- маскиране като истински потребител;
- използване на служебно положение с цел достъп до информация;
- физическо разрушаване на системата или нейни компоненти;

- изключване на системата за защита или нейни компоненти;
- изключване на подсистемите, обезпечаващи работата на системата (електроснабдяване, охлаждаща и вентилационна, комуникационна и др.);
- промяна на режима на работа на устройства и програми;
- подкуп и шантаж на персонала или отделни потребители;
- •кражба и несанкционирано копиране на информационни носители;
- незаконно използване на пароли, пропуски, магнитни карти и др.;
- разкриване на шифри при криптиране на информацията;
- включване на апаратни средства и програми, позволяващи несанкциониран достъп;
- заразяване с вируси;
- незаконно включване към комуникационните линии с цел подмяна на законен потребител и предаване на лъжлива информация от негово име;
- незаконно включване към комуникационните линии с цел прехващане на поверителна информация;
- незаконно включване към комуникационните линии с цел анализ на протоколите за връзка и последващото им имитиране за достъп до системата;
- използване на подслушвателни устройства и устройства за дистанционно видеонаблюдение;
- прехващане на ПЕМИ;
- четене на остатъчна информация от оперативната памет и външни запомнящи устройства;
- незаконно използване на терминали и компютри оставени без надзор.

Класификацията на видовете заплахи е необходима за оценка на системите за сигурност. Тя може да бъде направена по различни критерии. Според източника заплахите могат да бъдат външни и вътрешни. Външни са дейността на разузнавателни и специални служби, дейността на разни политически, икономически и други структури, насочени срещу интересите на организацията, и престъпни действия на отделни групи и лица. Вътрешни са нарушаване на правилата за събиране, обработка и предаване на информацията, незаконна дейност на групировки и лица за прикриване на закононарушения и нанасяне на вреди на интересите на физически и юридически лица на базата на тази информация.

Основните видове заплахи за сигурността на субектите в информационните отношения са [2]:

- Стихийни бедствия и аварии.
- Сривове и откази на техническите средства на информационната система.
- Последствия от грешки при проектиране и изработка на системата.
- Грешки на персонала при работа със системата.
- Преднамерени действия на нарушители и зложелатели

ЗАКЛЮЧЕНИЕ

Компютърните системи и мрежи, които са базата на съвременните информационни системи - са едни от най-високотехнологичните продукти на човешката материална култура. Обектът на защитата е структурен компонент на информационната система, в който има информация, подлежаща на защита. Такива обекти са компютрите (работни станции на потребители и администратори на системи, локално използвани персонални компютри, периферни устройства),

мрежови средства (модеми, апаратура за предаване на данни, рутери, мрежови сървъри, комуникационни канали) и помещенията.

ЛИТЕРАТУРА

[1] Мазаджиев Г., Г. Томов, Мрежова сигурност, Издателски комплекс при НВУ „Васил Левски", В. Търново, 2013.
[2] Мазаджиев Г., Д. Дойчинов, Администриране на компютърни мрежи, Издателски комплекс при НВУ „Васил Левски", В. Търново, 2013.
[3] Станев С. С, Компютърна и мрежова сигурност, Университетско издание при Шуменски университет Епископ Константин Преславски, 2005
[4] Terry D. Pardoe, Gordon Snyder, Network Security, Cengage Learning, 2005.

За контакти:

Денислав Пламенов Денчев, курсант сержант в НВУ „Васил Левски", Факултет „А, ПВО и КИС" – Шумен, E-mail: denintos@gmail.com

гл. ас. д-р инж. Веселка Тодорова, НВУ „Васил Левски", тел.:0888065638, e-mail: veselka_tr@abv.bg

Носими системи за проследяване начина на живот

автор: к-т Серж Щилияна Райнова Стоянова
научен ръководител: гл. ас. д-р инж. Веселка Тодорова

Wearable lifestyles tracking systems: *The paper focuses on researching using self-tracking devices. The research proves the necessary of personal data security. The paper analyses also the security threats in accordance with data lifecycle as well as the self-tracking models and their tracking.*

Key words: *Quantified Self, Self-Tracking, models, personal data, risks.*

ВЪВЕДЕНИЕ

Концепцията за фитнес/**лайф тракинг**, **обхваща носими сензорни технологии за проследяване на начина на живот,** физическата активност и физиологичния статус. Анализът на тези данни разкрива аномалии и създава предпоставки за здравословна корекция на поведението. Само-проследяването се осъществява чрез постоянно носим аксесоар, оборудван със система за събиране, съхранение и обработка на информацията. Текущите резултати се наблюдават върху собствен дисплей или се изпращат към смартфон, от където често се преминава и към **облачна услуга**.

Фитнес-тракерите [4] се обособиха като много успешен отделен клас носими компютъризирани системи с ясна функционалност и приложения, издръжливи батерии и привлекателен дизайн. Форм факторът е клипс, лента, компактен блок или маншет/гривна (фиг. 1). Традиционната им функционалност за пасивно наблюдение се усъвършенства до интерактивна функционалност на фитнес-асистент.

Фиг. 1 Носими системи за проследяване начина на живот

Потребителите са свикнали да споделят компромисно с доставчиците на онлайн-услуги традиционна информация за идентификация (Personally identifiable information, PII) като: име, дата на раждане, телефонен номер, адрес, имейл-адрес, парола, номера на социални осигуровки, данни за разплащане с карти и др. Рискът за поверителността обаче се увеличава значително, с увеличаване на обема и обхвата на данните за нас.

Допълнителната информация, генерирана чрез услуги за само-проследяване, издава това, което правим, къде сме били и потенциално защо правим нещо. Когато допълнителната информация от проследяващите устройства се комбинира с традиционната PII, потенциалът за злоупотреба става много по-голям. Колкото повече данни се обобщават, те се трансформират в прогнозна информация за личния профил и поведение на потребителите. Това е златна мина за маркетинг, но и за кибер престъпници.

С масовото навлизане на носими системи за само-проследяване става наложително да се анализират възникващите рискове за личните данни на

потребителите. На тази основа може да се изведат направления за тяхното ограничаване или преодоляване.

1. ВИДОВЕ НОСИМИ УСТРОЙСТВА И КАКВО СЛЕДЯТ ТЕ

1.1 Примери за носими устройства според категорията, в която се ползват:

- Спорт и фитнес - Garmin Vivosmart HR+, Fitbit Charge 2, Misfit, Fitbit Alta HR, Withings Steel HR, Moov Now, Xiaomi Mi Band 2
- Здравеопазване и Уелнес програми (програма за възприемане на здравословен начин на живот) - Garmin Vivoactive HR
- Игри и всекидневна употреба - Samsung Gear Fit2, Skagen Hagen Connected, Mondaine Helvetica Smart

1.2 Примери за информация, която може да бъде проследена, използвайки самопроследяващи устройства.

В таблица 1 са показани примери за информация, която може да бъде проследена. Това е само част от огромното количество информация, което се складира в определено устройство или сървър за даден потребител. Също така е персонална информация, която никой потребител не би искал да стане достъпна за всички потребители. Затова и в точка 2 ще бъдат анализирани някои области на заплахи и тяхното предотвратяване.

Таблица 1 Примери за информация следена, чрез самопроследяващи се устройства

Консумация:	**Функции на тялото:**	**Физическа активност:**
-Калории/храна -Алкохол -Никотин -Кофеин -Вода; -Лекарства	-Ph на тялото -Менструация -Бременност -Ходене по нужда	-Спорт -Сън -Пътешествия -Сексуална активност -Миене на зъбите
Медицински симптоми: -Главоболие -Болки -Пристъпи на астма -Алергии	**Пространство:** -Местоположение -Надморска височина -Време -Какво се вижда	**Физиологическа статистика:** -Удари на сърцето -Кръвна захар/Глюкоза -Температура -Кръвно налягане -Тегло -Дишане
Психично здраве: -Настроение -Ниво на стреса -Разтревоженост		

2. АНАЛИЗ НА ЗАПЛАХИ ЗА СИГУРНОСТТА НА ДАННИТЕ ПРИ САМОПРОСЛЕДЯВАНЕ

2.1 Области на заплахи

Жизненият цикъл на данните, в носимите системи за само-проследяване включва три етапа: локално събиране на данни, предаване на данни, съхранение и обработка в облачно пространство с потенциал за обратна връзка. Така се очертават три основни области на риск: в устройството (локално събиране, съхранение и обработка); при комуникация; в облака (съхранение, обработка и връщане на резултатите).

1. Заплахи в носимата система за проследяване

Данните са изложени на риск от зловреден софтуер, който може да открадне данни на местно ниво. Друг очевиден риск за локално съхранени данни е заплахата от кражбата на устройството. Много устройства за само-проследяване не предлагат начини на защита в случай на физическа кражба. Потребителите на смартфони могат поне да се възползват от заключващата функция на телефона, за

да се предотврати неоторизиран достъп до данни, ако устройството бъде откраднато.

2. Заплахи при предаване на информация

По време на предаване, данните са изложени на риск от различни заплахи:

- при атака „traffic sniffing“ [1], [5] (подслушване на трафика), атакуващите събират всички предавани данни;
- при атака „man-in-the-middle“ [1], нарушителят се намира между приемащия и предаващия, прихваща трафика, който минава транзитно. Той може да пренапише трафика или да променя пакетите преди те да достигнат до получателя без той да разбере за това;
- при „redirection“ [1] атаки данните биха могли да се пренасочат до грешен сървър. Подход за смекчаване на някои от тези рискове е да се използва криптиране и автентикация на данните, които се предават. Например, при безжичната комуникация Wi-Fi, връзката може да бъде шифрована със WPAv2. За комуникация „local-to-cloud“, решения за сигурност на мрежово ниво като например TLS и VPN, трябва да се използва при ненадеждни мрежи. Според чувствителността на данните, които се изпращат, данните могат да бъдат криптирани в приложния слой.

3. Заплахи при използване на облачни услуги

В зависимост от конфигурацията на системата, може да има различни заплахи като:

- атаки SQL injection [1] (атака на сървърна база от данни чрез техника за инжектиране на зловредно съдържание);
- атаки account Bruteforce login [2] (логическа атака на „грубата сила“);
- разпределена атака за отказ на услуга (distributed denial-of-service, DDoS) към даден сървър);
- атаки remote software vulnerability [2] (дистанционна атака на уязвими точки в софтуера);
- атаки default password [2] (атаки в системи с парола по подразбиране);
- атаки back door [2] (атака тип „задна врата“).

2.2. Сигурност на данните и архитектура на носимата система за самопроследяване

Архитектурата [5] и оттам функционалността на една система за самопроследяване може да се усложнява на три нива: самостоятелно физическо устройство, смартфон със сателитен сензорен аксесоар и накрая добавка на облачна услуга.

1. Самостоятелно физическо устройство за сензорно проследяване на активността, локално съхранение на данните и дисплей за визуализацията им не представлява голям риск за личната неприкосновеност. Единственият риск е някой друг да разбере какво е правил собственика, ако получи физически достъп до устройството.

2. Практически значима полезност при съвременното ниво на технологиите възниква, ако фитнес/лайф тракера е интелигентен периферен модул към смартфон. В този случай стандартно се поддържа функция за безжичното синхронизиране на носимата система с приложение на смартфон с по-добър дисплей и повече място за съхранение на данни.

3. Функционалността се разширява още с *облачна онлайн-услуга*. Потребителят е синхронизирал своите данни към смартфон-приложение (което е все още в рамките на физическия му домейн), но тези данни чрез облачна онлайн-услуга могат да се предадат за съхранение, анализ и социално споделяне. Като се добави

интеграция на социални медии и на API, за да се позволи на third party-разработчици (програмисти на софтуер за свободна употреба – трета страна) да изграждат приложения, базирани на данни за само-проследяване рисковете още се увеличават.

2.3. Възможнни злоупотреби с лични данни от носими системи за само-проследяване

1. Кражба на самоличност- Съществува престъпна индустрия, която процъфтява чрез събиране и продажба на толкова персонални данни PII, колкото могат да придобият. Комплекти на данни за дадено лице могат да бъдат продадени на други престъпници в пакети, известни като "fullz"(жаргон за пълен пакет с лични и финансови данни). Колкото по-пълен и актуален е набора от данни, толкова по-ценен е той. Например, детайли могат да бъдат използвани за създаване на фалшиви банкови сметки за пране на пари, опити за откуп, или IRS измами чрез фалшиви данъчни декларации (Internal Revenue Service – Данъчната служба на САЩ).

Заплахата от кражба на данни или злоупотреба не трябва да възниква в една легална организация. Например нелоялни служители, които за лична изгода продават информация за клиенти на трети лица. Такива инциденти могат да варират от малка кражба на данни до мащабни случаи, включващи милиони потребители.

2. Профилиране- Детайлите предоставени от потребителите на услугите за само-проследяване биха могли да позволят на маркетингови и правителствени агенции да организират и насочат действия към определени видове потребители. Профилирането е в ущърб на защитата на личните данни и човешките права, защото така лесно може да злоупотреби с определени групи или малцинства.

3. Локализация на потребителя- Личната информация PII, съдържаща текущи данни от проследяване местоположението на потребителя, също може да се злоупотреби за престъпни цели.

Например, достъпът до база от данни, съдържаща информация от спортно приложение за проследяване, позволява да се определи къде живее човек и кога той ще бъде най-вероятно далеч от дома си, както и дали планира почивка. Много хора намират своите домове, разбити и ограбени, защото публикуват в социалните мрежи данни за своята отдалеченост от дома. С тази информация може да злоупотребят натрапници, частни следователи и правителства, според техните цели.

4. Изнудване с чувствителна лична информация- Има редица приложения, които проследяват медицински или здравни дейности, свързани с телесни и психични функции. Може да се проследяват настроение, сексуална активност и дори ходене по нужда на потребителите. Едва ли някой би се чувствал комфортно да разкрие този вид информация за себе си пред света. Подобна чувствителна информация, попаднала в неподходящи ръце често се използва, за да се изнудят жертвите за пари. Тъй като все повече и по-чувствителна информация се събира и предава по целия свят, рискът високо чувствителни данни да попаднат в неподходящи ръце се увеличава.

5. Корпоративна употреба и злоупотреба- Някои от продавачите в технологията за активно проследяване насърчават използването на своите устройства с корпоративни wellness програми. Ползите, които са изтъквани може да са по-евтино здравно осигуряване, намаляване отпуската по болест, намаляване разходите за здравеопазване, и дори увеличаване на производителността заради по положителното настроение на служителите, в резултат на по-активен начин на живот, насърчаван технологично със системи за само-проследяване.

ЗАКЛЮЧЕНИЕ

Индустрията за технологично само-проследяване начина на живот, в това число физическата активност и физиологическия статус е във фаза на разцвет. Това обуславя от една страна позитивни очаквания за здравословна корекция на поведението за много потребители. От друга страна възниква широк спектър от сериозни заплахи за злоупотреба с личните данни, получени чрез носими системи за само-проследяване.

Основните резултати в настоящата работа са в направленията:

- Анализирани са видовете устройства в носимите системи за само-проследяване;
- Изведена е специална категория лични данни получени чрез самопроследяване - големи обеми широко-обхватна лична информация, с която може да се профилират потребители, да се прогнозира тяхното поведение и да се манипулират техните визии и решения;
- Анализирани са области на възможни заплахи според жизненият цикъл на данните в носимите системи за само-проследяване;
- Анализирана е зависимостта на риска за сигурността на личните данни от архитектурата на носимата система за само-проследяване;
- Анализирани са основните възможности за злоупотреба с лични данни от само-проследяване.

В редица случаи се предлагат решения за минимизация на риска за нарушаване на поверителността на личните данни от само-проследяване и недопускане на възможни злоупотреби с тях.

ЛИТЕРАТУРА

[1] IBIResearch. (2013) Wearable computing devices, like Apple's iWatch, will exceed 485 milion annual shipments by 2018. IBIResearch. retrieved from https://www.abiresearch.com/press/wearable-computing-devices-like-apples-iwatch-will.

[2] Deborah Lupton, Self-Tracking Modes: Reflexive Self-Monitoring and Data Practices, University of Canberra, 2014, HTML URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483549

[3] Mario Ballano Barcena, Candid Wueest, Hon lau, How safe is quantified self?, 2013, HTML URL:https://www.thesis.xlibx.info/th-order/4687184-1-how-safe-your-quantified-self-mario-ballano-barcena-candid-wuees.php

[4] Мазаджиев Г., Специализирани компютърни системи, Шумен, 2014.

[5] Мазаджиев Г., Г. Томов, Мрежова сигурност, Издателски комплекс при НВУ „Васил Левски", В. Търново, 2013.

[6] Мазаджиев Г., Д. Дойчинов, Администриране на компютърни мрежи, Издателски комплекс при НВУ „Васил Левски", В. Търново, 2013.

За контакти:

Курсант сержант Щилияна Райнова Стоянова, НВУ „Васил Левски" ,Факултет „Артилерия, Противовъздушна отбрана и Комуникационни и информационни системи", тел.:0883504425, e-mail: Sthiliqna1234@gmail.com

гл. ас. д-р инж. Веселка Тодорова, НВУ „Васил Левски", тел.:0888065638, e-mail: veselka_tr@abv.bg

Водещи фактори в сигурността на системите за индустриален контрол (ICS)

автор: к-т Серж Щилияна Райнова Стоянова
научен ръководител: гл. ас. д-р инж. Веселка Тодорова

Key Factors in Industrial Control System Security: *Key Factors in Industrial Control System Security are a less obvious part of the Internet of Things with their own unique security challenges. We introduce the structure and components of typical ICS installations. We also provide an overview of a number of ICS security approaches. Contrasting these with a sampling of documented ICS security incidents highlights the relevance of this topic. Finally, this approach allows us to identify unsolved problems with respect to securing ICS.*

Key words: Internet of Things, installations, ICS, risks, approaches.

ВЪВЕДЕНИЕ

Интернетът на нещата (IoT) е не само стереотип на "Умни" термостати, хладилници и други. Така например местното водоснабдяване и газоснабдяване могат също да бъдат част от него. Веднага до смартфоните и уеб сървърите може да се намери малък, но критичен клас устройства и мрежи, тоест системите за индустриален контрол (ICS).

ICS споделят същите проблеми със сигурността и съображенията, които идват с този вид комуникация. Терминът (системи за индустриален контрол) обхваща всичко от най - малките устройства, отчитащи единични показания на датчика до огромни инсталации, контролиращи тръбопроводи, разположени по цели държави. Те могат да наблюдават подземни газови резервоари или отворени критични клапани в точния момент, могат да бъдат и сложни мрежи от устройства, контролиращи деликатни производствени процеси.

Важно е, че ICS включват критични инфраструктури като водоснабдяването или производството и разпределението на електроенергия. Неизправности в такива системи може да доведе до незначителни неудобства или до загубата на живот, затова е притеснително, че точно ICS често страдат от недостатъци в сигурността. Това се доказва от много инциденти в миналото, като не най-маловажния от които е Stuxnet атаката. Някои от техните проблеми се коренят в основните им проекти, често наследени от дизайна на автоматизацията на процесите през 70 - те години, когато интернет все още не е бил въведен. Съществуват други проблеми, които се възползват от уязвимостите на софтуера и с това възможността ICS да бъдат изложени на риск от разпространение в интернет се увеличава.

В този доклад се предоставя кратък преглед на ICS и състоянието на сигурността на системите им, систематизират се няколко подходи за осигуряване на ICS. За да се оцени тяхната ефективност се сравняват с истински атаки срещу ICS.

1. СИСТЕМИ ЗА ИНДУСТРИАЛЕН КОНТРОЛ (ICS)

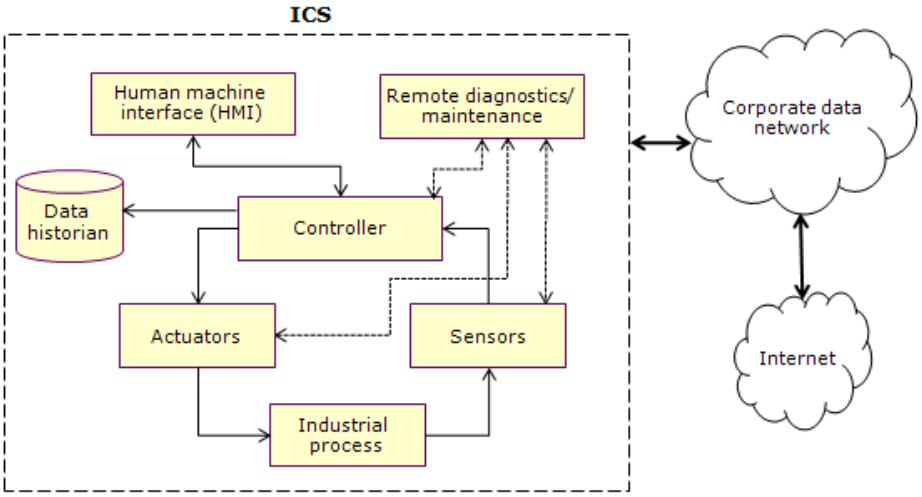
В този раздел предоставям кратък преглед на структурата и основните компоненти на системите за индустриален контрол (ICS).

А. Терминология

Терминологията около ICS често е двусмислена и следователно обърквaща. Системата за индустриален контрол (ICS) обикновено се използва като основен термин. Система за разпределен контрол (DCS) е ограничена до една точка, например конкретна фабрика. Системи за специализиран контрол и събирането на данни (SCADA), които са разположени върху голяма географска област, като например електрическа мрежа или тръбопровод.

Б. Компоненти

ICS обикновено се състоят от комбинация от компютри с общо предназначение и специализиран хардуер. На фигура 1 е показана архитектурата и компонентите на ICS.



Фиг.1 Архитектура на ICS

1) Програмируеми логически контролери (PLC): PLC са програмируеми вградени компютри, които четат стойности от външни сензори и ги обработват в малки програми. Техните изходни данни се предоставят на други устройства или се използват за управление на процеса. PLC често са проектирани така, че да издържат на неблагоприятна околна среда [1], [3]. Отделни PLC за безопасност могат да бъдат разположени да проверяват главния процес на PLC. Те могат да заменят основните PLC и съответно да запазят или да върнат целия процес в безопасно състояние [2].
2) Шини и устройства: Шината е локална мрежа за комуникация между полеви устройства. Те включват PLC, цифрови сензори и компоненти, но не и устройства с общо предназначение.
3) Интерфейси на човешка машина (HMI): HMIs визуализират състоянието на индустриален процес и позволяват пряко въздействие от човек. Те могат да бъдат реализирани като самостоятелен хардуер, полево устройство или софтуер, работещ на работно място [1], [4].
4) Инженерни работни станции: компютри с общо предназначение, оборудвани за програмиране с полеви устройства като PLC и HMI. Обикновено това са Windows компютри, намиращи се в една и съща локална мрежа като съответните полеви устройства.
5) Данни за запазване на историята: Те предоставят дългосрочна памет за четене на сензори и състояния на процеса. Те могат да бъдат като SQL база данни. И двете интегрирани решения, напр. заедно с HMI или самостоятелно устройство се използват. Тъй като тези данни могат да предоставят значителна информация за контролирания процес, те са важни цели за нападателите. [5]

2. ЗАЩИТА НА СИГУРНОСТ НА СИСТЕМИТЕ ЗА ИНДУСТРИАЛЕН КОНТРОЛ

Предложени са подходи за подобряване на сигурността на ICS. Структурните подходи, които предлагат дизайни за ICS и свързаните с тях мрежи, които възпрепятстват вирусите и атаките на първо място, но и правят по-труден достъпа до странично приложение или вътре в ICS. Подходите за откриване използват откритите аномалии в статистиката на битовете, за да информират операторите за възможните атаки. И накрая, направени са няколко модификации на протоколите за

ICS, като се използват криптографски методи за осигуряване на по-добра сигурност при обмена на съобщенията.

А. Структурни подходи

Работата на Dzung et al. [8] се фокусира върху въведените стандарти от индустрията и регулаторните организации. Тези стандарти често изискват разделянето на мрежите от защитни стени и да гарантира, че работните станции на ICS няма да се използват за редовни офис задачи. По-специално, ICS трябва да е достъпна само чрез строго наблюдаван DMZ. NIST предоставя по-изчерпателен наръчник [1], използвайки подобен модел. Докато ръководството, публикувано от Америка ICS-CERT [11] силно се припокрива с препоръките на NIST, той е единственият, който изрично препоръчва предпазна екипировка. Всички гореспоменати подходи предполагат използването на IDS и откриване на аномалии, но също така посочва какви допълнителни политики и процедури са необходими.

Б. Подходи за откриване

Обикновено полевите устройства, включително PLC, не са достатъчно мощни, за да използват сложния софтуер свързан с задачите по изпълнение на процеса. По този начин те не могат да изпълнят хост базирано проникване в системите за откриване. Въпреки това, има установени няколко мрежови навлизания в системите за откриване на ICS. Тъй като тези IDS се изпълняват на отделен хардуер, те не оказват влияние за ефективността на полевите устройства, но въпреки това трябва да бъдат способни да обработват трафик в почти реално време, за да бъдат полезни [12]. Snort IDS [10] разполага с модули за непатентованите протоколи ICS DNP3 и Modbus. Затова защитите могат да определят аномалиите на битовете в съобщенията от черни или бели списъци от тези протоколи. Mander et al. предлага такива правила за няколко сценария, използвайки протокола DNP3.

Genge et al. предлага подходът SPEAR [12] за да се намали необходимостта от ръчно дефиниране на правилата. Вместо това потребителят трябва да опише топологията на мрежата и очаквания поток на трафика между устройствата в тази мрежа.

SPEAR използва тази информация, за да генерира на Snort правила за бял списък на очаквания трафик, т.е. всеки друг трафик ще задейства алармата. Изпълняващите идеи, начертани от Cardenas et al., Fovino et al. [9] използват подход, който не изисква определянето на правила върху протоколите директно. Вместо това те разчитат на симулация на процесът, който се актуализира въз основа на контролните съобщения обменяни в мрежата на ICS. След това състоянието на симулираните процеси се сравнява с базата данни с критични състояния за задействане на алармата. Предложен е подход за откриване на аномалии от Caselli et al.. Те спорят, че контролираният трафик е по-унифициран от потребителския трафик, който им позволява да се определят състояния, в които всяко едно от тях се отнася за определен протокол за съобщенията на ICS. В процесът на обучение, състоянието на съобщението е без значение, тъй като контролното съобщение се наблюдава преди потребителското съобщение. След като приключи машината за състоянията се използва, за да засече необичайна обмяна на съобщения.

В. Протоколи

Тъй като полеви устройства обикновено нямат обработваща мощ да изпълняват криптографските протоколи , използвани за общо изчисляване, Igure et al. предлага използване на подходите, разработени за безжични сензорни мрежи, които са изправени пред подобни предизвикателства. Няколко групи следват различен метод, като предполагат да интегрират механизмите за сигурност в самите протоколи. Fovino et al. например предлага слой за сигурност Modbus, който работи

по много подобен начин на VPN point-to-point тунелът. Те твърдят, че вместо пряко прилагане на протокола върху полево устройство, той може да бъде реализиран и от gateway (шлюз), чрез който той се използва без промяна в полевите устройства [19]. Majdalawieh et al. предлага DNPsec подхода за DNP3 протокол, който има подобни свойства като подхода на Fovino. [9] По-късно обаче функцията за сигурно удостоверяване е въведена за DNP3, осигуряваща автентичност и интегрираност, но не и поверителност за обмена на DNP3 съобщенията. Въпреки това, Lee et al. твърдят, че протоколите за ICS трябва също така да предоставят поверителност и следователно предлагат променена версия на протокола DNP3, който предоставя подобни функции като протокола на Fovino.

3. ОЦЕНКА

За да се оценят подходите, представени в предния раздел, трябва да се прецени дали биха могли да предотвратят или засекат малка извадка от атаки, които ще бъдат разгледани и оценени в точки 3.1 и 3.2.

3.1 Извадки от някои атаки, при ICS

Ще бъдат разгледани атаки, реално случили се, при използване на системи за индустриален контрол (ICS). Те са:

1) Немска атомна централа: През 2016 г. системата за натоварване на атомната електроцентрала в Gundremmingen е заразена с " office malware ", по-късно идентифициран като червеите Conficker и Ramnit. Операторът не претендира за намеса в други системи в инсталацията поради отделяне на самата система
2) Dragonfly: В атаката Dragonfly атакуващите са използвали копия от достоверни имейли и инжектират в тях комплект в някой уебсайт, който представлява зловреден софтуер и се инсталира на компютрите на жертвите. Докато има такива, които са насочени само към настолни компютри, има и такива които са специално насочени към фирми в енергийния сектор, и по точно данни за преотстъпване на пълномощията и информация от класифицирани устройства.
3) Stuxnet: Stuxnet все още се счита за най-сложна атака срещу ICS. Открита през 2010 г. в иранско ядрено съоръжение, тя заразява инженерните работни станции като инжектира злонамерен код в програми, работещи на PLC. Този код ще задвижи цикли, променяйки скоростта на центрофугите, контролирани от тези PLC. В крайна сметка, прекомерното износване, предизвикано от тези цикли, би довело до унищожаване на центрофугите.

3.2. Оценка на отбранителните подходи

Ще бъдат оценени отбранителните подходи при разгледаните атаки в точка 3.1:

1) Структурни: Всички структурни подходи предполагат използването на антивирусен софтуер. Той обикновено е в състояние да открие и предотврати повреда от универсален зловреден софтуер като този откритит в германската ядрена електроцентрала. Ето защо тази атака е била възпрепятствана от този подход. Тези подходи не включват препоръки за защита на бизнес мрежи срещу сложни атакуващи като тези, които действат в атаката "Dragonfly". Следователно те няма да бъдат спрени от мерките, предложени от структурните подходи. Основен фокус на тези подходи е как бизнес мрежата трябва да бъде отделена от ICS мрежата. В насоченото от Stuxnet към ICS е пропуснато, че са напълно физически разделени. Въпреки това, той е разбит от Stuxnet зловреден софтуер. Тъй като той разчита на неразкрити възможности на системата

по това време, за да получи достъп до легитимиращи компоненти на ICS, няма достатъчно основание да се предположи, че някой от тези предложени мерки биха предотвратили тази атака.

2) Подходи за откриване: Подходите за откриване на проникване във ICS, представените в предния раздел се фокусират върху комуникацията с или между полеви устройства. В зловредния софтуер, който удря германската ядрена електроцентрала, няма необичайна комуникация, свързана с появата на полеви устройства, така че тези подходи не биха успели да открият всяка видима комуникация. Аналогично, щяха да пропуснат Dragonfly атаката, която също така не засяга пряко ICS на целевите компании. В случай на атака на Stuxnet, заразените работни станции комуникират с полеви устройства в ICS. Въпреки това, дори без да се обърне внимание на факта, че никой от подходите не е в състояние да се справи с използвания тук собствен протокол, трябва да заключим че не биха открили тази атака.
3) Протоколи: Тъй като тези протоколите се използват за комуникация с или между полеви устройства, те не могат да предотвратят атаки срещу работни станции като зловредния софтуер в германската ядрена електроцентрала. Също не защитават от атаки, които не включват полеви устройства или свързаните с тях работни станции. Следователно те не биха могли да предотвратят атаките на "Dragonfly". Основното свойство на защитените протоколи е, че те предотвратяват разкриването на информация или предоставянето на неоторизиран достъп. При атаката на Stuxnet работните станции не са част от обхвата на полевите протоколи. Веднъж щом тези работни станции са достъпни, зловреднията софтуер може да действа като автентичен потребител и да издава валидни команди. Следователно обсъжданите подходи не биха предотвратили тази атака.

ЗАКЛЮЧЕНИЕ

В настоящия доклад се реализира преглед на системите за индустриален контрол. Поради тяхното наследство, но и поради изискванията на индустриалната обработка, техните протоколи и устройства осигуряват малко или никаква сигурност. Въпреки това, съществуват редица подходи, за да се намали рискът за ICS. Оценката на разгледаните похвати показва, че само при наличните методи може да се постигне незначителна сигурност, въпреки че подходите смятат бизнес мрежата за потенциален атакуващ агент, те не го считат за цел на самите атаки, свързани с ICS. Следователно те не дават насоки по отношение на обезопасяването им. Също така, анализът разкрива границите на подходите, които използват само комуникацията с и между полевите устройства. За атаката Stuxnet, показана в доклада, компрометираната крайна точка ще използва протоколни съобщения, които са в границите на законната му употреба и биха могли да използват идентификационните данни на съответното устройство, когато е необходимо. Така може да се заключи, че за да се постигне дори и ограничена сигурност за ICS трябват да се използват най-съвременните механизми.

И накрая, системата трябва да бъде систематизирана, за да води до разработването на подходи, които позволяват подходяща защита на системите, които контролират нашите енергийни мрежи, водоснабдяване и други критични инфраструктури.

ЛИТЕРАТУРА

[1] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, *Guide to Industrial Control Systems (ICS) Security*, 2015.

[2] T. Macaulay and B. Singer, *Cybersecurity for Industrial Control Systems:SCADA, DCS, PLC, HMI, and SIS*, 1st ed. Boston, MA, USA: Auerbach Publications, 2012.
[3] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, 2013.
[4] Bundesamt fur Sicherheit in der Informationstechnik (BSI). (2013) ICSSecurity-Kompendium [ics security compendium].
[5] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in *2011 iThings/CPSCom*, 2011.
[6] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, 2013.
[7] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *Computers & Security*, vol. 25, no. 7, 2006.
[8] D. Dzung, M. Naedele, T. Von Hoff, and M. Crevatin, "Security for industrial communication systems," Proceedings of the IEEE, vol. 93, no. 6, 2005.
[9] I. N. Fovino, M. Masera, L. Guidi, and G. Carpi, "An experimental platform for assessing scada vulnerabilities and countermeasures in power plants," in Proc. of the 3rd HSI, 2010.
[10] A. A. C´ardenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in Proc. of the 6th ASIACCS, 2011.
[11] Department of Homeland Security. (2009) Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies.
[12] B. Genge, F. Graur, and P. Haller, "Experimental assessment of network design approaches for protecting industrial control systems," IJCIP, vol. 11, 2015.

За контакти:

Курсант сержант Щилияна Райнова Стоянова, НВУ „Васил Левски" ,Факултет „Артилерия, Противовъздушна отбрана и Комуникационни и информационни системи", тел.:0883504425, e-mail: Sthiliqna1234@gmail.com

гл. ас. д-р инж. Веселка Тодорова, НВУ „Васил Левски", тел.:0888065638, e-mail: veselka_tr@abv.bg

Възможности за стеганография в съвременните комуникационни канали

автор: Станислава Павлова
научен ръководител: гл. ас. д-р инж. Веселка Тодорова

Steganographic capabilities in modern communication channels - *This study explores some mobile applications for steganographic transmission of graphical information. The investigated mobile steganography application is Stegais and the hidden confidential message is transmitted through WhatsApp, Viber, Messenger, Bluetooth and Gmail.*

Key words: *Bluetooth, secret message, Stegais, stegoimages*

ВЪВЕДЕНИЕ

В наситеното ежедневие и непрекъсната нужда за обмяна на информация чрез мигновени съобщения, интерес представляват мобилните приложения, които предоставят тези възможности. В зависимост от държавата използваните от потребителите приложения са разнородни. В настоящата статия са разгледани някои от най-популярните сред тях.

Bluetooth е мрежов стандарт, който работи на две нива: осигуряване на комуникация между мобилни устройства на физическо ниво (тъй като представлява радио-честотен стандарт) и на ниво протокол (решава въпроси свързани с предаването на битове информация). Bluetooth предава данни, използвайки радио вълни с ниска мощност. Комуникацията се осъществява на честота от 2.45 GHz. Сигналите, които Bluetooth излъчва са много слаби – само около един миливат, по тази причина обхватът на едно Bluetooth устройство не е повече от десет метра в радиус, и не може да бъде органичен от прегради. Bluetooth може да свърже до осем устройства едновременно, като всяко от тези устройства излъчва на малко по-различна честота, за да се избегнат потенциални нарушения в мрежата. По-точно, всеки от предавателите (устройствата) сменя честотата си 1600 пъти всяка секунда, позволявайки по този начин на повече устройства да използват малкия дял от радио спектъра. Тази особеност би могло да се разгледа като предимство, което би послужило за нуждите за предаване на тайни съобщения чрез стеганографски методи и приложения.

WhatsApp е мобилно приложение за смартфони, служещо за изпращане на незабавни съобщение. Това приложение е изцяло криптирано.

Viber също е мобилно приложение подобно на WhatsApp, разликата е в това, че разполага с версии за настолни програми за Windows и OS X, така че може да се изпращат, получават и да се следят съобщенията, както от всеки компютър, така и от мобилно устройство.

Facebook Messenger се използва от потребителите, за да общуват с приятелите си във Facebook, които също използват приложението. Възможно е да се изпращат и получават съобщения от потребители на Messenger, които не използват Facebook изобщо.

ОСНОВНИ ХАРАКТЕРИСТИКИ ЗА ОЦЕНКА НА ИЗОБРАЖЕНИЯ

При сравнение на две изображения се пресмятат четири основни статистически характеристики, които описват степента на подобие между изображенията: средна квадратична грешка MSE (Mean Squared Error), отношение на пиковия сигнал към шума PSNR (Peak Signal-to-Noise Ratio), индекс за измерване на структурната прилика в изображение SSIM (Structural Similarity Index for Measuring) и ентропията в изображения [1].

Изчисляването на средната квадратична грешка е стандартен статистически подход за обективно измерване на степента на различие между две изображения [3]. Малка стойност на MSE означава, че средното ниво на разликата между тях е малко. В случай на две еднакви изображения, MSE има стойност, равна на нула. За разлика от MSE, по-голяма стойност на PSNR означава по-добро качество на изображението. При еднаквост на две изображения, PSNR има стойност клоняща към безкрайност. Основна цел на всички стеганографски методи е минимизиране на стойността на MSE и съответно максимизиране на стойността на PSNR.
Изследваните характеристики са представени съответно чрез формули (1) и (2), като PSNR се базира на стойностите, получени за MSE:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (1)$$

където m и n са ширина и височина на изображението; I(i, j) и K(i, j) са съответни пиксели с координати (i, j) в оригиналното и стего-изображение.

$$PSNR = 10.\log_{10}\left(\frac{\max^2}{MSE}\right) = 10.\log_{10}\left(\frac{\max}{\sqrt{MSE}}\right) \qquad (2)$$

където max = 255 за 8 битови изображения.

Степента на подобие на изображенията преди и след процеса на предаване на изображенията през каналите, измерена чрез средната квадратична грешка MSE и отношението на пиковия сигнал към шума PSNR, определя качеството на изображенията [2]. Когато подобието между изследваните изображение е малко се приема, че качеството на стего-изображението е по-ниско.

Индексът за измерване на структурната прилика в изображение SSIM (Structural Similarity Index for Measuring) е подобен на MSE и PSNR, но е създаден с цел да ги подобри. Като показател той измерва промяната в яркостта, контраста и структурата на дадено изображение. За получаването на SSIM се комбинират стойностите, получени за средната интензивност на яркостта, вариациите в контраста и структурата на взаимната корелация между оригиналното и стего-изображението.

ПРОУЧВАНЕ

За нуждите на експеримента е използвано изображение с размери 3024 x 4032. Тъй като всеки комуникационен канал, който се използва за предаване на стего-изображението трансформира размера му, е нужна предварителна подготовка на оригинала за нуждите на всеки канал. Поради тази причина предварително оригиналното изображение се преформатира в средата на Adobe PhotoShop до размер подходящ за комуникационния канал (мобилното приложение за предаване на данни). Така например за WhatsApp размерът се коригира до 1200 x 1600, за Viber-1024 x 1280, за Messenger-360 x 480, когато се използва Bluetooth не нужно да се променя размерът на оригиналното изображение.

Използвано е стеганографско приложение за мобилно устройство –Stegais изтеглено от Google Play.

В оригиналното изображения е вградена информация в размер от 5 байта. Предадено е стего-изображението през WhatsApp, Viber, Messenger, Bluetooth и G-mail. След предаването на стего-изображението при опит за прочитане на конфиденциалната информация, тя бе възстановена само в случаите, когато е предадена чрез Bluetooth. Във всички останали случаи тайната информацията се губи. Извода от това предаване на данни е, че единствения надежден канал за 100% възстановяване на скритата информация от изброените, е Bluetooth устройството, но то има недостатък, че е ограничено в обхвата си.

На фигура 1(а) е представен оригиналът на изображението, в което е скрито тайно съобщение, на фигура 1(б) е представен един скриншот на приложението при вграждане на конфиденциалната информация, а на фигура 1(в) резултатът при извличане на съобщението след предаване по WhatsApp комуникационния канал.

а) б) в)

Фиг. 1 Предаване на скрита информация през WhatsApp мобилно приложение

На фигура 2 са представени: 2(а) оригиналното изображение, 2(б) скриншот на приложението при вграждане на конфиденциална информация, а на 2(в) резултатът при извличане на съобщението след предаване по Bluetooth като комуникационен канал. Тази комуникация е с положителен резултат, видно е че имаме пълно възстановяване на тайното съобщение.

а) б) в)

Фиг. 2 Предаване на скрита информация през Bluetooth мобилно приложение

Резултатът от предаването на стего-изображението през Viber, Messenger и Gmail е същият като WhatsApp. Това означава, че всяко от тези приложения реализиращи комуникационен канал е неподходящо за реализиране на скрита комуникация.

ЗАКЛЮЧЕНИЕ

Настоящото изследване, позволява да се установи по какъв начин се променят изображенията, когато биват предавани чрез Bluetooth, WhatApp, Viber, Messenger, G-mail. Установено бе, че WhatsApp, Viber, Messenger, G-mail не са подходящи за предаване на скрити съобщения чрез стеганографски метод, защото информацията бива унищожена от обработващите им алгоритми. Единствено чрез Bluetooth се реализира тайна комуникация, но тя е ограничена в пространството и не достатъчно удовлетворяваща нуждите на една тайна комуникация. Предаденото по Bluetooth стего-изображение бе възстановено на 100%, без никакви загуби.

ЛИТЕРАТУРА

[1] Veselka Stoyanova, Zhaneta Tasheva, RESEARCH OF THE CHARACTERISTICS OF A STEGANOGRAPHY ALGORITHM BASED ON LSB METHOD OF EMBEDDING INFORMATION IN IMAGES ,*Publication: Trans MotAuto15*. Available from: https://www.researchgate.net/publication/304579312_Trans_MotAuto15, accessed Mar 30, 2017

[2] Rao K. R., and P. C. Yip. „The Transform and Data Compression Handbook“, 1st ed.: CRC Press, 2001

[3] Wang Z., A .C .Bovik, H. R. Sheikh, and E. P. Simoncelli. “Image quality assessment: From error measurement to structural similarity,” IEEE Trans.ImageProcessing,vol.13, Jan.2004

За контакти:

Серж. Станислава Бисерова Павлова, Катедра „Компютърни системи и технологии”, НВУ „Васил Левски“, факултет „А, ПВО и КИС“, тел.: 0897237340, e-mail: stanislavapavlovaa@gmail.com

гл. ас. д-р инж. Веселка Тодорова, НВУ „Васил Левски“, тел.:0888065638, e-mail: veselka_tr@abv.bg

Стеганализ на изображения чрез DCT метод

автор: Станислава Павлова
научен ръководител: гл. ас. д-р инж. Веселка Тодорова

Steganalysis of images created by DCT method*-There are many image steganalysis methods that detect presence of hidden data into the stegoimages generated by LSB steganography. However if the stegoimages is generated by JPEG steganography, these methods show inefficiency of the detection of hidden data. The JPEG steganography is a data hiding technique that performs data hiding in DCT domains. In the steganalysis side, any information about the stegoimage is not available; therefore many steganalisis methods for different types of stegoimages must be combined to generate an efficient steganalisis methodology. In this paper a reliable steganalysis method for JPEG steganography is presented, this steganalysis method later can be added into global steganalysis methodology. The evaluation of steganalysis methods is realized in terms of false negative and false positive error rates.*

Key words: *JPEG, secret message, steganalysis, steganography, stegoimages;*

ВЪВЕДЕНИЕ

Има много алгоритми за стеганография, които могат да се класифицират основно в два класа: LSB стеганография [1] и JPEG стеганография [2]. В LSB стеганографията, равнището на най-младшия значещ бит (LSB) е променено, за да вгради тайно съобщение, което обикновено е предварително кодирано. Докато в JPEG стеганографията, тайното съобщение е вградено в честотен домейн, който се трансформира чрез Дискретно косинусова трансформация (Discrete Cosine Transform, DCT) на изображението. Стандартният формат на изображението в интернет е JPEG формат, съществуват някои методи за JPEG стеганография, като CryptoBola, Jsteg и т.н. [19].

Стеганализът е техника, която се опитва да открие някои статистически доказателства за скритите данни в изображение, което е в процес на анализ. Досега в литературата са предложени редица методи за стеганализ [4-7]. Много от тях могат да открият стегоизображения, генерирани чрез LSB стеганография с висока степен на засичане, но ако дадено стегоизображение се генерира от JPEG стеганография, тези методи показват неефективност при откриването на скрито съобщение. От гледна точка на стеганализа не е налице информация за стегоизображението, като например методът за стеганография, използван за генериране на стегоизображението и размерът на тайно съобщение в стеганализа. Нещо повече, няма никакъв перфектен метод на стеганализ, който да открива наличието на скрито съобщение от всички видове стегоизображения. Ето защо, за да се създаде надеждна схема на стеганализа, трябва да бъдат комбинирани ефективно много методи за извличане.

Някои методи за стеганализ на JPEG стеганография са оценени, за да се избере метод, който отговаря на горепосочените условия. Методът, базиран на статистическите моменти [9], изчислява характерните функции на вълновите поддиапазони. От изображението се извличат общо 39 показани стойности и те се използват за различаване на стойностите за стегоизображението от оригиналното изображение. В [10] отношенията между стойностите на коефициентите на вълновите поддиапазони с различни нива на разлагане и ориентации се използват именно като характеристики. В тях общо 288 стойности на елементите се извличат от двете изображения (стегоизображения и оригинални изображения), за да бъдат класифицирани. Ефективността на двата метода е добра, ако размерът на тайното съобщение е 100% (максимален капацитет), но ако размерът на тайното съобщение е по-нисък от 50%, то процентът на грешки значително ще се увеличили.

Разгледаният метод за извличане, при който плътността на коефициентите между съседните 8x8 DCT блокове и плътността между стойностите на коефициента

на съседните в един DCT блок се използват като сравними характеристики [11]. За да се оцени този алгоритъм, се използват 100 оригинални изображения и 500 стегоизображения с различни по големина тайни съобщения за обучение на Neural Networks (BP алгоритъм) и в етапа на оценка се използват 210 изображения (35 природни изображения и 75 стегоизображения с различно количество тайни съобщения).

АНАЛИЗ НА МЕТОДИТЕ ЗА СТЕГАНАЛИЗ

Накратко са споменати три метода за стеганализ, които са оценени в [8] и показани в сравнението на ефективността по отношение на отрицателните (FN) и положителните (FP) грешки.

А. Разлика в изображенията- хистограмен метод

Хистограмното разпределение може да се използва за разграничаване на стегоизображенията от оригиналните изображения. Разликата в разпределението между различните типове изображения е по-голяма от разликата между оригиналното изображение и стегоизображението, поради което само хистограмното разпределение не е достатъчно. Zhang и колектив, предлагат метода на хистограмата с различно изображение [12], което да генерира различно изображение D, изчислявайки разликата между два съседни пиксела на изображението, дадени от формула (1)

$$D(i, j)=I(i+1, j)-I(i, j) \quad (1)$$

Има три разлики в изображенията: разликата в изображението на оригинала, разликата в изображението с обърната LSB и разликата в изображението с класическо LSB. Тези три разлики се изчисляват чрез формула (1). Връзките между тези три хистограми се използват, за да се разграничат стегоизображенията от оригиналните изображения. Този метод може да се приложи директно към изображенията в сивата скала, но за цветните изображения трябва да се вземат под внимание някои съображения.

Б. Метод на най-близката цветова двойки

Според Fridrich и колектив броят на затворените двойки цветове значително се увеличава, когато изображението има тайно съобщение, вградено в неговия най-младши значещ бит (LSB). Именно затова е предложен метод за стеганализ за LSB методи за вграждане, използвайки съотношение между числото на най-близката цветна двойка и цялата двойка цветови изображения [5]. При този метод се изчисляват броят на всички двойки цветове, съществуващи в изображението, и броят на близките цветни двойки във всички съществуващи двойки цветове. След предварителното LSB вграждане, алгоритъмът за стеганализ се прилага към изображението, както и броят на съществуващите цветови двойки, а самият брой на близките цветни двойки се изчислява с помощта на (2).

$$C_1=[R_1,G_1,B_1],C_2=[R_2,G_2,B_2]$$
$$(R_1-R_2)^2+(G_1-G_2)^{2+}(B_1-B_2)^2<=3 \quad (2)$$

Съотношенията **R** и **R'** между стойностите на близката двойка цветове и броя на всички двойки цветове се изчисляват за анализа на оригиналното изображението и неговия стего вариант, където **P** и **P'** са броят на двойки близки цветове, а **U** и **U'** са броя на всички двойки цветове в изображението и неговия стеганографски еквивалент. Ако формулата (4) е изпълнена, изображението може да се разглежда като естествено изображение, в противен случай изображението съдържа някакво тайно съобщение.

$$R=P/U \quad R`=P`/U` \quad (3)$$

$$R/R' >= T_h \quad (4)$$

В. Вълнови статически стойности

Разгледаният метод на стеганализ се базира на вълнови статистически характеристики. Хистограмите на всички вълнови поддиапазони отразяват само статистическото разпределение на коефициентите в подлента, но не отразяват корелацията на коефициентите в тази подлента. Вълновата трансформация е добре известна със способността си за разлагане в много разредки и декорелация на коефициентите. Известно е, че за дискретни вълнови трансформации, различни високочестотни поддиапазони в едно ниво няма да са свързани помежду си. Характеристиките, извлечени от една високочестотна подлента не са свързани с извлечена от друга високочестотна подлента на същото ниво. Следователно, функции от различни измерения най-вероятно не са свързани помежду си. От тази гледна точка този многоизмерен векторен елемент ще бъде подходящ за представяне на изображението за целите на стеганализа.

Процесът на скриване на данни може да бъде моделиран като допълнителен сигнал, който е независим от изображението. Този сигнал се добавя към прикриващия обект, както е предложено в [13]. Добре известно е, че ефектът на сигнала на добавката върху изображението е еквивалентен на конволюция на две функции с вероятностна плътност (PDFs). Според [14], една интерпретация на характеристичната функция (CF) е, че тя е сложен конюгат на трансформацията на Фурие на PDF файла. Може да се разгледа PDF файла като нормализирана версия на хистограма, в този случай хистограмата на изображението и на хистограмата на коефициентите на поддиапазоните се определя като:

$$H(f_i) = DFT(h[x]) = \sum_{x=0}^{N-1} h[x] e^{-\frac{2\pi j x f_i}{N}} \quad (5)$$

Където ***H(fi)*** е равно на ***CF, DFT (h [x])*** е дискретна трансформация на Фурие на хистограмата, N е общият брой точки в хоризонталната ос на хистограмата, f_i е честотен компонент.

Г. Сравняване на три метода за стеганализ

За да се оценят трите метода на стеганализ се използват 100 цветни изображения с размер 128x128 пиксела. С помощта на пет метода на стеганография [1,16-18] се генерират 500 стегоизображения. Таблица 1 показва резултатите от сравнението [8], а таблица 2 показва значението на символите, използвани в таблица 1.

От таблицата се вижда, че методът на стеганализ DH [12] показва добра ефективност на откриване на стегоизображенията, генерирани от LSB стеганография, но ако стегоизображения бъдат генерирани чрез JPEG стеганография или друг метод, като BPCS, отрицателеният процент грешки е значително по-висок. Също така оригиналните изображения се бъркат често със стегоизображения (FP = 93). Подобни резултати се получават за метода CC. Методът за стеганализ FE показва по-добра производителност за JPEG стеганография, но положителната грешка все още е висока, за да се генерира надеждна методология на стеганализа. Резултатите от сравненията показват, че липсва ефективен метод за стеганализа за JPEG стеганография.

Таблица 1 Сравнителни резултати на анализа

Data Hiding Method	DH	CC	FE
	FN	FN	FN
S-tool	0	0	2
IS	0	0	2
BPCS	91	100	24
Huang	90	100	45
Piva	84	100	34
	FP	FP	FP
Natural	93	0	50

Таблица 2 Съкращения използвани в таблица 1

Symbol	Meaning
DH	Difference Image Histogram Steganalysis [12]
CC	Close Color Steganalysis [5]
FE	Feature Extraction Steganalysis based in Wavelet [9]
S-tool	S-tool Steganography [1]
IS	Invisible Secret Steganography[1]
BPCS	Bit-Plane Complexity Segmentation Steganography [16]
Huang	DCT based Data hiding method by Huang [17]
Piva	DCT based Data hiding method by Piva [18]
FN	False Negative Error Rates
FP	False Positive Error Rates

РЕЗУЛТАТИ ОТ СТЕГАНАЛИЗА

За да се оцени методът на стеганализ на базата на DCT блок, се извършват четири различни оценки. Във всички случаи се използват цветни изображения с размер 512x512 в JPEG формат. За да се генерират стегоизображения чрез JPEG стеганографията е използван CryptoBola стеганографския метод [1] с различна степен на вграждане на тайно съобщение (10%, 20%, 50%, 80%, 100%). Той се прилага към оригиналните изображения. При всички оценки се използват многослойни невронни мрежи с алгоритъм за обратна пропускливост за класификацията (виж табл.3.)

Таблица 3 Ефективност на сравнения при различен капацитет на информация

Брой стегоизображения	Скрити данни от пълния капацитет %	FP	FN	Успешни опити
20	10 %	7	5	80%
20	20%			
20	50%			
20	80%			
20	100%			

ЗАКЛЮЧЕНИЕ

Като се вземат предвид резултатите от сравнението, е представен методът за стеганализ на базата на DCT блок за JPEG стеганализ, извършената компютърна симулация за оценка на производителността на алгоритъм, базиран на DCT блок, използвайки многослойни невронни мрежи, като дискриминатор на стегоизображението от оригиналните изображения. В експерименталните резултати

положителните и отрицателните грешки за JPEG стеганографията са достатъчно малки в сравнение с предишните три метода. Това означава, че алгоритъмът базиран на блокове DCT може да бъде добавен в методологията на стеганализа, за да се увеличи неговата надеждност.

ЛИТЕРАТУРА

[1] Veselka Stoyanova, Zhaneta Tasheva, Research of the characteristics of a steganography algorithm based on LSB method of embedding information in images, Publication: Trans MotAuto15, Available from: https://www.researchgate.net/publication/304579312_Trans_MotAuto15, accessed Mar 30, 2017
[2] Q. Cheng and T. Huang, "An Additive Approach to Transform- domain Information Hiding and Optimum Detection Structure", IEEE Trans. on Image Processing, vol. 12, no. 2, 2003, pp. 221-229.
[3] L. Marvel, C. Boncelet and C. Retter, "Spread Spectrum Image Steganography", IEEE Trans on Image Processing, vol. 8, no. 8, pp.10751083, 1999.
[4] J. Fridrich, M. Goljan and R. Du, "Detecting LSB Steganography in Color and Gray Scale Image", IEEE Multimedia, vol.8, no. 4, pp. 22-28, 2001.
[5] J. Fridrich, R. Du and M. Long, "Steganalysis of LSB Encoding in Color Images", in IEEE Int. Conf. on Multimedia and Expo, 2000, pp. 1279-1282.
[6] A. D. Ker, "Steganalysis of LSB Matching in Grayscale Images", IEEE Signal Processing Letters, vol. 12, no. 6, 2006, pp. 441-444.
[7] X. Lui, B. Liu, F. Liu, "Detecting LSB Steganography Based on Dynamic Mask", Proc. on 5th Conf. on Intelligent System Design and Application, 2005.
[8] A. Hernandez-Chamorro, A. Espejel-Trujillo, J. Lopez-Hernandez, M. Nakano-Miyatake, H. Perez-Meana "A Methodology of Steganalysis for Images", CONIELECOMP 2009.
[9] R. Martinez-Noriega, J. Lopez-Hernandez, M. Nakano-Miyatake, K. Yamaguchi, "Detection of BPCS-steganography using SMECF Steganalysis and SVM", to appear Int. Symp. of Information Theory and Its Applications (ISITA) 2008.
[10] S. Lyu, H. Farid, "Steganalysis using High-Order Image Statistics", IEEE Trans on. Information Forensics and Security, no. 1, vol. 1, pp. 111119, 2006.
[11] Qingzhong Liu, Andrew H. Sung, Mengyu Qiao, "Improved Detection and Evalution for JPEG Steganalysis", Proc. MM'09, October 1924,2009Beijing, China.
[12] T. Zhang, X. Ping,"A new approach to reliable detection of LSB steganography in natural images" Signal Processing, vol. 83, no. 10, pp. 2085-2093, 2003.
[13] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Steganalysis of Spread Spectrum Data Hiding Exploiting Cover Memory," the International Society for Optical Engineering, Electronic Imaging, San Jose, CA, USA, 2005.
[14] A. Leon-Garcia, Probability and random processes for electrical engineering, 2nd edition, reading, MA: Addison-Wesley Publishing Company, 1994.
[15] G. Xuan, Y. Q. Shi, D. Zou, J. Gao, C. Yang, Z. Zhabg, P. Chai, W. Chen, C. Chen, "Steganalysis based on multiple features formed by statistical moments of wavelet characteristic Functions," IH 2005 LNCS 3727, pp. 262-277, Springer-Verlag Berlin Heidelberg 2005.
[16] H. Noda, J. Spaulding, M. Shirazi, M. Niimi and E. Kawaguchi, "BPCS Steganography Combined with JPEG2000 Compression", Proceedings of Pacific Rim Workshop on Digital Steganography , pp. 98107, 2002.
[17] J. Huang and Y. Shi, "Adaptive image watermarking scheme based on visual masking", Elect. Lett., vol. 34, no. 8, pp. 748-750,1998.
[18] A. Piva, M. Barni, F. Bartolini and V. Capellini, "DCT-Based watermark recovering without restoring to the uncorrupted original image", in Proc. of IEEE ICIP, pp. 520-523, 1997.

[19] Rao K. R., and P. C. Yip. „The Transform and Data Compression Handbook“, 1st ed.: CRC Press, 2001

За контакти:

Серж. Станислава Бисерова Павлова, Катедра „Компютърни системи и технологии”, НВУ „Васил Левски“, факултет „А, ПВО и КИС“, тел.: 0897237340, e-mail: stanislavapavlovaa@gmail.com

гл. ас. д-р инж. Веселка Тодорова, НВУ „Васил Левски“, тел.:0888065638, e-mail: veselka_tr@abv.bg

Интерактивен софтуер за генериране на тестове за откриване на неизправности в последователни схеми

автор: Виктор Братоев
научен ръководител: доц. д-р Галина Иванова

Interactive software for generating tests for error detection in sequential logic circuits: *This paper discusses some problems which can occur in sequential logic circuits and how we can detect them. An interactive software for generating test for error detection in sequential logic circuits is described. The software is designed for academic purposes and guides students in solving the tasks during the workshops.*
Key words: *error detection, sequential logic circuits, logic Gates, testing*

ВЪВЕДЕНИЕ

Нарастващата сложност на съвременните технически системи, при които броят на елементите, от които те са съставени може да бъде много голям и относително малки и локални дефекти могат да доведат до нарушаване или до пълно прекратяване на функционирането на компютърните системи [4,5].

Ето защо е важно да се изследват проблемите за решаването на задачи от последователни схеми, което е и предмет на настоящия доклад.

Един от методите, с които може да се решават такъв тип проблеми е метод използващ таблиците за истинност. Методът включва създаване на таблица и матрица на локализацията, която в последствие се минимизира по определени правила. Като резултат се генерира списъкът на входните вектори, които образуват търсения диагностичен тест за локализиране на неизправностите.

ОТКРИВАНЕ НА НЕИЗПРАВНОСТИ В ПОСЛЕДОВАТЕЛНИ ЛОГИЧЕСКИ СХЕМИ

Генерирането на тестове за последователностни схеми е трудна задача, което се обуславя от следните фактори, [1]:

- Всеки възможен входен тестов вектор трябва да се изчислява за всяко състояние на схемата. Следователно, всеки елемент на памет в разглежданата схема удвоява обема на изчисленията, необходими за откриване на теста.
- Преди да се приложи даден тест, схемата трябва да се установи в начално състояние. Това става обикновено чрез нулиращи вериги. В този случай, при изграждането на теста трябва да се отчитат и неизправностите, които могат да възникнат в тях.

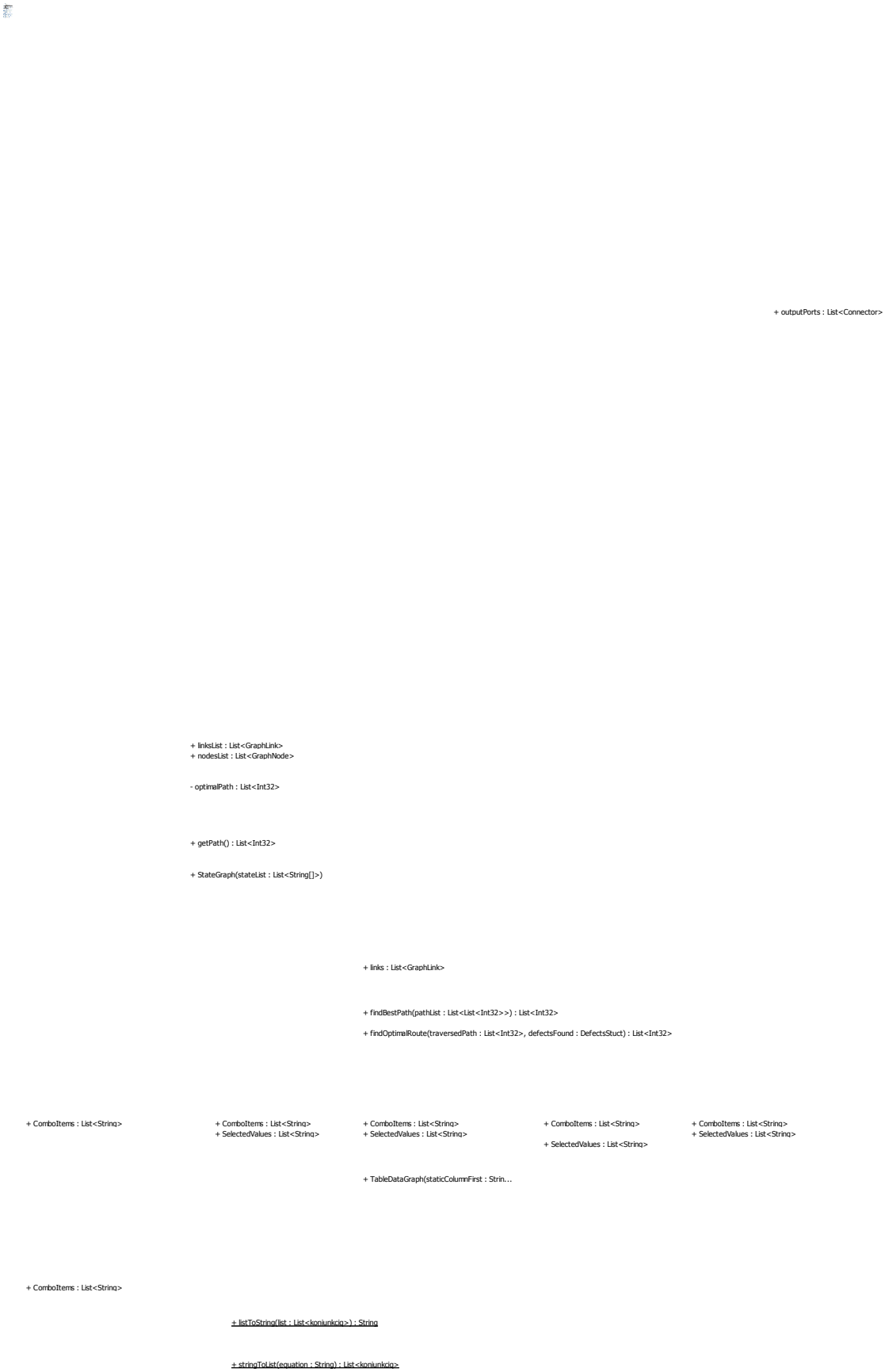
ИЗИСКВАНИЯ КЪМ ПРИЛОЖЕНИЕТО

- С приложението да се работи лесно и интуитивно;
- Да се правят проверки за грешки на студента в процеса на решаване;
- Да се вгради редактор за изчертаване на логически диаграми;
- Да се вгради тестов механизъм за динамична проверка на схемата, на базата на предварително зададеното уравнение за изчертаване;
- Да се изчислят автоматично всички възможни оптимални тестове за решаване на конкретната задача;
- Да се запази един от най-оптималните тестове и да се сравни с характеристиките на намерения от студента тест.
- Проектираният софтуер за решаване на задачи за последователни схеми да обхваща два типа запомнящи схеми: D тригер и JK тригер.
- Приложението да открива и локализира два типа неизправности: от тип „Тъждественна единица" (≡1) ; от тип „Тъждественна нула" (≡0).

ОПИСАНИЕ НА РАЗРАБОТКАТА НА АВТОРСКА СИСТЕМА ЗА РЕШАВАНЕ НА ЗАДАЧИ ОТ ПОДЛЕДОВАТЕЛНОСТНИ СХЕМИ

За реализиране на системата е използван езикът C# и среда за програмиране Visual Studio 2013 [2,3]. Избран е Windows Presentation Foundation GUI framework заради гъвкавостта която предлага и по-ефикасното изчертаване на графични елементи, необходими при построяване на логическата диаграма. Приложението започва да решава задачата веднага след като потребителят избере желаният тригер и стойности за графа. Резултатите се запазват в списъци и масиви и когато се налага проверка дали студентът работи вярно, просто се сравняват въведените стойностите с тези които програмата е изчислила скрито от потребителя. За проверката на логически уравнения се грижи помощният клас LogicString, който съдържа набор от статични функции за обработка и валидация на логическите уравнения. При логическата диаграма ситуацията е по-сложна, тъй като няма само една точно определена диаграма която да отговаря на получените уравнения. В този случай се налага динамична проверка. Всеки логически елемент наследява класът DiagramObject, който от своя страна е наследник на служебният клас Image за да може лесно да се визуализират елементите с помощта на статични изображения. Всеки логически елемент съдържа информация за всички свои входове и изходи, координатите им и свързаните към тях елементи. Връзката между логическите елементи се осъществява с класа Connector който изглежда като обикновена начупена линия за потребителя, но в действителност съдържа информация за свързаните елементи, наличие на поставена неизправност и функция за динамично изчертаване на линията в зависимост от координатите на свързаните логическите елементи и визуален индикатор за неизправност. С помощта на тези класове построената от потребителя диаграма се обхожда рекурсивно от края към началото и получените логически уравнения се сравняват с тези на които диаграмата е базирана и така разбираме дали студентът работи правилно. След потвърждаването на диаграмата приложението работи както в началото - решава задачата и сравнява резултата с този на потребителя. Единствената по-специфична операция е откриването на правилен оптимален тест, където отново може да има повече от едно решение. Този проблем е преодолян с помощта на специално дефиниран граф StateGraph, с дъги и възли съответно GraphLink и GraphNode. Изгражда се модел на последователната таблица на произведенията чрез графа и той се обхожда рекурсивно докато се намери един от оптималните тестове. Тестът направен от потребителя не се проверява за идентичност с този намерен от графа, но за да се счита тестът на студентът за оптимален, той трябва да има същия брой намерени и локализирани неизправности и същия брой стъпки. Тук приложението приключва и предоставя информация за брой допуснати грешки в задачата и времето за решаване.

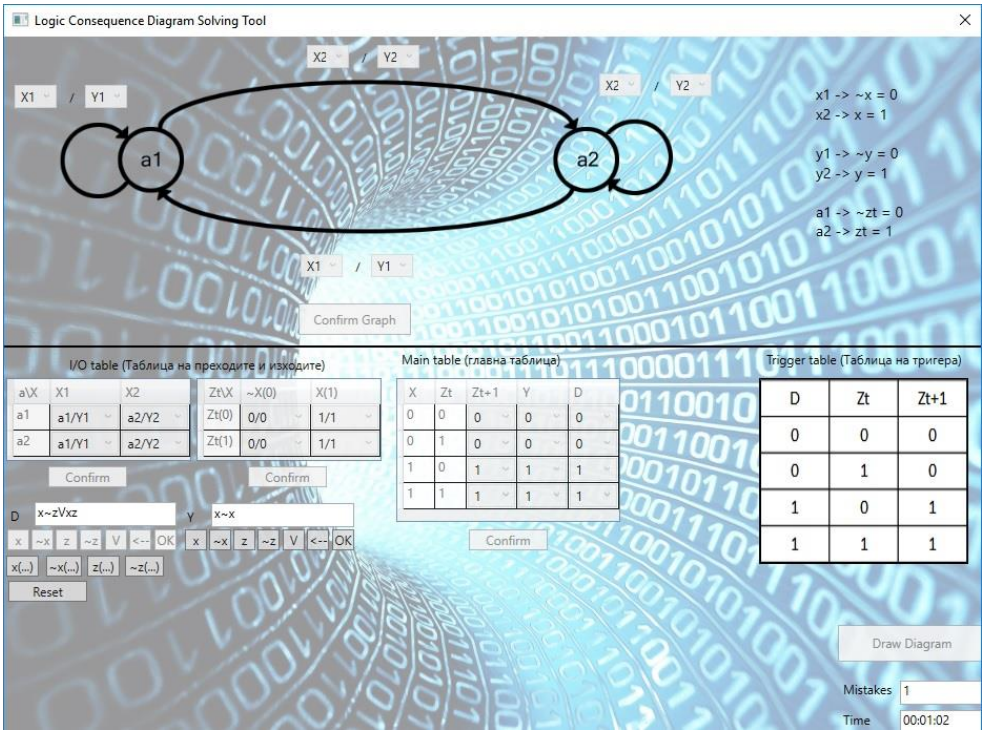
На фиг. 1 е представена клас диаграмата на приложението. В горната част е разположен класа DiagramObject и неговите наследници. След тях са изобразени гореописаните класове за специалния граф, а в долната част на диаграмата се намират група класове, които служат за посредници между въведената в потребителския интерфейс информация и програмния код.



Фиг. 1 Клас диаграма на приложението

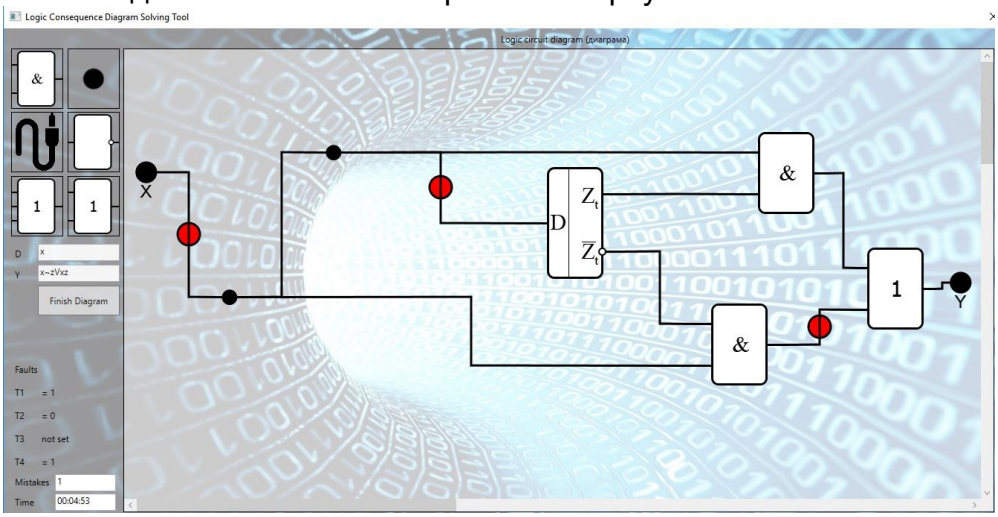
На фиг. 2 е представен първият екран на приложението с графът, който се решава. Първоначално студентът избира вида на тригера, с който ще работи автомата. С помощта на интерфейса потребителят попълва таблицата на преходите

и изходите и нейната кодирана версия. Следващата таблица зависи от вида на тригера и след нейното правилно попълване вече могат да се въвеждат логическите уравнения. Когато всичките уравнения се потвърдят от програмата студентът може да ги опрости ако това е възможно и да пристъпи към следващата стъпка – изчертаването на диаграмата.



Фиг. 2 Графът и неговите таблици

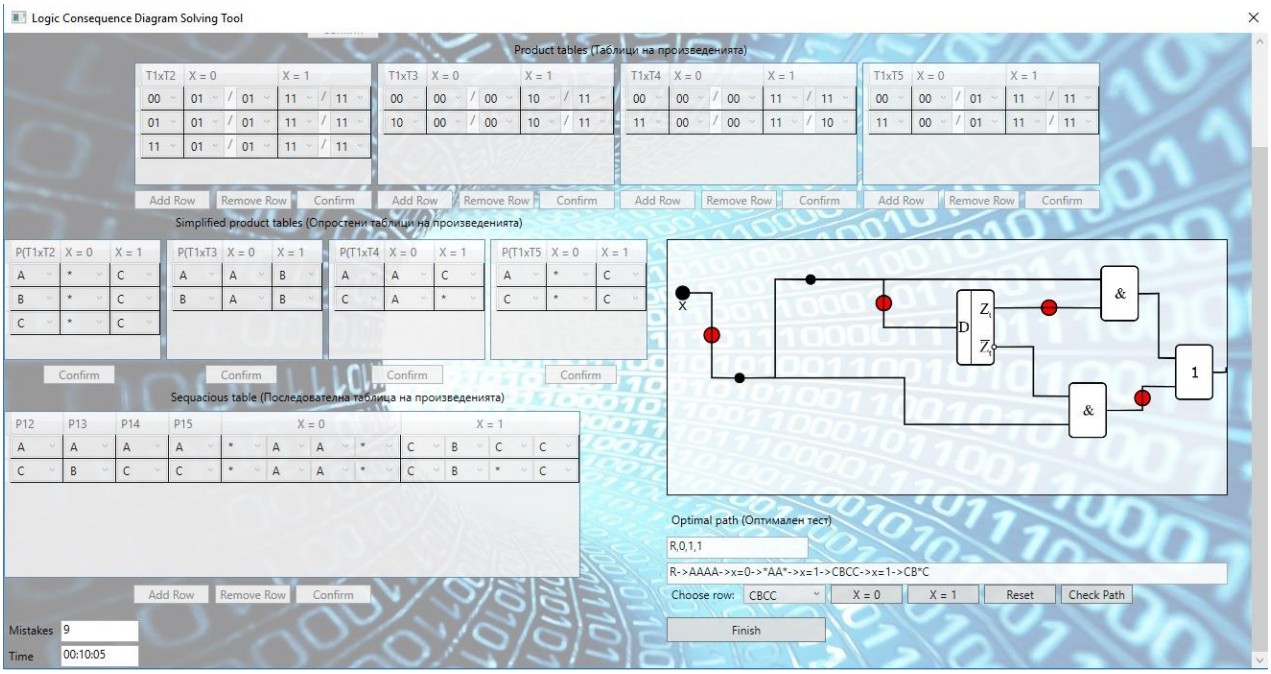
На фиг. 3. е представен редакторът, с помощта на който се изчертават логическите схеми. Входът X, изходът Y и тригерът са автоматично добавени в диаграмата, тъй като те винаги са необходими. Използвайки бутоните от дясната страна на прозореца, потребителят може да поставя нови логически елементи в диаграмата, както и връзки между тях. Елементите могат да бъдат подреждани и изтривани с помощта на мишката, а натискането на левия клавиш върху избрана връзка позволява добавянето на неизправност върху нея.



Фиг. 3 Редактор със създадена логическа схема

Създадената с генератора схема се валидира от приложението и ако тя отговаря на получените логически уравненията студентът започва да попълва таблиците на преходите и изходите (фиг. 4), таблиците на произведенията,

опростените таблици и последователната таблица на произведенията. Накрая потребителят има възможност да направи оптимален тест, който се валидира по три критерия: брой открити грешки, брой локализирани грешки и дължина на теста.



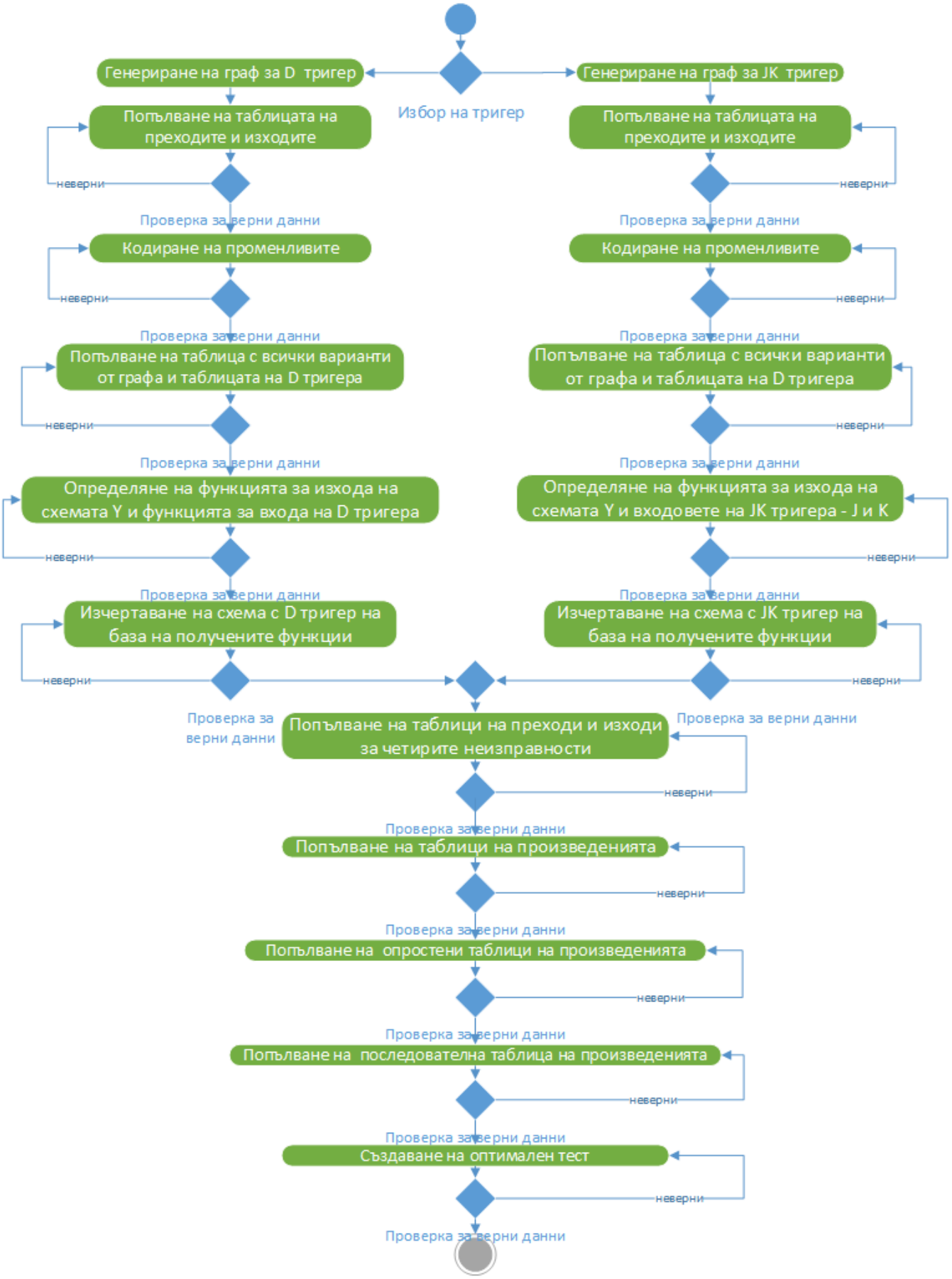
Фиг. 4 Таблици на произведенията и оптимален тест

ПРЕДИМСТВА НА СОФТУЕРНОТО РЕШЕНИЕ

- Интерактивен и интуитивен софтуер;
- Улесняване и автоматизиране на процесите за решаване на задачи за последователни схеми;
- Неограничен брой възможности за решаване на задачи за подготовка;
- Следене на времето за решаване и на допуснатите грешки от студента;
- Показване на местата с грешни отговори;
- Компютърно изчертаване на диаграмите за решаване на задачите;
- Бърза и лесна проверка на задачите от преподавателите.

ДИАГРАМА НА ДЕЙНОСТИТЕ ЗА РЕШАВАНЕ НА ПОСЛЕДОВАТЕЛНИ СХЕМИ

На фиг. 5 е представена диаграмата на дейностите за решаване на последователни схеми. Тя описва основните етапи в задачите от този тип и показва, че на всеки един от тези етапи въведените данни се проверяват и при откриване на несъответствие с вярното решение програмата не позволява на потребителят да продължи със следващият етап от задачата, докато той не въведе правилното решение.



Фиг. 5 Диаграма на дейностите за решаване на последователни схеми

ЗАКЛЮЧЕНИЕ

Представеният интерактивен софтуер за обучение ще бъде инсталиран в учебната лаборатория по дисциплината Надеждност и диагностика на компютърни системи в катедра Компютърни системи и технологии. Софтуерът ще се използва в часовете за решаване на задачи от последователни схеми.

Цели се улеснението на преподавателите и студентите, като задачите се генерират в приложението, а резултатитите от тяхното решение се визуализират и сравняват в процеса на решаване.

ЛИТЕРАТУРА

[1] Смрикарова, Ст., Г. Иванова, Учебни материали по Надеждност и диагностика на компютърни системи, E-learning Shell 2, 2016.
[2] Колев, В. С. Наков, Fundamentals of computer programming with C#, 2013.
[3] Тепляков, С. Шаблони за дизайн на платформата .NET, Издателство Асеневци, 2016.
[4] Peischl, Bernhard, and Franz Wotawa. Automated source-level error localization in hardware designs. IEEE Design & Test of Computers 23.1 , pp 8-19, 2006.
[5] Rothenberger, Roland D. Fully scan-set testable embedded edge-triggered dual D and J-K flip-flops through testing as inverter strings, Sperry Corporation, 1986.

За контакти

Виктор Братоев – студент от четвърти курс в специалност „Компютърни системи и технологии", катедра КСТ, Факултет ЕЕА, Русенски университет "Ангел Кънчев", e-mail: viktorbratoev@yahoo.com

доц. д-р Галина Иванова – преподавател в катедра „Компютърни системи и технологии", Факултет ЕЕА, Русенски университет "Ангел Кънчев", e-mail: givanova@ecs.uni-ruse.bg

Онлайн система за оптимизиране организационните процеси на танцови събития и фестивали

автор: Катерина Мицова
научен ръководител: доц. д-р Галина Иванова

Online system to optimize organizational processes of dance events and festivals: *This paper discusses an opportunity for online optimization of the organizational processes of dance events and festivals. The system was tested in real conditions for the needs of the first edition of Movmnt International Dance Competition – Ruse 2017.*

Key words: *dancing, festivals, event management, organizational process, algorithm, optimization*

ВЪВЕДЕНИЕ

Във века на технологичен прогрес, компютрите и интернет придобиват все по-голямо значение. Употребата им при организиране на танцови събития и фестивали е не само логична, а и наложителна.

Едно такова събитие, най-често е международно. Процесът на организация е дълъг и сложен. Използването на съвременни технологии, които са добре обмислени и реализирани, може да оптимизира този процес и да сведе рисковете от пропуски в организацията до минимум, [1,2].

За осъществяването на такъв тип начинание е необходимо да има ясни правила, които да бъдат сведени до знанието на всички желаещи да се включат, [3]. От изключителна важност е организаторът да е наясно с броя на участниците и хореографиите, които ще се включат. С не по-малко значение е и времетраенето на всяко изпълнение, за да може да се предвиди продължителността на събитието, тъй като по-голямата част от участниците са деца и трябва да се помисли за разумно време, в което те да са ангажирани с участието си.

В този вид състезания, изпълненията се разделят по стил, категория и възрастова група на изпълнителите, [4, 5, 6]. За организатора е много по-удобно, за изготвяне на стартовата листа, да получи информацията в синтезиран вид. Освен всичко останало, всеки участник заплаща такса участие, определена от регламента – за цялостно участие или за всяко изпълнение. Би било улеснение за всяка от страните, системата да прави изчисление на таксите и участниците да могат да сравнят своите изчисления, с тези, направени от софтуера, а организаторът да получава своевременно актуална информация за сумите, които предстои да получи.

Един от най-сложните етапи в организацията на едно състезание е анализирането на информацията от регистрациите и подреждането ѝ в стартова листа, която включва всички изпълнения, подредени по стил, категория и възрастова група. Създаването на работещ, универсален алгоритъм, би спестило много пропуски и загуба на време.

Всичко това налага необходимостта от софтуерен продукт, който да обединява в себе си всички функционалности за възможно най-точно и безпроблемно изпращане и получаване на информация от заинтересованите страни. Като оптимизира процеса на организация от регистрацията до подреждането на стартовия лист.

ФУНКЦИОНАЛНИ ВЪЗМОЖНОСТИ НА АВТОРСКА ОНЛАЙН СИСТЕМА ЗА ОПТИМИЗИРАНЕ ОРГАНИЗАЦИОННИТЕ ПРОЦЕСИ НА ТАНЦОВИ СЪБИТИЯ И ФЕСТИВАЛИ

Онлайн системата за оптимизиране организационните процеси на танцови събития и фестивали има следните възможности:

- Регистрация на групи, които могат да влязат в системата, след одобрение от администратор
- Администраторът получава уведомление на електронната си поща, че има регистрирана група, чакаща одобрение. След влизане в системата той може да одобри или изтрие съответната група
- Всяка група има възможност да регистрира своите участнци, да ги изтрива от системата, както и да редактира имената им
- Всяка група има възможност да регистрира своите хореографии, да ги редактира и изтрива.
- При регистриране на хореографии, участниците в съответния танц се избират от падащо меню, което съдържа имената на всички танцьори на групата
- Възрастовата категория, в която попада една хореография, се изчислява от системата според рождените дати на участниците и групите няма как да регистрират съответния танц в по-ниска възрастова категория
- Музиката за всяка хореография се качва в системата при регистрацията на танца, като системата проверява нейното времетраене и не допуска mp3 файлове с по-голяма от допустимата за категорията продължителност
- Таксата участие, която трябва да се заплати за всеки танц се изчислява от системата. Всяка регистрирана група вижда общата сума, която дължи, като в нея са включени всички танци, чиито данни са напълно въведени
- Администраторът има възможност през своя панел да види всички регистрирани до момента групи, както и броя участници и хореографии, регистрирани от всяка група
- След приключване на регистрацията на всички свои участници и хореографии и превеждане на дължимата сума по сметката на организатора, всяка една група се отбелязва като заплатила и от този момент нататък може да вижда своите регистрации, но не и да ги редактира или трие
- При получаване на сумата по своята сметка, организаторът отбелязва през своя панел групата като заплатила и това позволява тя да влезе в стартовата листа
- Проектиран е алгоритъм, който извлича информация от БД за всяка регистрирана хореография и чрез нея нарежда стартовия лист

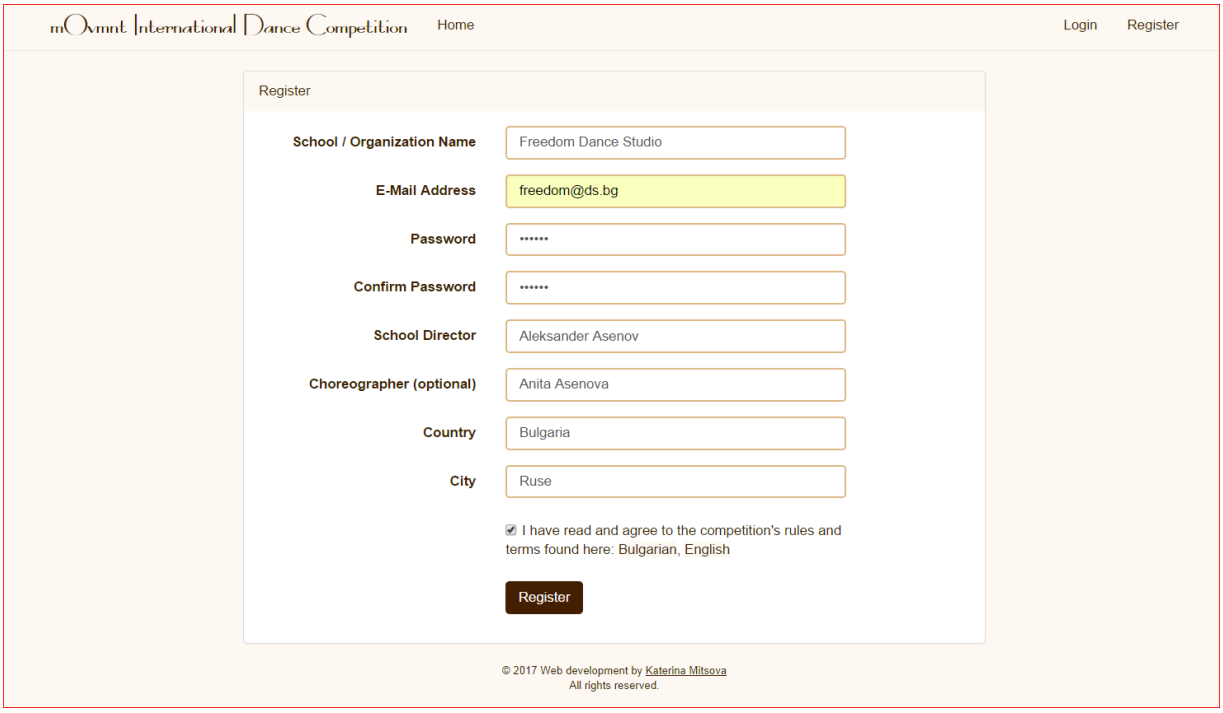
ОПИСАНИЕ НА СИСТЕМАТА

За реализация на системата, съобразно целите на проекта, са използвани:

- Laravel – рамка (framework) за бърза разработка на PHP приложения. Основно предимство – поддръжка на Model-View-Controller;
- Езици за програмиране: PHP, Java script, HTML, CSS;
- Система за управление на базите данни: сървър за бази данни MySQL;
- WEB сървър – Apache HTTP сървър.

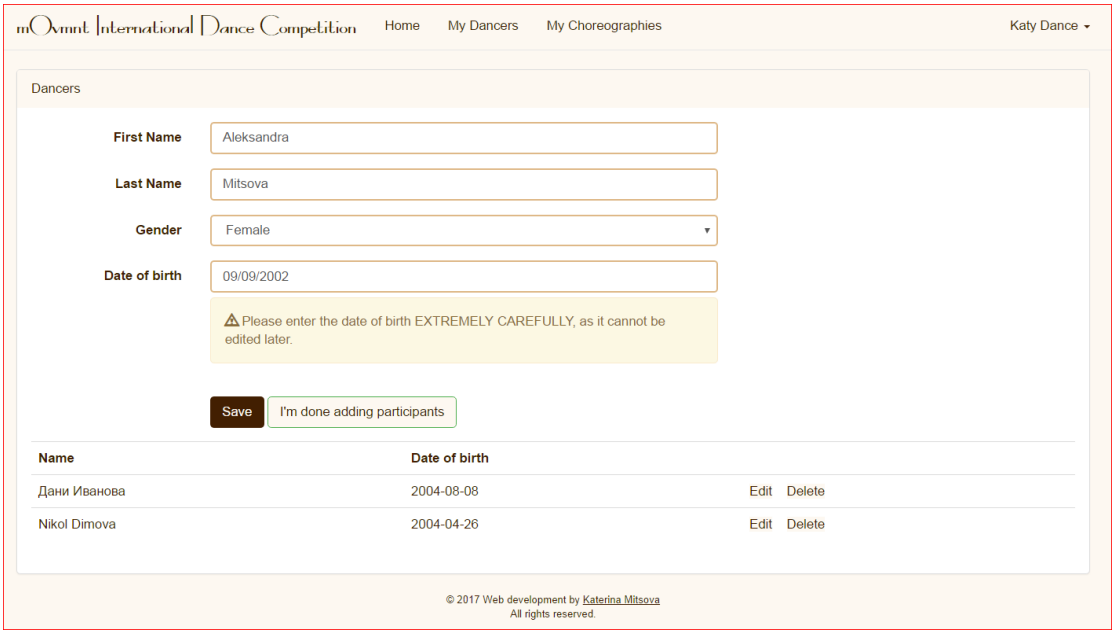
Системата е тествана в реални условия, за нуждите на първото издание на Movmnt International Dance Competition – Русе, 2017. В състезанието взеха участие близо 600 участници от 60 групи, танцови училища и организации, с над 400 хореографии, като всички те бяха регистрирани чрез платформата. Следващите фигури, показват процеса на регистрация.

На фигура 1 е показан екранът за регистрация на групи. След попълване на формата и поставяне на отметка за съгласие с общите условия, групата се регистрира и очаква одобрение.



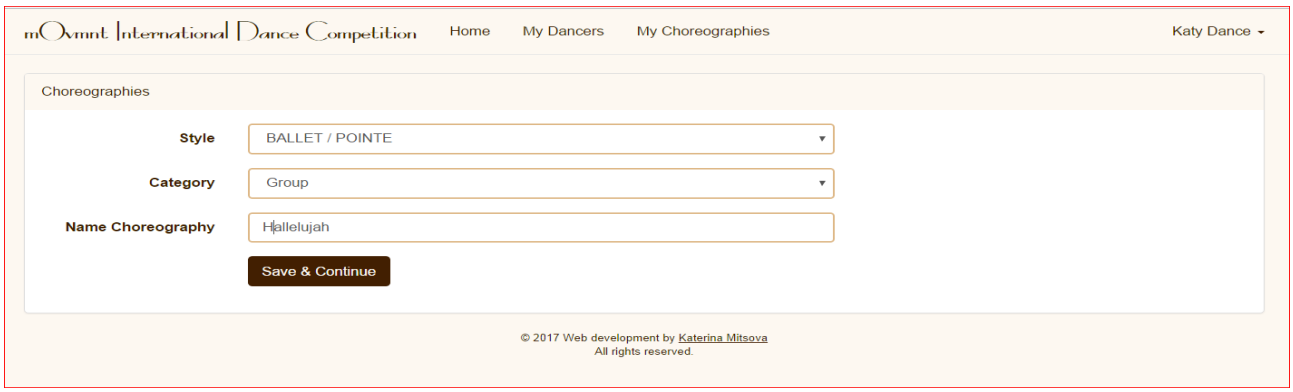
Фиг. 1 Екран за регистрация на групи

След получаване на одобрение всяка група има възможност да влезе в системата и да регистрира своите танцьори и хореографии. На фигура 2 е показан процесът по регистриране на участник.



Фиг. 2 Екран от регистрация на участник

След регистриране на своите танцьори, всяка група може да премине към регистрация на хореографии. Регистрирането на танци става на две стъпки. Първата от тях е показана на фигура 3.

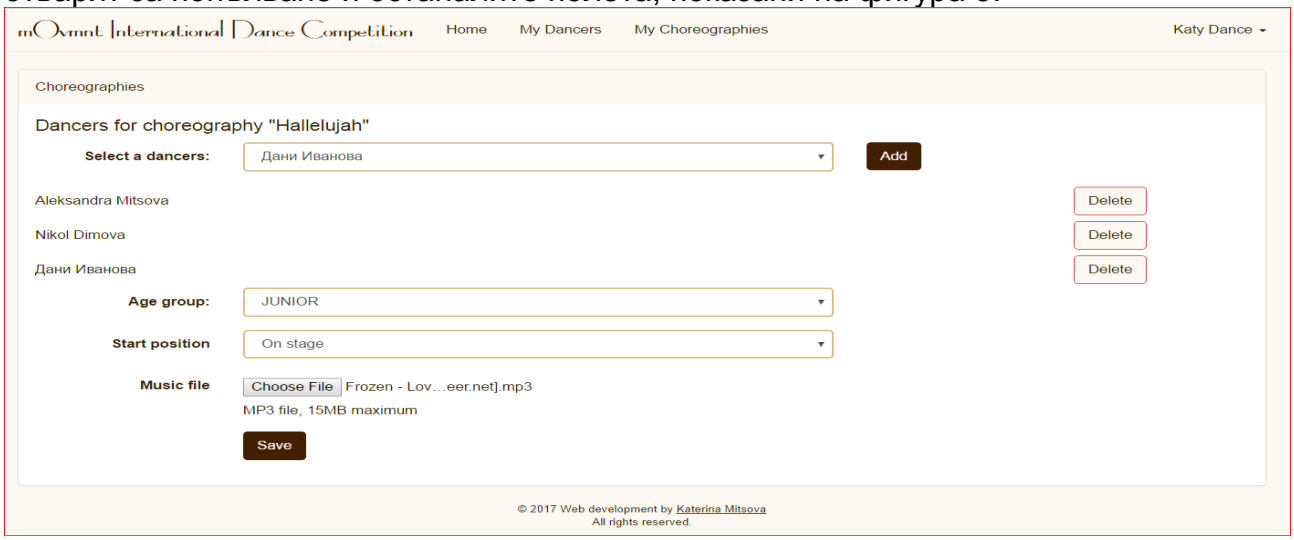


Фиг. 3 Първа стъпка по регистрация на танц

На фигури 4 и 5 е показана втора стъпка от регистрацията на хореография. Потребителят вижда екрана от фигура 4.

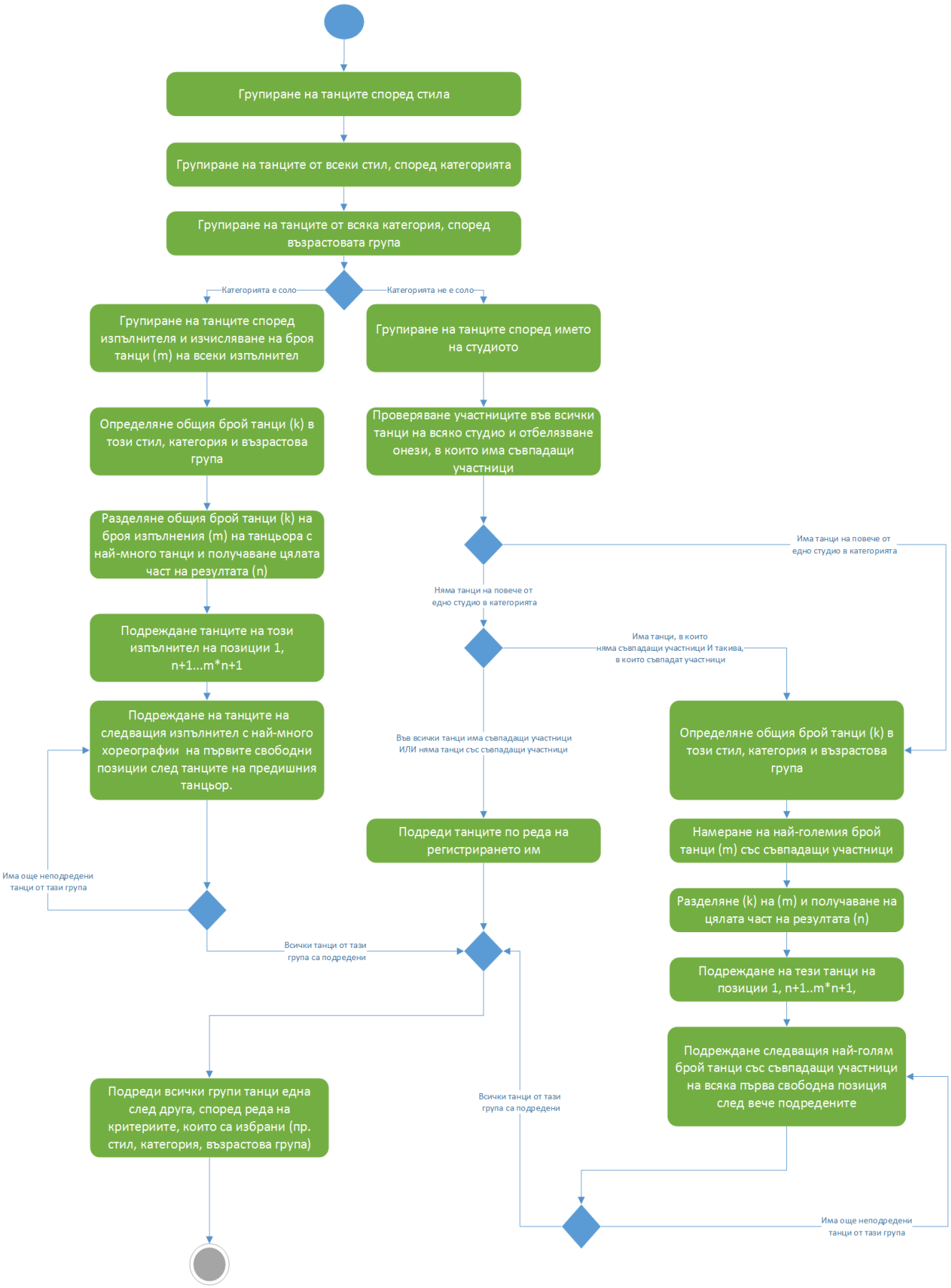
Фиг. 4 Избор на участници в хореографията

Едва след като бъде избран необходимия минимум участници за категорията се отварят за попълване и останалите полета, показани на фигура 5.



Фиг. 5 Довършване на регистрацията на хореография

Проектиран е алгоритъм, който подрежда регистрираните хореографии в старт лист, представен на фигура 6.



Фиг. 6 Алгоритъм за подреждане на стартов лист

АНКЕТНО ПРОУЧВАНЕ

Проведено е анкетно проучване на мнението на ръководителите на танцови групи, участници в Movmnt International Dance Competition - Русе, 2017, относно полезността на функционалностите на системата.

Резултатите от анкетата ще спомогнат за бъдещото развитие и усъвършенстване на софтуерната система.

Анкетата се състои от 14 въпроса от различен тип. След анализ на резултатите е направен извод за полезността на различните функционалности според мнението на анкетираните. На фигура 7 е представен един от обобщаващите въпроси за функционалностите на системата. Еднократната регистрация на танцьорите, която улеснява добавянето на участниците в хореографиите е оценена най-високо.

Фиг. 7 Въпрос от анкетно проучване

ЗАКЛЮЧЕНИЕ

След тестването на системата в реални условия, за първото издание на "Movmnt International Dance Competition – Русе, 2017", и добрите резултати, които дадоха тестовете, се предвижда софтуерът да се използва и за следващите издания на състезанието.

След внедряването на системата беше направен анализ и бяха планирани нови функционалности, които предстои да бъдат добавени в бъдещото доразвиване на системата.

ЛИТЕРАТУРА

[1] Yeoman, Ian. Festival and events management: an international arts and culture perspective. Routledge, 2004.
[2] Van der Wagen, Lynn. Event management. Pearson Higher Education AU, 2010.
[3] Dale, Malik. Event organizer, US20070016661 A1, 2007.
[4] Dance Star Festival Registration Site - http://register.dancestar.org
[5] Fest Info Festival Panel – http://go2festinfo.com
[6] Sly Dance Event System – http://www.slydance.in.rs/

За контакти

Катерина Мицова, Русенски университет "Ангел Кънчев", специалност „Компютърни системи и технологии", e-mail: katerinamitsova1@gmail.com

доц. д-р инж. Галина Иванова, Русенски университет "Ангел Кънчев", катедра „Компютърни системи и технологии", e-mail: givanova@ecs.uni-ruse.bg

Изследване на технологиите за реализация и визуализация на триизмерни обекти в уеб

автор: Пламен Димитров
научен ръководител: доц. д-р Галина Иванова

Research on technologies for creation and visualization of three-dimensional objects in web: The problem discussed in this paper concerns 3D technologies and their application in the web. The tools necessary for solving this problem are presented. The paper introduces 3D web applications in multiple scientific fields. An experiment showing creation and visualization of three-dimensional models in web is described.

Key words: *three dimensional, graphics, web*

ВЪВЕДЕНИЕ

Глобална тенденция е преместването на различни приложения и услуги от локални системи в уеб пространството. Забързаното ежедневие , лесния достъп до интернет пространството от различни устройства и бързо развиващите се технологии са някои от предпоставките за използването на уеб. Благодарение на HTML 5, освен аудио и видео, вече можем да използваме, както двуизмерни, така и триизмерни обекти в нашите приложения [1,2,3].

ВИЗУАЛИЗАЦИЯ НА 3D ОБЕКТИ В УЕБ

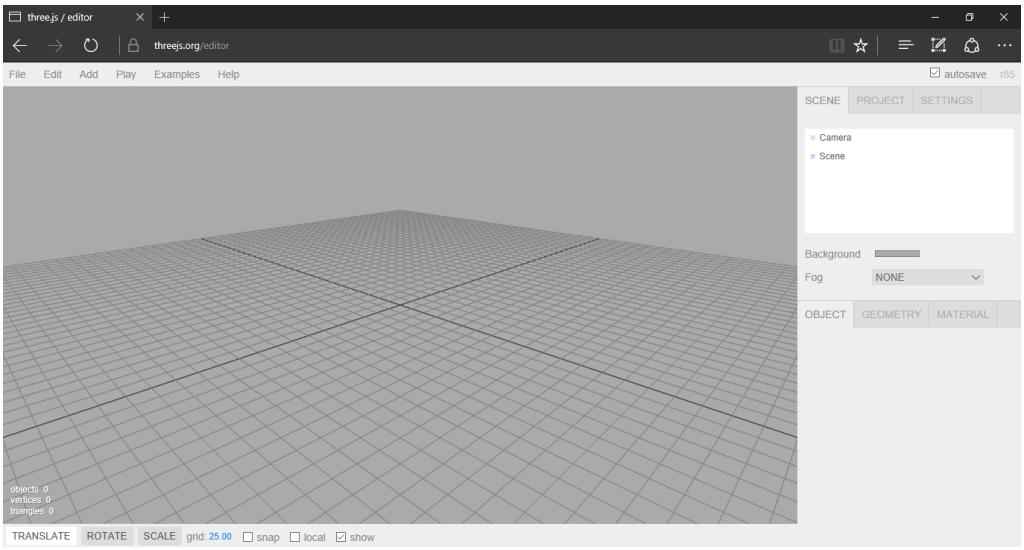
Основното средството за визуализация на 3Д в уеб е WebGL,[4]. WebGL, или WebGraphicsLibrary (на български графична библиотека за уеб) е библиотека написана на JavaScript позволяваща на браузърът да превръща написан код в графика. Тя е аналогична на OpenGL, която се използва при визуализацията на 3Д в десктоп приложения като SketchUp, 3D Maya и други. Основната разлика е езикът, на който са написани библиотеките, за разлика от WebGL, OpenGL е написан на C/C++. Съвременните версии на JavaScript позволяват лесното му имплементиране в браузърът и работата му в Интернет. Също така и оптимизация засягаща директната работа с графичния процесор на устройството и бързото визуализиране на обектите. Както се вижда на фиг. 1 [5] WebGL е вграден и се поддържа от актуалните версии на по-често срещаните браузъри, което прави работата с 3Д обекти в уеб изключително лесна. Със зелен цвят на фиг. 1 са отбелязани браузърите с пълна поддръжка, с жълт частична и с червен без поддръжка. Единствено изключение прави версията на Opera за мобилни устройства, това е поради специфичния начин на обработка на информазция върху Opera сървър, който не позволява обработката на JavaScript. Това прави достъпът до тази технология не само лесен, но и безплатен.

Фиг. 1 Поддръжка на WebGL в различните браузъри

РЕАЛИЗАЦИЯ НА 3D ОБЕКТИ В УЕБ

За разработването на 3Д приложения в уеб е нужен 3Д JavaScript Engine. Това е набор от правила написани на JavaScript, който ни позволява сами да създаваме

различни триизмерни модели директно в уеб документ или в отделен JavaScript файл. Добър пример за такъв е threejs, който е безплатен, добре документиран и предоставя много примерни приложения с отворен код създадени от други разработчици. Въпреки, че можем да пишем код за създаването на различните обекти, много по-лесно е да използваме редактор с графичен интерфейс, фиг. 2 [6]. Подобни редактори позволяват бързо и лесно добавяне и редактиране на 3Д обекти без необходимост от писане на код.



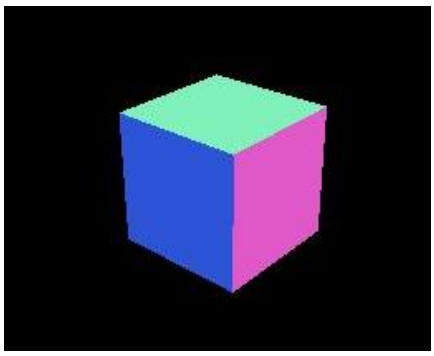
Фиг. 2 Уеб 3Д редакторът на threejs

Освен създаване на обекти можем да импортираме и свои модели направени с друг софтуер. Редакторът не позволява директно добавяне на всички 3Д формати, но с помощта на конвертори се допускат много от тях. Също така имаме възможността да превръщаме проектите, създадени с threejs, в приложения за виртуална реалност лесно и бързо без допълнителни корекции. Когато крайният продукт е готов можем да експортираме резултата, като редакторът ще генерира необходимите файлове за имплементиране на 3Д модела в уеб приложението. На фиг. 3 е представен авторски код за реализирането на 3Д обект.

```
<script src="js/three.js"></script>
<script src="js/OrbitControls.js"></script>
<script>
var scene = new THREE.Scene();
var camera = new THREE.PerspectiveCamera( 75, window.innerWidth / window.innerHeight, 0.1, 1000 );

var renderer = new THREE.WebGLRenderer();
renderer.setSize( window.innerWidth, window.innerHeight );
document.body.appendChild( renderer.domElement );
var geometry = new THREE.BoxGeometry( 1, 1, 1 );
var material = new THREE.MeshNormalMaterial();
var cube = new THREE.Mesh( geometry, material );
scene.add( cube );

camera.position.z = 5;

var controls = new THREE.OrbitControls( camera );
controls.addEventListener('change', render);

function render() {
requestAnimationFrame( render );
renderer.render( scene, camera );
}
render();
</script>
```

Фиг. 3. Авторски кодов сегмент за създаването на 3Д обект

Създадена е функция за визуализацията на модела в уеб браузер и някои от основните елементи необходими за създаването му. На фиг. 4 е визуализиран резултатът от написания код, представящ куб с възможности за завъртане и приближаване.



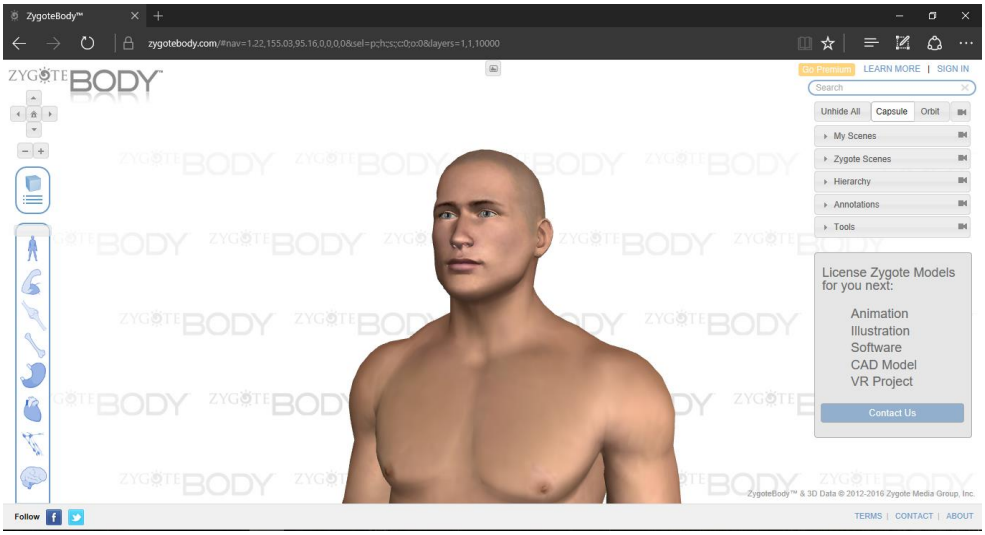
Фиг. 4 Резултатът от кодовият сегмент

ПРИЛОЖЕНИЕ НА 3D ТЕХНОЛОГИИТЕ В УЕБ

WebGL и threejs дават възможността за използване на изключително перспективна технология. Някои от възможните приложения са в сферата на:

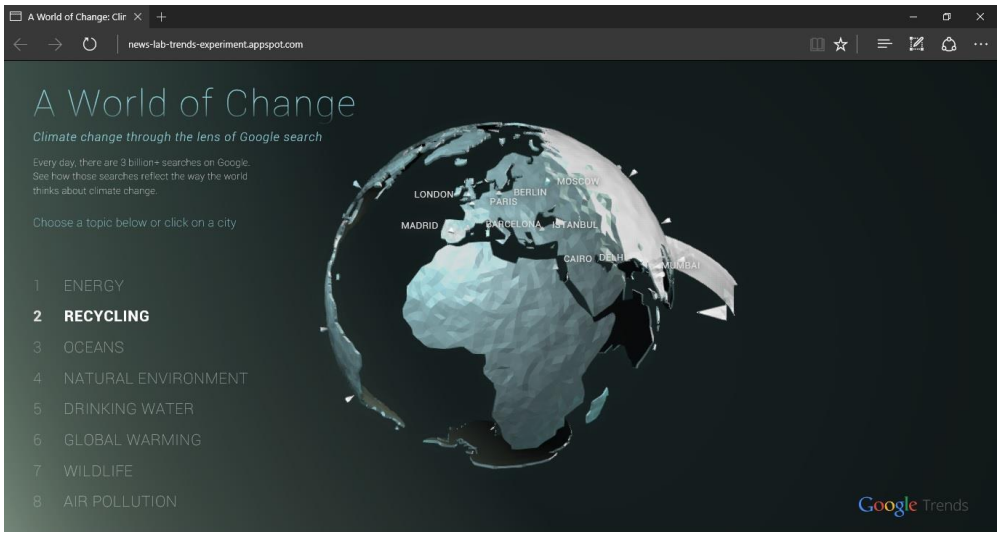
- Медицина;
- Образование;
- Туризъм;
- Архитектура;
- Географски информационни системи;
- Транспорт;
- Машиностроене;
- Култура;
- Разработка на игри;
- Виртуална и добавена реалност.

В интернет пространството има голям брой приложения използващи WebGL и threejs. Един интересен пример, включващ модел на човешкото тяло, е представен на фиг. 5 [7] с възможност за визуализация на мускулите, органи и кости.



Фиг. 5 3Д модел на човешкото тяло

На фиг. 6 е представен друг интересен пример – проект на Google, който показва модел на земното кълбо с най-честите търсения на теми като енергетика, глобално затопляне или замърсяване на въздуха в различни държави.

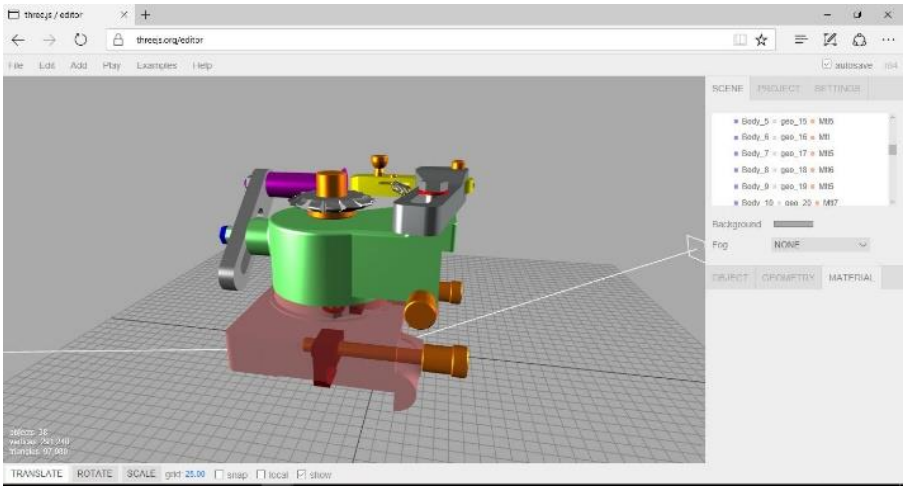


Фиг. 6 Информационен проект на Google, представящ модел на земното кълбо

Изграждането на географски информационни системи в уеб дава възможност на потребителите лесно да се ориентират и опознават триизмерни модели на градове [1]. Друг вид системи, които използват 3Д технологии в уеб, включват библиотеки, архиви, музеи и други информационни организации. Те позволяват използването на виртуални среди от много потребители едновременно [3].

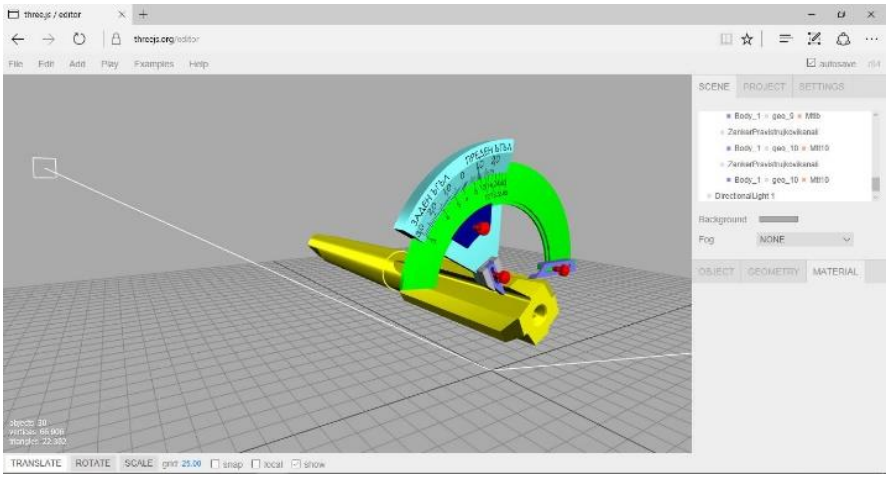
Приложение в академичните среди например биха намерили проекти свързани с математически изчисления, илюстрация на процеси свързани с различни видове сигнали, симулации на физични явления, визуализация на електрически елементи или дизайн на архитектурни обекти.

Направен е експеримент с визуализацията на някои модели, които биха намерили приложение в учебен процес на машинни инженери. Моделите са създадени в SolidWorks и са конвертирани за визуализация във уеб-базираният редактор на threejs. Модел на приспособление за заточване на дискови модулни фрези, предоставен ми от научния ръководител, е представен на фиг. 7.



Фиг. 7 3Д модел на приспособление за заточване на дискови модулни фрези

На фиг. 8 е представен триизмерен модел на Бабчиницер, измерващ задния ъгъл на зенкер.



Фиг. 8 3Д модел на Бабчиницер, измерващ задния ъгъл на зенкер

В последните години стават все по популярни и образователни системи използващи 3Д, като Sloodle (Second life (3D) object-oriented learning environment) [3].

ЗАКЛЮЧЕНИЕ

Технологиите за създаване и визуализация на 3Д обекти в уеб все още са в етап на развитие, но нарастващия брой на 3Д приложения в Интернет е признак за перспективата им. Те са добра основа за имплементирането на виртуалната реалност в уеб, която става все по-актуална през последните години и също така лесно достъпна. Друг положителен фактор за развитието на 3Д в уеб е интереса от страна на разработчиците. Примери за това са международните събития и конференции свързани с тази тема, споделянето на изходен код, и активните дискусии в социални мрежи, като GitHub и StackOverflow. Световни корпорации като Porsche, Ford и Google бързо се адаптираха към тези технологии, което показва възможностите им за развитие в бизнес сферата.

ЛИТЕРАТУРА

[1] Takase, Y., Sone, A., Hatanaka, T., Shiroki, M., & Masumi, T. (2004). A development of 3D urban information system on web. Proc. of Processing and Visualization Using High-Resolution Images.
[2] Livingstone, D., & Kemp, J. (2008). Integrating web-based and 3D learning environments: Second Life meets Moodle. CEPIS UPGRADE: European Journal for the Informatics Professional, 2008(3), 8-14.
[3] Urban, R. J. (2007). A second life for your museum: 3D multi-user virtual environments and museums.
[4] Parisi, T. (2012). WebGL: up and running. O'Reilly Media, Inc..
[5] WebGL - 3D Canvas graphics - http://caniuse.com/#search=WebGL
[6] Уеб редакторът представен от threejs - https://threejs.org/editor/
[7] Модел представящ човешкото тяло - https://zygotebody.com/

За контакти

Пламен Димитров – студент от трети курс в специалност „Информационни и комуникационни технологии“, Факултет ЕЕА, Русенски Университет „Ангел Кънчев“, e-mail: s143223@stud.uni-ruse.bg

доц. д-р Галина Иванова – преподавател в катедра „Компютърни системи и технологии”, Факултет ЕЕА, Русенски университет “Ангел Кънчев”, e-mail: givanova@ecs.uni-ruse.bg

РУСЕНСКИ УНИВЕРСИТЕТ
“АНГЕЛ КЪНЧЕВ”

СТУДЕНТСКА НАУЧНА СЕСИЯ СНС’18

П О К А Н А

Русе, ул. ”Студентска” 8
Русенски университет
“Ангел Кънчев”

Факултет „Електротехника, електроника и автоматика”

СБОРНИК ДОКЛАДИ
на
СТУДЕНТСКА НАУЧНА СЕСИЯ – СНС’17

Под общата редакция на:
доц. д-р Милко Маринов

Отговорен редактор:
проф. д-р Диана Антонова

Народност българска
Първо издание

Формат: А5
Коли: 11,25
Тираж: 40 бр.

ISSN 1311-3321

ИЗДАТЕЛСКИ ЦЕНТЪР
на Русенски университет “Ангел Кънчев”

http://conf.uni-ruse.bg/