ISSN 1311-3321

РУСЕНСКИ УНИВЕРСИТЕТ „Ангел Кънчев“
UNIVERSITY OF RUSE „Angel Kanchev“

Факултет „Електротехника, електроника и автоматика“
Faculty of Electrical and Electronic Engineering and Automation

СБОРНИК ДОКЛАДИ
на
СТУДЕНТСКА НАУЧНА СЕСИЯ – СНС’12

СБОРНИК ДОКЛАДОВ
СТУДЕНЧЕСКОЙ НАУЧНОЙ СЕСИИ – СНС’12

PROCEEDINGS
of
the SCIENTIFIC STUDENT SESSION – SSS’12

Русе
Ruse
2012

Сборникът включва докладите, изнесени на студентската научна сесия **СНС'12**, 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 (РУ) 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.т.н. Христо Белоев – РЕКТОР на РУ
    Александър Стойчев – ПРЕДСЕДАТЕЛ на СС

  - **Научни секретари:**
    проф. д-р Ангел Смрикаров –
    Заместник-ректор на Русенския университет
    ASmrikarov@ecs.uni-ruse.bg; 082-888 249
    Мирослав Петков –
    Заместник-председател на Студ. съвет
    mirko_b88@abv.bg; 082-888 390

  - **Членове:**
    Факултет „Аграрно индустриален"
    доц. д-р Калоян Стоянов
    kes@uni-ruse.bg; 082-888 542
    Камен Милушев
    kamen.milushev@abv.bg

    Факултет „Машинно технологичен"
    доц. д-р Стоян Стоянов
    sgstoyanov@uni-ruse.bg; 082-888 572
    Виктория Карачорова
    Vickie_best@abv.bg

    Факултет „Електротехника, електроника, автоматика"
    доц. д-р Теодор Илиев
    tiliev@ecs.uni-ruse.bg; 082-888 839
    Валентин Коларов
    soly_@abv.bg

    Факултет „Транспортен"
    доц. д-р Валентин Иванов
    vdivanov@uni-ruse.bg; 082-888 373
    Селиме Чолакова
    the_green_eyess@abv.bg

Факултет „Бизнес и мениджмънт"
проф. д-р Диана Антонова
dantonova@uni-ruse.bg; 082 888 726
Виктория Гединач
vgedinach@uni-ruse.bg

Факултет „Юридически"
ас. д-р Антонина Димитрова
andimitrova@uni-ruse.bg; 082-888 719
Диляна Пеева
semeremida@dir.bg

Факултет „Природни науки и образование"
доц. д-р Емилия Ангелова
evelikova@uni-ruse.bg; 082/ 888 848
Ина Георгиева
georgievi_92@abv.bg

Факултет „Обществено здраве и здравни грижи"
доц. д-р Стефан Янев
snyanev@uni-ruse.bg; тел. 082-821 883
Александър Атанасов
raceface@abv.bg

Филиал Разград
доц. д-р Цветан Димитров
tz_dimitrow@abv.bg; 0887-631 645
Живка Иванова
ivanova_jivka@abv.bg

Филиал Силистра
гл.ас. Галина Лечева
lina_acad.bg@abv.bg; 0897-912 702
Илияна Михайлова
mihaylova_3009@abv.bg

СЕКЦИЯ
„Електротехника, електроника и автоматика"

С Ъ Д Ъ Р Ж А Н И Е

СЕКЦИЯ
„Комуникационна и компютърна техника и технологии"

С Ъ Д Ъ Р Ж А Н И Е


ECEO
специалност
"Електроенергетика
и
електрообзавеждане"
специалност
"Електроника"
Русенски университет
"Ангел Кънчев"
А М
специалност
"Автоматика и
мехатроника"
факултет
"Електротехника, електроника
и автоматика"
специалност
"Компютърни
системи и
технологии"
специалност
"Телекомуникационни
системи"

Секция

Електротехника, електроника и автоматика


ЕСЕО
специалност
"Електроенергетика
и
електрообзавеждане"
специалност
"Електроника"
Русенски университет
"Ангел Кънчев"
А М
специалност
"Автоматика и
мехатроника"
факултет
"Електротехника, електроника
и автоматика"
специалност
"Компютърни
системи и
технологии"
специалност
"Телекомуникационни
системи"

Приложение на фотоволтаичните централи в България

автори: Назлъ Нури, Салим Салимов
научен ръководител: проф. д-р Никола Михайлов

Abstract: *Depletion of energy resources such as oil, natural gas and coal leads to an increase in their prices. An alternative to thermal power stations (TPP) to produce electricity from nuclear power plants (NPP) is not the best, because of the danger of nuclear contamination. Use of solar energy is the most recent growing trend in the work of research teams. Major efforts are underway for the development of converters of solar energy into electrical energy called photovoltaic.*

Key words: *photovoltaic, renewable energy sources.*

ВЪВЕДЕНИЕ

Модернизация на обществения, политически и икономически живот в страната в съответствие с европейските норми и стандарти е приоритетна цел за управлението на България. Включването ѝ в международните усилия за предотвратяване изменението на климата и широко - мащабния пакет от мерки в областта на енергетиката, дават нов тласък на енергийната сигурност в Европа. Сред приоритетите в енергийната политика на страната са масово използване на възобновяемите енергийни източници (ВЕИ) и въвеждането на мерките за енергийна ефективност.

Европейски цели 2020г.

Целта на статията е да анализира възможностите за приложение на фотоволтаиците у нас. През януари 2008г. Европейската комисия (ЕК) постигна съгласие по мащабен законодателен пакет от предложения, чрез които да се изпълнят ангажиментите на Европейския съвет (ЕС) за борба с изменението на климата и за насърчаване използването на възобновяема енергия – Пакет „Енергетика/Околна среда" [5].

От 2012г. насоката на енергийната стратегия на България е свързана с решаването на средносрочните проблеми на прехода към финансово стабилна и пазарно ориентирана енергетика.

Поради изпълнението на приоритетите от 2012г. България трябва да подготви нова Енергийна стратегия. Към момента, ЕС е в процес на преглед на настоящата си енергийна стратегия и на интензивни дискусии по отношение на предложението на ЕК от януари 2010г. «Енергийна политика за Европа» и произтеклите от него Трети либерализационен енергиен пакет (м. септември 2011г.) и Пакет «Енергетика/ Околна среда» (м. януари 2010г.). Те изискват значително по-висока степен на обвързаност на общностните и националните решения и с цел постигане на амбициозни цели в дългосрочна перспектива поставят основата на радикални промени в сектора.

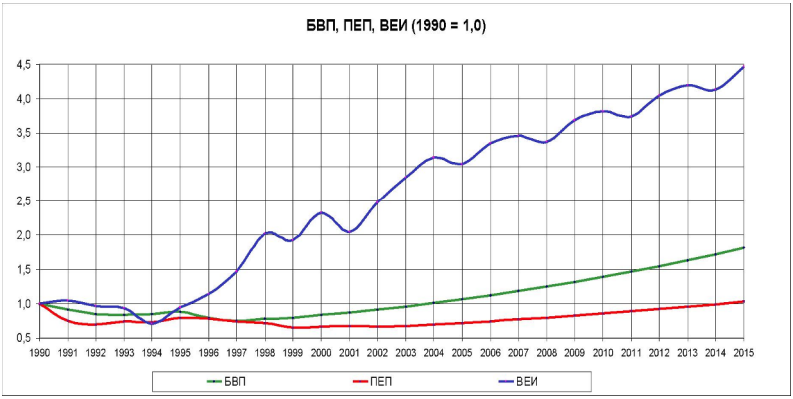
Създаваните условия за дългосрочна сигурност на доставките на електроенергия, намаляване на зависимостта от вносни енергийни доставки, намаляване на емисиите на парковите газове, опазване на климата, възможност за избягване на конфликти, свързани с полезните изкопаеми, са следствие от развитието на производството на електрическа енергия от ВЕИ. Чрез стимулиране на развитието на технологиите за производство на електрическа енергия от ВЕИ се създават предпоставки за изпълнение на задължението за производство на електрическа енергия от ВЕИ в размер на 11% от брутното вътрешно потребление на страната, съгласно Договора за присъединяване на България към ЕС.

Увеличаване на дела на ВЕИ в крайното общо потребление на енергията

Използването на възобновяемите енергийни източници намалява зависимостта от внос, подобрява сигурността на енергоснабдяването, осигурява изпълнението на задълженията по опазване на околната среда и намаляване на емисиите на CO2, облекчава търговския баланс и подпомага трудовата заетост. Поради това втората ключова цел на ЕС е увеличаването на дела на ВЕИ до 20% в крайното енергийно потребление до 2020г [5].

През базовата 2010г. делът на възобновяемата енергия в общото крайно потребление на енергия на ЕС е 8,5%, от което следва, че за постигане на целта от 20% през 2020 г. е необходимо средно увеличение на потреблението от 11,5%.

За изпълнението на общоевропейската цел за ВЕИ с най-малко разходи се предвиждат гъвкави механизми. За тази цел се предлагат идея, тези държави – членки, които могат да развиват ВЕИ относително евтино, да имат възможността да продават излишък на страните, в които това производство е по-скъпо.



Фиг. 1 – Историческо развитие и прогноза за скоростта на нарастване на БВП, ПЕП и енергията от ВЕИ в България[6]

Прогнозираната скорост на нарастване на енергията, произведена от ВЕИ е около 4.0% годишно (взети са под внимание само водната енергия и биомасата). При тази скорост се очаква делът на ВЕИ в общово електро потребление през 2015 година да бъде 5.0%. Този процент не е достатъчен за реализиране на целите на устойчивото енергийно развитие. Поради включването и на други видове ВЕИ и ускореното нарастване на цените на конвенционалните горива и произвежданите от тях енергии, скоростта на нарастване на енергията от ВЕИ ще бъде по-висока. Въпреки това анализът показва, че скоростта на въвеждане на ВЕИ в страната е недостатъчна, за да се прогнозира сценарий, при който страната се доближава до т.н. „устойчиво енергийно развитие" и са необходими специални мерки, за да бъде ускорен този процес.

Цената на електроенергията ще продължи да нараства поради следните по-важни причини:

- нарастване на потреблението на електроенергия, както у нас, така и в ЕС;
- намаляване на използваемия капацитет на наличните електропроизводствени мощности поради амортизацията им;
- нарастване на дела на електроенергията, произведена от вносни въглища след затварянето на 3-ти и 4-ти блок на АЕЦ "Козлодуй" ЕАД в периода 2007-2010 година;

- недостиг на генериращи мощности в периода до 2010 година, поради снемане от експлоатация на блокове в АЕЦ "Козлодуй" ЕАД, ТЕЦ "Марица 3" ЕАД и " Брикел" ЕАД;
- необходимост от инвестиции за рехабилитация на съществуващите енергийни електроцентрали на въглища във връзка с повишаването на изискванията за опазване на околната среда.

От 08.09.2011г. насърчаването на производството на електрическа енергия от ВЕИ е регламентирано в Закона за енергетиката (ЗЕ). С приемането на Закона за енергетиката е регламентирана долна граница на цената на електрическата енергия, която е с 70% по-ниска от средната продажна цена за предходната календарна година. Доставката също е определена от комисията по критерии, в зависимост от вида на първичния енергиен източник. Изисква се определяне на преференциална цена, която да покрие освен обоснованите разходи и нормата на възвръщаемост.

Трансгранична зона Румъния – България

Условията в България са особено перспективно за изграждането на фотоволтаични електрически централи (ФВЕЦ). Стойностите на слънчевата радиация и продължителността на слънчевото греене са изключително подходящи за посочените обекти[9]. Много от ФВЕЦ са разположени в трансграничната зона Румъния-България (фиг.2). Проучванията, извършени от екип в РУ „Ангел Кънчев", показват, че в българската част на зоната са инсталирани 17 фотоволтаични електрически централи.

Фиг. 2 – Трансгранична зона Румъния – България

Едни от най-големите изградени фотоволтаични паркове са:

- Соларен парк край с.Калипетрово, община Силистра. Инсталирана мощност е 3,9 MWp. Инвеститорът на проекта е AES Solar, а поддизпълнител – Соларпро Холдинг. За реализирането на проекта на площ от 100 дка са монтирани 51480 панела тънкослойни CdTe [8].
- Фотоволтаична централа край с.Мокреш –това е първият голям проект на Greentech Engineering Solutions. Изграждането ѝ започва през 2010 г. Теренът се намира в с.Мокреш, близо до Лом. За реализация на проекта при изграждането ѝ са използвани поликристални фотоволтаични модули, инвертори – TMEIC (TOSHIBA MITSUBISHI-ELECTRIC INDUSTRIAL SYSTEMS CORPORATION), конструкции – TATASTEEL и SADEF, кабелна система – HIS Solarsysteme. Централата е една от най-големите на територията на България. До момента са изградени и

включени в националната електроразпределителна мрежа 3 MW. След довършването се очаква паркът да достигне предвидените 4 MW мощност.

- Фотоволтаичен парк в Самоводене – инвеститор е фирмата SDN, която има завършени повече от 200 фотоволтаични проекти в света. В парка, разположен на площ от 618 294 m2, ще се произвежда чиста енергия без въглеродни емисии. Инсталираната мощност е 45 MWp.
- фотоволтаичен парк „ЗИТА –Русе" - стартира през 2007 година. СТС Солар АД подготвя проекта, като са използвани 484 броя фотоволтаични модула Kyocera KC130GH-2P, 2 броя - Kyocera KC130GHT, 324 броя - Solar Swiss SSM – 150/24M с обща инсталирана мощност 117,24 kWh. За да се свърже централата с електропреносната мрежа са използвани 12 броя инвертори Sunny Mini Central 5000A и 6 броя – Sunny Mini Central 8000TL [12].

Фиг. 3 – Фотоволтаична централа „ЗИТА – Русе"

- "Корина Експорт" ЕООД – инсталираната мощност на система е 25,92 kW. Фотоволтаичните модули са 144 броя по 180 W, 6 броя инвертори по 4,2 kW изграден трафопост 100 kW и собствена електропреносна мрежа от 286 m.

Фиг. 4 – Фотоволтаична площадка, с.Червен

ЗАКЛЮЧЕНИЕ

В Трансгранична зона Румъния - България са инсталирани разнообразни ВЕИ. Съществена част от тях са ФВЕЦ, което се дължи на благоприятните климатични условия. Отчитайки световните тенденции и темпа на нарасване на цетралите с ВЕИ у нас, трябва да се фокусира вниманието на образователните институции върху подготовката на кадри за проектиране и експлоатация на тези съоръжения.

ЛИТЕРАТУРА

[1] Анализ на постигнатите резултати от водената политика в областта на енергетиката и реализирането на енергийната стратегия на Република България, януари 2012 г.
[2] Андонов, К. , Л. Михайлов, О. Динолов, К. Коев, Медоти и средства за изследване в електроенергетиката, Русе, Издателски център РУ „Ангел Кънчев", 2010 г.
[3] Георгиева В. Слънчевата енергия – да погледнем на Света с други очи! Министерство на икономиката и енергетиката. Главен експерт в дирекция "Енергийна ефективност и опазване на околната среда", (http://www.mee.government.bg/geoterm/docs/solar_utility2.pdf)
[4] Евстатиева Н. Алгоритъм за управление на енергийните потоци в хибридна инсталация за топла вода. „Електротехника и електроника", 11-12, 2009, с.21-26.
[5] Енергийна стратегия на Република България, София, 2012 г.
[6] Закон за енергетиката, София, 2012 г.
[7] Закон за устройство на територията, София, 2012 г.
[8] Ключови фотоволтаични проекти в България. Преглед на инсталираните или в процес на реализация соларни инсталации у нас.(http://energy-review.bg/energy-statii.aspx?br=64&rub=628&id=108)
[9] Михайлов Н., И. Евстатиев, И. Стоянов, К.Габровска. Изследване на слънчево радиационното излъчване за условията на регион Русе през есенния сезон. Трудове на научна сесия РУ'2004, 1-3 ноември 2004, Русе, с.114-118
[10] Михайлов, Н., Л. Христова. Възможности за приложение на възобновяеми енергийни източници в земеделието на Република България, Енергиен форум 2002, МДУ "Ф. Ж. Кюри", Варна, 14...17 юни 2002, с. 547-550
[11] Младенчева, Р. Фотоволтаични генератори, Ековат Технологии, София, 2007г.
[12] Слънчева централа ЗИТА – Русе (http://www.zita-ruse.com/index.php?option=com_content&view=article&id=30&Itemid=50)

За контакти:
Салим Салимов, Русенски Университет „Ангел Кънчев", e-mail: davampire90@gmail.com
Назлъ Нури, Русенски Университет „Ангел Кънчев", e-mail: nazli_s@abv.bg
проф. д-р инж. Никола Михайлов, Русенски университет "Ангел Кънчев", Катедра „Електроснабдяване и електрообзавеждане", тел.: 082-888 843, e-mail: mihailov@uni-ruse.bg

Изследване на волт-амперни и волт-мощностни характеристики на фотоволтаични панели при реални условия

автор: Ауад Бауазир
научен ръководител: доц. д-р Валентин Димов

Investigation of volt-ampere and volt-power characteristic of photovoltaic panels under real conditions: *The article presents research results of the volt-ampere and volt-power characteristics of two types of polycrystalline and mono crystalline silicon kind of photovoltaic panels. Studies were made under real conditions by the end of winter in Rousse region. These conditions differ substantially from the standard conditions of measurement. Determined the optimum value of load resistance for maximum power extracted panels tested in the particular real conditions.*

Key words: *solar panels, volt-ampere characteristic, volt-power characteristic, the maximum extracted power, resistance of the load.*

ВЪВЕДЕНИЕ

Слънчевата енергетика навлиза все по-масово в съвременното ежедневие. Фотоволтаичните панели се използват не само в соларни паркове, но навлизат и в бита. В България се наблюдава масово използване и съответно разнообразно предлагане на фотоволтаични панели с различни технически параметри. Правилният и подходящ избор на панел зависи не само от параметрите на панелите, но и от конкретния консуматор на електрическа енергия и от условията на околната среда, при които ще се използва.

Основните електрически параметри на фотоволтаичните панели зависят от различни фактори на околната среда. Те се определят при така наречените стандартни условия за измерване (Standard Test Conditions - STC). Към стандартните условия се включват температура на клетката 25°C, енергия на светлината EI = 1000W/m2 и слънчев референтен спектър (Air Mass, Spectrum, Spectral Distribution) AM1. 5. При условия различни от стандартните, се получават други стойности за основните електрически параметри на фотоволтаичните панели.

Действителните условия се различават от стандартните условия, поради което се налага необходимост от изследване на реалната производителност на фотоволтаичните модули чрез експериментално снемане на техните волт-амперни характеристики и определяне на изходната мощност при реални работни условия.

Целта на изследването е при реални условия да се определят волт-амперните характеристики на различни фотоволтаични панели и оптималните съпротивления на товарите за осигуряване на максимален добив на енергия.

ИЗЛОЖЕНИЕ

Изборът на обект на изследването е направен след анализ на използваните технологии за фотоволтаични панели и предлагането им на българския пазар. Като най-добър материал за фотоволтаични панели се посочва галевият арсенид (GaAs), който достига ефективност 35%. За съжаление технологията с този материал е прекалено скъпа и поради високата цена галевият арсенид намира ограничено приложение в практиката.

Основният материал използван при изработването на фотоволтаични панели е силицият (Si), който може да бъде монокристален, поликристален или аморфен. Най-масово използвани са кристалните силициеви панели. Монокристалите се произвеждат на основата на скъпи технологии, което определя и високата цена на този тип клетки. Те обаче осигуряват относително висок коефициент на полезно действие, който за предлаганите на пазара фотоволтаици е от порядъка на 14%. Ефективността на поликристалните силициеви панели е по-ниска и е до 12%, но цената е по-ниска. Фотоволтаичните панели с аморфен силиций въпреки, че са с

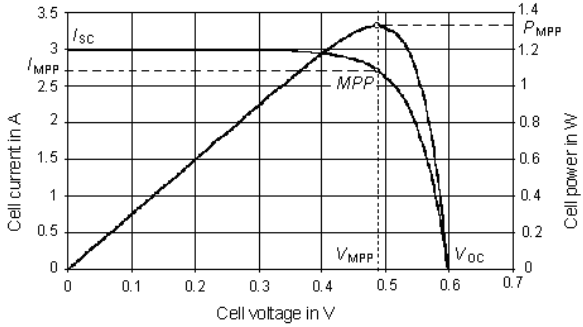
най-ниска цена, засега намират ограничено приложение поради това, че са с най-ниска ефективност. При аморфните силициеви панели КПД е в диапазона едва 6-9%. Счита се, че в бъдеще основните фотоволтаични панели ще са с аморфен силиций, понеже времето за възстановяване на финансовите разходи изразени чрез доставена енергия от панели с аморфен силиций е значително по-кратко от съответното време за кристалните силициеви панели.

Като се има предвид масовото предлагане и използване на кристални силициеви фотоволтаични панели, за обект на изследването са избрани два панела с поликристални клетки и един панел с монокристални клетки. В таблица 1 са представени избраните за изследването фотоволтаични панели с техните най-основни параметри посочени от производителите при стандартни условия.

Таблица 1. Основни параметри на избрани фотоволтаични панели

Параметър	Модел		
	BGSP-P230	PX 120/6	AS 110
Вид на клетките	поликристални	поликристални	монокристални
Максимална мощност, Wp	230	120	110
Напрежение на отворена верига, V	37,7	21	20,7
Работно напрежение, V	29,5	16,9	16,7
Ток на късо съединение, A	8,36	7,7	7,5
Работен ток, A	7,8	7,1	6,6

На фиг. 1 са представени волт-амперната и волт-мощностната характеристики на идеална фотоволтаична клетка при стандартни условия [3].



Фиг. 1 – Волт-амперна и волт-мощностна характеристики на идеална фотоволтаична клетка при стандартни условия за измерване.

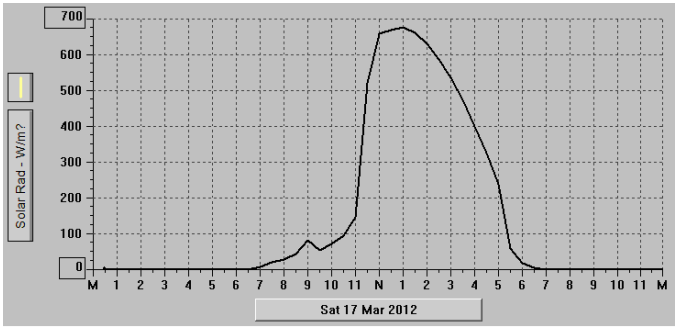
От представените примерни характеристики при стандартни условия за измерване се вижда, че фотоволтаичните клетки имат поведение на източник на ток

от I_{SC} до I_{MPP} и поведение на източник на напрежение от V_{MPP} до V_{CC}. В широкия диапазон на получавани напрежения и токове съществува екстремум на добиваната мощност в точката с максимална мощност P_{MPP}.

Като важни фактори, които определят производителността на фотоволтаичните панели могат да се посочат: слънчева радиация, която се изменя в рамките на денонощието и годишните сезони, температура, ъгъл на наклон на панела, конструкция на закрепване на панелите (фиксирана или слънце-следяща), засенчване, запрашеност, вятър, мъгливост.

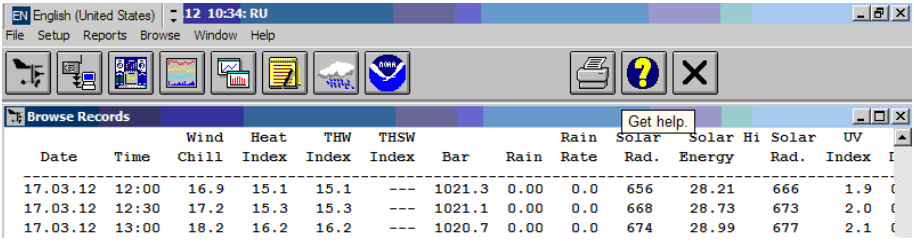
Действителните работни условия в Русенския регион се различават от стандартните условия, поради което се налага необходимост от изследване на реалната производителност на фотоволтаичните модули чрез експериментално снемане на техните волт-амперни характеристики и определяне на изходната мощност при реални работни условия.

Изследването е проведено в края на зимния сезон на територията на Русенски университет „Ангел Кънчев", при слънчево безоблачно време и положение на слънцето около зенита и с фиксирана конструкция на закрепване на панелите. На фиг. 2 е представена слънчевата радиация в деня на провеждане на изследването на 17 март 2012г.



Фиг. 2 – Изменение на слънчевата радиация на територията на Русенски университет „Ангел Кънчев" на 17 март 2012г.

За времето на провеждане на измерванията от 12:00 до 13:00 часа слънчевата радиация върху хоризонтална плоскост се е променяла в границите от 656 до 674 W/m^2 (фиг. 3).

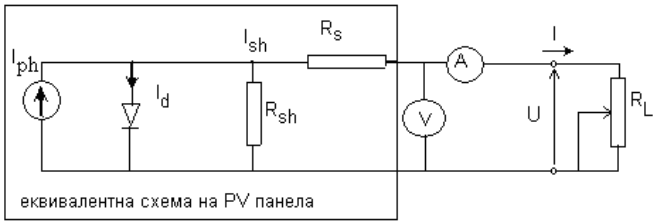


Date	Time	Wind Chill	Heat Index	THW Index	THSW Index	Bar	Rain	Rain Rate	Solar Rad.	Solar Energy	Solar Hi Rad.	UV Index
17.03.12	12:00	16.9	15.1	15.1	---	1021.3	0.00	0.0	656	28.21	666	1.9
17.03.12	12:30	17.2	15.3	15.3	---	1021.1	0.00	0.0	668	28.73	673	2.0
17.03.12	13:00	18.2	16.2	16.2	---	1020.7	0.00	0.0	674	28.99	677	2.1

Фиг. 3 – Изменение на слънчевата радиация на територията на Русенски университет „Ангел Кънчев" за периода от 12:00 до 13:00 часа на 17 март 2012г.

На фиг. 4 е представена схемата за извършване на изследването. Фотоволтаичният панел е представен с неговата еквивалентна схема. Към панела е

включен товар R_L, който променя стойностите си от 1Ω до 50Ω. С волтметър и амперметър се измерват изходното напрежение на панела и тока през товара.



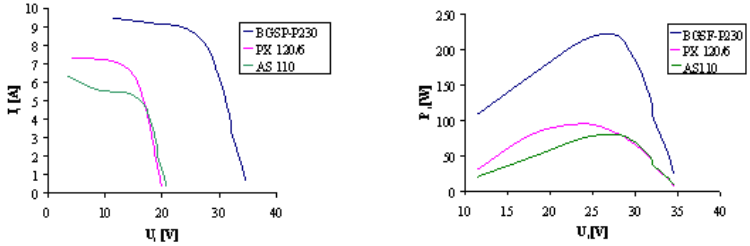
Фиг. 4 – Схема на свързване за провеждане на изследването.

За схемата от фиг. 4 може да се запише следната математическа зависимост за волт-амперната характеристика на фотоволтаичните клетки: [2]

$$I = I_{ph} - I_0 \left\{ \exp\left[\frac{q\left(U + IR_s\right)}{mkT} \right] - 1 \right\} - \frac{U + IR_s}{R_{sh}} \qquad (1)$$

където: I – ток генериран във фотоволтаичните клетки, A;
U – напрежение на изхода на фотоволтаичните клетките, V;
Iph – фототок (зависи от слънчевата радиация и температурата), A
Io – ток на насищане на P-N прехода (зависи от температурата), A;
q – елементарен електрически заряд ($1{,}602.10^{-19}$ C);
m – коефициента на качествения фактор на диода (1...2);
k – коефициент на Болцман ($1{,}381.10^{-23}$ J.K-1);
T – температура на клетката, K;
Rs – последователно съпротивление на клетката, Ω;
Rsh – паралелно съпротивление на клетката, Ω;
RL – съпротивление на товара, Ω.

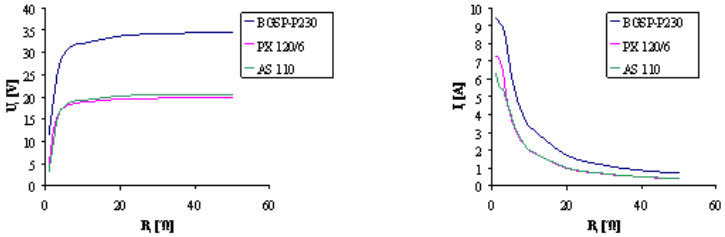
Волт-амперните и волт-мощностните характеристики на изследваните панели са представени на фигура 5. Поликристалният панел PX 120/6 и монокристалният панел AS 110 имат сходни характеристики, като поликристалният осигурява малко по-голям изходен ток и добивана мощност. Значително по-високи стойности на тока, напрежението и мощността се наблюдава при поликристалният панел BGSP-P230.



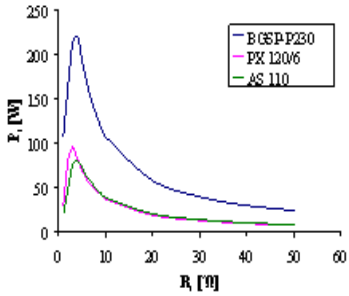
Фиг. 5 – Волт-амперни и волт-мощностни характеристики на изследваните панели.

За изпълнение на критерия управление на натоварването на фотоволтаичните панели с цел осигуряване на максимален добив на енергия е необходимо да се поддържа такъв товар на панела, при който съотношението напрежение-ток осигурява постигането на максимално добивана мощност [1]. Затова е важно да се изследва и да се знае зависимостта на изходните напрежения, токове и мощности от стойността на съпротивлението на товара.

На фиг. 6 са представени изходните напрежения и токове в зависимост от стойността на съпротивлението на товара за трите вида панели. Стойността на напрежението се увеличава бързо при съпротивления на товара до около 4 – 5 Ω и при товар над тези стойности напрежението се запазва сравнително постоянно. При изходния ток се наблюдава стръмно намаляване при съпротивление на товара до около 10 Ω, бавно намаляване при товар със съпротивление в границите 10 – 20 Ω и слабо намаляване при съпротивления на товара над 20 Ω.



Фиг. 6 – Зависимост на изходните напрежения и токове от стойността на съпротивлението на товара.



Фиг. 7 – Зависимост за добиваната мощност от съпротивлението на товара.

На фиг. 7. е представена графичната зависимост за добиваната мощност от трите вида изследвани панели. Както се вижда от фигурата, максималната добивана мощност от трите вида панели е различна (80, 95 и 220 W), но и за трите панела тя е при приблизително еднакви съпротивления на товара около 3 - 4 Ω.

ЗАКЛЮЧЕНИЕ

Практическото изследване на фото волтаичните панели при реалните условия за Русенския регион в края на зимния сезон, позволява да се направят следните изводи:

Монокристалният панел AS 110 работи като източник на ток за 5,5 А при изходно напрежение до 15 V. Поликристалният панел PX 120/6 е източник на ток за 7А при изходно напрежение до 13 V, а поликристалният панел BGSP-P230 е източник на ток за 9 А при изходно напрежение до 24 V. При по-високи от посочените стойности на напреженията фотоволтаичните панели стават източник на напрежение.

Оптималните стойности за съпротивлението на товара за трите вида панели е в границите 3-4 Ω. При такива стойности на товара се постига максимално добивана мощност от трите вида панели.

ЛИТЕРАТУРА

[1] Евстатиев И. Алгоритъм за работа и структура на електронна система за управление на автономна фотоволтаична инсталация. Научни трудове На Русенския университет-2011, том 50, серия 3.1.
[2] Smoliński S., Fotowoltaiczne źródła energii i ich zastosowania. Wyd. SGGW, Warszawa, 1998.
[3] http://www.volker-quaschning.de/articles/fundamentals3/index.php

За контакти:

маг. инж. Ауад Бауазир, Русенски университет "Ангел Кънчев", Катедра "Електроника", тел.: 082 888 682, e-mail: abawazir@uni-ruse.bg

доц. д-р Валентин Димов, Русенски университет "Ангел Кънчев", Катедра „Електроника", тел.: 082-888 772, e-mail: vdimov@ecs.ru.acad.bg.

Разработване и изследване на ветрогенератор

автор: Кирил Мицов
научен ръководител: проф. д-р Никола Михайлов

An attempt to construct a wind generator: *The paper reviews the advantages and disadvantages of wind generators. The structure of wind turbines is described. Stages associated with planning and setting up the system are listed. Some research on the effectiveness of the energy produced is carried out. An electronic system associated with charging the battery is proposed.*
Key words: *wind generator, electronic system, renewable energy sources.*

ВЪВЕДЕНИЕ

1. Анализ на съществуващото положение, предимства и недостатъци на вятърните генератори

1.1. Предимства на вятърните генератори (фиг.1):

Вятърът се оказва привлекателен поради няколко причини:

- Има го в изобилие.
- Практически е неизчерпаем източник на енергия.
- Не води до замърсяване и до климатични аномалии.

Това са качества, с които нито един от традиционните енергиини източници на производство на електричество не може да се похвали [1]. Днешните ефективни и модерни технологии дават надежда, че бъдещето ще се развива в насока към неизчерпаеми и незамърсяващи околната среда производства.

Приложенията на вятърната енергия са за производство на електроенергия, за зареждане на акумулатори, осветление на сгради, паркове, захранване на офис оборудване и задоволяване на всякакъв вид енергийни нужди.

Фиг.1 – Действащ ветрогенератор

1.2. Недостатъци на вятърните генератори:

- Вятърните турбини работят само с 30% от капацитета си.

При направено проучване върху работоспособността на вятърните генератори във Великобритания, се оказа, че те са работили с 27,18% от капацитета си през 2009г., 21,14% през 2010г. и 24,08% средно за период от две години назад [2]. Според проучването турбините произвеждат енергия средно между (65-80)% от времето, но често работят с много по-нисък капацитет. Тенденциите са за неговото увеличение със средно 15% за всяка година.

- Вятърът е възобновяем ресурс, но с различна интензивност.

Американската асоциация по вятърна енергия отчита, че за периода ноември 2008г.- декември 2010г. са съществували 124 случая, когато вятърните турбини във Великобритания са произвели 20 kWh електроенергия. Капацитетът на използваните турбини е 1600 kW [2]. Разбира се и в други области на електроиндустрията се забелязват моменти на спад в производителността. Известен е случаят в американския щат Тексас по-рано през тази година, когато 50 ТЕЦ-а отказаха да работят и оставиха огромна част от населението без захранване.

- Вероятността за поява на слаб вятър в период на засилено енергопотребление е много висока.

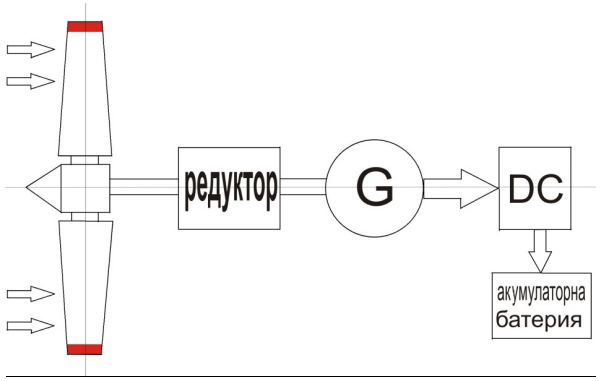
Друго проучване, проведено в САЩ, показва, че в периоди на засилено енергопотребление, като празничните сезони и др., капацитетът на работа на вятърните турбини никога не надвишава 6% от средната консумация на електроенергия за тях [2]. В САЩ турбините също не работят с максималната си мощност, там обаче, средния капацитет е между 10 и 40% в зависимост от територията.

Цел на изследването е разработване и изследване на ветрогенератор, който да генерира малка мощност.

Разработване и изследване на ветрогенератор

Вятърна турбина

На фиг.2. е показана структурната схема на вятърната турбина.



Фиг. 2 – Структурна схема на вятърна турбина

Вятърът задвижва перката на енергийното съоръжение, монтирана на ротор. В резултат на силата, която създава въртене между високото налягане върху плоската повърхност на витлата и ниското налягане на обратната им страна се получава въртене, което води до директно превръщане на механична енергия в електрическа с помощта на електрогенератора (G). Електрогенераторите са със две или три витла, като при тях основната цел е да се постигне висока скорост на въртене.

Перката се състои от три витла, като всички компоненти са разположени срещу на вятъра. Те са със специална аеродинамична форма, за да могат да създават и използват силата на въздушното течение. Механичната мощност на роторните витла се подава към генератора посредством трансмисионната система. Тя се състои от кутия с предавателен блок от зъбни колела, блокираща система, както и от спомагателни смазваща и охлаждаща системи. Предавателният блок от зъбни колела осъществява преобразуване на честотата на въртене. Блокиращата система е създадена да изключва генератора, когато турбината е спряна. Въртящата система обръща корпуса на ротора по направление посоката на вятъра, използвайки задвижващ зъбен механизъм.

Ветрогенератор „STORM"

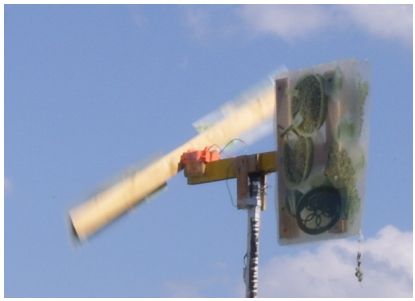
Фиг. 3 – Общ вид на ветропоказателя

Първоначалната идея за конструирането на ветрогенератора започва с малко парче дърво, което в последствие се оформи като перка с няколко витла. Нейните размери трябва да са около 800mm в диаметър и 100mm в ширина. Тя се прикрепва към тялото, така че да може да се развърта свободно. Това би довело до проблем, свързан със стабилноста на ветрогенератора и влиянието на посоката на вятъра спрямо него. За решаването на този проблем е добавена опашка, която да насочва ветрогенератора срещу посоката на вятъра. Това води до повишаване на резултатите, постигнати до момента. Системата се ориентира сама и е сравнително стабилна, но за да се завърти перката е необходимо скоростта на вятъра да бъде по-голяма.

С течение на времето системата е превърната във ветропоказател (Фиг.3), за който е нужен съвсем лек полъх на вятъра.

Направено е изследване, породено от момента на развъртане на перката, при което е установено, че при сегашните си мощностти ветропоказателят е в състояние не само да завърта себе си, а и при товар.

Тази система може да превръща механична енергия от въртенето на витлата в електрична енергия. За целта е конструирана по-голяма перка (φ 1200mm), добавени са и пластмасови уширения, които същевременно са и доста пластични в краищата. Това от своя страна помага ветрогенераторът да се справи със завихрянето на вятъра, който кара всичко да се тресе. Поставя се предавателна кутия, която завърта генератора до 50 пъти спрямо тази на перката. По този начин се увеличава съпротивлението, но така подобрената перка работи по-добре. Ветропоказателят се превърна във ветрогенератора, показан на фиг.4.



Фиг. 4 – Общ вид на ветрогенератора

От направено изследване може да се констатира, че при развъртане на перката ω=13 min^{-1}, роторът на генератора се завърта 650 пъти около оста си. За целите на проведеното изследване са направени шест опита. Резултатите са представени в табл. 1 и с оглед тяхната визуализиране на фиг. 5.

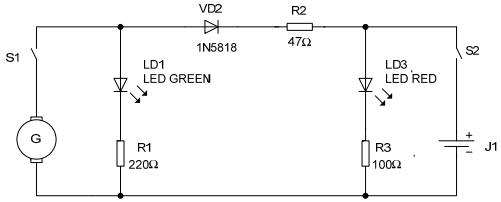
Таблица 1. Резултати от проведените експериментални изследвания

№	Ъглова скорост на перката ω, min-1	Ъглова скорост на ротора ω, min-1	Напрежение V
1	13	650	1,2
2	20	1000	3,5
3	24	1200	6,8
4	32	1600	8,4
5	41	2050	9,7
6	45	2250	11,8

Фиг. 5 – Резултати от проведените експериментални изследвания

Големият проблем е предаването на енергията до земята, поради въртенето на ветрогенератора покрай оста му. Това налага разработването на нов метод, чрез който този недостатък да бъде отстранен. Този проблем е решен чрез два проводими пръстена, по които се плъзгат четки. С това ветрогенераторът е готов да създава електроенергия.

Наименованието, което носи ветрогенератора е „STORM". Той отдава максимално напрежение 12V при силен вятър, при нормани условия - лек вятър до 6V. Токът е напълно достатъчен да се съхранява в батерии или да се употребява в момента. За зареждането на батериите трябва да се създаде електрическа схема, която е показана на фиг. 6.



Фиг. 6 – Електрическа схема за зареждане на акумулаторна батерия

Схемата се състои от два прекъсвача S1 и S2, три диода, два от които са светодиодиодите LD1 и LD2 и три резистора. Принципът на работа е следният: при затворен S2 и отворен S1 светодиодът LD3 се отпушва и светва в червен цвят. Това е знак, че към акумулаторната батерия J1 не се подава захранващо напрежение. При затваряне на двата прекъсвача и подаване на напрежение от генератора, LD1 се отпушва и светва в зелен цвят. В това положение и двата диода светят, което е показател, че батерията се зарежда. Диодът VD2 служи за предотвратяване случаите, когато генераторът спира да произвежда електричество и мигновено прекъсва електрическата схема. Това предотвратява разреждането на батерията J1.

ЗАКЛЮЧЕНИЕ

1. Разработен е и е изследван ветрогенератор „STORM".
2. Резултатите от направеното изследване показват, че при голяма скорост на вятъра, ветрогенератора генерира 12V напрежение, а при по-малка 6V.
3. Разработена е електрическа схема за зареждане на батерии.

ЛИТЕРАТУРА

[1] Тончев Г. Вятърни електроцентрали I част, Ековат Технологии, 2005
[2] Публикуван доклад на John Muir Trust, 6 недостатъка на вятърните генератори http://www.digital.bg/novini/6-недостатъка-на-вятърните-генератори-news24435.html

За контакти:

Кирил Мицов, Русенски университет „Ангел Кънчев", специалност „Автоматика, информационна и управляваща техника", e-mail: kikoto91@abv.bg

проф. д-р инж. Никола Михайлов, Русенски университет "Ангел Кънчев", Катедра „Електроснабдяване и електрообзавеждане", тел.: 082-888 843, e-mail: mihailov@uni-ruse.bg

Образователни услуги в сферата на възобновяеми енергийни източници

автор: Явор Стефанов
научен ръководител: проф. д-р Никола Михайлов

Abstract: *Brief overview of degrees offered in the field of renewable energetic sources in the country. A prerequisite for the development of young generation in international companies offering realization.*
Key words: *Education, renewable energetic sources.*

ВЪВЕДЕНИЕ

За активното развитие на страната в областта на възобновяеми енергийни източници (ВЕИ) е нужно подготовката на кадри. Затова представлява интерес предлагането на образователни услуги в посочената област.

Целесъобразно е структурата на образование в областта на ВЕИ да се разглежда на 3 нива:

- Първа група – Специализирани курсове;
- Втора група – Професионални гимназии;
- Трета група – Висши училища.

Тези три основни групи имат пряка връзка помежду си и образуват една своеобразна пирамида на образователно равнище.

Първа група – Специализирани курсове

В страната се предлагат различни курсове в сферата на ВЕИ. Най-често те се организират по различни програми, финансирани от Европейския съюз (ЕС). С увеличаването на интереса на фирмите за инвестиране във възобновяемата енергетика нараства и интереса за подготовка на специалисти в тази област. Част от фирмите преквалифицират своите работните чре включване им в специализирани курсове, предлагани от водещи компании, неправителствени организации, университети и други.

Например, Бургас е организиран курс за обучение на специалисти по соларна техника с инициативата на Регионалната занаятчийска камара в Кобленц, Германия, по проект за икономическо сътрудничество на район Райнландпфалц с Югоизточна Европа и на Балканското бюро за подпомагане на средното съсловие. В течение на курса специалистите избират между две направления – фотоволтаична техника и слънчеви колектори за производство на топла вода и системи за охлаждане.

Подобна практика се използва и в чужбина. Например: агенцията EUREC обединява много изследователски центрове в областта на ВЕИ:

- European Commission, DG Joint Research Centre, Institute for Energy, Renewable Energy Unit;
- CEA-INES;
- The Fraunhofer Institute for Solar Energy Systems ISE;
- ZSW Centre for Solar Energy and Hydrogen Research;
- IEE- Institute for Electrical Engineering, University of Kassel ;
- Carl von Ossietzky Universität Oldenburg;
- The Centre for Renewable Energy Sources and Saving (CRES).

Много международни проекти реализират дейности, свързани с образование и квалификация. Например проекта RES-OP-DEV (Румънско - българско съвместно сътрудничество за дългосрочно и устойчиво развитие на младите човешки ресурси в областта на технологии за възобновяема енергия, с цел преодоляване на социално-

културната бариера и откриване на общи възможности за намирането на работа в трансграничната зона" от програма за „Трансгранично сътрудничество Румъния – България 2007-2013), предлага обучение по фотоволтаици, енергийна ефективност, биомаса и биогорива, ветрова енергетика и др. Тези обучения са предназначени за ученици от професионални гимназии, студенти и работници.

Втора група – Средни училища

Професионалните гимназии в нашата страна предлагат в професионалното направление Електротехника и електроника две нива на образователна квалификационна степен - „Монтьор на енергийни съоръжения и инсталации" и „Техник на енергийни съоръжения и инсталации".

Таблица 1. Професия "Монтьор на енергийни съораженията и инсталации"

Професионално направление:		
522	Електротехника и енергетика	
Наименование на професията:		
522040	Монтьор на енергийни съоръжения и инсталации	
Специалност:		Степен на професионална квалификация:
5220408	Възобновяеми енергийни източници	Втора

Общите професионални умения и компетенции за професията „Монтьор на енергийни съоръжения и инсталации" включват знания по шлосерски и заваръчни операции, такелажни операции с подемно-транспортна техника, монтажно-демонтажни и ремонтни операции с машинни елементи, детайли и възли, изработване на елементи от инсталации и съоръжения.

Специфичните компетенции за специалността 5220408 „Възобновяеми енергийни източници" обхващат - монтираж/демонтираж на съоръжения и инсталации за производство на енергия от ВЕИ, участие при подготовка, пускане в действие и въвеждане в експлоатация на съоръжения и инсталации за производство на енергия от ВЕИ, извършване на профилактика на съоръжения и инсталации за производство на енергия от ВЕИ, ремонт на детайли и възли от съоръжения и инсталации за производство на енергия от ВЕИ.

Таблица 2. Професия "Техник на енергийни съораженията и инсталации"

Професионално направление:		
522	Електротехника и енергетика	
Наименование на професията:		
522030	Техник на енергийни съоръжения и инсталации	
Специалност:		Степен на професионална квалификация:
5220308	Възобновяеми енергийни източници	Трета

Сходни умения трябва да притежава и обучаемия за техник на енергий съоръжения и инсталации (табл.2).

Техникът следи за спазване на санитарно-хигиенните норми и здравословните и безопасни условия на труд на работното място, осъществява превантивна дейност за опазване на околната среда, изпълнява шлосерски и заваръчни операции. Той ръководи такелажни операции с подемно-транспортна техника, извършва монтажно-

демонтажни и ремонтни операции на машинни елементи, детайли и възли.

Специфичните компетенции за специалността 5220308 „Възобновяеми енергийни източници" се свеждат до - ръководство на монтаж/демонтаж на съоръжения и инсталации за производство на ВЕИ, експлоатация на съоръжения и инсталации за производство на енергия от ВЕИ, ремонт на детайли и възли от съоръжения и инсталации за производство на енергия от ВЕИ и др.

В държавния план-прием за учебната 2011/2012 г., утвърден със Заповед № РД 09-461/30.03.2011 г. на МОН, в държавните и общинските професионални гимназии, професионални училища и в паралелки за придобиване на професионална квалификация в основни, професионални, средни образователни, спортни и специални училища се планира обучение в областта на ВЕИ. Такова се извършва в 20 професионални гимназии в 17 области. Може да се очаква, че интензивното въвеждане на ВЕИ в страната ще предизвика необходимост от допълнителни кадри за експлоатация и техническо обслужване на различни централи.

Трета група - Висши училища

В Трансграничната зона Румъния – България са изградени 93 ветрови паркове, 17 фотоволтаични инсталации и 36 малки водноелектрически централи. Те ангажират голям брой инженери и специалисти за проектиране и експлоатация на технически съоръжения.Кадровата политика се осигурява от редица висши училища:

- Русенски университет „Ангел Кънчев" – Магистърски курс по Възобновяеми енергийни източници и технологии ;
- Технически университет Варна - Магистърска програма по възобновяеми енергийни източници;
- Бургаски свободен университет – Магистърски курс по Възобновяема енергия. Вятърни генератори и фотоволтаици;
- Софийски университет „Св. Климент Охридски" – Магистърска програма Регионални геоенергийни ресурси и стратегии ;
- Европейски политехнически университет – Перник – Бакалавър по Зелена енергетика и Магистър по Слънчева Енергетика;

Очаква се въвеждането на бакалавърско обучение по ВЕИ и в други технически университети. Проучванията показват, че интереса на младите хора за подобен род обучение е голям.

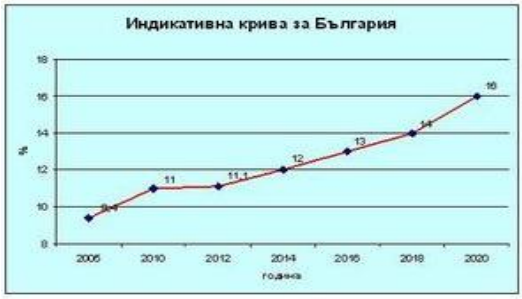
Висше образование в областта на ВЕИ в Европа:

Проучванията, които са извършени показват, че в Европа огромен брой технически университети предлагат обучение: бакалавърска и магистърска степен по ВЕИ. Сред реномираните университети са:

- Университета на Касел, Германия – предлага обучение по хибридни системи;
- Националния технически университет в Атина, Гърция – акцентът е върху ветровата енергетика ;
- Northumbria университет, Великобритания – фотоволтаични системи и технологии;
- Университета на Сарагоса, Испания - енергийни системи, интеграция;
- Университета на Перпинян, Франция - слънчева енергетика;
- Висше техническо училище „Instituto Superior Técnico", Португалия – енергия получавана от океан.

ЗАКЛЮЧЕНИЕ

Един от приоритетите на България, с цел финансово стабилна и пазарно ориентирана енергетика, е повишаването на дял на ВЕИ от 11.1% на 16% до 2020г. (фиг.1).



Фиг. 1 – Национална обща цел за България-увеличаване на дела на ВЕИ на 16% до 2020г.

Мащабното развитие на възобновяемата енергетика изисква подготовката на средни и висши кадри с висока квалификация. Затова е нужно да се насочат допълнителни средства за изграждане на модерна техническа инфраструктура, доставка на специализиран софтуер, литература и други, които да гарантират качествен учебен процес.

ЛИТЕРАТУРА

[1] Бургаски свободен университет (http://www.bfu.bg/)
[2] Европейска комисия, (http://ec.europa.eu/index_bg.htm)
[3] Европейски политехнически университет (http://epu.bg/index.php/en/)
[4] Закон за енергетиката, София, 2012 г.
[5] Русенски университет „Ангел Кънчев" (http://www.uni-ruse.bg/)
[6] Софийски университет „Св. Климент Охридски" (http://www.uni-sofia.bg/)
[7] Технически университет Варна (http://www.tu-varna.bg/)
[8] Circe De Investigacion De Recersos Y Consumos Energeticos(http://www.fcirce.es)
[9] European Master in renewable energy http://www.master.eurec.be/en/About-the-Master/Overview/
[10] European Master in renewable energy(http://www.master.eurec.be/en/About-the-Master/Calendar/)
[11] FraunhoferISE (www.ise.fhg.de)
[12] Instituto Superior Techino (http://www.ist.utl.pt)
[13] National Technical University of Athens (http://www.aerolab.ntua.gr/
[14] NewcastleGateshead (http://www.visitnewcastlegateshead.com)
[15] PROCEDES, MATERIAUX ET ENERGIE SOLAIRE (http://www.promes.cnrs.fr)

За контакти:

Явор Алдинов Стефанов, Русенски Университет „Ангел Кънчев", e-mail: yavor.a.stefanov@gmail.com

проф. д-р инж. Никола Михайлов, Русенски университет "Ангел Кънчев", Катедра „Електроснабдяване и електрообзавеждане", тел.: 082-888 843, e-mail: mihailov@uni-ruse.bg

Базисни линии на електропотребление в индукционни пещи за топене на стомана

автор: Силвия Димитрова
научен ръководител: проф. дтн Кондю Андонов

Studying the electric power consumption of induction furnaces for steal melting: *The electric power consumption of induction furnaces for steal melting is studied. A procedure is proposed for determination of the theoretically-needed electric-power consumption for ensuring the thermal processes and the usage of a heat pump for residual-heat utilization in chilling the furnaces. The expected electric power savings are stated and the basis levels of electric-power consumption in the consumers' existing operation conditions, and after the heat recovery, are determined.*
Key words: *Energy efficiency, electric-energy savings.*

ВЪВЕДЕНИЕ

Топенето на металите в множеството леярски заводи в страната се осъществява чрез индукционни пещи. Такива са заводите Алуковм– Плевен, Осъм Ловеч и Центромет Враца. Проучването на електропотреблението за леенето на металите в тези заводи показва, че енергийната ефективност на процеса е незадоволителна. В настоящия доклад са представени резултатите от анализа на базисните линии на електропотребление и специфичния разход на електроенергия при топенето на метала в индукционните пещи при леене на стомана при съществуващото положение и след прилагане на мярка за енергийна ефективност.

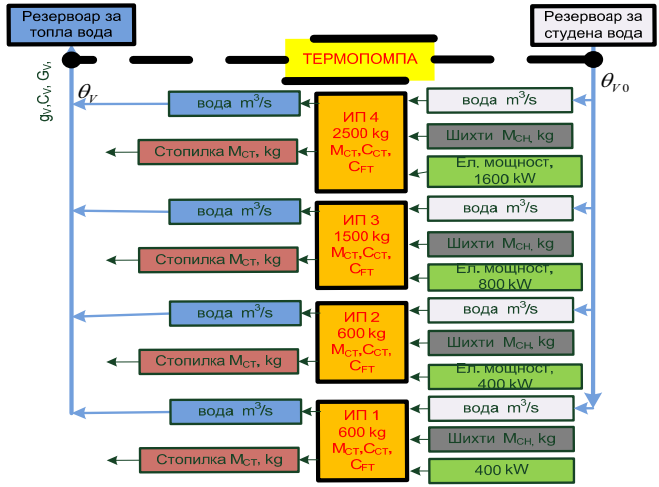
ИЗЛОЖЕНИЕ

Обект и методика на изследването

Обектът на изследването е завод „Центромет" – Враца, по-специално леярски цех, където са монтирани четири индукционни пещи (фиг.1). Охлаждането на пещите е водно, където водата циркулира по контурите на пещите, охлажда ги, преминава през охладителни кули, чрез които отнетата топлина се отдава под формата на загуби на енергия в околната среда.

Фиг. 1 – Индукционни пещи за леене на стомана и чугун

Функционират четири пещи, с капацитет от 5700 kg и мощност от 4200 kW. Схемата на материалните и енергийни потоци при топене на метала е представена на фиг.2. Въз основа на балансната схема се извеждат зависимостите за определяне на теоретично необходимата енергия да загряване и топене на метала в пещите при леенето, като:



Фиг. 2 – Схема на материалните и енергийни потоци при топене на метала в „Центромет"АД - Враца

$$W_{CT} = W_F + W_{FT} \quad (1)$$

$$W_{CT} = C_{CH}.M_{CH}.(\theta_T - \theta_0).3,6.10^{-3} + C_{FT}.M_{CT}.3,6.10^{-3} \quad (2)$$

където W_{CT} е енергията, съдържаща се в стопилката, **kWh**;

W_F енергията, необходима за загряване на метала до температурата на топене, **kWh**;

W_{FT} енергията, погълната за фазово превръщане при разтапенето на метала, **kWh**;

C_{CH} - специфичният топлинен капацитет на шихтовия материал, **kJ/kg.K** (желязо – $C_{CH} = 0,460\,kJ/kg.K$);

M_{CH} - маса на шихтите в пеща след зареждане, kg;

C_{FT} - специфичната топлина на топене (фазово превръщане) на метала, **kJ/kg** (желязо – C_{CH} = 272 **kJ/kg**);

M_{CT} - маса на стопения матал, kg;

θ_T - температура на стопения метал, ^0C;

θ_0 - температура на шихтите при зареждане на пеща, ^0C.

Енергията отнасяна при охлаждането на пещите е:

$$W_V = C_V.g_V.(\theta_V - \theta_{V0}).T_{CT} \quad (3)$$

Където W_V е енергията отнесена от водата, **kWh**;

C_V - специфичният топлинен капацитет на водата, **kJ/kg.K** (вода - $C_{CT} = 4,19\,kJ/kg.K$);

θ_V - температурата на водата на изхода от охлаждащия контур, ^0C;

θ_{V0} - температурата на на водата на входа на охлаждащия контур, ^0C;

g_V - дебитът на потока охлаждаща вода, **kg/s**.

Електропотребление и базисни линии на разхода на електроенергия

В табл.1 са представени данните за месечния разход на електроенергия общо за завода и отделно за индукционните пещи. Общо за годината пещите израсходват 36,3 % и са основния консуматор на електроенегия в завода. При този разход в завода са стопени 74200 kg стомана (табл.1). Специфичният разход на електроенергия общо за завода е в диапазон от 4,1 до 7,8 kWh/kg, а за пещите е от 1,4 до 3,3 kWh/kg (табл.1, колона 5 и 6).

Таблица 1. Баланс на разхода на електроенергия по месеци през 2010 г. в Центромет - Враца

Месец	*Ел. енергия,kWh*		*Стопен метал, kg*	*Специфичен разход, kWh/kg*	
	завод	*пещи*		S_Z, *завод*	S_P, *пещи*
1	2	3	4	5	6
I	336 747	108 665	76000	4,4	1,4
II	335 139	107896	68000	4,9	1,6
III	309 561	111 444	64000	4,8	1,7
IV	297 340	121 043	69000	4,3	1,8
V	348 614	121 129	78000	4,5	1,6
VI	352 322	185 947	57000	6,2	3,3
VII	172 039	64 227	22000	7,8	2,9
VIII	252 758	101 423	43000	5,9	2,4
IX	295 767	122 544	54000	5,5	2,3
X	326 489	132 665	58000	5,6	2,3
XI	369 337	157 054	69000	5,4	2,3
XII	344 939	131 158	84000	4,1	1,6
∑	3 741 052	1 357 299	742000	5,0	1,8

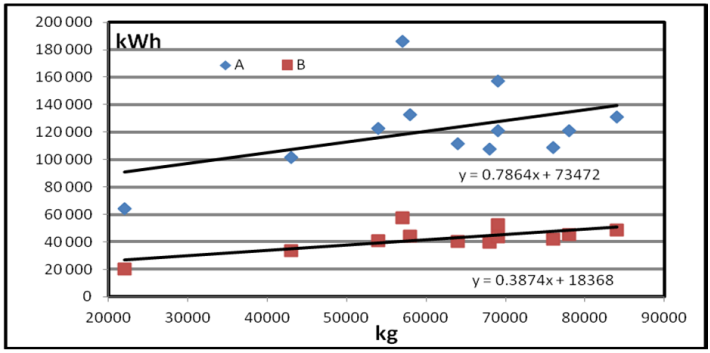
Като са използвани данните от табл.1 и изведените зависимости (2.1)-(2.3) са определени енергията, необходима за загряване на метала до температурата на топене W_F и енергията, погълнатата за фазово превръщане при разтапенето на метала W_{TF}, както и енергията, съдържаща се в стопилката W_{CT}. Данните са представени в табл.2. Неполезният разход (загубата) на електроенергия ΔW е даден в колона 5, табл. 2. Общо за годината достига 1 168 501 kWh. Приема се, до 25 % от неполезния разход не може да се улови.

Таблица 2. Нива на теоретично необходимия разход на енергия за топенето на стоманата и възможната икономия на електроенергия в Центромет - Враца

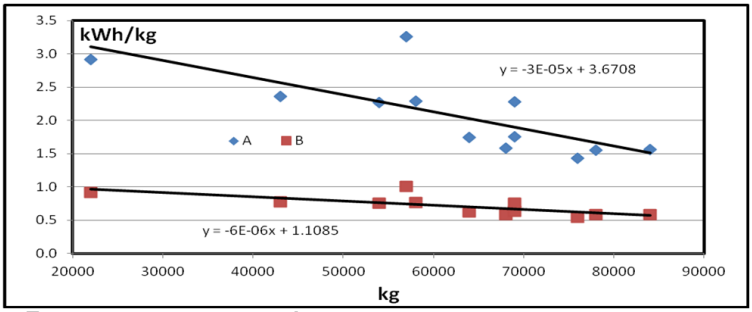
1	2	3	4	5	6	7	8	9
Месец	W_F, kWh	W_{TF}, kWh	W_{CT}, kWh	ΔW, kWh	ΔW_S, kWh *(75%ΔW)*	W_E	S_{ZE}, *(A)*	S_{PE}, *(B)*
I	13596	5742	19338	89 327	66995	41 670	1,4	0,55
II	12164	5138	17302	90 594	67945	39 951	1,6	0,59
III	11449	4836	16284	95 160	71370	40 074	1,7	0,63
IV	12343	5213	17557	103 486	77615	43 428	1,8	0,63
V	13953	5893	19847	101 282	75962	45 167	1,6	0,58
VI	10197	4307	14503	171 444	128583	57 364	3,3	1,01
VII	3936	1662	5598	58 629	43972	20 255	2,9	0,92
VIII	7692	3249	10941	90 482	67861	33 562	2,4	0,78

IX	9660	4080	13740	108 804	81603	40 941	2,3	0,76
X	10376	4382	14758	117 907	88430	44 235	2,3	0,76
XI	12343	5213	17557	139 497	104623	52 431	2,3	0,76
XII	15027	6347	21373	109 785	82339	48 820	1,6	0,58
Σ	132736	56062	188798	1 168 501	876376	480 923	1,8	0,65

На тази основа се приема, че около 75 % от неполезния разход ще се усвои чрез енергоефективната мярка (EEM). Това е електроенергията ΔWS, представена в табл.2, колона 6. Като EEM се приема вграждането на термопомпа, чрез която да се отвежда и полезно използва топлината от водоохлаждащия контур. Очакваното ниво на разхода на електрическа енергия от пещите WE след въвеждането на EEM е дадено в табл.2, колона 7. При така приетите и определени нива на електропотребление са определени променения специфичния разход на електроенергия общо за завода (S_{ZE}) и пещите (S_{PE}) – табл.2, колони 8 и 9.



Фиг. 3 – Базисна линия на разхода на електроенергия при топене на метала
А – при съществуващото състояние; В – след усвояване на енергията при охлаждане на пещите



Фиг. 4 – Базова линия на специфичния разход на електроенергия за килограм отлят метал в индукционните пещи
А – при съществуващото състояние; В – след усвояване на енергията при охлаждане на пещите

По данните от табл. 1, колона 3 и табл.2, колона 7 са построени базовите линии на разхода на електроенергия при топене на метала и показани на фиг.3.(А – при съществуващото ниво, В – след усвояване на енергията при охлаждане на пещите).

Нивото на разхода А се описва с уравнението y = 0,7864x + 73472 , а нивото на разхода с уравнението y = - y = 0,3874x + 18368.

Базовате линии на специфичния разход на електроенергия за килограм отлят метал в индукционните пещи са представени на фиг.4 (А – при съществуващото ниво, уравнение y = -3E-05x + 3,6708); В – след усвояване на енергията при охлаждане на пещите, y = -6E-06x + 1,1085).

ЗАКЛЮЧЕНИЕ

Практическото позволява да се направят следните изводи:

1. Нивата на теоретически необходимия (базисен) разход за осигуряване на топлинните процеси има еталонен характер. Това е количеството физически (може да се нарече полезен, неизбежен разход) необходима енергия.

2. Количествата над еталонния разход са загубите на енергия, която чрез мероприятията по енергийна ефективност следа да се намалява.

3. Мониторингът на разхода на енергия за осигуряване на топлинните процеси следва да се осъществява на базата на еталонния разход.

ЛИТЕРАТУРА

[1] Закон за енергийна ефективност. Д В бр., от 2004 г.
[2] Ковачев Н. Електротехнолигии и електротермия. С. Техника, 1977.

За контакти:

Силвия Димитрова, Русенски университет "Ангел Кънчев", Катедра "Електроснабдяване и електрообзавеждане", тел.: 082-888 212,

проф. дтн Кондю Андонов, Русенски университет "Ангел Кънчев", Катедра „Електроснабдяване и електрообзавеждане", тел.: 082-888 329, e-mail: kandonov@uni-ruse.bg.

Автоматизирана технологична линия за химично делинтиране на памукови семена

автори: Иван Иванов, Ива Иванова, Илиян Йорданов
научни ръководители: доц. Кирил Сираков, проф. Иван Палов

Automated technological line for chemical delinting of cotton seeds: *Applied in Bulgaria a technology for chemical delinting of cottonseeds is with manual control and many disadvantages. The worked reconstructions of the basic technological line elements to be adapted for automatic control is considered in the paper. A block diagram of the technological line is worked out. The realized automatic line has worked flawlessly for two years.*
Key words: *automatic control, cottonseeds.*

ВЪВЕДЕНИЕ

Основната първична преработка на прибрания от полето памук включва отделянето на памучните влакна от семената чрез маганене. Получените при това семена са покрити с остатъчни влакна, дълги до 10 mm, наречени линт. Процесът на отделяне на линта от семената се нарича делинтиране. В памукопреработвателните предприятия на България се прилага химично делинтиране на семената за посев с нагрята концентрирана сярна киселина. Използваната технология обаче има редица недостатъци.

Целта на работата е да се анализира прилаганата досега технология за химично делинтиране и да се обоснове автоматизирана технологична линия, осигуряваща качествени памукови семена за посев.

ИЗЛОЖЕНИЕ

Технологията за химично делинтиране на памукови семена включва следните основни процеси [4]: нагряване на сярната киселина; дозиране и подаване на сярна киселина и памукови семена в смесителния съд (лотра); разбъркване (обработка) на семената в лотрата; начално измиване на семената в лотрата; допълнително измиване на семената в извозващия шнек; сушене на семената.

Състояние на съществуващите линии за химично делинтиране на памукови семена

Анализът на съществуващите в България линии за делинтиране на памукови семена дава основание за следните заключения:

1. Избраният директен начин за нагряване на киселината не е подходящ [3]. При него трудно се достига и поддържа необходимата й температура от 120 °C и затова част от семената не могат да се делинтират напълно.

2. Използвани са големи по обем метални съоръжения, които изискват тежък физически труд и нервно напрежение от работника. Необходими са голям брой операции за ръчно пускане, спиране или задвижване на различните съоръжения. Поради ръчните операции съществува субективизъм и неточност при подаване на необходимите количества семена, киселина, вода и при определяне продължителността на делинтиране.

3. Нагрятата сярна киселина се подава "залпово" върху част от семената. Лотрата се запълва бавно с вода при началното измиване на семената, поради което те престояват продължително време (над 2 min) в бавно разреждащата се киселина. Описаното води до намаляване жизнеспособността на семената [2].

4. Извозващият шнек е с несъобразена производителност. Затова се получава некачествено измиване на семената и неравномерно натоварване на сушилнята.

5. Машините и съоръженията в линията нямат взаимни блокировки. Това води

до получаване на недостатъчно качествени семена вследствие например на подаване на недонагрята киселина, започване на процес делинтиране без наличие на достатъчни количества семена, киселина, вода и т.н.

6. В помещението на цеха се получават серни и други вредни пари, които влошават здравето на работниците и водят до ускорена корозия на съоръженията.

Разработване на автоматизирана технологична линия за химично делинтиране на памукови семена

Схемата за управление на линията е разработена така, че да отговаря на следните изисквания:

1. Да осигурява точно спазване на параметрите на технологичния процес, а с това да гарантира високо качество на делинтираните семена.

2. Да дава възможност за работа в ръчен и в автоматичен режим и да не допуска грешни манипулации от страна на обслужващия персонал.

3. Да контролира наличието на семена, вода, сярна киселина и нейната температура. При липса на някой от тези компоненти да не започва нов технологичен цикъл на делинтиране преди осигуряването на наличността му.

4. Да следи работния режим на технологичното обзавеждане и при евентуална авария да прекратява работния процес.

5. Да има светлинни и звукови сигнализации.

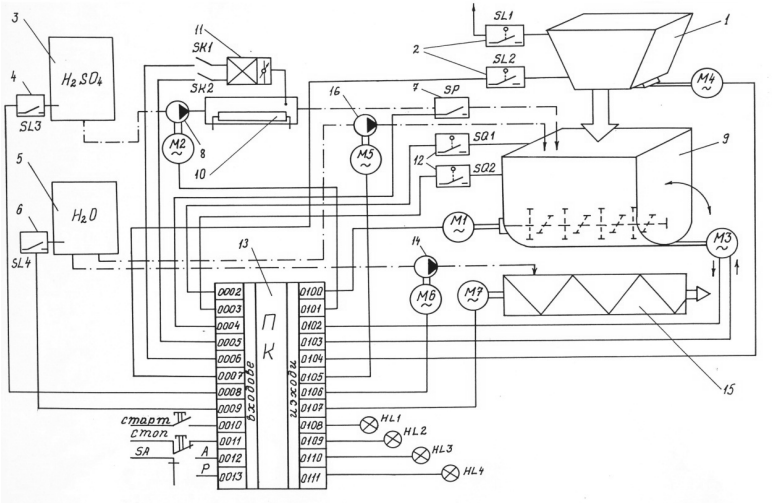
6. Да осигурява висока степен на безопасност.

При съществуващата технология част от съоръженията се задвижват и управляват ръчно, и не подлежат на автоматизация. Липсват датчици за следене на параметрите на технологичния процес. Затова, за да се изпълнят посочените изисквания, преди разработване на схемата за управление, всички елементи на технологичната линия трябва да се реконструират. Принципна схема, с основните елементи на технологична линия и входните и изходни връзки на системата за управление, е показана на фиг.1.

Предлагат се следните принципно нови, подходящи за автоматизация конструктивни решения: индиректна нагревателна уредба [3]; устройства с електрозадвижване за подаване на семена (с битер) и на киселина (с помпа), осигуряващи точно дозиране и подходящо смесване на компонентите; разделено подаване на вода (с помпи) за измиване на семената в лотрата и в шнека; устройство за еднократно изливане на лотрата с контрол на положението;

С цел удовлетворяване на изискванията на схемата за управление са променени устройството и производителността на извозващия шнек [1], монтирани се подходящи датчици за следене температурата на киселината, наличието на семена, вода и киселина, пътни прекъсвачи за положението на лотрата и др. (фиг.1).

Основните етапи от технологичния процес протичат последователно и циклично. Затова те се разглеждат като дискретни обекти за автоматизация. Системата за автоматично управление на технологичната линия е синтезирана по съставената блокова схема, чиито основни елементи и функционални връзки са показани на фиг.2. Взаимодействието между всички блокове се осигурява от блок 1. Преди започване на работа е необходимо операторът да включи схемата. Технологичният цикъл може да започне само при наличие на семена в бункера (блок 2), вода в резервоара (блок 3), изправено положение на лотрата (блок 13) и достатъчна температура на киселината (блок 4). Блок 6 контролира подаването на киселина. Разработената линия може да работи в автоматичен и в ръчен (полуавтоматичен) режим.

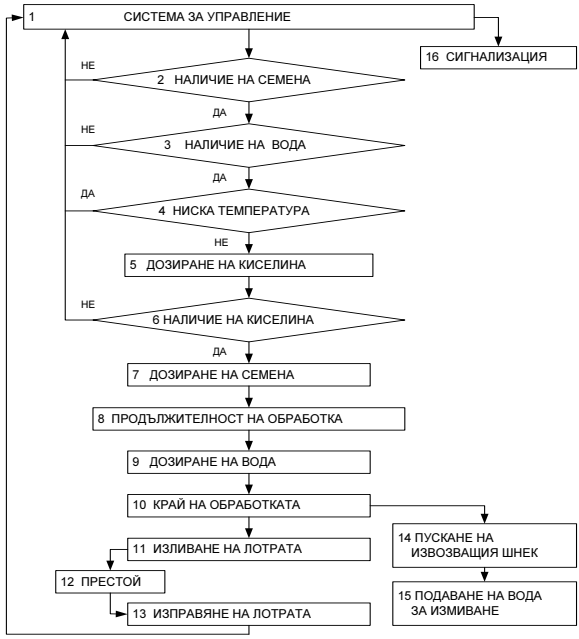


Фиг. 1 – Структурна схема на технологичната линия за делинтиране на памукови семена с програмируем контролер
1- бункер за семена; 2- датчици за ниво на бункера; 3- резервоар за сярна киселина; 4 - датчик за наличие на сярна киселина; 5- резервоар за вода; 6- датчик за наличие на вода; 7- датчик за наличие на струя киселина; 8- помпа за киселина; 9- лотра; 10- нагревателна уредба; 11- електронен регулатор на температурата на нагревателната уредба; 12- крайни изключватели за положението на лотрата; 13- програмируем контролер; 14- помпа за вода, подавана към извозващия шнек; 15- извозващ шнек; 16- помпа за вода, подавана към лотрата.

При автоматичен режим технологичният процес започва след подаване на сигнал към схемата и то след изпълнението на описаните по-горе условия. Процесът протича без допълнителна намеса от страна на оператора. Особеност на сйемата е, че при липса на някой от компонентите (подава се сигнал към блока 16) се довършва започнатия цикъл, изчаква се до отпадането на съответния блокиращ сигнал, след което автоматично започва нов цикъл. При ръчно подаване на сигнал за спиране се довършва започнатия цикъл и след това спира работата на всички съоръжения.

При ръчен режим операторът подава сигнал със съответен бутон за започване на всеки етап от цикъла. След приключване на етапа съответното съоръжение се изключва автоматично и линията изчаква следващ сигнал.

Приложението на индиректно нагряване на киселината, както и реконструирането вентилационна система ще осигуряват в помещението естествен въздух, без серни и др. изпарения.



Фиг. 2 – Блокова схема на автоматизирана технологична линия за химично делинтиране на памукови семена

По предложената схема е изпълнено автоматично управление на технологична линия с програмируем контролер По предварителна оценка внедрението на линия ще осигури повишение на производителността на труда 2 пъти и намаление на специфичния разход на вода, на сярна киселина – 1,4 пъти, на електрическа енергия – 2,1 пъти и на дизелово гориво - 2,4 пъти.

ЗАКЛЮЧЕНИЕ

1. Съществуващите в България технологични линии за химично делинтиране на памукови семена позволяват работа само в ръчен режим, с много на брой тежки операции и не могат да осигурят точно спазване на технологичните параметри. Така се нарушават посевните качества на семената, а околната среда в помещенията е наситена със серни изпарения.

2. С цел реализиране на автоматично управление всички основни елементи на технологичната линия трябва да бъдат преустроени.

3. Изпълнена по предложената схема и внедрена в производствено предприятие, автоматизираната технологична линия ще реализира значителни икономии.

ЛИТЕРАТУРА

[1] Отчет по тема № 9711 "Проектиране на автоматизирана технологична линия за третиране на памукови семена със сярна киселина", НИС при Русенски Университет "Ангел Кънчев"

[2] Сираков К., Ив. Палов, Ст. П. Стефанов, Изследване влагопоглъщането на делинтирани памукови семена, Научни трудове на РУ "Ангел Кънчев", т. 37, с. 3, Русе, 1999.

[3] Стефанов Ст. П., Ив. Палов, К. Сираков, Л. Михайлов, Изследване възможностите за нагряване на концентрирана сярна киселина, използвана при предпосевна обработка на памукови семена, София, Селскостопанска техника,1998, №3.
[4] Технология за производство на памукови семена, Институт по памука и твърдата пшеница, Чирпан, 1995.

За контакти:

Иван Иванов, Русенски университет "Ангел Кънчев", Специалност " Електроенергетика и електрообзавеждане", e-mail: ivanivanov_ru@abv.bg

Ива Иванова, Русенски университет "Ангел Кънчев", Специалност " Електроенергетика и електрообзавеждане", e-mail: ivaivanova_90@abv.bg

Илиян Йорданов, Русенски университет "Ангел Кънчев", Специалност " Електроенергетика и електрообзавеждане", e-mail: ilianiordanov_90@abv.bg

доц. д-р инж. Кирил Сираков, Русенски университет "Ангел Кънчев", Катедра „Електроснабдяване и електрообзавеждане", тел.: 082-888 364, e-mail: csirakov@uni-ruse.bg

проф. д-р инж. Иван Палов, Русенски университет "Ангел Кънчев", Катедра „Електроснабдяване и електрообзавеждане", тел.: 082-888 364, e-mail: ipalov@uni-ruse.bg

Активен тонкоректор

автор: Светослав Плачкинов
научен ръководител: гл. ас. Явор Нейков

Active equalizer: *The main purpose of the active frequency correction is to obtain better audio efficiency with clear-toned signals for preamplifiers and end-stage amplifiers. The report represents the structure and analysis of real home-made equalizer for low-frequency audio amplifier with some sonority effects at low frequency ranges.*

Key words: *frequency equalizer, low-frequency amplifier, audio efficiency, sonority effect*

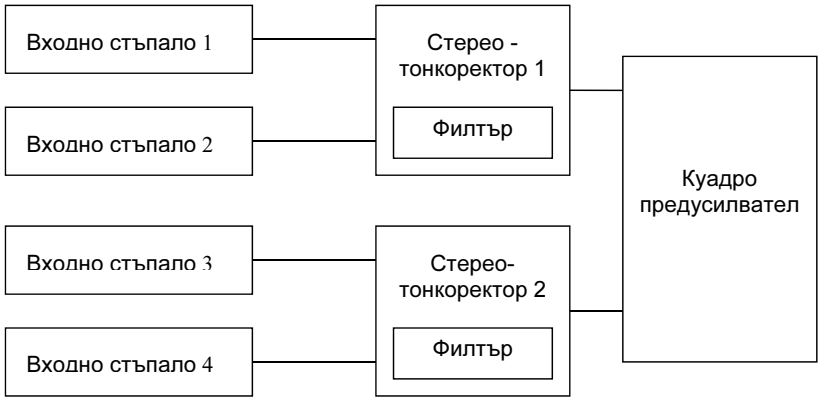
ВЪВЕДЕНИЕ

Проектирането и изграждането на честотнокоригиращи електронни устройства е в основата на конструирането на съвременни звукотехнически системи за аудиообработка. Тяхното непрекъснато усъвършенстване води до създаването на все по-качествени и търсени от потребителите ефекти, които значително подобряват и обогатяват общото звучене на музикалните композиции.

Настоящата разработка има за цел да представи реализацията и изследване на работоспособността на реален активен тонкоректор за любителски нужди. Предназначена е за използване в предусилвателни и усилвателни нискочестотни крайни стъпала в битовата техника. Анализирана е работата на устройството и на получените звукови ефекти при свързване към стандартен нискочестотен аудиоусилвател за звукови честоти в диапазона 20Hz÷20kHz.

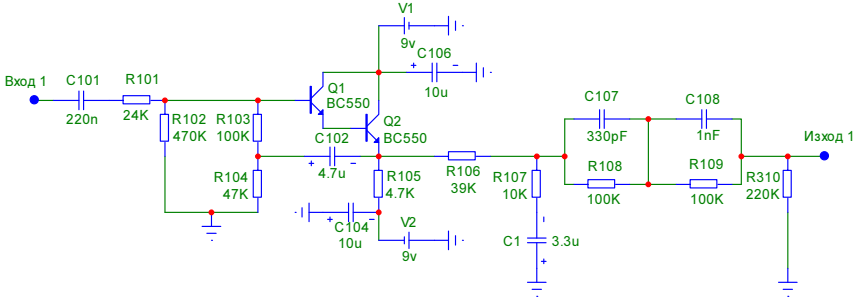
ИЗЛОЖЕНИЕ

Структурната схема на устройството се състои от няколко еднотипни входни стъпала, тонкоректори за ниски и високи честоти и краен предусилвател (фиг.1.).



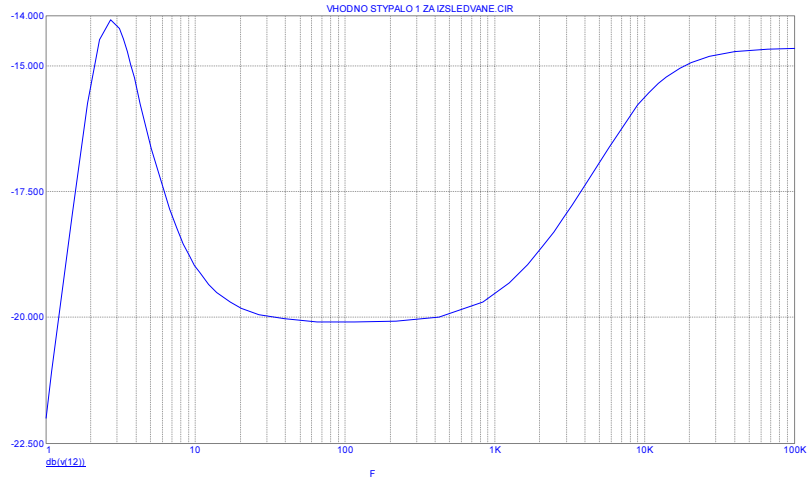
Фиг. 1 – Структурна схема на устройството

Входното стъпало представлява повторител на напрежение и същевременно усилвател на ток. На края има честотно зависим делител на напрежение. За изработването на стъпалото е използвана базова схема [1]. Схемата е с положителна обратна връзка за повишаване на входното й съпротивление. Всички входни стъпала са еднотипни, като на фиг.2. е показано само входно стъпало 1. Обратната връзка е осъществена посредством кондензатора C102.



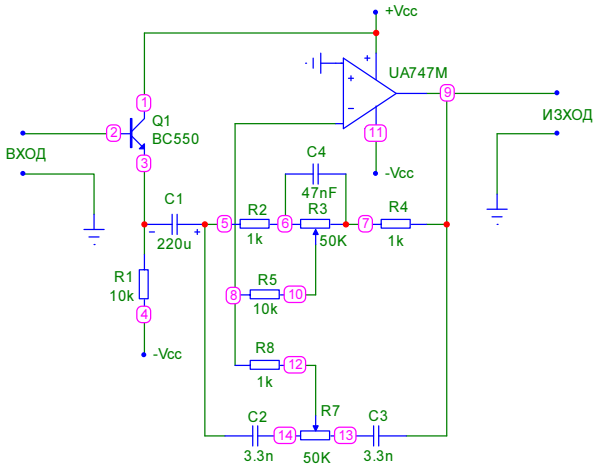
Фиг. 2 – Принципна електрическа схема на входното стъпало

Входното стъпало потиска средните честоти, като по този начин заедно с предусилвателя се получава частично повдигане на ниските и високите честоти. Схемата повдига ниските честоти още от 3Hz, което позволява баса да звучи по-плътно. Амплитудно-честотната характеристика е построена чрез симулатор на схеми Circuit Maker студентска версия, както и с MicroCap демо версия. Резултатите са онагледени на фиг.3



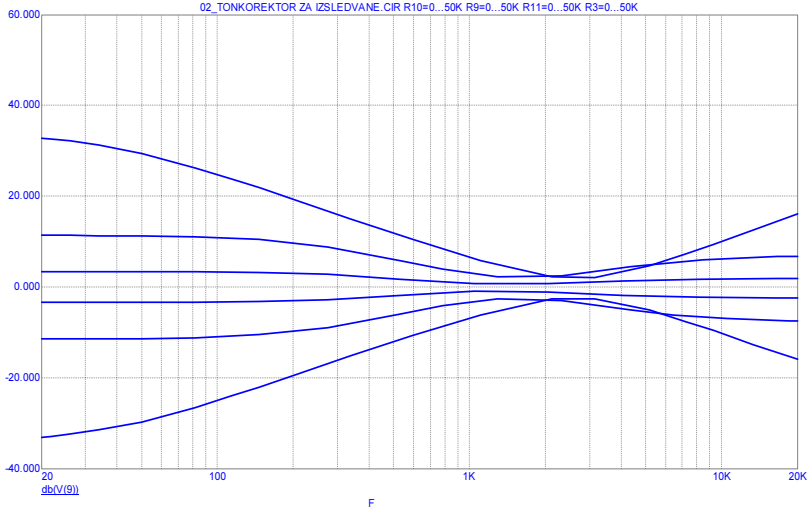
Фиг. 3 – Симулационен анализ на АЧХ в изхода на входното стъпало

Схемата на тонкоректора е реализирана с използване на транзистор BC550, работещ в схема общ колектор за усилване на сигнала по ток (фиг. 4.). Усилвателят служи за регулиране степента на усилване на съответните групи честоти. C4 действа като шунт за високите честоти, а за ниските има достатъчно голямо съпротивление. C2 и C3 също пропускат само високите честоти, а за ниските имат голямо съпротивление. Така потенциометърът R3 служи за коригиране на амплитудите на нискочестотните сигнали, а потенциометърът R7 - за коригиране на високочестотните сигнали.



Фиг. 4 – Принципна схема на тонкоректора

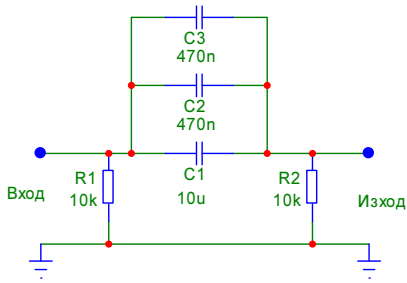
Изследвано е състоянието на АЧХ на сигналите на изхода на тонкоректора във възел 9 при различни комбинации на потенциометрите за регулиране на честотите. Вижда се идеалната симетрия на повдигане или потискане на НЧ и ВЧ групите в избрания диапазон 20 Hz – 20 KHz (фиг.5.).



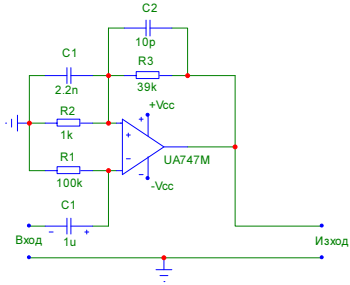
Фиг. 5 – АЧХ при изменение на потенциометрите R3 и R7от 0KΩ до 50KΩ през 10KΩ.

На фиг. 6. е показана схема на пасивен филтър, който е поставен между тонкоректора и предусилвателя. Целта на филтъра е да предпазва устройството от самовъзбуждане и да служи за изкуствен товар.

Крайното стъпало е предусилвател с коефициент на усилване около 32db. Схемата му е показана на фиг. 7. Съпротивлението R1 служи за изкуствен товар.

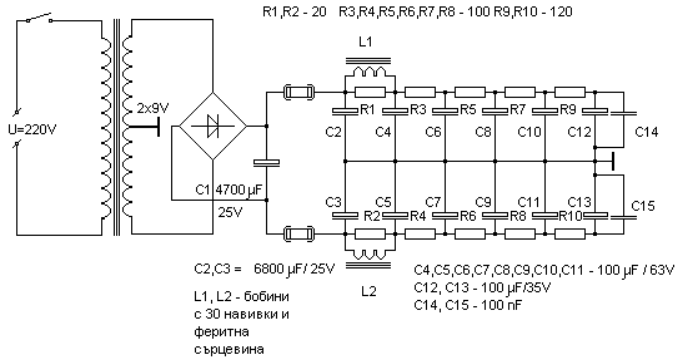


Фиг. 6 – Междинен филтър



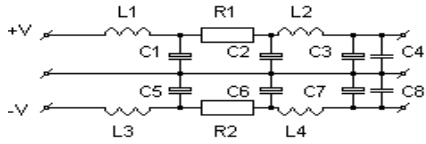
Фиг. 7. Схема на предусилвател

Използвано е двуполярно захранване ±9V (Фиг. 9), защото в схемата на устройството са включени операционни усилватели μA747 (два μA741 в един корпус).



Фиг. 8 – Принципна схема на захранването

Ако не се изглади добре захранващото напрежение се получава внасяне на неприятен за възприемане брум с честота около 100Hz. За филтриране на този брум между тонкоректора и захранващата схема е използван допълнителен RLC филтър, състоящ се от бобини и резистори свързани последователно и кондензатори свързани паралелно (фиг.8).



L1, L2, L3, L4 - бобини
R1, R2 - 47Ω
C1,C2,C3,C5,C6,C7 - 100 μF
C4,C8 - 100nF

Фиг. 9 – Допълнителен изглаждащ филтър за захранване на тонкоректора

ЗАКЛЮЧЕНИЕ

Реализирано е устройство за корекция на ниски и високи честоти, подходящо за използване в битова усилвателна апаратура.

Изследвани са и са получени подходящи нива на АЧХ, като е проектирано и реализирано необходимото схемотехническо изпълнение.

При много ниски честоти полученото повдигане и изкривяване на характеристиката при 3Hz изглеждащо като несъвършенство в работата на усилвателя практически се явява звуков ефект, който обогатява основния звук с хармоници в диапазона на чуваемост над 20Hz. Това внася реалистично звучене на изкуствено обработените звукови сигнали при възпроизвеждане.

ЛИТЕРАТУРА

[1] Р. М. Марстън "110 схеми с операционни усилватели" превел от английски език к.т.н. инж. Стефан И. Куцаров София, 1982 Държавно издателство "Техника"
[2] сп. „Радио, телевизия, електроника", бр.5, стр.30, София, 1981

За контакти:

Светослав Плачкинов, Русенски университет "Ангел Кънчев", Специалност "Компютърни системи и технологии", e-mail: splachkinov@rambler.ru

гл. ас. Явор Нейков, Русенски университет "Ангел Кънчев", Катедра „Електроника", тел.: 082-888 772, e-mail: yneikov@ecs.uni-ruse.bg


ЕСЕО
специалност
"Електроенергетика
и
електрообзавеждане"
специалност
"Електроника"
Русенски университет
"Ангел Кънчев"
А М
специалност
"Автоматика и
мехатроника"
факултет
"Електротехника, електроника
и автоматика"
специалност
"Компютърни
системи и
технологии"
специалност
"Телекомуникационни
системи"

Секция

Комуникационна и компютърна техника и технологии


ECEO
специалност
"Електроенергетика
и
електрообзавеждане"
специалност
"Електроника"
Русенски университет
"Ангел Кънчев"
А М
специалност
"Автоматика и
мехатроника"
факултет
"Електротехника, електроника
и автоматика"
специалност
"Компютърни
системи и
технологии"
специалност
"Телекомуникационни
системи"

Синтез и анализ на заграждащи активни биквадратни филтри от втори ред с използването на MATLAB и MicroCAP

автор: Йордан Райчев
научен ръководител: гл. ас. Адриана Бороджиева

Synthesis and Analysis of Band-Stop Active Second-Order Biquads Using MATLAB and MicroCAP: *In this paper synthesis and analysis of band-stop active biquads are considered. It is done according to a given normalized voltage transfer function and known normalizing resistance and central frequency of the filter. The synthesis is realized by means of MATLAB and the analysis of the filters designed after choosing standard values of the resistors and capacitors in the networks is done using MicroCAP. The results will be used in the educational process in the course "Communication Circuits".*

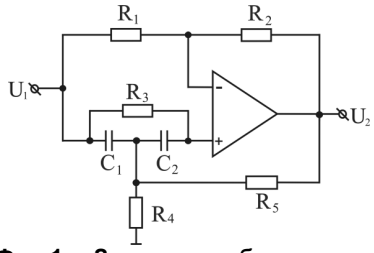
Key words: *Communication circuits; ARC filters, MATLAB, MicroCAP.*

ВЪВЕДЕНИЕ

Активните заграждащи биквадратни филтрови звена са изградени от един операционен усилвател, резистори и кондензатори. Синтезът и анализът се извършват при зададена нормирана предавателна функция по напрежение , средна честота , както и нормиращо съпротивление . В настоящата публикация ще бъдат разгледани два метода за синтезиране на биквадратните филтрови звена.

ИЗЛОЖЕНИЕ

На фиг. 1 е представена схемата на заграждащото биквадратно звено. В табл. 1 са представени нормираната предавателна функция по напрежение на активни заграждащи филтри (ЗФ) от втори ред (колона 1), както и тяхната предавателна функция, записана чрез коефициента на усилване в лентата на пропускане , средната кръгова честота и полюсния качествен фактор (колона 2) [1, 2, 3].



Фиг. 1 – Заграждащо биквадратно филтрово звено [1, 2, 3]

Таблица 1. Предавателни функции на ЗФ от втори ред

Нормирана предавателна функция	Предавателна функция, изразена чрез k_0, ω_0, Q
$T(p)=\dfrac{H\left(p^2+a\right)}{p^2+b_1p+b_0}$	$T(p)=\dfrac{k_0\left(p^2+\omega_0^2\right)}{p^2+\dfrac{\omega_0}{Q}p+\omega_0^2}$

В [3] е изведен аналитичният израз за предавателната функция на проектирания заграждащ филтър:

$$T(p)=\frac{p^2C_1.C_2.G_2+p.\left[G_2.G_3.\left(C_1+C_2\right)-G_1.C_2.\left(G_4+G_5\right)\right]+G_2.G_3.\left(G_4+G_5\right)}{p^2C_1.C_2.G_2+p.\left[G_2.G_3.\left(C_1+C_2\right)+C_2.G_2.G_4-C_2.G_1.G_5\right]+G_2.G_3.\left(G_4+G_5\right)} \quad (1)$$

Условието за реализиране на предавателна функция на заграждащ филтър е коефициентът пред p^1 в числителя да е равен на нула:

$$G_2.G_3.\left(C_1+C_2\right)=G_1.C_2.\left(G_4+G_5\right) \quad (2)$$

при което за предавателната функция на филтъра окончателно се записва:

$$T(p)=\frac{p^2C_1.C_2.G_2+G_2.G_3.\left(G_4+G_5\right)}{p^2C_1.C_2.G_2+p.\left[G_2.G_3.\left(C_1+C_2\right)+C_2.G_2.G_4-C_2.G_1.G_5\right]+G_2.G_3.\left(G_4+G_5\right)} \quad (3)$$

ОПИСАНИЕ НА АЛГОРИТЪМА И РЕЗУЛТАТИ ОТ СИНТЕЗА И АНАЛИЗА

Алгоритъмът на разработеното приложение на програмен продукт MATLAB [4] съдържа следните стъпки:

1. Избор на метод (първи или втори метод). При въвеждане на грешна стойност от страна на потребителя, програмата се връща в начално състояние и изчаква до въвеждане на правилен избор.
2. Въвеждане на коефициентите a, $b_0 = a$, b_1 в нормираната предавателна функция по напрежение $T(p)$ на филтъра.
3. Извеждане на нормираната предавателна функция по напрежение, след въвеждане на коефициентите от точка 1.
4. Изчисляване на нормираните стойности на елементите на синтезирания филтър.
   - Първи метод: условие за прилагане на методиката - $2.\sqrt{2.a} > b_1 > 0$ и условие за проектиране - $C_1 = C_2 = C = 1$ и $G_1 = G_2 = G = 1$ (нормирани стойности).
   - Втори метод: условие за проектиране - $C_1 = C_2 = C$ и $G_4 + G_5 = G$; изборът на нормирани стойности за C, G_1, G_3 е произволен, като при избора на G_3 се спазва точно определено ограничение в зависимост от коефициентите a, b_1
     - $b_1^2 - 8.a > 0 \Rightarrow G_3 \in \left(0; \frac{C}{4}\left(b_1 - \sqrt{b_1^2 - 8a}\right)\right) \cup \left(\frac{C}{4}\left(b_1 + \sqrt{b_1^2 - 8a}\right); +\infty\right)$
     - $b_1^2 - 8.a = 0 \Rightarrow G_3 \in \left(0; \frac{b_1 C}{4}\right) \cup \left(\frac{b_1 C}{4}; +\infty\right)$, т.е. $G_3 \neq \frac{b_1 C}{4}$
     - $b_1^2 - 8.a < 0 \Rightarrow G_3 \in (0; +\infty)$.

Стойностите на останалите елементи се получават чрез решаване на системи от уравнения:

- Първи метод: $G_3 = \frac{\sqrt{2.a}}{2} > 0$, $G_4 = \frac{b_1}{2} > 0$, $G_5 = 2.G_3 - G_4 = \sqrt{2.a} - \frac{b_1}{2} > 0$.
- Втори метод:

$$G_2 = \frac{a.C^2.G_1}{2.G_3^2},\ G_4 = \frac{a.b_1.C^3}{a.C^2 + 2.G_3^2},\ G_5 = G - G_4 = \frac{a.C^2\left(a.C^2 + 2.G_3^2 - b_1.C.G_3\right)}{G_3.\left(a.C^2 + 2.G_3^2\right)}.$$

5. Въвеждане на стойността на нормиращото съпротивление R_N.
6. Въвеждане на средната честота f_0 и изчисляване на нормиращата кръгова честота $\omega_N = 2\pi f_0$.
7. Изчисляване на денормираните стойности на елементите според правилата:
   - за резисторите: получените стойности на съпротивленията $R_k = 1/G_k$, където $k = 1...5$, се умножават с нормиращото съпротивление R_N
   - за кондензаторите: получените стойности за капацитетите се умножават с $\sqrt{a}/(\omega_N.R_N)$.
8. Избор на стандартни стойности. Той се извършва ръчно от потребителя след извеждане на списък със стандартните стойности на съпротивленията на резисторите и на капацитетите на кондензаторите по

скала E-24.

9. Изчисляване на средната честота, полюсния качествен фактор и коефициента на усилване в лентата на пропускане на заграждащия филтър. Прави се сравнение между получените стойности и тези зададени по условие.

- $f_0 = \frac{1}{2\pi}\sqrt{\frac{R_4+R_5}{R_3R_4R_5C_1C_2}}, Hz;\ Q = \frac{\sqrt{\frac{R_4+R_5}{R_3R_4R_5C_1C_2}}}{\frac{C_1+C_2}{R_3C_1C_2}+\frac{1}{R_4C_1}-\frac{R_2}{R_1R_5C_1}};\ k_0 = 1$

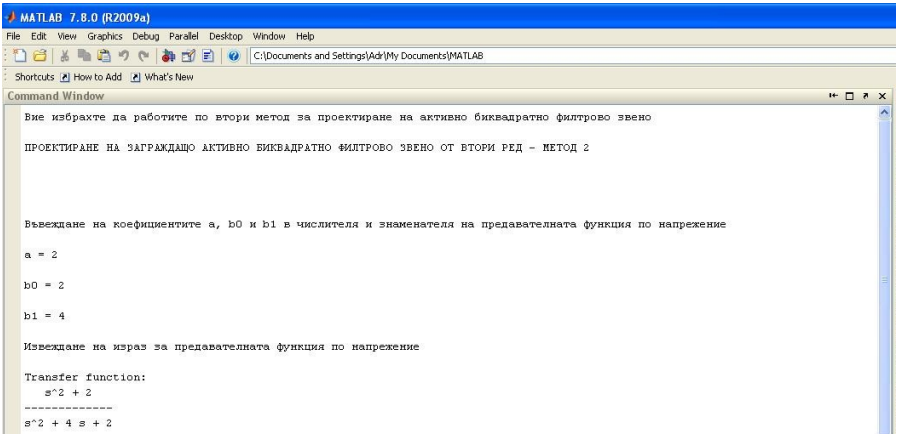
Пример: Проектиране на заграждащи биквадратни филтри със средна честота f_0 и нормирана предавателна функция по напрежение $T(p)$. Денормирането по честота и по съпротивление се извършва с нормираща кръгова честота $\omega_N = 2\pi f_0$ и нормиращо съпротивление R_N. Резултатите са показани в табл. 2. След това е извършен избор на стандартни стойности по скалата E-24, които се използват при симулацията с MicroCAP [5] за изчертаване на амплитудно-честотните характеристики (в dB) на проектираните филтри. В последната колона са посочени стойностите на средната честота f_0, на полюсния качествен фактор Q и на коефициента на усилване в лентата на пропускане k_0 за проектирания заграждащ филтър, след избора на стандартни стойности.

Таблица 2. Резултати от проектирането на ЗФ с MATLAB

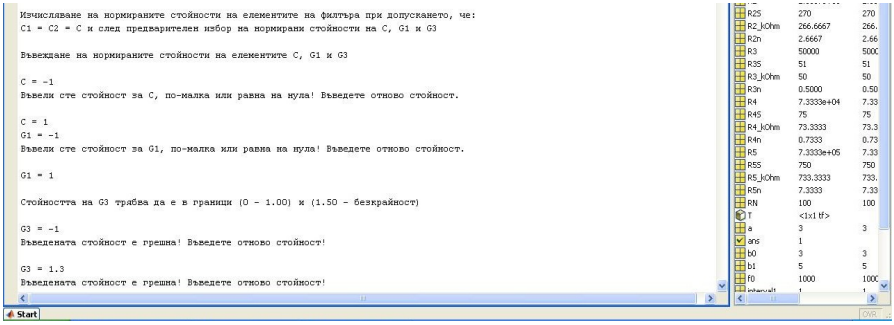
Метод	Нормирани стойности	Денормирани стойности	Стандартни стойности (E-24)	Забележка
Първи метод	$R_1 = 1$ $R_2 = 1$ $R_3 = 0{,}82$ $R_4 = 1{,}33$ $R_5 = 0{,}59$ $C_1 = 1$ $C_2 = 1$	$R_1 = 100\ k\Omega$ $R_2 = 100\ k\Omega$ $R_3 = 81{,}65\ k\Omega$ $R_4 = 133{,}33\ k\Omega$ $R_5 = 58{,}84\ k\Omega$ $C_1 = 2{,}76\ nF$ $C_2 = 2{,}76\ nF$	$R_1 = 100\ k\Omega$ $R_2 = 100\ k\Omega$ $R_3 = 82\ k\Omega$ $R_4 = 130\ k\Omega$ $R_5 = 62\ k\Omega$ $C_1 = 2{,}7\ nF$ $C_2 = 2{,}7\ nF$	$f_0 = 1000\ Hz$, $T(p) = \frac{p^2+3}{p^2+1{,}5p+3}$, $R_N = 100\ k\Omega$. --- $f_0 = 1004{,}69\ Hz$, $Q = 1{,}07$, $k_0 = 1$.
Втори метод	$R_1 = 1$ $R_2 = 4$ $R_3 = 0{,}5$ $R_4 = 1{,}25$ $R_5 = 5$ $C_1 = 1$ $C_2 = 1$	$R_1 = 100\ k\Omega$ $R_2 = 400\ k\Omega$ $R_3 = 50\ k\Omega$ $R_4 = 125\ k\Omega$ $R_5 = 500\ k\Omega$ $C_1 = 2{,}25\ nF$ $C_2 = 2{,}25\ nF$	$R_1 = 100\ k\Omega$ $R_2 = 390\ k\Omega$ $R_3 = 51\ k\Omega$ $R_4 = 130\ k\Omega$ $R_5 = 510\ k\Omega$ $C_1 = 2{,}2\ nF$ $C_2 = 2{,}2\ nF$	$f_0 = 1000\ Hz$, $T(p) = \frac{p^2+2}{p^2+4p+2}$, $R_N = 100\ k\Omega$. --- $f_0 = 995{,}28\ Hz$, $Q = 0{,}35$, $k_0 = 1$.

Показани са снимки от екрана при изпълнение на програмата на MATLAB за проектиране на заграждащи филтри, като са илюстрирани процесите на въвеждане

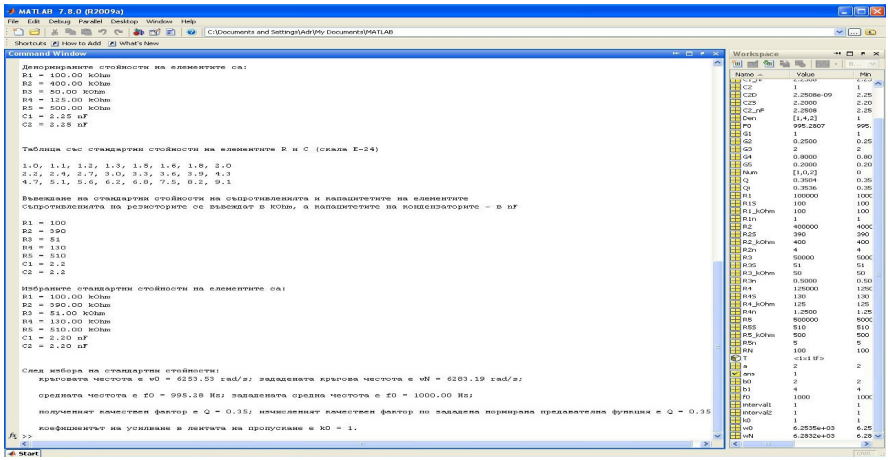
на коефициентите на нормираната предавателна функция по напрежение (фиг. 2), извеждане на съобщения за грешка при въвеждане на некоректни стойности (фиг. 3), както и на избора на стандартни стойности на елементите на схемата след изчисляване на денормираните стойности на съпротивленията и капацитетите в схемата (фиг. 4). В табл. 3 са показани резултатите при симулационното изследване с MicroCAP, като са посочени и стойностите на средната честота, полюсния качествен фактор и коефициента на усилване в лентата на пропускане на проектирания заграждащ филтър.



Фиг. 2 – Въвеждане на коефициентите на предавателната функция по напрежение

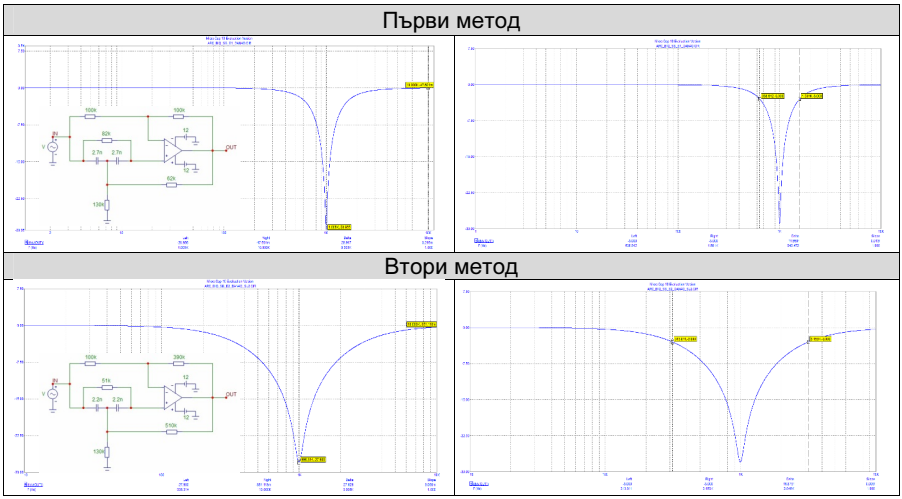


Фиг. 3 – Съобщения за грешка при въвеждане на некоректни стойности



Фиг. 4 – Извеждане на изчислените денормирани стойности на елементите в схемата, както и на параметрите й f_0, Q, k_0, след избора на стандартни стойности

Таблица 3. Резултати при симулационно изследване с MicroCap



Първи метод: $f_0 = 1{,}005\ kHz$; $f_{01} = 638{,}912\ Hz$; $f_{02} = 1{,}581\ kHz$;

$B = f_{02} - f_{01} = 942{,}472\ Hz$; $Q = f_0 / B = 1{,}066$; $k_0 = 10^0 = 1$

Втори метод: $f_0 = 995{,}314\ Hz$; $f_{01} = 313{,}811\ Hz$; $f_{02} = 3{,}159\ kHz$;

$B = f_{02} - f_{01} = 2{,}846\ kHz$; $Q = f_0 / B = 0{,}35$; $k_0 = 10^0 = 1$

ЗАКЛЮЧЕНИЕ

В публикацията е описан алгоритъм, заложен в програмен модул, с използване на MATLAB, създаден за синтез и анализ на заграждащи активни биквадратни филтри от втори ред. Приложени са и симулационните резултати от изследването на проектираните филтри с MicroCAP. Разработеният програмен модул ще намира приложение в учебния процес по дисциплината „Комуникационни вериги", включена като задължителна в учебния план на специалността „Телекомуникационни системи" за образователно-квалификационна степен „Бакалавър".

ЛИТЕРАТУРА

[1] Николова, Зл. Ръководство за семинарни упражнения по комуникационни вериги. София, издателство „Николов", 2001.
[2] Стоянов, Г. Теоретични основи на съобщителната техника. София, Техника, 1993.
[3] Стоянова, Т., А. Бороджиева. Синтез и анализ на заграждащи активни биквадратни филтрови звена с използването на MATLAB и MicroCAP. 8th Summer School, Advanced Aspects of Theoretical Electrical Engineering, Sozopol '2010, 19.09. – 22.09.2010, Sozopol, Bulgaria, Regular papers, Part 2, pp. 53 – 62.
[4] http://www.mathworks.com
[5] http://www.spectrum-soft.com/index.shtm

За контакти:

Йордан Райчев, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: s103304@stud.uni-ruse.bg

гл. ас. Адриана Бороджиева, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации", тел.: 082-888 734, e-mail: aborodjieva@ecs.uni-ruse.bg

Софтуерна реализация на четиритаблични шифри, базирани на шифъра на Playfair, с използване на MATLAB

автор: Сехяр Ахмедова
научен ръководител: гл. ас. Адриана Бороджиева

Software Implementation of Four-Square Ciphers Based on the Playfair Cipher Using MATLAB: *In this paper the principle of operation of the four-square ciphers is given. The publication describes the algorithm and the program module using MATLAB, designed for encryption and decryption of English texts using four-square ciphers. The module may be used by students studying the course "Telecommunications Security" and in other disciplines dealing with cryptographic methods the information protection.*
Key words: *cryptography, cryptosystems, Playfair cipher, four-square ciphers, MATLAB.*

ВЪВЕДЕНИЕ

Криптографията е наука за сигурността на информацията. Тя използва техники, като миниатюрни точки, маскиране на думи в изображения и други начини за скриване на информацията, която се съхранява или пренася.

Думата „криптография" е от гръцки произход и означава „тайнопис" („крипто" – таен, „графос" – пиша). Тя се използва още от древността, но намира огромно приложение в областта на компютърните науки и в наши дни.

Мрежовата сигурност, компресирането, интернет достъпът, заключването на персоналните компютри и криптирането на секретни съобщения са немислими без тази наука. И все пак, основната функция на криптографията си остава скриване на значението на съобщения, както и в някои случаи, скриване на процеса на предаване на самите съобщения (стеганография) [1].

ИЗЛОЖЕНИЕ

Четиритабличният шифър е ръчна техника за симетрично криптиране. Той е изобретен от известния френски криптограф Felix Delastelle.

Техниката криптира двойки букви (диграфи) и следователно попада в категорията на шифрите, известни като полиграфни субституционни шифри. Те добавят значителна мощ на криптирането, в сравнение с монографните субституционни шифри, които обработват единични символи. Използването на диграфи прави четиритабличната техника по-малко податлива на атаки на честотния анализ, тъй като анализът трябва да се направи върху 676 възможни диграфа, а не само върху 26 символа при монографното заместване. Честотният анализ на диграфи е възможен, но значително по-труден и обикновено изисква много по-голям шифриран текст, за да бъде полезен [2].

ОПИСАНИЕ НА ЧЕТИРИТАБЛИЧНИТЕ ШИФРИ

Четиритабличният шифър използва четири матрици с размерност 5 x 5, подредени в квадрат. Всяка от матриците с размерност 5 x 5 съдържа буквите от азбуката (обикновено се пропуска "Q" или се поставят двете букви "I" и "J" в една и съща клетка за намаляване на азбуката с цел „побиране" в матрицата). Като цяло, горната лява и долната дясна матрици са „квадратите на открития текст" и всяка от тях съдържа „стандартната" азбука. Горната дясна и долната лява матрици са „квадратите на шифрирания текст" и съдържат „смесена" азбучна последователност.

За да се генерират „квадратите на шифрирания текст", първо в клетките на матрицата се попълват буквите на дадена ключова дума, като се елиминират повтарящите се символи, а след това се допълват и останалите „липсващи" символи от азбуката. Ключът може да бъде написан в първите редове от таблицата, от ляво на дясно, или по някакъв друг модел [2].

Шифрирането на текст на английски език се реализира като предварително се извършват следните операции:

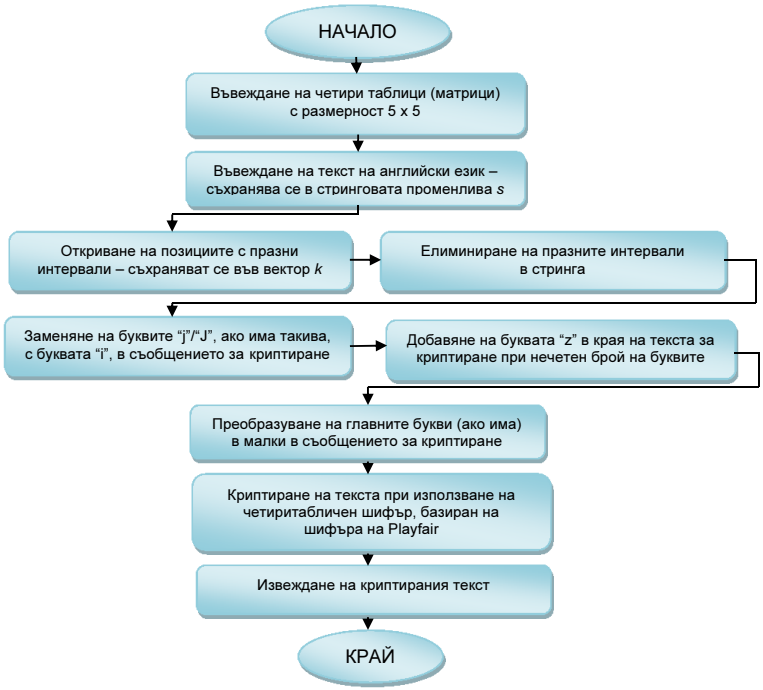
1) Откритият текст се разбива на двубуквени блокове (първи с втори символ, трети с четвърти и т.н.).

2) Общата дължина на откритият текст трябва да е четна, т.е. да съдържа четен брой символи. Ако това изискване е нарушено, в края на откритият текст се въвежда една от нискочестотните букви в английския език "z" или "x".

ОПИСАНИЕ НА РАЗРАБОТЕНИТЕ ПРИЛОЖЕНИЯ

Разработено е приложение (скрипт, m-файл) на програмен продукт MATLAB, чрез което се шифрира съобщение на английски език, въведено от потребителя.

Принципът на действие на разработеното приложение се описва със следната блок-схема (фиг. 1).



Фиг. 1 – Блок-схема на алгоритъма за криптиране на текст чрез четиритаблични шифри, базирани на шифъра на Playfair

КРИПТИРАНЕ

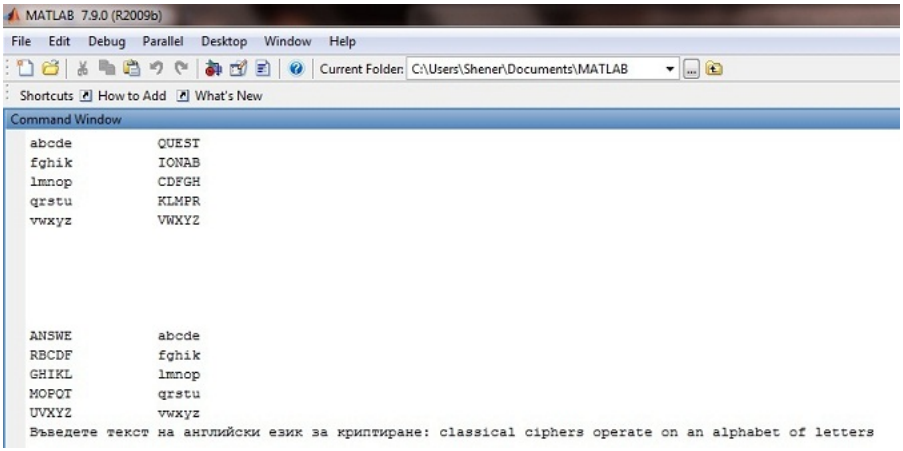
В примера за криптиране, който се разглежда в доклада, се използват четири матрици, съхранявани в променливите MA1, MA2, MA3, MA4. Матриците MA1 и MA4 съдържат буквите от „стандартната" азбука, а матриците MA2 и MA3 са изградени на базата на следните ключовите думи: за MA2 – QUESTION, за MA3 – ANSWER.

Разположението на матриците е в следната последователност:

MA1 MA2
MA3 MA4

Откритият текст, който ще се криптира в примера, е: "classical ciphers operate on an alphabet of letters".

На фиг. 2 се вижда извеждането на четирите матрици, чрез които ще се осъществи криптирането. След това програмата изисква потребителят да въведе текста за криптиране и изчаква въвеждането на текста от клавиатурата.



Фиг. 2 – Извеждане на четирите матрици и въвеждане на открития текст за криптиране

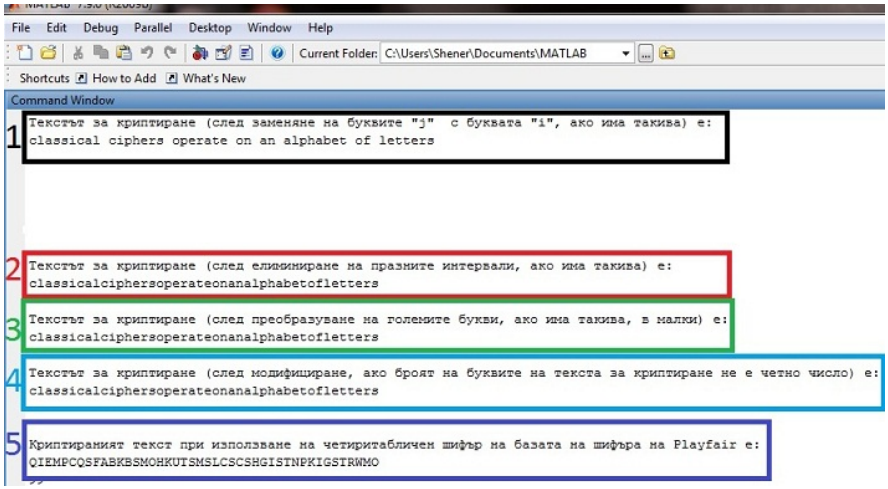
След въвеждането на съобщението за криптиране, следва претърсване на цялото съобщение за наличие на буквите "j"/"J" и ако бъдат открити, скриптът ги трансформира в буквата "i". Резултатът от тази операция може да се види в прозорец 1 на фиг. 3.

За да се криптира правилно откритият текст, трябва да се премахнат празните интервали между отделните думи. Резултатът след премахването на интервалите е показан в прозорец 2 на фиг. 3.

Ако има главни (големи) букви в откритият текст, те трябва да бъдат преобразувани в малки букви, като резулататът е показан в прозорец 3 на фиг. 3.

След направените модификации, скриптът проверява общата дължина на новополучения текст – дължината трябва да бъде четно число. Ако това изискване е нарушено, в края на откритият текст се въвежда една от нискочестотните букви в английския език "z" или "x" (в случая е избрано скриптът да въвежда буквата "z"). Резултатът се извежда в прозорец 4 на фиг. 3.

След като всичко това бъде изпълнено, може да се извърши и самото криптиране. Криптирането се извършва поблоково. За i-тия символ $s(i)$ се определят координатите *ra* и *ca*, указващи реда и стълба на съответния символ в матрица MA1. За $(i+1)$-вия символ $s(i+1)$ също се определят координатите *rb* и *cb*, указващи реда и стълба на съответния символ в матрица MA4. След откриването на двата символа от двубуквения блок на открития текст, се образува правоъгълник, като тези два символа са разположени в единия диагонал, свързващ матрица MA1 с матрица MA4, а символите в шифрирания текст, с които се заместват, са разположени в другия диагонал на формирания правоъгълник, диагонала, който свързва матрица MA2 с матрица MA3. По този начин се извършва криптирането на текстове с използване на четиритаблични шифри, базирани на шифъра на Playfair. Резултатът от криптирането се извежда в прозорец 5 на фиг. 3.



Фиг. 3. Заменяне на буквите "j"/"J" с буквата "i", елиминиране на празните интервали, преобразуване на главните букви в малки, проверка на броя на буквите в текста за криптиране, криптиране

ДЕКРИПТИРАНЕ

В примера за декриптиране, който се разглежда в доклада, се използват същите четири матрици, като при криптирането.

Шифрираният текст, който ще се декриптира в примера, е:

"QIEMPCQSFABKBSMOHKUTSMSLCSCSHGISTNPKIGSTRWMO".

Алгоритъмът за декриптиране съдържа аналогични етапи. Първоначално се извеждат четирите матрици, чрез които се осъществява декриптирането. След това програмата изисква потребителят да въведе текста за декриптиране и изчаква въвеждането на текста от клавиатурата. Освен това, с цел правилно декриптиране, е предвидена опция да се въведе вектор k, указващ позициите на празните интервали в откритият текст, които биват елиминирани при криптирането.

След въвеждането на съобщението за декриптиране, следва претърсване на цялото съобщение за наличие на буквите "j"/"J" и ако бъдат открити, скриптът ги трансформира в буквата "i". За да се декриптира правилно криптираният текст, отново трябва да се премахнат празните интервали във въведения криптиран текст. Ако има малки букви в шифрирания текст, те трябва да бъдат преобразувани в главни (големи) букви. След като всичко това бъде изпълнено, може да се извърши и самото декриптиране. Декриптирането се извършва поблоково. За *i*-тия символ се определят координатите *ra* и *ca*, указващи реда и стълба на съответния символ в матрица MA2. За $(i+1)$-вия символ също се определят координатите *rb* и *cb*, указващи реда и стълба на съответния символ в матрица MA3. След откриването на двата символа от двубуквения блок на шифрирания текст, се образува правоъгълник, като тези два символа са разположени в единия диагонал, свързващ матрица MA2 с матрица MA3, а символите в дешифрирания текст, с които се заместват, са разположени в другия диагонал на формирания правоъгълник, диагонала, който свързва матрица MA1 с матрица MA4. По този начин се извършва декриптирането на текстове с използване на четиритаблични шифри, базирани на шифъра на Playfair. Резултатът от декрипти¬ра¬нето е изведен на фиг. 4. При последното преобразуване се вмъкват и необходимите празни интервали между

думите, които са въведени предварително чрез вектора k (получен в процеса на шифриране).

Фиг. 4 – Заменяне на буквите "j"/"J" с буквата "i", елиминиране на празните интервали, преобразуване на малките букви в главни, декриптиране, вмъкване на празните интервали между отделните думи, с използване на вектора k, указващ позициите на празните интервали в шифрирания текст

ЗАКЛЮЧЕНИЕ

В публикацията е описан алгоритъм, заложен в програмен модул, с използване на MATLAB, създаден за шифриране и дешифриране чрез четиритаблични шифри, базирани на шифрите на Playfair, на текстове на английски език. Приложени са и резултатите от шифрирането и дешифрирането на произволен текст на английски език. Разработеният програмен модул може да намира приложение в учебния процес по дисциплината „Телекомуникационна сигурност", включена като задължителна в учебния план на специалността „Телекомуникационни системи" за образователно-квалификационна степен „Бакалавър", както и в други дисциплини, разглеждащи криптографските методи за защита на информацията. Бъдещата работа предвижда разработването на модул за шифриране и дешифриране на текстове на български език със съответното модифициране на квадратите, влизащи в състава на четиритабличния шифър.

ЛИТЕРАТУРА

[1] http://bg.wikibooks.org/wiki/Криптография
[2] http://en.wikipedia.org/wiki/Four-square_cipher

За контакти:

Сехяр Ахмедова, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: sesi_rs@abv.bg

гл. ас. Адриана Бороджиева, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации", тел.: 082-888 734, e-mail: aborodjieva@ecs.uni-ruse.bg

Разработване на програмни модули за синтез и анализ на електрически филтри, изучавани по дисциплината „Комуникационни вериги"

автор: Гергана Георгиева
научен ръководител: гл. ас. Адриана Бороджиева

Development of Software Modules for Analysis and Synthesis of Electrical Filter Studied in the Course "Communication Circuits": *In this paper software modules for synthesis and analysis of electrical filters (LC filters of type "K", LC filters of type "m", passive and active RC filters) are described. The modules will be used in the educational process in the course "Communication Circuits", included as compulsory in the curriculum of the specialty "Telecommunication Systems" for the Bachelor educational degree.*

Key words: *Communication circuits; LC filters, RC filters, MATLAB, MS Excel.*

ВЪВЕДЕНИЕ

Съгласно действащата в момента учебна програма по дисциплината „Комуникационни вериги", включена като задължителна в учебния план на специалността „Телекомуникационни системи", за образователно-квалификационна степен „Бакалавър", в Русенски университет „Ангел Кънчев", материалът обхваща следните три раздела: 1) Трептящи кръгове; 2) Електрически филтри; 3) Модулации [2].

Разделът „Електрически филтри", предвиден да се изучава в рамките на четири седмици, включва следните теми – реактивни (LC) филтри от тип "K", реактивни (LC) филтри от тип "m" – последователно-производни и паралелно-производни, пасивни RC филтри и активни RC филтри с един операционен усилвател по модела с едноконтурна и с многоконтурна отрицателна обратна връзка. Всички тези електрически филтри намират широко приложение в областта на телекомуникациите, което обосновава необходимостта от разработването на приложения, улесняващи синтеза и анализа на разглежданите електрически филтри.

В доклада се описва разработен MS Excel-базиран модул за синтез и анализ на електрически филтри, а също и софтуерна система, реализирана чрез средствата на MATLAB, за решаване на задачите от раздела „Електрически филтри", предвидени за самостоятелна работа на студентите в практическите упражнения по дисциплината „Комуникационни вериги".

ИЗЛОЖЕНИЕ

Съгласно учебната програма по дисциплината „Комуникационни вериги", темите, изучаващи електрически филтри, са формулирани, както следва [2]:

1. Проектиране и симулационно изследване на реактивни LC-филтри тип „K" – нискочестотни (НЧФ), високочестотни (ВЧФ), лентови (ЛФ) и режекторни (РФ). Изследване на влиянието на каскадно свързване на две и повече звена на LC-филтри тип „K".
2. Проектиране и симулационно изследване на реактивни филтри тип „m" – последователно-производни и паралелно-производни. Изследване на каскадното свързване на две и повече звена на LC-филтри тип „K" и тип "m".
3. Проектиране и симулационно изследване на пасивни RC-филтри – НЧФ, ВЧФ, ЛФ и РФ. Изследване на каскадното свързване на две и повече звена на пасивни RC-филтри.
4. Проектиране и симулационно изследване на активни RC-филтри с операционен усилвател по метода на едноконтурната и многоконтурната

отрицателна обратна връзка – НЧФ, ВЧФ и ЛФ. Изследване на каскадното свързване на две и повече звена на активни RC-филтри.

По време на практическите упражнения, преподавателят задава индивидуално задание на всеки студент, което по представените в [1, 2] методики студентът трябва да реши и да представи крайните резултати на преподавателя в края на упражнението. По-долу са посочени различните типове задачи от раздел „Електрически филтри".

Задача 1 (2.5.2). Да се определи честотата, за която затихването на нискочестотно звено тип „K", е $\alpha = \ldots dB$, ако граничната му честота е $f_c = \ldots kHz$. **(Тема 1)**

Задача 2 (2.5.3). Да се изчислят елементите на високочестотно Т-образно филтрово звено тип „K" с номинално характеристично съпротивление $R = \ldots \Omega$ и гранична честота $f_c = \ldots kHz$. Да се определят стойностите на собственото затихване, коефициента на фазата и входния импеданс на звеното Z_T при съгласувано натоварване за честоти $f_1 = \ldots kHz$ и $f_2 = \ldots kHz$. **(Тема 1)**

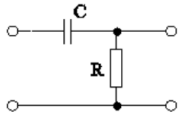
Задача 3 (2.5.6). Да се изчислят елементите $0{,}5.L_{1m}$, $2.L_{2m}$ и $0{,}5.C_{2m}$ на последователно-производно нискочестотно филтрово полузвено с гранична честота $f_c = \ldots kHz$, номинално характеристично съпротивление $R = \ldots \Omega$ и коефициент $m = \ldots.$ Да се определи честотата, при която затихването става безкрайно голямо. **(Тема 2)**

Задача 4 (2.5.8). Да се изчислят елементите $0{,}5.L_{1m}$, $2.C_{1m}$ и $2.L_{2m}$ на паралелно-производно високочестотно филтрово полузвено с гранична честота $f_c = \ldots kHz$, номинално характеристично съпротивление $R = \ldots \Omega$ и коефициент $m = \ldots.$ Да се определи честотата, при която затихването става безкрайно голямо. **(Тема 2)**

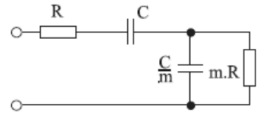
Задача 5 (3.4.2). Да се изчислят елементите на високочестотно филтрово звено (фиг. 1), което да има гранична честота $f_c = \ldots kHz$. Да се определят стойностите на модула и фазата на коефициента на предаване, и стойността на затихването за честоти $f_1 = \ldots kHz$, $f_2 = \ldots kHz$ и $f_3 = \ldots kHz$. За стойност на съпротивлението да се приеме, че $R = \ldots k\Omega$. **(Тема 3)**

Задача 6 (3.4.3). Четириполюсникът на фиг. 2 представлява лентов филтър (схема на Робинзон-Вин). Да се определят изразите за амплитудно-честотната характеристика (АЧХ), затихването и фазово-честотната характеристика (ФЧХ) на този филтър във функция от $x = \omega CR$ при работа на празен ход. Да се пресметнат качественият фактор, коефициентът на усилване в лентата на пропускане и средната честота на филтъра, ако $m = \ldots.$ Да се определят стойностите на АЧХ, ФЧХ и затихването, ако лентовият филтър има средна честота $f_0 = \ldots kHz$, $R = \ldots k\Omega$ и $m = \ldots$ за честоти $f_1 = \ldots kHz$ и $f_2 = \ldots Hz$. **(Тема 3)**

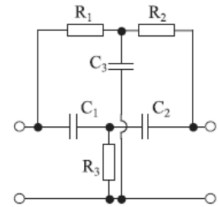
Задача 7 (3.4.5). Да се изчислят елементите на режекторен RC-филтър по схемата от фиг. 3, предназначен за подтискане на смущенията от електрическа мрежа с честота $f = 50Hz$. За стойност на съпротивлението във филтъра да се приеме, че $R = \ldots k\Omega$. Честотата на безкрайно голямо затихване трябва да бъде $f_\infty = 50\ Hz$. **(Тема 3)**



Фиг. 1 – Високочестотен пасивен RC филтър



Фиг. 2 – Лентов RC филтър по схемата на Робинзон-Вин



Фиг. 3 – Режекторен RC филтър, „двоен Т-мост"

Задача 8 (3.4.8). Да се синтезира лентов филтър чрез метода с операционен усилвател с едноконтурна отрицателна обратна връзка, който да има средна честота $f_0 = \ldots Hz$ и да реализира следната предавателна функция $T(p) = -\frac{\ldots p}{\ldots p^2 + \ldots p + \ldots}$. Денормирането по съпротивление да се извърши с $R_N = \ldots k\Omega$. Да се изчисли полюсният качествен фактор на схемата. **(Тема 4)**

Задача 9 (3.4.10). Да се синтезира по метода с многоконтурна отрицателна обратна връзка високочестотен филтър, имащ следната предавателна функция по напрежение $T(p) = -\frac{\ldots p^2}{\ldots p^2 + \ldots p + \ldots}$. Звеното да има гранична честота $f_c = \ldots Hz$ и елементите му да се денормират по съпротивление с $R_N = \ldots k\Omega$. **(Тема 4)**

РЕЗУЛТАТИ

Разработен е MS Excel-базиран модул за синтез (оразмеряване) и анализ (определяне на стойностите на търсени параметри при зададена схема) на електрическите филтри, предвидени за разглеждане по време на практическите упражнения по дисциплината „Комуникационни вериги". Модулът позволява удобно таблично представяне на резултатите, улесняващи дейността на преподавателя. Приложението обхваща оразмеряването на Т-образно високочестотно филтрово звено тип „K", последователно-производно нискочестотно филтрово полузвено от тип „m", паралелно-производно високочестотно филтрово полузвено от тип „m", високочестотно RC-филтрово звено, лентов RC-филтър по схемата на Робинзон-Вин, режекторен RC-филтър по схемата „двоен Т-мост", активен лентов RC-филтър чрез метода с операционен усилвател с едноконтурна отрицателна обратна връзка и активен високочестотен RC-филтър по метода с многоконтурна отрицателна обратна връзка. Алгоритмите за синтез и анализ на разглежданите комуникационни вериги са представени в [1, 2, 3]. Маркираните в таблиците клетки са първоначално зададените от преподавателя стойности. В доклада са приложени таблици, съдържащи резултатите от синтеза и анализа на разглежданите електрически филтри.

Таблица 1. Решаване на задача 1

f_c,kHz	α,dB	α,Np	0,5.α,Np	ch(0,5.α)	f,kHz
8	25	2,8750	1,4375	2,2238	17,791

Таблица 2. Решаване на задача 2

		ЛП	ЛЗ					индукт.				акт.		
f_c,kHz	R,Ω	f_1,kHz	f_2,kHz	α_1,Np	α_1,dB	β_1,rad	β_1,°	Z_{T1},Ω	α_2,Np	β_2,rad	β_2,°	Z_{T2},Ω	C_1,nF	L_2,mH
1	600	0,5	2	2,634	22,878	$-\pi$	−180	j 1039,2	0	-1,047	-60,00	519,6	132,6	47,7

за Г-схема		за П-схема		за Т-схема		Т	П
$2C_1$,nF	$2L_2$,mH	C_1,nF	$2L_2$,mH	$2C_1$,nF	L_2,mH	R_L,Ω	R_L,Ω
265,3	95,5	132,6	95,5	265,3	47,7	480	750

Таблица 3. Решаване на задача 3

				K		K, Г-схема		m		
R,Ω	f_c,kHz	m	f_∞,Hz	L_1,mH	C_2,nF	0,5.L_1,mH	0,5.C_2,nF	L_{1m},mH	C_{2m},nF	L_{2m},mH
600	1	0,542	1190	190,99	530,52	95,49	265,26	103,51	287,54	62,21

m, Г-схема			m, П-схема				
0,5.L_{1m},mH	0,5.C_{2m},nF	2.L_{2m},mH	0,5.C_{2m},nF	2.L_{2m},mH	1.L_{1m},mH	0,5.C_{2m},nF	2.L_{2m},mH
51,76	143,77	124,43	143,77	124,43	103,51	143,77	124,43

Таблица 4. Решаване на задача 4

				K		K, Г-схема		m		
R,Ω	f_c,kHz	m	f_∞,Hz	C_1,nF	L_2,mH	2.C_1,nF	2.L_2,mH	C_{1m},nF	L_{1m},mH	L_{2m},mH
600	1	0,542	840,38	132,63	47,75	265,26	95,49	244,70	146,57	88,09

m, Г-схема			m, Т-схема				
2.C_{1m},nF	0,5.L_{1m},mH	2.L_{2m},mH	2.C_{1m},nF	0,5.L_{1m},mH	1.L_{2m},mH	2.C_{1m},nF	0,5.L_{1m},mH
489,41	73,29	176,19	489,41	73,29	88,09	489,41	73,29

Таблица 5. Решаване на задача 5

R,kΩ	f_c,kHz	f_1,kHz	f_2,kHz	f_3,kHz	C,nF	x_1	x_2	x_3	T_1	T_2	T_3
10	0,1	0,01	0,1	0,3	159,15	0,10	1	3,00	0,0995	0,7071	0,9487

α_1,dB	α_1,Np	α_2,dB	α_2,Np	α_3,dB	α_3,Np	φ_1,°	φ_2,°	φ_3,°
20,0432	2,3050	3,0103	0,3462	0,4576	0,0526	84,2894	45,0000	18,4349

Таблица 6. Решаване на задача 6

R,kΩ	f_0,kHz	m	f_1,kHz	f_2,kHz	C,nF	x_1	x_2	T_1	T_2	α_1,dB	α_1,Np	α_2,dB	α_2,Np
10	0,05	1	0,01	1	318,31	0,20	20,00	0,1767	0,0496	15,0569	1,7315	26,0960	3,0010

φ_1,°	φ_2,°	Q	k_0	R_1,kΩ	R_2,kΩ	C_1,nF	C_2,nF
57,9946	-81,4482	0,3333	0,3333	10	10	318,3099	318,3099

Таблица 7. Решаване на задача 7

R,kΩ	f_∞,Hz	C,nF	R_1,kΩ	R_2,kΩ	R_3,kΩ	C_1,nF	C_2,nF	C_3,nF
10	50	318,31	10	10	5	318,31	318,31	636,62

Таблица 8. Решаване на задача 8

a	b_1	b_0	R_N,kΩ	f_0,Hz	ст.	R_a	C_a	R_{1b}	R_{2b}	C_{1b}	C_{2b}
7	0,55	1	100	1000	H	0,1429	12,7273	0,5128	0,0372	1,0000	52,4483
					Д,nF/kΩ	14,2857	20,2561	51,2821	3,7179	1,5915	83,4740
					C,nF/kΩ	15,0000	20,0000	51,0000	3,6000	1,6000	82,0000

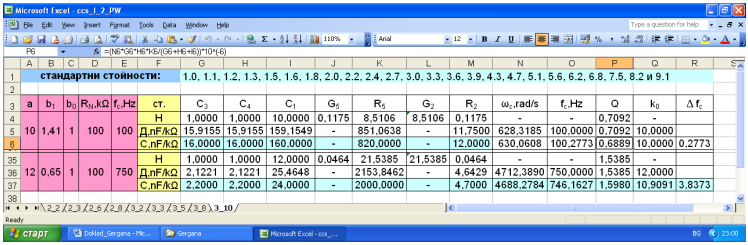
ω_0,rad/s	f_0,Hz	Q	k_0	Δf_0
-	-	1,8182	-	
6283,1853	1000,0000	1,8182	0,7997	
6443,1278	1025,4556	1,7766	0,7631	25,4556

Таблица 9. Решаване на задача 9

a	b_1	b_0	R_N,kΩ	f_c,Hz	ст.	C_3	C_4	C_1	G_5	R_5	G_2	R_2
10	1,41	1	100	100	H	1,0000	1,0000	10,0000	0,1175	8,5106	8,5106	0,1175
					Д,nF/kΩ	15,9155	15,9155	159,1549	-	851,0638	-	11,7500
					C,nF/kΩ	16,0000	16,0000	160,0000	-	820,0000	-	12,0000

ω_c,rad/s	f_c,Hz	Q	k_0	Δf_c
-	-	0,7092	-	
628,3185	100,0000	0,7092	10,0000	
630,0608	100,2773	0,6889	10,0000	0,2773

На фиг. 4 е показана снимка на екрана с разработената система с работен лист, илюстриращ процеса на оразмеряване на активен високочестотен RC-филтър по метода с многоконтурна отрицателна обратна връзка (Задача 9). Интересен момент при Задача 8 и Задача 9 е изборът на стандартни стойности на съпротивленията на резисторите и капацитетите на кондезаторите и изследването на влиянието им върху основните параметри на схемата – средна или гранична честота, качествен фактор и коефициент на усилване в лентата на пропускане.

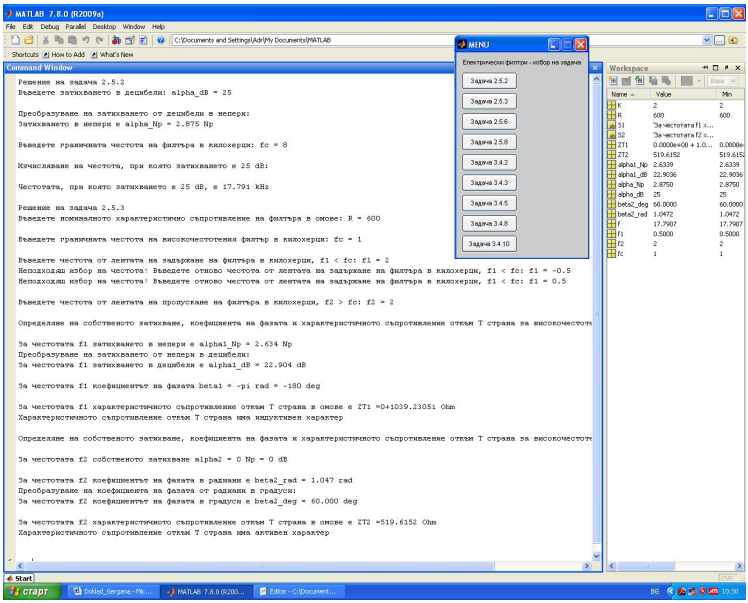


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	стандартни стойности:						1.0, 1.1, 1.2, 1.3, 1.5, 1.6, 1.8, 2.0, 2.2, 2.4, 2.7, 3.0, 3.3, 3.6, 3.9, 4.3, 4.7, 5.1, 5.6, 6.2, 6.8, 7.5, 8.2 и 9.1									
2																		
3	a	b_1	b_0	R_N,kΩ	f_c,Hz	ст.	C_3	C_4	C_1	G_5	R_5	G_2	R_2	ω_c,rad/s	f_c,Hz	Q	k_0	Δf_c
4						H	1,0000	1,0000	10,0000	0,1175	8,5106	8,5106	0,1175	-	-	0,7092	-	
5	10	1,41	1	100	100	Д,nF/kΩ	15,9155	15,9155	159,1549	-	851,0638	-	11,7500	628,3185	100,0000	0,7092	10,0000	
6						C,nF/kΩ	16,0000	16,0000	160,0000	-	820,0000	-	12,0000	630,0608	100,2773	0,6889	10,0000	0,2773
35						H	1,0000	1,0000	12,0000	0,0464	21,5385	21,5385	0,0464	-	-	1,5385	-	
36	12	0,65	1	100	750	Д,nF/kΩ	2,1221	2,1221	25,4648	-	2153,8462	-	4,6429	4712,3890	750,0000	1,5385	12,0000	
37						C,nF/kΩ	2,2000	2,2000	24,0000	-	2000,0000	-	4,7000	4688,2784	746,1627	1,5980	10,9091	3,8373

Фиг. 4 – Снимка на екрана с разработената система

Разработен е и скрипт на MATLAB, filtersSA.m, позволяващ решаването на посочените по-горе задачи. На фиг. 5 е показана снимка на екрана при изпълнението на скрипта с командния прозорец и с работното пространство, които илюстрират процесите на анализ на нискочестотно филтрово звено тип „K" (при избор на Задача 2.5.2), включващ определянето на затихването на филтъра при зададена честота от лентата на задържане на филтъра и при известна гранична честота на филтъра, и на оразмеряването на Т-образно високочестотно филтрово звено тип „K" (при избор на Задача 2.5.3). На фиг. 5 се вижда менюто, което се извежда на екрана при изпълнение на скрипта и чрез което се извършва избора на задачата за решаване. Вижда се, че резултатите на фиг. 5 и тези в табл. 1 и табл. 2 са еднакви.

Предимството при използване на MATLAB в случая е възможността за контролиране на въвежданите от студента данни, например, проверките, извършвани за честотитите fc, f1 и f2, и извеждане на съобщение „Неподходящ избор на честотата" и подканване за ново въвеждане на данни (фиг. 5).



Фиг. 5 – Снимка на екрана от изпълнението на скрипта filtersSA.m в MATLAB

ЗАКЛЮЧЕНИЕ

Работата е продължение на разработения и описания в [3] модул за синтез и анализ на трептящи кръгове. Разработените приложения, на базата на MATLAB и MS EXCEL, и описани в доклада, ще намират приложения в учебния процес по дисциплината „Комуникационни вериги". Бъдещата работа предвижда разработването на подобни приложения за решаване на задачи и от раздела „Модулации", улесняващи студентите в практическите упражнения по „Комуникационни вериги".

ЛИТЕРАТУРА

[1] Манукова, А., А. Бороджиева. Комуникационни вериги – ръководство за упражнения. Русе, 2002.
[2] http://ecet.ecs.uni-ruse.bg/else/index.php?lang=bg
[3] http://conf.uni-ruse.bg/bg/docs/sns/2011/SNS2011-EEA.pdf

За контакти:

Гергана Георгиева, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: giga71423@abv.bg

гл. ас. Адриана Бороджиева, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации", тел.: 082-888 734, e-mail: aborodjieva@ecs.uni-ruse.bg

Телевизия с висока разделителна способност

автор: Валя Василева
научен ръководител: доц. д-р Теодор Илиев

HD television: *The term high definition once described a series of television systems originating from the late 1930s. These systems were only high definition when compared to earlier systems that were based on mechanical systems with as few as 30 lines of resolution. Since the formal adoption of digital video broadcasting's (DVB) widescreen HDTV transmission modes in the early 2000s the 525-line NTSC (and PAL-M) systems as well as the European 625-line PAL and SECAM systems are now regarded as standard definition television systems. In Australia, the 625-line digital progressive system (with 576 active lines) is officially recognized as high-definition.*
Key words: *High definition, systems, digital.*

ВЪВЕДЕНИЕ

HDTV (High Definition TeleVision) е цифрова телевизионна система с по-висока разделителна способност от традиционните системи, като PAL, SECAM и NTSC.

HDTV прави възможно да се наслаждаваме на домашни забавления с невероятна картина и звук. Независимо дали гледаме HDTV канал, гледаме филм на Blu-Ray Disc или играем игри, от героите и сцените на екрана струи живот. Това се дължи на много по-високата разделителна способност при HDTV устройствата, които създават изключително ясна и детайлна картина.

Фиг. 1 – HDTV картина

Класическата телевизионна картина представлява множество точки. Ако гледаме същия образ (фиг. 1.1) на по-голям екран, картината ще изгуби своят контраст и яснота и ще стане леко размазана. Цветовете на HDTV са наситени, образът съдържа повече детайли и е най-високата резолюция, предлагана от появата на телевизионното излъчване [1].

ИЗЛОЖЕНИЕ

Видове разделителна способност:

720x576 (4:3)

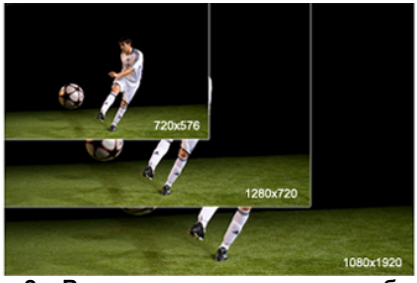
Телевизорите със стандартна разделителна способност са със 720x576 пиксела или 576 реда с по 720 пиксела (стандарта PAL);

1280x720 (16:9)

Телевизорите с разделителна способност са с 1280x720 пиксела или 720 реда с по 1280 пиксела;

1920x1080 (16:9)

Телевизорите с разделителна способност са с 1920x1080 пиксела или 1080 реда с по 1920 пиксела. Тоя вид разделителна способност е най-разширеният и най-добрият вариант.



Фиг. 2 – Видове разделителна способност

Колкото повече пиксели има, толкова по-добра разделителна способност и по-фини детайли ще имаме.

Телевизорите, които са способни да визуализират HDTV с разделителна способност 1080p, се наричат Full HD, а тези, които визуализират 720p и 1080i – HD Ready.

Full HD и HD Ready

Full HD представлява оптимално решение за HD с хоризонтални 1080 реда в кадър. Това означава, че телевизора може да се свърже с Handycam, Cyber-Shot, Blu-ray Disc плейър или Playstation 3 конзола за пълна Full HD система;

HD Ready (относителна готовност) е с минимална разделителна способност от 720 хоризонтални реда с информация за всеки отделен кадър. Такива телевизори могат да приемат HD видео формати в режим 720p и 1080i, но не могат да възпроизвеждат пълна разделителна способност от по-съвременните 1080p източници. Изображенията може да са деформирани малко, но все пак се получава много добро качество на изображението при Blu-ray Disc и игри на Platstation 3. За да се използва тази емблема, телевизорът трябва да е широкоекранен и задължително да има вход за аналогов компонентен сигнал и DHMI връзка [2].

Предимства на HDTV:

- Многократно по-детайлна картина с много ясен образ – Наситеността на телевизионните пиксели на квадратен сантиметър е многократно по-голяма от тази на SD (Standart Definition). От това идва по-голямата плътност и качество на изображението. Резолюцията обикновено е между 1280x720 и 1920x1080, което е от 3 до 6 пъти повече от тази на PAL DVD 720x486 или NTSC DVD 648x486;

Фиг. 3 – Разлика между HD и SD

- Изкрящи цветове – Отношението между най-светлата част и най-тъмната част на екрана се нарича контраст. HDTV има по-висок коефициент на контраст от SDTV, затова възпроизвежда черния цвят много близо до истинското черно и показва повече подробности и по-наситени цветове на слабо осветени сцени;

Фиг. 4 – Разлика между HDTV и SD

- Широк екран – Увеличената резолюция в прогресивен разгънат образ създава още по-ясна картина. HDTV има екранно покритие от 16:9, за разлика от някои телевизионни емисии с екранно покритие 4:3. В света все повече телевизионни програми преминават на разпространение 16:9;
- Пространствен звук – HDTV използва стандарта Dolby Digital 5.1 или AC-3 технология, която осигурява 6-канален звук. Пет независими канала осигуряват звук за 5 точки, разположени в пространството около нас, а допълнителния канал е предназначен за subwoofer (нискочестотен говорител) [3].

ЗАКЛЮЧЕНИЕ

В България все повече навлиза HDTV. Тя внася ново измерение в реалността и осигурява истински емоционално изживяване. Когато гледаме HDTV наистина се чувстваме "Все едно сме там".

ЛИТЕРАТУРА

[1] http://www.onastra.bg/4116072/hdtv
[2] http://blog.chiliev.com/?p=3603
[3] http://wwwcores.cores.biz/video/cat01/post_1/

За контакти:

Валя Василева, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: malka_f@mail.bg

доц. д-р Теодор Илиев, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации'', тел.: 082-888 665, e-mail: tiliev@ecs.uni-ruse.bg

Анализ на функционалността на Microsoft Lync Server

автор: Джюнеит Ахмедов
научен ръководител: гл. ас. д-р Пламен Захариев

Analysis of the functuality of Microsoft Lync Server: *The Lync Server (previously Microsoft Office Communications Server) is an enterprise real-time communications server, providing the infrastructure for enterprise instant messaging, presence, file transfer, peer-to-peer and multiparty voice and video calling, ad hoc and structured conferences (audio, video and web) and, through a 3rd party gateway or SIP trunk, PSTN connectivity [1]. These features are available within an organization, between organizations, and with external users on the public internet, or standard phones, on the PSTN as well as SIP trunking [2]. In this paper I outline some of the functionality requirements and the characteristics of this platform. Additionally I present some of the installation scenarios, which can provide a better overlook of the tools and services, which this powerful platform can provide.*

Key words: *Unified communications, Lync server.*

ВЪВЕДЕНИЕ

В условията на нарастваща глобализация, компаниите и организациите непрекъснато се изправят пред повишаващите се изисквания за все по-високи нива на обслужване при по-ниски оперативни разходи. Това се превръща в корпоративна политика. Унифицирането на комуникации ще помогне да се отговори на тези предизвикателства. [3]

Унифицираните комуникации (Unified Communications, UC) са един от най-новите сегменти в пазара на корпоративните ИТ решения. Тази концепция обединява няколко направления на информационните и комуникационни технологии, които дълго време се развиха паралелно - корпоративна телефония, контакт-центрове, VoIP, аудио- и видеоконференции, технологии за обмен на съобщения, Web-портали и бизнес приложения. С други думи интегриране в едно цяло на комуникации, които не се осъществяват в реално време с услуги в реално време [4, 5].

ИЗЛОЖЕНИЕ

Microsoft Lync предоставя търсеното решение, обединявайки различните начини, по които хората комуникират помежду си в общ, единен интерфейс. Платформата свързва потребителите навсякъде и по всяко време, независимо от технологията, която използват в момента – компютър, телефон или браузър. Тя интегрира мигновени съобщения, аудио, видео и уеб конференции и гласови комуникации, работи отлично с приложенията, които потребителите и бизнесът използват ежедневно като Microsoft Office, Microsoft SharePoint и Microsoft Exchange [6].

Lync обединява три основни инструмента: IM (незабавни съобщения), видеоконференции и телефонни обаждания (Фиг. 1).

Съществуват няколко типа инсталации на Microsoft Lync Server – базова, разширена и глобална. В зависимост от броя на потребителите и нуждите на корпорацията се взема решени за типа на инсталацията.

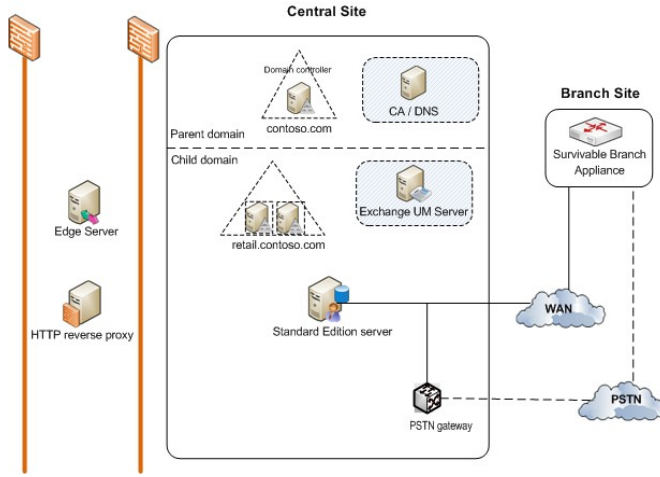
Фиг. 1 – Microsoft Lync

БАЗОВА ИНСТАЛАЦИЯ НА КОМУНИКАЦИОННАТА СИСТЕМА

Базовата инсталация покрива всички функции на комуникационния софтуер в една корпоративна мрежа на най-ниска цена. Препоръчва се за корпорации със сравнително малък брой служители, поради ограничението от 5000 потребители за този тип инсталация [7].

При тази инсталация комуникационната архитектура се състои от два сървъра-домейн контролера и самия комуникационен сървър (Standard Edition), които са разположени в една активна директория (Фиг. 2).

Предлага се вариант, при който може да се увеличи броят на потребителите при тази конфигурация. За целта е необходимо да се добави още един Standard Edition Server. Добавянето на втория сървър дава възможност да се увеличи не само броят на потребителите, а и надеждността на системата, както и да намали натоварването [7].



Фиг. 2 – Базово интегриране на системата

В организацията използваща топологията разгледа на Фиг. 2 се прилага

резервираност на Voice Enterprise функцията на комуникационния сървър между две територии. Резервираността се налага поради факта, че клоновия сайт не разполага с надеждна WAN връзка към централния сайт, поради това там се разполага един Survivable Branch Appliance. Ролята на това устройство е да подържа някои основни комуникационни функции (мигновени съобщения, гласова поща и обаждане) при проблем с WAN връзката [7].

Ако искаме да интегрираме Microsoft Lync Server като напълно обединена комуникационна мрежа и да премахнем съществуващата PBX система, освен добавяне на втори Lync Server можем да организираме 'басейн' от Front End сървъри [7].

Този басейн всъщност представлява съвкупност от Front End сървъри, конфигурирани идентично, които работят заедно, за предоставяне на услуги на обща група потребители. Басейнът предоставя мащабируемост и възможност за защита при срив на потребителите си.

Front End сървъра всъщност е основният сървър в Lync, който обработва много негови основни функции [8].

Въпреки, че не е необходимо, но се препоръчва инсталирането на Edge Server, дори и за малки организации. Това се прави с цел, за да се предоставят услуги на потребители, които понастоящем са извън защитните стени на дадената организация. Ползите от това са:

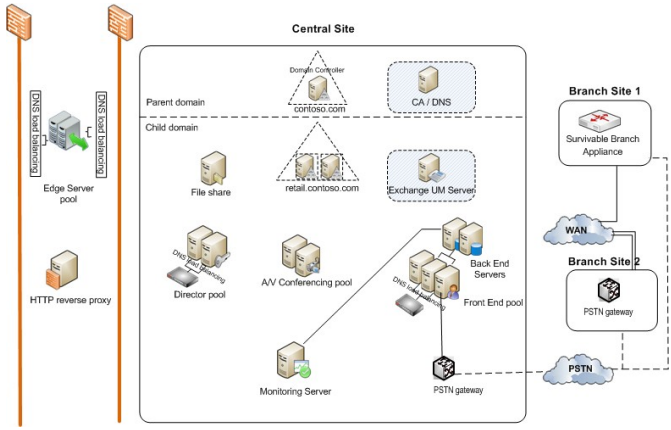
- Потребители на дадена фирма могат да се възползват от функциите на Lync сървъра, дори и когато са си у дома или на път;
- Ако организацията има партньори или клиенти, които също използват Lync Server, може да се създаде специална връзка между тези организации, което от своя страна ще допринесе до по добро им сътрудничество;
- Edge Server дава възможност да се обменят незабавни съобщения между потребители на Lync Server и потребители, които нямат Lync с малко помощ от Windows Live, AOL, Yahoo, Google Talk и Jabber (за последните две е необходимо и XMPP gateway) [7].

РАЗШИРЕНА ИНСТАЛАЦИЯ НА КОМУНИКАЦИОННАТА СИСТЕМА

Разширената инсталация е предназначена за малки или средни по големина организации от 5000 до 30 000 потребители с възможност за увеличаване броя на потребителите на повече от 30 000. На следващата Фиг. 3 е разгледан случай, при който броят на потребителите е 15 000 [9].

При тази инсталация както и при всички инсталации на Microsoft Lync Server, домейн контролера и самия комуникационен сървър се намират в една обща директория гора (contoso.com).Освен първите два сървъра тук имаме още три допълнителни сървъра – Front End, A/V Conferencing и Director.

Функцията на A/V Conferencing сървърът е да осигурява възможност за аудио и видео конференции. Той може да бъде инсталиран заедно с Front End Server на една физическа машина или да бъде разделен като самостоятелен. Ако се инсталира отделно трябва да се има предвид, че е нужен по един сървър на всеки 20 000 потребители. Въпреки, че дадения пример е за организация с по малък брой потребители от 20 000, се използват два A/V Conferencing сървъра за по голяма надеждност и отказоустойчивост. Поради същата причина са организирани и Front End pool и Director pool [9].



Фиг. 3 – Разширено интегриране на системата [9]

Разглежданата топология разполага с два отделни клонови сайта – Branch Site1и Branch Site2. Поради факта, че главния сайт и Branch Site1 не разполагат с надеждна WAN връзка, там е разположен Survivable Branch Appliance, който ще поддържа много от функциите на комуникационния сървър, в случай отпадане на WAN свързаността. Наличието на PSTN gateway в клон 2 е достатъчен, понеже на това място връзката е устойчива [9].

ЗАКЛЮЧЕНИЕ

Microsoft Lync Server 2010 предоставя на потребителите добре организирани рационални комуникации, така че те лесно могат да намерят и комуникират с правилния човек, директно от приложенията, които използват най-често (например Microsoft SharePoint). С помощта на Microsoft Lync Server се премахва нуждата от скъпи подобрения на инфраструктурата и комуникационната мрежа, а освен това се предоставя разнообразно комуникиране, включително софтуерен VoIP, Web - конферентни обаждания и изпращането на текстови съобщения и много други.

Microsoft Lync Server 2010 предоставя възможността за комуникиране между потребителите от множество устройства, когато е необходимо, без значение къде се намират, използвайки само интернет връзка и то без изискване за виртуална частна мрежа (VPN).

Потребителите могат да се свържат с търсения от тях човек по много ефективен метод-те могат да проверят достъпността на автора на даден документ и просто да проведат телефонно обаждане директно от Microsoft Outlook.

ЛИТЕРАТУРА

[1] Microsoft Lync Server 2010 Unleashed By Alex Lewis, Andrew Abbate, Tom Pacyk
[2] http://en.wikipedia.org/wiki/Microsoft_Lync_Server
[3]http://cio.bg/1955_edinni_resheniya_za_unificirani_komunikacii_na_siemens_enterprise_communications
[4] http://cio.bg/3141_obedinenite_komunikacii__resheniya_dostavchici_perspektivi.0
[5]http://cio.bg/2621_integriranite_komunikacii__tochniyat_chovek_za_tochnata_rabota_v_tochniya_moment
[6] http://www.computermagazine.bg/bg/Статии/Комуникации/ Microsoft-Lync/547/
[7] http://technet.microsoft.com/en-us/library/gg398095.aspx
[8] http://technet.microsoft.com/en-us/library/gg398536.aspx
[9] http://technet.microsoft.com/en-us/library/gg425939.aspx

За контакти:

Джюнеит Ахмедов, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: jibriu_cice@abv.bg

гл. ас. д-р Пламен Захариев, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации", тел.: 082-888 663, e-mail: pzahariev@uni-ruse.bg

Анализ на UMTS и HSPA технологиите при мобилни мрежи от трето поколение

автор: Валентин Коларов
научен ръководител: ас. Григор Михайлов

3G or 3rd generation mobile telecommunications is: *a generation of standards for mobile phones and mobile telecommunication services fulfilling the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union. Application services include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile environment.*

Key words: *mobile telecommunication International Telecommunication Union telephone, mobile Internet video calls mobile TV.*

ВЪВЕДЕНИЕ

Понятието мобилни комуникации може да бъде разгледано в широк и тесен смисъл, според степента на общност, която му придаваме. В широк смисъл то отразява обмена на информация без наличието на някаква фиксирана стационарна мрежа и без да е необходимо включването на абонатите към мрежата през някакви специални физически точки за достъп. В светлината на това широко по смисъл определение към мобилните комуникации можем да причислим системите за радиокомуникации, системите за радио и телевизионно ефирно разпръскване, както и системите, използващи звукови и светлинни сигнали за обмен на информация.

ИЗЛОЖЕНИЕ

Приложение на услугите от трето поколение

Третото поколение мобилни системи открива новия свят на възможнос¬тите на мобилните услуги. Това са нови начини за комуникация, достъп до информация, управление на бизнеса, обучение и забавления.

В близко бъдеще мобилността няма да бъде само атрактивен атрибут - тя ще стане основен аспект на много услуги. Очакванията са за високоскоростен достъп до услуги на Интернет, забавления, информация и електронна търго¬вия където и да е, не само пред компютъра или пред телевизора. Възможни са следните приложения:

- Информационни: търсене в WWW (World Wide Web), интерактивно (диалогово) пазаруване, он-лайн еквиваленти на печатни издания, он-лайн преводи, локално разположени разпръсквателни радиоуслуги, инте¬лигентно търсене и филтриращи удобства за достигане до желаната ин¬формация;
- Образование: виртуално училище, он-лайн научни лаборатории, он- лайн научни библиотеки, он-лайн езикови упражнения;
- Развлечения: избор на аудио- и видеопрограми (като алтернатива на CD, касетофон или радио), игри по избор, виртуални изображения;
- Обществени услуги: аварийни ситуации, правителствени процедури, проучване на общественото мнение;
- Бизнес информация: подвижен офис, виртуални работни групи, бизнес конференции;
- Комуникационни услуги: телефон, видеотелефон, видеоконференция, персонално локализиране;
- Финансови услуги: виртуална банка, он-лайн заплащане, универсална SIM карта и кредитна карта.

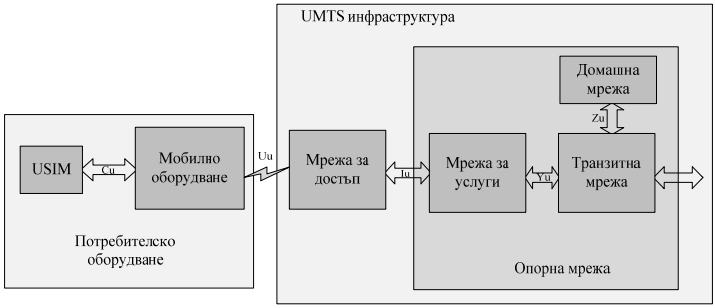
UMTS и HSPA технологиите при мобилни мрежи от трето поколение

Обща архитектура на UMTS

Общата структура на UMTS може да бъде представена от една страна като система от физическите компоненти, които я изграждат, а от друга страна като система от функции. Във връзка с това физическите аспекти на архитектурата се разглеждат чрез използване концепцията на областите, а функционалните аспекти – чрез използване концепцията на слоевете.

Области в архитектурата на UMTS

Главните области в архитектурата на UMTS и връзката между тях, под формата на интерфейси е показана на фиг 1.



Фиг. 1 – Обща физическа архитектура на UMTS

Основновното разделяне във физическата архитектура е при радиоинтерфейса Uu, в резултат на което се обособяват две основни части на архитектурата: потребителско оборудване и инфраструктура. Често този важен интерфейс бива означаван и като UTRA (UMTS Terrestrial Radio Access), а мрежата за достъп като UTRAN (UMTS Terrestrial Radio Access Network). Модулът за идентификация на абоната се обозначава като USIM (User Services Identity Module).

Мрежата за достъп съдържа физическите обекти, които осигуряват и управляват радиоресурсите на системата, за да предоставят достъп на потребителите до компонентите на опорната мрежа на системата: мрежа за услуги и транзитна мрежа.

Опорната мрежа се състои от физическите обекти, които осигуряват телекомуникационните услуги и мрежовата свързаност в системата. Опорната мрежа е разделена на три основни части:

- мрежа за услуги, която представя функциите на опорната мрежа, свързани към точката за достъп на потребителя и неговата мобилност – прехвърляне на повикванията и пренос на данни;
- домашна мрежа, която представя функции на системата за съхраняване и предоставяне не специфична за потребителя и определени услуги информация, която не е свързана с конкретна точка за достъп на потребителя и мобилността му – информация за идентификация и потребителския профил;
- транзитна мрежа – освен за връзка между вътрешните части на опорната мрежа, служи и за връзка с външни системи.

HSDPA

High Speed Packet Access (HSPA) представлява UMTS базирана технология от трето поколение. Основната цел на HSPA е разширяване и подобряване работата, осигуряване на по-високи скорости за трансфер на данните на вече съществуващият UMTS (WCDMA) протокол. HSPA обединява в себе си два мобилни протокола High Speed Downlink Packet Access (HSDPA) и High Speed Uplink Packet Access (HSUPA).

Общи сведения за HSDPA

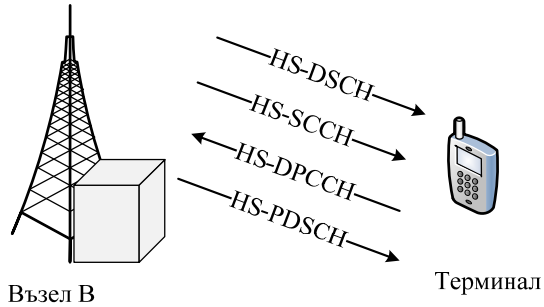
HSDPA (висококоростно сваляне на пакети данни) представлява стандарт за мобилна телефония, известен като 3,5G. HSDPA е стандартизиран от 3GPP Release 5, през март 2002, като първата HSDPA мрежа е внедрена на пазара в края на 2005. HSDPA е много подходяща за мобилен и широколентов достъп до Интернет, като например за изтегляне на приложения, видео, музика и т.н.

Стандартът е внедрен в България през март 2006г., когато мобилният оператор М-Тел въвежда първото HSDPA устройство на пазара и става петият световен оператор предлагащ тази технология. Първоначалната скорост за пренос на данните в България е 1.8 Mbps downlink. Година по късно М-Тел са въвели HSDPA устройства със downlink скорост за пренос на данните 7.2 Mbps.

HSDPA канали

За успешната работата по HSDPA са необходими да се въведат нови канали. Работата с каналите по HSDPA стандарта е показана на фигура 2. За потребителски данни се използва High-Speed Downlink Shared Channel (HS-DSCH) и съответсващият му канал от физическия слой High-Speed Physical Downlink Shared Channel (HS-PDSCH). За служебната информация са необходими два канала: High-Speed Shared Control Channel (HS-SCCH) съответно за downlink посока и High-Speed Dedicated Physical Control Channel (HS-DPCCH) в uplink посока.

В допълнение към основните HSDPA канали обхванати в Release 5, е въведен нов канал от Release 6 – the Fractional Dedicated Physical Channel (F-DPCH) като помощен за работата в HS-DSCH при надвишаване на downlink трафика.



Фиг. 2 – Канали в HSDPA

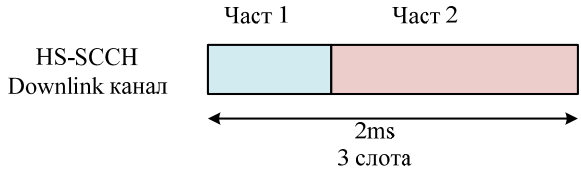
High-Speed Downlink Shared Channel (HS-DSCH)

HS-DSCH е единственият канал за стандарта HSDPA от транспортния слой за downlink връзка. Чрез него се осъществява пренос на реални потребителски данни с HSDPA. Еквивалент на HS-DSCH във физическият слой е каналът HS-PDSCH. В HS-DSCH липсва бързо управление на мощността в сравнение с DCH, но за сметка на това при осъществяване на връзка се избира подходяща комбинация от кодиране и модулация. Каналът използва 16–quadrature amplitude modulation (16-QAM) (броят на

битовете на символите се удвоява при благоприятни условия в сравнение с QPSK модулация). Важно свойство на HS-DSCH е динамичния характер на разпределение на ресурсите за кратък период от 2ms. Каналът използва турбокодиране, това е мотивирано от факта, че турбокодирането превъзхожда конволюционното кодиране, в противен случай скоростите за трансфер ще бъдат много малки.

High-Speed Shared Control Channel (HS-SCCH)

HS-SCCH е downlink канал от физическият слой, който се грижи служебната информация. Каналът съдържа три слота в две части (фиг. 3.), това дава възможност за минимално време да се предаде служебната информация, което от своя страна позволява на терминала да се декодират правилните кодове.

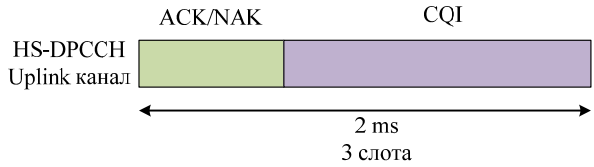


Фиг. 3 – HS-SCCH канал

Първата част за първият слот се грижи главно за преноса на служебна информация. Втората част, втори и трети слот се грижат за преноса на транспортирания блоков размер и Hybrid ARQ параметри. Транспортираният блоков размер – HS-SCCH показва колко данни ще се изпратят при следващата стъпка. [13]

High-Speed Dedicated Physical Control Channel (HS-DPCCH)

HS-DPCCH е единственият канал от физическият слой предаващ в uplink посока (от терминала към базовата станция) при HSDPA. Каналът също има три слота в две части (фиг. 4).



Фиг. 4 – HS-DPCCH канал

Първият слот съдържа ACK или NAK информация за получените резултати при HS-DSCH. Втората част (втори и трети слот) съдържат Channel Quality Indicator (CQI). Основната функция на обратната връзка е да информира базовата станция, дали пакетите данни са декодирани правилно или не. CQI дава информация на базовите станции за скоростите на пренос на данните към даден терминал в определен момент от време.

ЗАКЛЮЧЕНИЕ

Тенденцията в мобилните услуги - както и в съвременните фиксирани мрежи - е към богати на съдържание услуги, които може да се разработват като се използват дефинирани и специфицирани мрежови възможности. За много нови услуги "мобилността" ще бъде и причината и ефектът - добавяйки безценната "мобилна свобода" към предишните фиксирани услуги (безжична електронна търговия, Интернет достъп, корпоративна свързаност). Тя ще бъде движеща сила за нови услуги, които потребителите и приложенията ще изискват, тъй като самите те са мобилни (информация, зависеща от местоположението, забавления в превозно средство, проследяване, планиране на маршрути и диагностика). По този начин разработчиците на 3G в широк смисъл не са само сред операторите на мобилни мрежи, а и сред продавачите на хардуер и софтуер за информационни технологии, банкови и финансови фирми, транспортни ком¬пании и много други.

ЛИТЕРАТУРА

[1] Бояджиева. Е., Въведение в телекомуникационните системи, София, Нови знания, 2004 г.
[2] Мерджанов. П., Телекомуникационни мрежи, София, Нови знания, 2005 г.
[3] http://www.radio-electronics.com/

За контакти:

Валентин Коларов, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: soly_@abv.bg

ас. инж. Григор Михайлов, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации", тел.: 082-888 836, e-mail: gimihaylov@uni-ruse.bg

MS EXCEL-базиран модул за реализация на афинни шифри, прилагани в криптографските системи

автор: Радостина Иванова
научен ръководител: гл. ас. Адриана Бороджиева

MS EXCEL-Based Module for Implementing Affine Ciphers Applied in Cryptosystems: *In this paper the principle of operation of the affine ciphers is given. The publication describes the algorithm and the program module using MS Excel, designed for encryption and decryption of English and Bulgarian texts using affine ciphers. The module may be used by students studying the course "Telecommunications Security" and in other disciplines dealing with cryptographic methods the information protection.*
Key words: *cryptography, cryptosystems, affine ciphers, MS Excel.*

ВЪВЕДЕНИЕ

Началото на криптографията е поставено още в далечното минало – от времето на древните гърци и спартанци, и император Юлий Цезар. По-нататъшното й развитие се стимулира основно от военното дело, дипломацията и разузнаването. В средните векове с проблемите на тайнописите са се занимавали Франсис Бейкън, Франсоа Виет, Джеронимо Кардано и др. Появили са се множество кодове и алгоритми, някои от които дълго време са били смятани за абсолютно сигурни, като например предложеният от френския дипломат Блез дьо Виженер криптографски алгоритъм. Интересни и надеждни криптографски средства са били използвани от известните разузнавачи на миналия век – Шандор Радо, Рихард Зорге, полковник Абел и др. Окончателното формиране на криптографията като научна дисциплина, занимаваща се с разработката на сигурни криптографски алгоритми, кодове и протоколи, както и на ефективни средства за тяхната реализация, може да се отнесе към средата на XX век [1, 2].

ИЗЛОЖЕНИЕ

Афинният шифър е вид моноазбучен субституционен шифър, в който всяка буква в азбуката се съпоставя на нейния цифров еквивалент, криптира се с помощта на проста математическа функция и се превръща обратно към буква. Като субституционен шифър, афинният шифър притежава слабостите на субституционните шифри. Всяка буква в английския език се шифрира с функцията $(ax+b) \mod (26)$, където b е големината на преместването [3].

Описание

В афинния шифър буквите на азбуката с размер m най-напред се съпоставят на цели числа в диапазона $0 \ldots m-1$. След това се използва модулна аритметика, за да се трансформира цялото число, съответстващо на всяка буква в откритият текст, в друго цяло число, съответстващо на буква от шифрирания текст. Функцията за шифриране за една буква е:

$$E(x) = (ax+b) \mod m, \quad (1)$$

където модулът m е размерът на азбуката, а a и b са ключът на шифъра. Стойността на a трябва да бъде избрана така, че a и m да са взаимно-прости. Функцията за декриптиране е:

$$D(x) = a^{-1}(x-b) \mod m, \quad (2)$$

където a^{-1} е модулната мултипликативна инверсия на a по модул m, т.е. тя удовлетворява уравнението:

$$1 = a.a^{-1} \mod m \quad (3)$$

Мултипликативната инверсия на a съществува само, ако a и m са взаимно-прости. Следователно, без ограничението върху a декриптирането може да не е възможно. Може да се покаже, както следва, че функцията за декриптиране е обратна на функцията за криптиране [3]:

$$D(E(x)) = a^{-1}(E(x) - b) \mod m = a^{-1}(((ax + b) \mod m) - b) \mod m = \\ = a^{-1}(ax + b - b) \mod m = a^{-1}ax \mod m = x \mod m. \quad (4)$$

Слабости

Тъй като афинният шифър е едноазбучен субституционен шифър, той наследява слабостите на този клас шифри. Шифърът на Цезар е афинен шифър, за който $a = 1$, като функцията за криптиране се свежда до линейно преместване.

Като се има предвид специфичния случай на криптиране на съобщения на английски език (т.е. $m = 26$), има общо 286 нетривиални афинни шифри, без да се броят 26-те тривиални шифъра на Цезар. Този брой идва от факта, че има 12 числа, по-малки от 26, които са взаимно-прости с 26 (това са възможните стойности на a). Всяка стойност на a може да има 26 различни адитивни премествания (стойността на b); следователно, има 12 * 26 или 312 възможни ключа. Тази липса на разнообразие прави системата много несигурна, когато се разглежда в светлината на принципа на Kerckhoffs [3]. За българската азбука, $m = 30$, възможните варианти на афинни шифри са още по-малко, 8 * 30 или 240 възможни ключа.

Основната слабост на шифъра идва от факта, че ако криптоаналитикът може да открие открития текст на два символа от шифрирания текст, тогава ключът може да бъде получен чрез решаване на едно уравнение. Тъй като се знае, че a и m са взаимно-прости, това може да се използва за бързо отхвърляне на много „фалшиви" ключове в автоматизираната система.

Описание на разработените приложения – алгоритъм и симулационни резултати

Разработено е MS EXCEL-базирано приложение за шифриране и дешифриране на текстове на английски или български език, с малки и/или главни букви, чрез афинен шифър, с цел илюстриране на процесите на шифриране и дешифриране. Разработеното приложение съдържа следните 5 работни листа:

1) Буква – цифров код, където е посочено съответствието между буквата и нейния цифров код съгласно 7-битовия ASCII-код, който се получава чрез вградената в MS EXCEL функция CODE.

2) Шифриране-EN – предназначен за шифриране на открит текст на английски език с малки и/или главни букви;

3) Дешифриране-EN – предназначен за дешифриране на шифриран текст на английски език с малки и/или главни букви;

4) Шифриране-BG – предназначен за шифриране на открит текст на български език с малки и/или главни букви;

5) Дешифриране-BG – предназначен за дешифриране на шифриран текст на български език с малки и/или главни букви.

Алгоритъмът на разработеното приложение за шифриране на текстове на английски език съдържа следните стъпки:

1. Избор на параметри на афинния шифър: a и b. Изведено е подсказващо съобщение относно възможните стойности на двата параметъра. В случая са избрани $a = 7$ и $b = 19$ (фиг. 1).

2. Въвеждане на открития текст (буква по буква) в маркираните клетки (ред 1, фиг. 1).

3. Определяне на цифровия код (7-битов ASCII-код) на всяка буква от открития

текст (ред 2, фиг. 1) чрез вградената в MS EXCEL функция CODE.

4. Определяне на номера на съответната буква в английската азбука (ред 3, фиг. 1), напр. буквата A има ASCII-код 65 (в десетична бройна система), но е прието да се номерира с 0. За целта се проверява дали буквата е малка, за да се извади числото 97 от десетичния й код, или е главна, за да се извади числото 65 от десетичния й код. Трябва да се отбележи, че главните букви в латиницата са с цифрови кодове от 65 до 90, а малките букви в латиницата са с кодове от 97 до 122.

5. Определяне на $ax + b$, където x е номерът на буквата в английската азбука (ред 4, фиг. 1).

6. Определяне на $(ax + b) \mod (26)$, т.е. определяне на остатъка при деление на $ax + b$ с 26 (ред 5, фиг. 1). Получените в резултат числа са в диапазона от 0 до 25.

7. Преобразуване на цифровия код в символ посредством вградената в MS EXCEL функция CHAR (ред 6, фиг. 1). Тук отново се проверява дали буквата е малка или главна (съгласно резултата на ред 2, фиг. 1) и преди трансформирането й в символ се добавя числото 97 (за малка буква) или числото 65 (за главна буква).

ШИФРИРАНЕ НА АНГЛИЙСКИ ТЕКСТ ЧРЕЗ АФИНЕН ШИФЪР

Брой символи в английската азбука: **26**

Въведете коефициент a: 7 Възможни стойности: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
Въведете коефициент b: 19 Възможни стойности: (0...25)

1	Открит текст	A	f	f	i	n	e	C	i	p	h	e	r
2	Цифров код	65	102	102	105	110	101	67	105	112	104	101	114
3	x	0	5	5	8	13	4	2	8	15	7	4	17
4	ax + b	19	54	54	75	110	47	33	75	124	68	47	138
5	(ax + b) mod m	19	2	2	23	6	21	7	23	20	16	21	8
6	Шифриран текст	T	c	c	x	g	v	H	x	u	q	v	i

Фиг. 1 – Пример за шифриране на английския текст Affine Cipher (главни и малки букви) чрез афинен шифър с параметри $a = 7$ и $b = 19$

Алгоритъмът на разработеното приложение за шифриране на текстове на български език е аналогичен, но модулът $m = 30$, малките букви на кирилица са с кодове (отново ASCII-код) в диапазона от 224 до 255, а главните букви са в диапазона от 192 до 223. Следователно, нужните корекции с цел трансформиране на цифров код в номер на буквата са с числата 224 (вместо 97) и 192 (вместо) 65. На фиг. 2 е показан пример за шифриране на българския текст Афинен шифър (главни и малки букви) чрез афинен шифър с параметри $a = 7$ и $b = 19$.

ШИФРИРАНЕ НА БЪЛГАРСКИ ТЕКСТ ЧРЕЗ АФИНЕН ШИФЪР

Брой символи в българската азбука: **30**

Въведете коефициент a: 7 Възможни стойности: 1, 7, 11, 13, 17, 19, 23, 29
Въведете коефициент b: 19 Възможни стойности: (0...29)

1	Открит текст	А	ф	и	н	е	н	ш	и	ф	ъ	р
2	Цифров код	192	244	232	237	229	237	248	232	244	250	240
3	x	0	20	8	13	5	13	24	8	20	26	16
4	ax + b	19	159	75	110	54	110	187	75	159	201	131
5	(ax + b) mod m	19	9	15	20	24	20	7	15	9	21	11
6	Шифриран текст	У	й	п	ф	ш	ф	з	п	й	х	л

Фиг. 2 – Пример за шифриране на българския текст Афинен шифър (главни и малки букви) чрез афинен шифър с параметри $a = 7$ и $b = 19$

Алгоритъмът на разработеното приложение за дешифриране на текстове на английски език съдържа следните стъпки:

1. Избор на параметри на афинния шифър: a^{-1} и b. Изведено е подсказващо съобщение относно възможните стойности на двата параметъра. В случая са избрани $a^{-1} = 15$, което се явява мултипликативната инверсия на $a = 7$, използван при криптирането, и $b = 19$ (фиг. 3).

2. Въвеждане на шифрирания текст (буква по буква) в маркираните клетки (ред 1, фиг. 3).

3. Определяне на цифровия код (7-битов ASCII-код) на всяка буква от шифрирания текст (ред 2, фиг. 3) чрез вградената в MS EXCEL функция CODE.

4. Определяне на номера на съответната буква в английската азбука (ред 3, фиг. 3), напр. буквата A има ASCII-код 65 (в десетична бройна система), но е прието да се номерира с 0. За целта се проверява дали буквата е малка, за да се извади числото 97 от десетичния й код, или е главна, за да се извади числото 65 от десетичния й код.

5. Определяне на $a^{-1}(y-b)$, където y е номерът на буквата в английската азбука (ред 4, фиг. 3).

6. Определяне на $a^{-1}(y-b) \mod (26)$, т.е. определяне на остатъка при деление на $a^{-1}(y-b)$ с 26 (ред 5, фиг. 3). Получените в резултат числа са в диапазона от 0 до 25.

7. Преобразуване на цифровия код в символ посредством вградената в MS EXCEL функция CHAR (ред 6, фиг. 3). Тук отново се проверява дали буквата е малка или главна (съгласно резултата на ред 2, фиг. 3) и преди трансформирането й в символ се добавя числото 97 (за малка буква) или числото 65 (за главна буква).

При правилен подбор на параметрите на шифъра, в случая $a^{-1} = 15$ и $b = 19$, в клетките на дешифрирания текст, който трябва да съвпада с откритият текст, се получава смислен текст (ред 6, фиг. 3). При неправилен подбор на параметрите на шифъра, например, при $a^{-1} = 15$, но $b = 20$, в клетките на дешифрирания текст, който трябва да съвпада с откритият текст, се получава безсмислен текст (ред 6, фиг. 4).

ДЕШИФРИРАНЕ НА АНГЛИЙСКИ ТЕКСТ ЧРЕЗ АФИНЕН ШИФЪР

Брой символи в английската азбука: **26**

a: Възможни стойности: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

Въведете коефициент a^{-1}: 15 Възможни стойности: 1, 9, 21, 15, 3, 19, 7, 23, 11, 5, 17, 25

Въведете коефициент b: 19 Възможни стойности: (0...25)

1	Шифриран текст	T	c	c	x	g	v	H	x	u	q	v	i
2	Цифров код	84	99	99	120	103	118	72	120	117	113	118	105
3	y	19	2	2	23	6	21	7	23	20	16	21	8
4	$a^{-1}(y–b)$	0	-255	-255	60	-195	30	-180	60	15	-45	30	-165
5	$a^{-1}(y – b) \mod m$	0	5	5	8	13	4	2	8	15	7	4	17
6	Открит текст	A	f	f	i	n	e	C	i	p	h	e	r

Фиг. 3 – Пример за дешифриране на шифрирания текст Tccxgv Hxugvi (главни и малки букви) чрез афинен шифър с параметри $a^{-1} = 15$ и $b = 19$: дешифриран текст Affine Cipher (английски език, смислен текст)

ДЕШИФРИРАНЕ НА АНГЛИЙСКИ ТЕКСТ ЧРЕЗ АФИНЕН ШИФЪР

Брой символи в английската азбука: **26**

	a:	Възможни стойности: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
Въведете коефициент a^{-1}:	15	Възможни стойности: 1, 9, 21, 15, 3, 19, 7, 23, 11, 5, 17, 25
Въведете коефициент b:	20	Възможни стойности: (0...25)

1	Шифриран текст	T	c	c	x	g	v	H	x	u	q	v	i
2	Цифров код	84	99	99	120	103	118	72	120	117	113	118	105
3	y	19	2	2	23	6	21	7	23	20	16	21	8
4	a^{-1}(y–b)	-15	-270	-270	45	-210	15	-195	45	0	-60	15	-180
5	a^{-1}(y – b) mod m	11	16	16	19	24	15	13	19	0	18	15	2
6	Открит текст	L	q	q	t	y	p	N	t	a	s	p	c

Фиг. 4 – Пример за дешифриране на шифрирания текст Tccxgv Hxugvi (главни и малки букви) чрез афинен шифър с параметри $a^{-1} = 15$ и $b = 20$: дешифриран текст Lqqtyp Ntaspc (английски език, безсмислен текст)

Алгоритъмът на разработеното приложение за дешифриране на текстове на български език е аналогичен, но модулът $m = 30$, малките букви на кирилица са с кодове (отново ASCII-код) в диапазона от 224 до 255, а главните букви са в диапазона от 192 до 223. Следователно, нужните корекции с цел трансформиране на цифров код в номер на буквата са с числата 224 (вместо 97) и 192 (вместо) 65.

ЗАКЛЮЧЕНИЕ

В публикацията е описан алгоритъм, заложен в програмен модул, с използване на MS Excel, създаден за шифриране и дешифриране чрез афинни шифри на текстове на английски или български език, съставени от малки и/или главни букви. Приложени са резултатите от шифрирането и дешифрирането на произволен текст. Разработеният програмен модул може да намира приложение в учебния процес по дисциплината „Телекомуникационна сигурност", включена като задължителна в учебния план на специалността „Телекомуникационни системи" за образователно-квалификационна степен „Бакалавър", както и в други дисциплини, разглеждащи криптографските методи за защита на информацията.

Бъдещата работа предвижда разработване на аналогичен модул с използване на възможностите на MATLAB за криптиране и декриптиране чрез афинни шифри на текстове на английски и български език, който да улеснява процесите на шифриране и дешифриране.

ЛИТЕРАТУРА

[1] Антонов, П., С. Малчев. Криптография в компютърните комуникации. Варна, 2000
[2] Скляр, Б. Цифровая связь. Теоретические основы и практическое применение. Москва, Вильямс, 2003
[3] http://en.wikipedia.org/wiki/Affine_cipher

За контакти:

Радостина Иванова, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: radostina6112@abv.bg

гл. ас. Адриана Бороджиева, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации", тел.: 082-888 734, e-mail: aborodjieva@ecs.uni-ruse.bg

Реализация на систоличния алгоритъм за умножение в SMT/TLP среда

автор: Бисер Николов
научен ръководител: гл. ас. д-р Милен Луканчевски

An Implementation of Systolic Multiplication Algorithm in SMT/TLP environment: *The transition from sequential John von Neumann computing model to the new parallel one continues from a long time. Even after emerge of multicore architectures there passed about ten years. And no unified methodology exists for their programming. The author's opinion is that the main reason for those difficulties is in general purpose computer architectures itself. These traditional architectures although burrow of many advanced features from pure parallel machines are sequential in essence. As a result they do not support at hardware level any form of global parallelism – process creation/deletion, execution, communication and synchronization. Hence, the need of an operating system for those tasks. At the opposite are CSP implementations in the form of transputers/OCCAM and XCore/XC. The latest alternative is the subject of this paper. It considers an implementation of the systolic array multiplication as example of unified methodology for parallel programming based on CSP.*

Key words: *CSP, XC, XCore, XMOS, XS1, SMT, TLP.*

ВЪВЕДЕНИЕ

Предпоставка за прехода от последователния фоннойманов към паралелния изчислителен модел са физическите ограничения за увеличаването на производителността, по-конкретно светлинната и топлинната бариера, достигнати около 2003 година.

Пионерите на RISC архитектурите Хенеси и Патерсън обръщат внимание на втората особена точка в графиката на развитието на производителността, настъпила в този период [4]. Тази особена точка отговаря на изчерпването на локалния паралелизъм и навлизането на структурните методи за повишаване на производителността – многоядрените архитектури, които са пример за глобален паралелизъм.

Смяната на фундаменталния изчислителен модел е свързана с прехода от скрития локален паралелизъм на ниво инструкции (ILP) към явния глобален паралелизъм на ниво нишки (TLP) и на ниво данни (DLP).

Пред автора на доклада е поставена задачата да предложи група контролни примери за работа в паралелна SMT/TLP среда с използване на TLP и DLP. Примерите са предназначени за обучението на студентите по дисциплината „Паралелни компютърни системи". В доклада се представят основните моменти от контролния пример за реализацията на систоличния алгоритъм за умножение в SMT/TLP среда.

ПАРАЛЕЛЕН ИЗЧИСЛИТЕЛЕН МОДЕЛ CSP

Един от разпространените паралелни изчислителни модели е CSP (Communicating Sequential Processes, Взаимодействащи си последователни процеси), предложен от Чарлз Хоар [2]. Моделът се базира на понятието процес като базова единица активност. Процесът може да бъде съставен и се определя от рекурсивния израз (1)

$$P := < \text{линеен участък} > < \text{комуникация} > P \qquad (1)$$

Структурата на процеса е естествено следствие от разширяването на последователните машини и последователните езици със средства за комуникация с оглед на разпределения модел памет. В съответствие с този модел се дефинира абстрактна паралелна машина (CSP-машина), състояща се от множество апаратни

възли и физически канали. Възлите осигуряват локалната защитена среда на процесите. Каналите формират комуникационната среда за обмена на съобщения – единствения начин за взаимодействие между процесите.

Важна особеност на CSP е обединяването в едно на математически модел, формална спецификация на паралелна система и език за паралелно програмиране. Нещо повече, съществуват апаратни реализации на CSP машината и реални езици за паралелно програмиране, производни на CSP (фиг. 1).

Първият пример за практическо приложение на CSP са транспютърните паралелни системи и езикът за паралелно програмиране OCCAM [1, 3]. Транспютрите представляват специализирани едночипови микрокомпютри, предназначени за изграждане на масово-паралелни системи (MPP). За разлика от процесорите с общо предназначение, осигуряват цялостна апаратна поддръжка на процеса, като базов активен елемент, и превръщането му в елементарна единица работа. Притежават вградени комуникационни средства – физически канали.

Фиг. 1 – Връзка между абстрактната и реалната страна на CSP

Съвременната апаратна реализация на CSP е фамилията XS1 на фирмата XMOS [5]. Микропроцесорите от тази фамилия съдържат едно или повече ядра от типа XCore. Ядрото е 32 bit събитиен (event-driven) RISC процесор и осигурява SMT/TLP апаратна среда, поддържаща едновременното изпълнение на 8 нишки. Съдържа силносвързана входно-изходна система, физически канали за връзка, ресурси за работа в реално време, статична RAM с нулева латентност. Наличната апаратна поддръжка на паралелизма изключва необходимостта от операционна система и свързаните с нея служебни загуби.

Фамилията XS1 обединява възможностите на процесор с общо предназначение, DSP процесор и FPGA. Ударението е поставено на възможността апаратните функции да се реализират с програмни средства (software defined silicon). В основата на този унифициран подход за разработка на хардуера и софтуера е езика XC, на който се програмира фамилията [6].

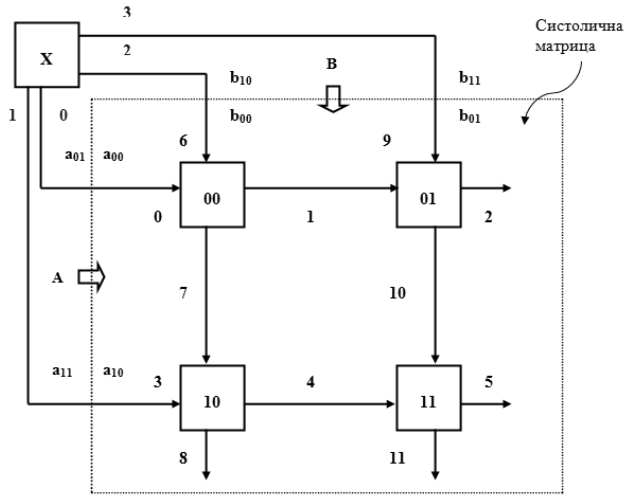
Езикът XC е разширение на езика C с конструкции за паралелно програмиране. Може да се проследи семантическата връзка между конструкцията par на XC и паралелната команда на CSP; между оператора select и алтернативната команда на CSP; между операторите за въвеждане :> и извеждане <: и командите на CSP за изпращане ! и получаване ? на съобщения.

Благодарение на апаратната поддръжка на CSP модела, операторите на XC се транслират в къси RISC инструкции с време за изпълнение един машинен цикъл, като се избягват служебните загуби, характерни за ОС.

РЕАЛИЗАЦИЯ НА СИСТОЛИЧНИЯ АЛГОРИТЪМ ЗА УМНОЖЕНИЕ

Едно от класическите приложения на паралелните системи са интензивните изчисления и в частност матричната обработка [7].

Последователният алгоритъм за умножение на квадратни матрици с размерност n изисква n^3 умножения и n3 събирания. Следователно, времето за изпълнение на последователния алгоритъм се оценява като $O(n^3)$. Паралелните методи за умножение се основават на взаимната независимост при изчислението на отделните елементи на матрицата на произведението C. Ако се игнорира времето за комуникация между възлите, при n^2 възела времето за паралелно умножение се оценява като $O(n)$.



Фиг. 2 – Структура на систоличната матрица за умножение

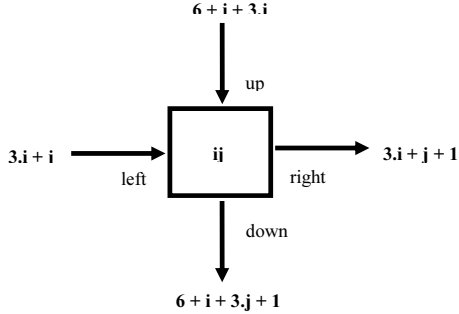
При паралелната обработка възниква необходимостта от паралелното подаване на елементите на матриците към изчислителните възли. Тази задача не е тривиална поради големия брой възли, а и не всички възли са свързани с входно/изходните устройства. Систоличният метод предлага специфичен начин за синхронно подаване на елементите на матриците към изчислителните възли [1, 7]. Отделя се един главен, диспечерски възел X, свързан с входно/изходните устройства. Данните се разпространяват синхронно, на тласъци, от него по главния диагонал на систоличната матрица.

На фиг. 2 е показана предложената в работата структура на четиривъзлова паралелна система за изпълнение на систоличния алгоритъм за умножение на квадратни матрици. В основата ѝ е четириядреният SMT/TLP микропроцесор XS1-G4 [5].

Матрицата A постъпва отляво надясно по редове, а матрицата B – отгоре надолу по колони. На фигурата е отбелязана и конкретната номерация на каналите, свързващи процесите в системата.

Индексацията на каналите е представена в обобщен вид на фиг. 3. Всеки процес Pij, разположен в изчислителен възел, има четири канала – left и up (входни), right и down (изходни). Тази схема на именоване на каналите позволява да се извърши пълна репликация на системата: всички n2 процеси Pij, които изчисляват елемента cij на произведението, са копия на един и същ процес P. Конкретният

екземпляр на този процес се параметризира единствено с индексите на конкретните канали, към които е свързан, в зависимост от разположението си.



Фиг. 3 – Обобщена индексация на каналите на процес P_{ij}

Разглежда се вариантът на процеса P с най-висока степен на паралелизъм, описван от CSP уравнението

P = { c = 0; k = 0;
**{{ left?a || up?b }; { right!a || down!b};* (2)
c = c + a x b; k = k + 1;
{ k < n -> SKIP □ k >= n -> SKIP } } }

Двете паралелни команди в тялото на P са високоефективни, вследствие на пълната апаратна поддръжка на паралелизма и липсата на допълнителни нива, като например задължителната при микропроцесорите с общо предназначение многозадачна операционна система.

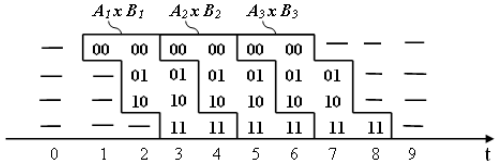
```
while(TRUE)
{
        par
        {
                chanLeft :> intA;
                chanUp   :> intB;
        }

        par
        {
                if(boolRight) chanRight <: intA;
                if(boolDown) chanDown <: intB;
        }

        intC = intC + intA*intB; intK = intK + 1;

        if(intK >= n)
                STOP;
}
```

Фиг. 4 – Тяло на главната функция на процес P

Семантичната връзка между паралелния модел CSP и паралелния език XC определя главната функция taskNode() на процеса P като директно следствие на уравнението (2), както се вижда от фиг. 4.

Максимална ефективност се постига при непрекъснато конвейерно подаване на двойките матрици за умножение, при което всички възли на матрицата работят. На фиг. 5 е представен един участък от подобно конвейерно изпълнение. След

освобождаването на даден възел от обработката на предходната двойка матрици, се преминава към обработката на следващата двойка.



Фиг. 5 – Диаграма на работа при конвейерно умножение

Диаграмата от фиг. 5 представя систоличната матрица като машина, управлявана от потока данни и е илюстрация на паралелизъм на ниво данни (DLP).

ЗАКЛЮЧЕНИЕ

Преходът от последователния фоннойманов към паралелния изчислителен модел продължава от десетилетия. Появата на многоядрените архитектури преди около 10 години налага все по-остро намирането на обща методология за паралелно програмиране. Самият принцип на работа на архитектурите с общо предназначение обаче е основна пречка – тези архитектури са последователни по определение. Изражение на това е практическото отсъствие при тях на апаратна поддръжка на глобален паралелизъм – създаването и унищожаването, изпълнението, взаимодействието и синхронизацията на процесите по правило се осигуряват от операционната система, а не от самата архитектура.

Алтернатива представляват реализациите на CSP, каквито са транспютрите и езика OCCAM, XCore и езика XC. В доклада е представен, разработения от автора пример за прилагането на единна методология за паралелно програмиране, основана на паралелния изчислителен модел CSP и поддържащата този модел паралелна SMT/TLP фамилия XS1 на фирмата XMOS.

ЛИТЕРАТУРА

[1] Джоунз, Г. Программирование на языке OCCAM. - М.: Мир, 1989
[2] Hoare, C.A.R. Communicating Sequential Processes. – New Jersey: Prentice Hall Int, 1985-2004
[3] Nicoud, J-D., A. Tyrrell. The Transputer T414 Instruction Set. // IEEE Micro, Jun 89, pp. 60-75
[4] Patterson, D., J. Hennessy. Computer Architecture: A Quantitative Approach, 5th Ed. - New York: The Morgan Kaufmann, 2011
[5] XC-2 Hardware Manual. – XMOS Ltd, 2009
[6] Watt, D. Programming XC on XMOS Devices. – XMOS Ltd, 2009
[7] Wilkinson, B., M. Allen. Parallel Programming: Techniques and Applications Using Networked Workstations and Parallel Computers. – New Jersey: Prentice Hall Int, 1999

За контакти:

Бисер Николов, Русенски университет "Ангел Кънчев", Център за Информационно и Компютърно обслужване, e-mail: bnikolov@uni-ruse.bg

гл. ас. д-р Милен Луканчевски, Русенски университет "Ангел Кънчев", Катедра „Компютърни системи и технологии", тел.: 0887 303 850, e-mail: mil@ieee.org

Криптиране и декриптиране с последователно прилагане на субституционни шифри

автор: Петър Пенев
научен ръководител: гл. ас. Елена Дянкова

***Encryption and decryption by sequentially applying substitution ciphers**: The classical cryptographic algorithms do not provide reliable data security against various attacks. The sequential multiple applying of symmetric algorithms is an option for solving the problem. The paper describes a software tool for data encryption/decryption by keyword substitution cipher and Hill cipher.*

***Key words**: cryptography, encryption, decryption, cipher, substitution ciphers, Hill cipher, keyword cipher, cipher text*

ВЪВЕДЕНИЕ

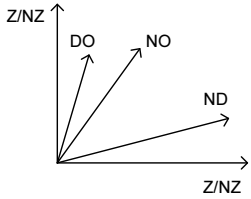
В редица приложения на симетричните криптографски системи се използва многократно шифриране на явния текст, което е полезно за целите на усложняване на задачите при криптоанализа. Понякога се използва един и същи шифър, което не внася особени трудности за атакуващия системата. По-добър вариант е използването на два или повече различни шифъра, които прилагат субституция на символи от едно множество с други от същото множество или от друго със същата кардиналност.

В настоящата статия се предлага програмен продукт, използван за шифриране и дешифриране на информация при последователно прилагане на шифър с ключова дума и шифър на Хил. Множеството от използвани символи за явния и шифрования текст е едно и също.

ИЗЛОЖЕНИЕ

1.Шифър на Хил. Шифриране на таблици.

Ако се приеме, че се използва N-буквена азбука и е необходимо да се изпращат диграфи, т.е. текстът е разделен на блокове от два символа, то тогава е известно, че на всеки диграф отговаря едно цяло число в множеството ***{0, 1, 2,…,N²}*** , т. е. то е елемент на ***Z/N²Z***. Една графична интерпретация е показана по-долу, като на всеки диграф отговаря вектор, т. е. на двойки цели числа $\begin{vmatrix} x \\ y \end{vmatrix}$, като ***x*** и ***y*** се определят при ***modN***. Нека азбуката е от 26 букви ***(A-Z)*** с числови еквиваленти ***(0-25)***, тогава на диграфа "**NO**" отговаря на вектор $\begin{vmatrix} 13 \\ 14 \end{vmatrix}$.



Фиг. 1. Изобразяване на диграф с вектор

Всеки диграф представлява точка в матрица ***NxN***, т. е. в ***xy***-равнината, само че в случая осите не са ***x*** и ***y***, а ***Z/NZ***. Тъй като равнината най-често се означава с R^2 (в множество на реалните числа), то ***NxN*** матрицата ще се запише като ***(Z/NZ)²***.

След шифрирането на диграфа като вектор той се визуализира в нова позиция (в нов вектор). Или ще има таблица за шифриране като на функцията "one-to-one" от ***(Z/NZ)²*** върху себе си.

1.1 Кратък преглед от линейната алгебра за намиране на обратни матрици.

Разглежда се матрица ***2x2***, съставена от цели числа $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ и един вектор в равнината $\begin{vmatrix} x \\ y \end{vmatrix}$, като се извършва умножението на матрицата с вектора, при което се

получава нов вектор: $\begin{vmatrix} a & b \\ c & d \end{vmatrix} . \begin{vmatrix} x \\ y \end{vmatrix} = \begin{vmatrix} ax + by \\ cx + dy \end{vmatrix} mod N^2$ (1)

За една фиксирана матрица, тази функция на получаване на един вектор от друг се нарича линейна трансформация, означавайки, че се запазва сумирането и константите умножаващи векторите. От тук е ясно, че всяко множество от уравнения от вида ***ax + by = e***, ***cx + dy = f*** е еквивалентно на едно матрично уравнение ***A.X=B***, като с ***A*** е означена матрицата $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = A$, с $X = \begin{vmatrix} x \\ y \end{vmatrix}$, а с $B = \begin{vmatrix} e \\ f \end{vmatrix}$. Така един определен вектор умножен по известна матрица дава друг определен вектор. Това е равносилно на уравнението ***ax=b***, което се решава при ***a≠0*** с умножение и двете страни на a^{-1} От казаното по-горе следва да се намери матрица A^{-1} за да се определи $X=A^{-1}.B$.

Да се инвертира квадратна матрица ***A*** означава, че ако се умножи с обратната ѝ (A^{-1}) и се получава единична матрица $\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$. Не всички матрици имат обратни. Не е трудно да се докаже, че ***A*** има обратна само, ако детерминантата - ***D = ad - bc ≠ 0*** и нейната обратна в този случай е $A^{-1} = \frac{1}{D}\begin{vmatrix} d & -b \\ -c & a \end{vmatrix} = \begin{vmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{vmatrix}$.

Нека съществува един сноп от вектори $X_1 = \begin{vmatrix} x_1 \\ y_1 \end{vmatrix}, X_2 = \begin{vmatrix} x_2 \\ y_2 \end{vmatrix}, \dots, X_k = \begin{vmatrix} x_k \\ y_k \end{vmatrix}$, подредени като колони в матрица ***(2xK)***. Тогава може да се дефинира произведение на следните матрици: $A.X = \begin{vmatrix} a & b \\ c & d \end{vmatrix} . \begin{bmatrix} x_1 & \dots & x_k \\ y_1 & \dots & y_k \end{bmatrix} = \begin{vmatrix} ax_1 + by_1 & \dots & ax_k + by_k \\ cx_1 + dy_1 & \dots & cx_k + dy_k \end{vmatrix}$.

1.2. Изчисления на обратна матрица при ***modN***

По-горе се извърши шифриране на един знак в Z/NZ и беше показано, че се използват два прости вида на таблици:

- „линейна" таблица ***C=a.P***, където ***a*** има обратно в ***Z/NZ***;
- „афинна" таблица ***C=a.P+b***, където ***a*** има обратно в ***Z/NZ***;

Съществува подобна ситуация, когато съобщението се състои от диграфи – вектори. За целта се анализира линейна таблица. Разликата, когато се работи с $(Z/NZ)^2$ в сравнение с ***Z/NZ*** е, че вместо едно цяло число ***a*** има нужда от ***2x2*** матрица означена като ***A***. Ще бъде направено систематично обяснение за типа на матрицата.

Нека ***R*** е комутативен пръстен, т.е. множество с две бинарни операции - умножение и събиране, отговарящи на същите правила като в едно поле, с изключение на това, че не се изисква кой и да е ненулев елемент да има мултипликативно обратен. Например, ***Z/NZ*** винаги е пръстен, но не е поле освен, ако ***N*** е просто число. Нека ***R**** е подмножество на ***R*** и съдържа елементите, които имат обратни. Например, ***(Z/NZ)* = {0 < j < N | gcd(j,N) = 1}***.

Ако ***R*** е комутативен пръстен, тогава с ***M_2(R)*** се означава множеството на всички матрици ***2x2*** с елементи от ***R*** - със събиране и умножение, определени по обикновения начин за матрици. ***M_2(R)*** ще се нарича „матрица пръстен върху ***R***"; ***M_2(R)*** от само себе си е един пръстен, но не е комутативен пръстен, т. е. в умножението на матрици има значение реда на множителите.

Подобно на разгледаното за матрицата $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ и нейната обратна, ако детерминантата ***D≠0*** има подобна ситуация за пръстена ***R***.

Именно, приема се че $A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \in M_2$ и ***D = det(a) = $_{def}$(ab-cd)*** е в ***R****. Нека D^{-1} означава мултипликативно обратното на ***D*** в ***R***. Тогава лесно се получава

$$\begin{vmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{vmatrix} . \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} D^{-1}(da - bc) & 0 \\ 0 & D^{-1}(-cb + ad) \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$$

Ще се получи същия резултат, ако се умножава в обратен ред. Така ***A*** има обратна матрица. Тя е представена с израза:

$$A^{-1} = \begin{vmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{vmatrix}$$

В случая с реално числа, една ***2x2*** матрица $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ с елементи от ***R*** може да бъде умножена по вектор стълб $\begin{vmatrix} x \\ y \end{vmatrix}$ с ***x,y*** ϵ ***R*** и да се получи нов вектор $\begin{vmatrix} x' \\ y' \end{vmatrix} = \begin{vmatrix} ax & by \\ cx & dy \end{vmatrix}$. Това дава „линейна карта" от вектори на вектори, което означава, че линейната комбинация $\begin{vmatrix} k_1x_1 + k_2x_2 \\ k_1y_1 + k_2y_2 \end{vmatrix}$, където k_1 и k_2 са от пръстена ***R*** дава $\begin{vmatrix} k_1x_1' + k_2x_2' \\ k_1y_1' + k_2y_2' \end{vmatrix}$. Разликата с предишната ситуация е само, че тук става въпрос за ринг (пръстен) ***R*** с реални числа. Сега това ще се приложи за пръстен ***R=Z/NZ***.

Допускане: Нека $A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \in M_2(Z/NZ)$ и множество ***D = ad - bc***. Има следните елементарни валентности:

- ***gcd(D, N) = 1***;
- ***A*** има обратна матрица;
- Ако ***x*** и ***y*** не са нули в ***(Z/NZ)²***, тогава $A.\begin{vmatrix} x \\ y \end{vmatrix} \neq \begin{vmatrix} 0 \\ 0 \end{vmatrix}$.;
- ***A*** дава *one-to-one* отношение в ***(Z/NZ)²*** само на себе си.

Ако се обърне внимание отново на допускането по-горе,а именно, че всеки явен текст $D = \begin{vmatrix} x \\ y \end{vmatrix}$ има шифриран текст $C = \begin{vmatrix} x' \\ y' \end{vmatrix}$ с правилото ***C = A.P***, т.е. $\begin{vmatrix} x' \\ y' \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix}.\begin{vmatrix} x \\ y \end{vmatrix}$. За да се дешифрира текста се прилага ***P = A⁻¹.A.P = A⁻¹.C***, т.е. $\begin{vmatrix} x \\ y \end{vmatrix} = \begin{vmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{vmatrix}.\begin{vmatrix} x' \\ y' \end{vmatrix}$.

В случая се разполага с източник на информация, знае се, че става въпрос за дограф – вектори в ***N***-буквена азбука и една линейна трансформация на шифриране ***C = A.P***. Обаче не се знае ключът за шифроване на матрица ***A*** или ключът за дешифриране на матрица A^{-1}.

Нека се приеме, че е възможно да се определят две двойки на явния текст и шифрования дограф: $C_1 = A.P_1$ и $C_2 = A.P_2$. Тази информация е получена вследствие на анализ на честотата на срещане на дографите в дълъг шифрован текст. Сега трябва да се определят ***A*** и A^{-1}. За целта се поставят двете колони P_1 и P_2 в матрица ***(2x2)*** → ***P*** и същото - за C_1 и C_2, т.е. ***C = A.P***.

(***C*** и ***P*** са известни!) ***A*** – не е известно. Умножават се двете страни на уравнението на P^{-1}. Тогава $C.P^{-1} = A.P.P^{-1}$, от което се получава $C.P^{-1} = A$.

От това (***C = A.P***) уравнение може да се определи $A^{-1} = P.C^{-1}$ (от $P = A^{-1}.C$).

2. Шифриране с ключова дума

Използва се едноазбучен шифър. При шифриране и дешифриране трябва да се въведат 2 стойности:

- ключ ***K*** - ключова дума, която ще се използва за криптиране и декриптиране;
- позиция ***P*** - позиция, на която ще се сложи ключовата дума в последователността от множеството на символите.

При това са налице две секретни информации - ключовата дума и номерът на позицията, което е число от множеството $Z_N = \{0,1,2,\ldots, N-1\}$

За криптиране или декриптиране с помощта на шифър с ключова дума се използва таблица, която съдържа цялото множество от използвани символи, разположени в първия ред, а на втория ред се поставя същото множество от символи, но с вмъкната ключова дума, съгласно избраната позиция на вмъкване. При вмъкването на ключа в множеството, ако той съдържа повтарящи се символи, то те се записват еднократно. След и преди ключа се поставят останалите символи от множеството, като се запазва последователността им и се отстраняват тези, които участват в ключа, както и тези, които се повтарят в ключа. Това означава, че ако ключът е вмъкнат в ненулева позиция, закодираната азбука се вписва в таблицата до достигане на максималния индекс и след това се продължава с 0-левия. При

кодиране всеки символ от явния текст, намиращ се на първия ред на таблицата се разменя със съответния му от долния ред на същата. При декодиране е обратното.

Пример: Нека се използват буквите от латинската азбука, т.е. ***N=26, K="CRYPTO", P=0***

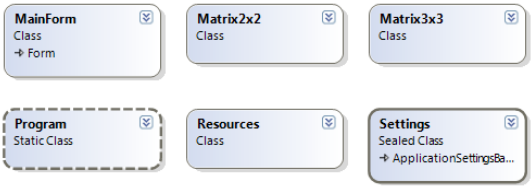
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C	R	Y	P	T	O	A	B	D	E	F	G	H	I	J	K	L	M	N	Q	S	U	V	W	X	Z

Криптиране: ***keyword → FTXVJMP***

Декриптиране: ***YDKBTM → cipher***

3. Програмна реализация

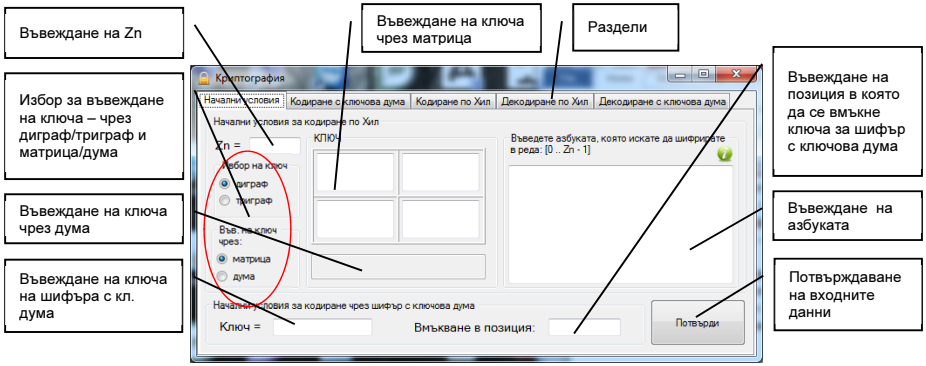
Софтуерното средство за криптиране и декриптиране е изградено от три класа – клас на формата и два класа, които прилагат действията с матрица ***2x2*** и матрица ***3x3***. На фиг. 2 са изобразени използваните класове за разработване на проекта.



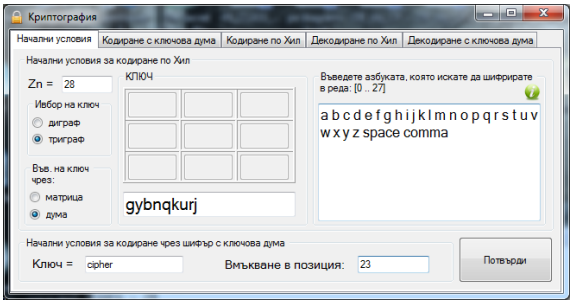
Фиг. 2 – Клас диаграма на класовете

3.1 Графичен интерфейс

На фиг. 3 са посочени функциите на главните елементи в началния екран на програмата. Той се разделя на два модула - начални данни (ключ, азбука) за шифриране по метода на Хил и начални данни за шифриране, чрез шифър с ключова дума. На фиг. 4 са показани примерни начални условия на програмата.

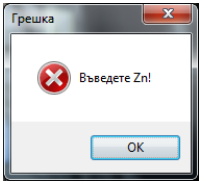


Фиг.3 – Основни елементи на началния екран на програмата

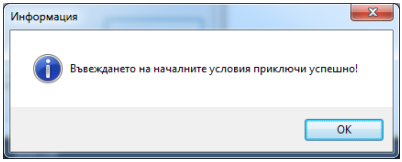


Фиг. 4 – Примерни начални условия

Предвидени са 24 различни съобщения, свързани с логически и синтактични грешки при въвеждането на информацията (фиг. 5) .



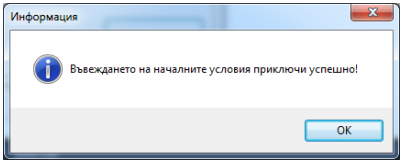
Фиг. 5 – Съобщение за грешка



Фиг. 6 – Информационно съобщение за потвърждаване на верността на въведените начални данни

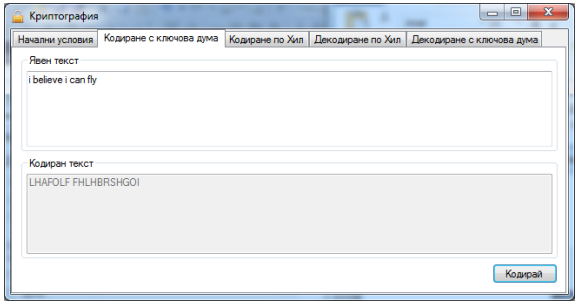
3.2 Указания за работа с програмата

След като се въведат начални данни (фиг. 3) трябва да се натисне бутон „*Потвърди*“. Ако данните, които са въведени са коректни се получава информационно съобщение (фиг. 7).



Фиг. 7 – Информационно съобщение за потвърждаване на верността на въведените начални данни

След получаването на това съобщение се преминава към раздел „*Кодиране с ключова дума*“. В текстовото поле озаглавено „*Явен текст*“ трябва да се въведе текст, който ще се кодира. Например “***i believe i can fly***”, след което се натиска бутона „*Кодирай*“. Ако всичко е извършено в посочения ред трябва в полето „*Кодиран текст*“ да се получи резултатът от прилагането на първия шифър (фиг. 8).



Фиг. 8 – Кодиране на „i believe i can fly", чрез шифър с ключова дума и ключ "cipher" на позиция 23

Следващата стъпка е кодирането, чрез използване на шифъра на Хил. За целта се преминава към следващия раздел - „*Кодиране по Хил*". За явен текст се използва вече получения от прилагането на първия шифър - с ключова дума кодиран текст. Единствената опция на тази стъпка е натискането отново на бутона „*Кодирай*". За кодиран текст трябва да се получи (за посочения пример) - "***KDDNHRP,,FB MRXETEUUU***".

Декодирането се извършва в обратен ред на прилагане на шифрите след натискане на бутоните „*Декодирай*" при прилагане на шифър на Хил и „*Декодирай*" с ключова дума, където всичко е идентично с останалите раздели. При натискане на бутона „*Декодирай*" трябва да се получи текста въведен в началото - "***i believe i can fly***", но се получава "***i believe i can flybb***", защото при кодирането чрез шифъра на Хил може да се наложи добавяне на служебни символи - „***bb***". След като се премахнат се получава началният (явният) текст.

ЗАКЛЮЧЕНИЕ

Предлаганият програмен продукт дава възможност за:

1. Многократно криптиране и декриптиране с последователно прилагане на два различни шифъра.
2. Задаване на множество от входни и изходни символи с произволна кардиналност.
3. Определянето на ключа за шифър на Хил става с ключова дума или матрица.
4. Показване на междинните резултати от криптирането и декриптирането.

ЛИТЕРАТУРА

[1] Modern Cryptography: Theory and Practice, By Wenbo Mao Hewlett-Packard Company, Prentice Hall PTR, 2003, ISBN: 0-13-066943-1, 648p
[2] Oppliger,R. Contemporary Cryptography, Artech House, 2005
[3] Stinson, D. Cryptography: Theory and Practice, Second Edition, CRC Press, Boca Raton, 2002, ISBN 1584882069

За контакти:

Петър Пенев, Русенски университет "Ангел Кънчев", Специалност "Компютърни системи и технологии", , e-mail: pesho.pfp@gmail.com

гл. ас. Елена Якимова, Русенски университет "Ангел Кънчев", Катедра "Компютърни системи и технологии", тел.: 082 – 888276, e-mail: ESimeonova@ecs.uni-ruse.bg

Многократно шифриране/дешифриране с използване на класически криптографски алгоритми

автор: Венцислав Атанасов
научен ръководител: гл. ас. Елена Дянкова

Multiple encryption/decryption by classical cryptographic algorithms: *The paper describes a software tool for multiple encryption/decryption by applying chosen ciphers sequence from set of four symmetric algorithms - Affine cipher, shift cipher, Vigenere cipher and Hill cipher. Increasing stability against cryptographic attacks achieves not only by used secret keys but also by the selected sequence of applied ciphers.*

Key words: *cryptography, encryption, decryption, cipher, Affine cipher, shift cipher, Vigenere cipher, Hill cipher, cipher text*

ВЪВЕДЕНИЕ

В криптографията се използват различни видове алгоритми за шифриране и дешифриране на информация, съдържаща се в съобщения, данни и други. Симетричните криптографски системи се използват от дълбока древност и до наши дни. Криптирането и декриптирането на информацията в тези системи се извършва с един и същи ключ от множеството на възможните ключове. Използваните в класическата криптография алгоритми не осигуряват сигурна защита на информацията от различни атаки. Един вариант за усложняване работата на криптоанализаторите е многократно шифриране с последователно прилагане на различни видове алгоритми и ключове върху една и съща информация. Това значително затруднява откриването както на явния текст, така и на използваните ключове, поради необходимост от разпознаване както на последователността от приложените алгоритми така и на съответстващите им ключове, които могат да бъдат и от различни множества.

Настоящата работа е посветена на разработване на необходимия софтуер за прилагане на многократно шифриране на текст при избор на произволна последователност от шифри от множество състоящо се от четири класически шифъра.

ИЗЛОЖЕНИЕ

По-долу е направен кратък преглед на използваното множество от шифри.

Афинен шифър

Афинният шифър е вид субституционен шифър, при който се използва числовият еквивалент на символите от едно множество, което най-често съдържа буквите от зададена азбука. Прилагайки определена несложна функция се определя нова числова стойност, чиято модулна редукция дава нов числов еквивалент, съответстващ на друг символ от същото множество. По този начин се осъществява замяната на символ от открития текст със съответния му в шифрования текст. Множеството от символи съдържа m елемента, като числовите им еквиваленти заемат стойности от 0 до m-1 Използваната функция за шифриране се състои от адитивна и мултипликативна компоненти:

$$E(x) = a.x + b \ (mod\ m) \quad (1)$$

където x е номерът на буквата от явния текст;

m - броят на символите в азбуката;

a и b – компонентите на ключа на шифъра (a, b).

Последните две стойности трябва да принадлежат на множеството Zm = {0, 1, 2, …, m-1}.

Декодиращата функция е

$$\mathbf{D(x) = a^{-1}(y - b)(mod\ m)} \quad (2)$$

където a^{-1} е мултипликативното обратно число на a mod m, т. е. $a.a^{-1} \equiv 1 \bmod m$, а y - номерът на буквата от закодирания текст. За да е възможно декодирането а трябва да има мултипликативно обратно при модул m, т.е. а и m да са взаимно прости числа или gcd(a, m) = 1.

Намирането на мултипликативно обратно на а при модул m става с използването на различни методи, но най често се прилага разширения Евклидов алгоритъм (EEA).

Шифърът се използва и в други две разновидности:

- при избор за a = 1 се получава шифт трансформация или шифърът се свежда до транслиращ шифър;
- при избор на b = 0 – линейна трансформация.

Не представлява трудност да се заместват не отделни символи, а групи от два или три символа (диграфи или триграфи), като се използва афинния шифър. Диграф, състоящ се от два символа, с числови еквиваленти x и y, е с числената стойност, определена по формулата z = x.m+y, а функцията на шифриране е

$$\mathbf{E(z) = a.z + b\ (mod\ m^2)} \quad (3)$$

Транслиращ шифър

Транслиращият шифър, известен още като Шифър на Цезар, е едноазбучен шифър, който както беше споменато по-горе, може да се получи от афинния шифър при избор на ключ от вида (1, b). При това номерът на закодираната буква се определя от израза

$$\mathbf{E(x) = x + b\ (mod\ m)} \quad (4)$$

където x е номерът на буквата от явния текст, m - броят на символите в азбуката, а b - ключът на шифъра.

Декодиращата функция е

$$\mathbf{D(x) = y - b\ (mod\ m)} \quad (5)$$

където y е номерът на буквата от закодирания текст.

Шифър на Виженер

Шифърът на Виженер е многоазбучен субституционен шифър. Той се състои от няколко изместващи шифъра с различни стойности на отместването.

За кодиране и декодиране може да се използва таблицата на Виженер. В нея азбуката е разписана 26 пъти, като на всеки следващ ред буквите се отместват циклично с по една наляво. Това на практика представлява 26 изместващи шифъра. Кодирането се извършва като се избере ключова дума k1k2…ks , която се нанася под явния текст x1x2…xn. Дължината на ключа обикновено е по-малка от явния текст и той се записва няколкократно до края на откритият текст. При недостигане на символи от явния текст в последния запис на ключа може да се извърши допълване на текста.

Таблица 1. Съответствие текст – ключ

x_1	x_2	…	x_i	…	x_j	x_{j+1}	…	x_n
k_1	k_2	…	k_i	…	k_s	k_1	…	k_z

След това се вземат двойките букви текст-ключ и се отчита от таблицата заместващият символ. След повтаряне на действието за всички двойки се получава кодирания текст.

Декодирането се извършва по същия начин, като вместо явния текст се използва кодирания.

Алгебричният запис на шъфъра използва числовите еквиваленти на буквите от

0 до m-1. При криптирането се извършва сумиране на номерата на xi и ki при модул m. Формулата има следния вид:

$$\mathbf{E_k(X_i) = X_i + K_{i(mod\ s)} (mod\ m)} \quad (6)$$

където Xi е числовата интерпретация на i-я символ от явния текст, а Ki(mod s) - съответстващият му символ от ключа. Декриптирането се извършва в обратен ред, като от номера на кодирания символ Yi се изважда номерът на Ki(mod s) на ключа.

$$\mathbf{E_k(Y_i) = Y_i - K_{i(mod\ s)} (mod\ m)} \quad (7)$$

където Yi е числовата интерпретация на i-тата буква от кодирания текст.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Фиг. 1 – Таблица на Виженер

Шифър на Хил

В класическата криптография шифърът на Хил е многоазбучен субституционен шифър, базиран на изчисления и от линейната алгебра. Първо символите се номерират от 0 до m-1, където m е броят на всичките символи в избраното множество. След това явният текст x1x2…xk се разделя на блокове от по n символа. За всеки блок се съставя вектор от номерата на съставящите го символи. След това се избира матрица n x n (mod m) и всеки един от векторите се умножава с нея.

$$(\mathbf{x_\alpha} \quad \dots \quad \mathbf{x_{\alpha+n-1}}).\begin{pmatrix} \mathbf{a_{11}} & \cdots & \mathbf{a_{1n}} \\ \vdots & \ddots & \vdots \\ \mathbf{a_{n1}} & \cdots & \mathbf{a_{nn}} \end{pmatrix} = \quad (8)$$

$$(\boldsymbol{x_\alpha . a_{11} + \cdots + x_{\alpha+n-1} . a_{n1}} \quad \dots \quad \boldsymbol{x_\alpha . a_{1n} + \cdots + x_{\alpha+n-1} . a_{nn}}) \equiv (\boldsymbol{y_1} \quad \dots \quad \boldsymbol{y_n})\ \boldsymbol{(mod\ m)}$$

При това матрицата се разглежда като ключ на шифъра. За да може една матрица да се използва като ключ, тя задължително трябва да има обратна в избраното множество. В противен случай декодирането е невъзможно. Една квадратна матрица има обратна тогава и само тогава, когато детерминантата ѝ е различна от нула и със стойността за m са взаимно прости числа.

Намирането на обратна матрица може да се извърши по метод на Крамер. Първо се намира детерминантата на матрицата. След това се определя нейното мултипликативното обратно число в множеството на целите числа . За всеки елемент на матрицата се изчислява неговото адюнгирано количество

$$\mathbf{A} = \begin{pmatrix} \mathbf{a_{11}} & \cdots & \mathbf{a_{1n}} \\ \vdots & \mathbf{a_{ij}} & \vdots \\ \mathbf{a_{n1}} & \cdots & \mathbf{a_{nn}} \end{pmatrix} \quad (9)$$

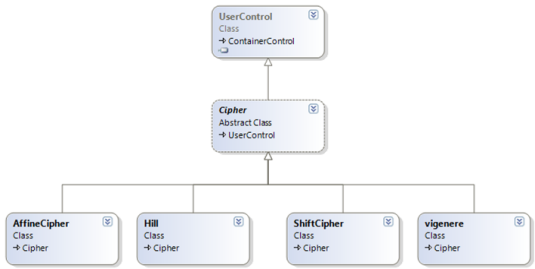
$$\mathbf{A^{-1}} = \mathbf{det(A)^{-1}} \begin{pmatrix} \mathbf{A_{11}} & \cdots & \mathbf{A_{n1}} \\ \vdots & \mathbf{A_{ij}} & \vdots \\ \mathbf{A_{1n}} & \cdots & \mathbf{A_{nn}} \end{pmatrix} \quad (10)$$

$$\mathbf{A_{ij}} = \mathbf{(-1)^{i+j} . det(A'_{ij})}, \quad (11)$$

където A_{ij} е адюнгираното количество на елемента a_{ij}, а A'_{ij} - матрицата, получена след премахването на i-я ред и j-я стълб.

Реализация на софтуера за многократно шифриране

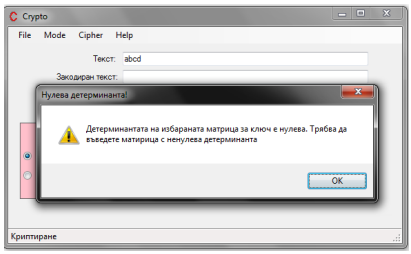
Програмният продукт е реализиран във вид на визуално приложение. Продуктът дава възможност за верижно криптиране на един и същи текст в избрана последователност от различни шифри от зададено множество.



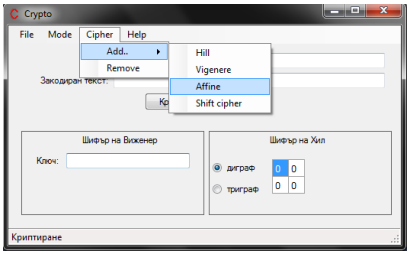
Фиг. 2 – Клас-диаграма на шифрите

За реализиране на верижно криптиране е реализирана клас-диаграмата показана на фиг. 2. При това всички шифри на абстрактния базов клас Cipher наследяват виртуалните методи за криптиране и декриптиране, което позволява създаване на контейнер от тип Cipher и съхраняване на обекти - наследяващите го класове.

След стартиране на програмата от меню Cipher->Add.. се избира последователността от шифри, с която ще се кодира текста (фиг. 3). При погрешно избиране на някой от шифрите, той може да бъде премахнат от последователността чрез бутона „X“, който се появява в горния десен ъгъл на всеки шифър при позициониране на курсора върху него.



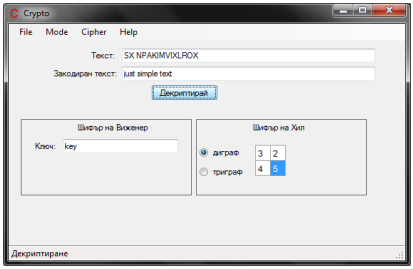
Фиг. 3 – Избор на шифър



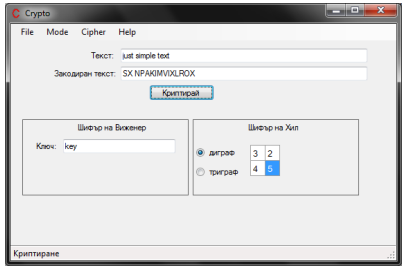
Фиг. 4 – Съобщеие за нулева детерминанта

Въвеждат се явния текст и ключовете за всеки шифър в предвидените за целта полета. В полето за въвеждане на текст програмата допуска въвеждане единствено на символи от множеството $\mathbb{Z}_{27}$ – английските букви a – z и интервал. След това се натиска бутон „Криптирай“, показан на фиг. 5.

При пропускане въвеждането на някой от ключовете, въвеждане на некоректни символи, например букви в матрата на шифъра на Хил, програмата издава подходящо съобщение за конкретната грешка, която е възникнала. Също така, при някои от шифрите, ключовете трябва да отговарят на определи условия, за да бъде възможно декриптирането на съобщение. При въвеждане на ключ, който не отговаря на тези условия програма извежда съобщение за това (фиг. 4)



Фиг. 5 – Криптиране



Фиг. 6 – Декриптиране

За декриптиране се избира последователността, с която е закодиран текста и съответните ключове. От меню Mode се избира Decrypt. Програмата влиза в режим на декриптиране след натискане на бутона „Декриптирай" (фиг. 6). При въвеждане на последоватленост, различна от тази, с която е криптиран текста, няма да се получи правилният открит текст.

ЗАКЛЮЧЕНИЕ

Разработеното програмно осигуряване дава възможност за:

1. Извършване на мнократно шифриране на текст при използване на субституционни шифри.
2. Избиране на използваната последователност от множеството на шифрите, при което е възможно и неограничено по брой използване на един и същ шифър на различни места в последователността.
3. Повишаване на секретността не само поради многократното шифриране, но и вследствие на използването на ключове, които могат да бъдат и от различни множества.
4. Повишаване на устойчивостта на атаки вследствие на секретността не само на използваните ключове, но също така и на избраната последователност от прилагани шифрирания.

ЛИТЕРАТУРА

[1] Modern Cryptography: Theory and Practice, By Wenbo Mao Hewlett-Packard Company, Prentice Hall PTR, 2003, ISBN: 0-13-066943-1,648p
[2] Oppliger, R. Contemporary Cryptography, Artech House, 2005, ISBN I-58053-642-5.
[3] Stinson, D. Cryptography: Theory and Practice, Second Edition, CRC Press, Boca Raton, 2002, ISBN 1584882069

За контакти:

Венцислав Атанасов, Русенски университет "Ангел Кънчев", Специалност "Компютърни системи и технологии", e-mail: ventsislav_atanasov@hotmail.com

гл. ас. Елена Якимова, Русенски университет "Ангел Кънчев", Катедра „Компютърни системи и технологии", тел.: 082-888 276, e-mail: ESimeonova@ecs.uni-ruse.bg

Телеметрия на електрически параметри и комутиране на енергозависими устройства посредством Интернет

автор: Божидар Петров
научен ръководител: гл.ас. д-р Пламен Захариев

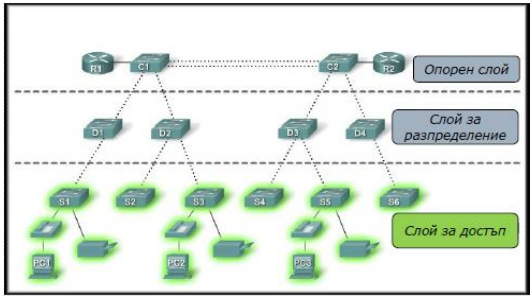
Electrical parameters telemetry and electrical devices switching via internet: *This article describes how to build a station for measurement and remote control on electrical devices, based on microcontroller and IP network technology. The device is small and compact with low energy consumption. The results from the conducted measurements are presented to the client terminal (PC, laptop) through the use of specially developed software, which is also used for control by the user and is written on the software language Delphi [1]. The main hardware part is a controller that actually is an embedded Ethernet IP module. The module can be read and write using SNMP.*

Key words: *PicoIP, voltage measurement, temperature measurement, remote control, monitoring, SNMP*

ВЪВЕДЕНИЕ

Скоростното развитие на микропроцесорната техника и мрежовите технологии доведоха до една съвременна тенденция на технологията за дистанционен мониторинг, която е известна като телеметрия (произлиза от гръцки: tele – отдалечен и metron – следене). Същността на телеметрията се изразява във възможността за измерване на различни физически величини от разстояние, посредством радиовълни или мрежови технологии.

Разработеното устройство се базира именно на същата концепция, като са предвидени функции не само за следене нивото на електрически параметри, но и за комутиране на различни ел. вериги (като най-често това могат да бъдат старт и стоп функциите на всеки вид ел. консуматор).



Фиг. 1 – Логическа топология на съвременните LAN мрежи

И двете функции са достъпни от клиентската станция (лаптоп, персонален компютър). Като обект на разглеждане от към технически профили разработката би представлявала интерес за сферата на микроконтролерите и IP мрежовите технологии. Предвид йерархичното разположение на съвременните LAN мрежи, разработената станция намира място в най-нисшият слой на топологията – именно слоят за достъп (Фиг. 1). Главната цел на IP технологията в случая е предаването на събраната информация и изпращане на команди до контролера, който от своя страна извършва „измерванията" на въпросните параметри.

АПАРАТНА ЧАСТ

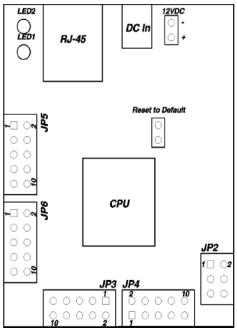
Основна съставяща част се явява интегрирания IP модул, на фирмата „НЕОМОНТАНА-ЕЛЕКТРОНИКС", PicoIP (Фиг. 2) [2]. Модула може да се разглежда като автономно мрежово устройство със стандартен 10Mb/s Ethernet интерфейс.

PicoIP като апаратни възможности разполага с [2]:

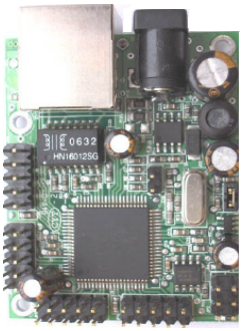
- 8+8 цифрови входове/изходи;
- 8 аналогови (цифрови) входа (10bit ADC);
- Допълнителен 8 канален I/O порт за управление на комутатори;
- Хардуерен RS-232 порт.

Изведените пинове са директни връзки към пиновете на процесора. За изходните портове те са с максимален ток 1mA и нива при 3.3V логика (т.е. лог. 1 се равнява на 3.3V, лог. 0 на 0V). За входните портове максималното напрежение е 3.3V.

На Фиг. 3 е показано разположение на I/O портовете на модула, а в Таблица 1 са дадени значенията им. Като за обслужване нуждите на цялостното устройство се ползват 2 порта, именно JP5 ползващ се като аналогов вход и JP4 ползващ се като цифров изход.



Фиг. 2 – Модул PicoIP



Фиг. 3 – Разположение на I/O портовете

Таблица 1. Значение на входно-изходните портове [2]

	JP3-цифров, I/O			JP4-цифров, I/O			JP5-анал.,цифр., входен		
PIN No.	Bit	Func	DIR	Bit	Func	DIR	Bit	Func	Dir
1	1	Free	I/O	1	Free	I/O	1	Free	Ain
2	2	Free	I/O	2	Free	I/O	2	Free	Ain
3	3	Free	I/O	3	Free	I/O	3	Free	Ain
4	4	Free	I/O	4	Free	I/O	4	Free	Ain
5	5	Free	I/O	5	Free	I/O	5	Free	Ain
6	6	Free	I/O	6	Free	I/O	6	Free	Ain
7	7	Free	I/O	7	Free	I/O	7	Free	Ain
8	8	Free	I/O	8	Free	I/O	8	Free	Ain
9	-	GND	PWR	-	3,3V	PWR	-	3,3Vref	PWR
10	-	GND	PWR	-	GND	PWR	-	GND	PWR

"Free" – пинът е свободен за ползване от потребителя;
"In" – входен пин;
"Out" – изходен пин;
"Ain" – аналогов вход.

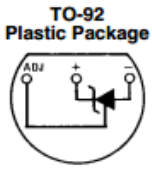
Отдалеченото управление на енергозависимите уреди се изразява в същността на следващата апаратна част, която реално представлява реле, чиято оперативна верига се командва дистанционно посредством PicoIP. Ползва се комплект от 4 релета на фирмата „НЕОМОНТАНА-ЕЛЕКТРОНИКС“ – RelayBoard (Фиг. 4).

Фиг. 4 – Модул RelayBoard

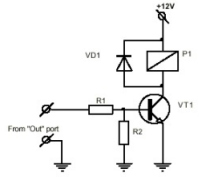
Технически данни на модул RelayBoard [2]:

- Брой канали (релета): 4бр.
- Контактна система: превключващ контакт за 7A/240VDC
- Захранващо напрежение: 12VDC/0.15A;
- Ниво на управляващия входен сигнал: +(2-12)VDC;
- Защита от обратен поляритет на захранването;
- Защита от отрицателно управляващо напрежение;
- LED индикация за включен контакт;

На Фиг. 5 е представена принципна електрическа схема за един от каналите на RelayBoard. Практически оперативната верига, която може да бъде управлявана дистанционно е преходът емитер-колектор на транзистора T1, който работи в ключов режим. Базата на същия се свързва към цифров изход на PicoIP, от където подаваме и управляващите импулси.



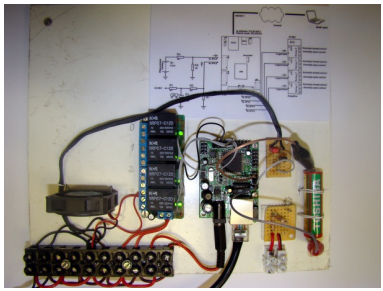
Фиг. 5 – Модул PicoIP



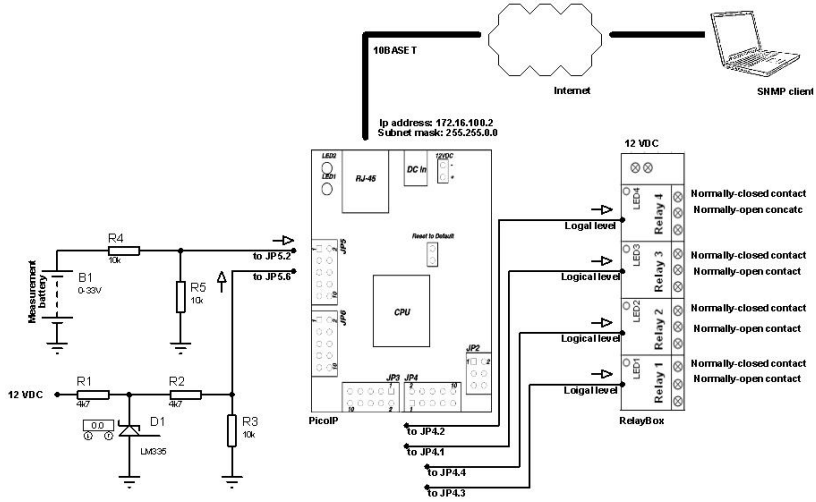
Фиг. 6 – Температурен сензор LM335

Следенето на електрически сигнал по същество представлява аналогово напрежение подавано на АЦП на модула PicoIP. За следенето на други параметри е нужен „преобразувател“ на въпросния параметър в напреженов сигнал. Това е и ролята на температурния сензор LM335Z (фиг.6). Съгласно документацията от производителя трябва да се отбележи, че типична стойност, за 25° C, на изходното напрежение е 2980mV със стъпка 10mV за градус целзий. Предвид допустимото максимално напрежение, на входа на АЦП в PicoIP, което е 3.3V, се препоръчва допълнителен напреженов делител в изхода на сензора. По същата причина се налага ползването на такъв делител и при измерване работните напрежения на акумулатори. В случая е реализиран делител с отношение 1/10, което дава възможност за измерване на акумулатори с максимално напрежение, един порядък по-голям от максималното напрежение за аналогово-цифровия преобразувател или това са 33 V.

Изработен е макет като на Фиг. 7 е показана негова снимка, а на Фиг. 8 е дадена символична схема изобразяваща свързването на отделните компоненти към PicoIP модула. Стойностите, на Фиг. 8, на елементите са използваните при изграждане на макета.



Фиг. 7 – Макет на устройството

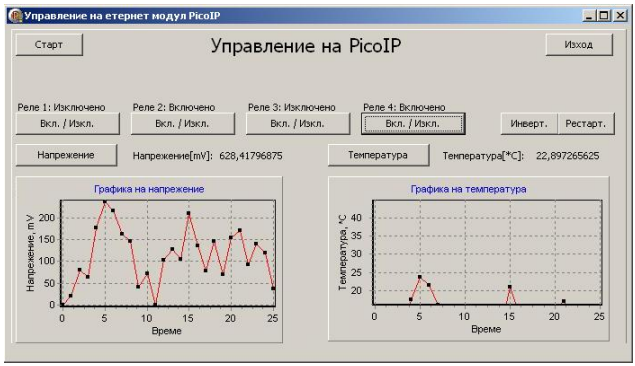


Фиг. 8 – Символична схема изразяваща принципа на свързване с модул PicoIP

СОФТУЕРНО ОСИГУРЯВАНЕ

Всички устройства позволяващи мрежово управление ползват SNMP (Simple Network Management Protocol) [3]. В най-общ случай това е протокол от TCP/IP стека и като значимост трябва да се отбележи, че протокола, който се ползва от транспортния слой е UDP. Идеята за протокола се състои в следните съставни части: SNMP manager, SNMP agent и база данни с управляваща информация. SNMP manager-а и SNMP agent-а ползват същата управляваща информация (Management Information Base – MIB) и относително малък брой инструкции за обмяна на информация. SNMP ползва пет основни съобщения за комуникация между manager-а и agent-а. Две от тях се използват за четене от и записване върху модула PicoIP, съответно snmpget и snmpset. И двете заявки се изпращат от страна на manager-а към agent-а.

За улесняване нуждите на крайният потребител и графично представяне на получените съобщения от модула е реализиран програмен продукт с графична среда (фиг.9).



Фиг. 9 – Потребителски интерфейс на разработеното приложение за управление на PicoIP модула

При стартиране на продукта се дава начално установяване на устройството с бутон Старт. Преди натискането му, никоя от останалите функции на продукта не е активна и не може да бъде използвана. За системата, начално установяване означава изключване на всички консуматори (т.е. релетата са в състояние с отворен контакт); слагане на начална точка за изчертаване на графиките за напрежение и температура. Функцията на бутона се дава със следния псевдо-код:

when press Start do
Turn off all relays;
Start from now to draw graphics;
end

Софтуера предоставя на потребителя четири бутона Вкл. / Изкл. за комутиране съответно на четирите релета. Над всеки бутон е записан номера на релето, което управлява, както и неговото състояние. Като за състояние „Включено" се има в предвид, че съответното реле е със затворен контакт; респективно състояние „Изключено" съответства на отворен контакт. Алгоритъма на четирите бутон Вкл. / Изкл. е еднакъв и се обяснява с псевдо кода:

when press on/off button do
if relay is turn on then turn off;
if relay is turn off then turn on;
end

Продуктът е оборудван и с бутон Инверт., който променя състоянията на релетата или натискането му води до затваряне на всички отворени контакти, съответно отваряне на всички затворени. Действието се обяснява с псевдо код:

when press invert button do
if relay1 is on then relay1 is off;
else if relay1 is off then relay1 is on;
…….
If relay4 is on then relay4 is off;
else if relay4 is on then relay4 is on;
end

Непосредствено в дясно от бутон Инверт. е позициониран бутон Рестарт. Неговата функция е рестартиране на устройствата свързани към релетата, като

бутона рестартира само тези релета, които преди натискането му са били в режим със затворен контакт (т.е. режим: Включено). Процеса за рестартиране отнема 10 секунди, като за това време релетата влезли в такъв режим са маркирани с таг „Рестартиране..."; след като изтекат десетте секунди минават в режим „Включено". Псевдо код за бутон Рестарт:

```
when press restart button do
if relay1 is on then turn off relay1;
wait 10 secs;
turn on relay1;
else
if relay1 is off then do nothing;
…….
if relay4 is on then turn off relay4;
wait 10 secs;
turn on relay4;
else
if relay4 is off then do nothing;
end.
```

Бутони Напрежение и Температура извеждат стойностите на напрежението и температурата като освен това, активират изчертаването на съответните графики с начална точка, приемаща се за център на хоризонталната ос, моментът, в който е натиснат бутон Старт. Всяко натискане на бутон Напрежение или Температура поставя и маркер на стойността върху съответната графика.

ЗАКЛЮЧЕНИЕ

Макета на устройството е тествано и постигна очакващите цели. Идеята за създаване на устройството е ползването му в апаратни зали на телекомуникационни доставчици, където поради технически причини често се налага хардуерно рестартиране (изкл. и вкл. от и към ел. мрежа), както и поставянето на устройството в релейни кули за следене на акумулатори, следене на заряда в UPS-и и др. Идеята е устройството да автоматизира поне по един процес от бранша, който процес иначе се явява разход за управляващата фирма (в предвид изпращането на техник за рестартиране на устройство или направа на измерване). От друга гледна точка предимство е и бързината за изпълнение на задачата.

Приложимостта му в битови условия го прави удобно с възможността му да се осъществява любителски термоконтрол и мониторинг на помещения, водни ризи на парна, бойлери и т.н.

Като развитие на устройството би могло да се добави допълнителен програмен код, който да комутира релетата в зависимост от интервал температура или напрежение, както и съхраняване на отчетената информация.

ЛИТЕРАТУРА

[1] Bob Swart, Delphi 2007 for Win32 Development Essentials, Swat Consult 2012
[2] PicoIP ръководство на потребителя, http://www.neomontana-bg.com
[3] http://www.dpstele.com

За контакти:

Божидар Петров, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: bozhidarpetrov_@abv.bg

гл. ас. д-р Пламен Захариев, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации", тел.: 082-888 663, e-mail: pzahariev@uni-ruse.bg

Цифров оборотомер

автор: Божидар Петров
научен ръководител: доц. д-р Йоана Русева

Digital tachometer with microcontroller: *This article describes how to build a contact-less tachometer (device used to count the revolutions per minute of a rotating shaft) using a PIC18F452 microcontroller, infrared LED and photodiode. The result is presented on alpha-numeric LCD module. The idea behind most digital frequency meters and tachometers is a microcontroller, used to count the pulses coming from a sensor or any other electronic device.*
Key words: *Digital tachometer, contact-less tachometer, PIC18FXX2 microcontroller, display.*

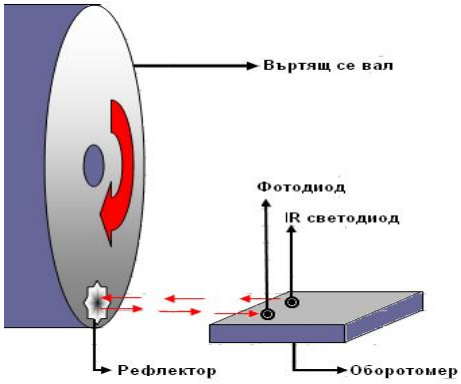
ВЪВЕДЕНИЕ

Тахометърът или оборотомерът е устройство, което следи кръговата честота на детайли, имащи ротационно движение. Честотата е пряко свързана със скоростта на въртене. Най-често срещаната единица в практиката за измерване на тази скорост е обороти за минута – RPM. Традиционния метод за измерване на RPM на въртящ детайл се базира на концепцията на обратната връзка, където постояннотоков генератор е свързан към детайла, така че напрежението, индуктирано в терминалите на генератора, е пропорционално на скоростта на въртене.

Благодарение на развитието на микропроцесорната техника днес е по-лесно да се разработи такъв оборотомер, който да представя информацията в цифров вид, като не е нужен физически контакт между детайла и измерващото устройство.

Изграждане на безконтактен оборотомер

Безконтактният оборотомер е реализиран на базата на микроконтролер PIC18F452. Оборотомерът може да следи скорости до 99930 RPM с точност до +-30 оборота в минута. Взимайки в предвид точността на устройството, както и горната граница на обхвата, е значително важно да се отбележи, че оборотомера е пригоден за високи скорости (от порядъка на хиляди оборота за минута).

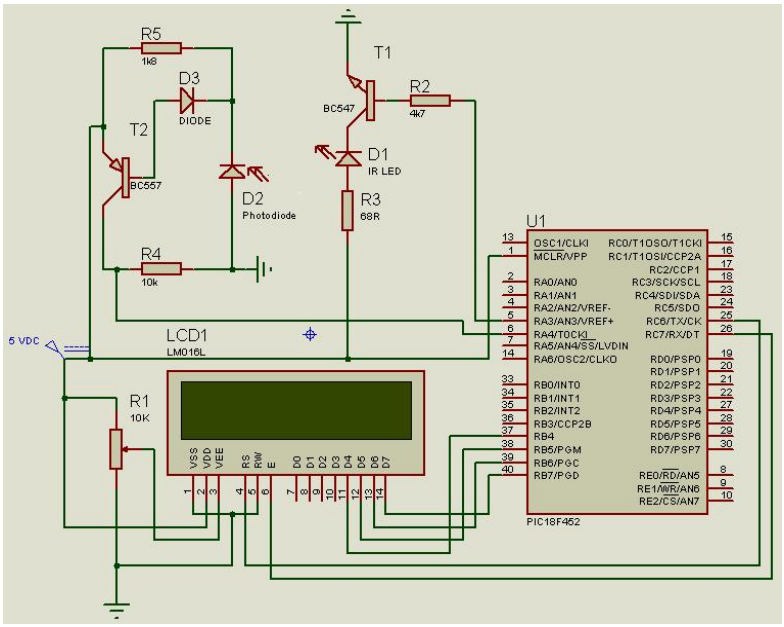


Фиг. 1 – Обобщена схема на оборотомера и въртящия вал

Резултатите се извеждат на двуредов LCD дисплей. Контактът между оборотомера и детайла се осъществява посредством двойка оптични прибори – светодиод, излъчващ в инфра¬червената област (IR светодиод) и фотодиод. IR светодиодът излъчва инфра¬червена светлина в близост до детайла, а фотодиодът приема рефлектираната от детайла светлина. За да може светлината да се отрази и

породи фототок в диода, на детайла се залепя малко парче рефлектор (фолио). Фотодиодът и светодиодът не трябва да бъдат открити един към друг. Така фотодиодът ще бъде осветен само когато излъчването на IR светодиода срещне рефлектора. При наличие на един рефлектор, всяко отражение в него, отговаря на едно завъртане на детайла.

Принципната електрическа схема на оборотомера е представена на фиг. 2. [2]



Фиг. 2 – Принципна електрическа схема на оборотомера

Когато изводът RA3 на микроконтролера е в състояние 1, преходът емитер-колектор на транзистора T1 е отпушен. IR светодиодът D1 започва да излъчва. Отпушването и запушването на транзистора се управлява посредством изход RA3. Той е в състояние 1 в продължение на 2 секунди. През това време отразената светлина създава електрически импулси посредством фотодиода. Получените на колектора на транзистора T2 импулси постъпват на извод RA4/T0CKI на контролера. Това събитие се явява външно за Timer0, който е програмиран да брои външните импулси, постъпили на извод RA4. В положение на покой фотодиодът има много голямо съпротивление и се възприема като прекъсната верига. Транзисторът BC557 е запушен и в колекторната му верига няма ток. Когато фотодиодът получи отразената IR светлина, неговото съпротивление намалява, T2 става проводящ и в колектора му протича ток. Тази проста верига „конвертира" отразената светлина в подходящи импулси за микропроцесора. Всеки импулс съответства на едно завъртане на детайла.

Timer0 е модул в микроконтролера. Той е софтуерно програмируем, като настройките му зависят от състоянията на съответните битове. Операциите се контролират посредством регистъра T0CON. Функцията на всеки бит от регистъра е показана на фиг. 3.[1,3]

За обслужване на оборотомера timer0 е конфигуриран като 16-битов брояч, който отброява импулсите, получени на извод RA4/T0CKI. Броячът е активен за 2 секунди. Броят на импулсите, постъпили за това време, се записват и се умножават по 30, за да се получат оборотите за минута. Бит T0SE е нулиран, за да се инкрементира броячът при преход от ниско към високо ниво (т.е. нарастващ фронт) на импулса. С установяване на бит T0CS в 1 се задава броячният режим на таймер0. Бит PSA се установява в 1, с което се указва, че входящият делител няма да се използва.

R/W-1	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1
TMR0ON	T08BIT	T0CS	T0SE	PSA	T0PS2	T0PS1	T0PS0
бит 7							бит 0

бит 7: TMR0ON: бит за включване/изключване на Таймер0
1 = разрешава Таймер0
0 = спира Таймер0
бит 6: T08BIT: бит за избор на 8-разряден/16-разряден режим
1 = Таймер0 се конфигурира като 8-разряден таймер/брояч
0 = Таймер0 се конфигурира като 16-разряден таймер/брояч
бит 5: T0CS: бит за избор на източника на такт за Таймер0
1 = преход на извод T0CKI
0 = вътрешният такт за цикъл на инструкцията (CLKOUT)
бит 4: T0SE: бит за избор на активния фронт на такта за Таймер0
1 = преход от високо към ниско ниво на извод T0CKI
0 = преход от ниско към високо ниво на извод T0CKI
бит 3: PSA: бит за предоставяне на делителя
1 = делителят е предоставен на стражевия таймер
0 = делителят е предоставен на таймер 0
бит 2:0: T0PS2:T0PS0: битове за избор на коефициент на деление

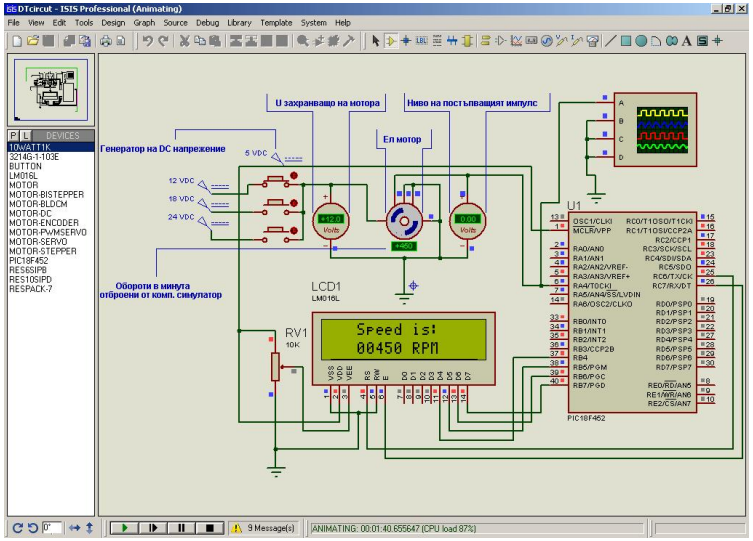
Фиг. 3 – T0CON: управляващ регистър за модул TIMER0

В общия случай алгоритъмът на цикъла, описващ действието на устройството, може да се представи със следния псевдокод:

```
Constant
i : integer
Variable
x : integer
i=1
for i>0 do
start pulse counter; // Start timer0
zero pulse counter; // Load Timer0 with 0x00
turn on IR LED; // Generate current on every revolution
wait for 2 seconds then;
turn off IR LED; // Stop to generate current
stop pulse counter; // Stop timer0
value from pulse counter=x; // Store in variable number of revolutions for 2 secs
x=30*x; // (Revolutions for 2 secs)*30 is actually revolutions for one minute
present value from x; // present result on Display
end.
```

РЕЗУЛТАТИ

Алгоритъмът на програмата е тестван с компютърна симулация с помощта на програмния продукт PROTEUS (фиг.4), където отражението на IR светлината няма как да се симулира. Поради тази причина симулацията беше реализирана с постояннотоков двигател, съдържащ изход, на който се генерира импулс при всяко завъртане на мотора. Показанието на LCD дисплея отговаря на показанията от вградения компютърно симулиран оборотомер на двигателя. Честотата на опресняване на резултатите е 2 секунди.



Фиг. 4 – Симулация на цифровия оборотомер с програмен продукт PROTEUS

ЗАКЛЮЧЕНИЕ

Чрез въвеждане на допълнителен програмен код и използване на допълнителни модули на микроконтролера, оборотомерът може да се развие в станция, която да съхранява отчетената информация и да бъде анализирана от компютър.

ЛИТЕРАТУРА

[1] http://www.microchip.com
[2] http://embedded-lab.com/
[3] Русева Й., Бенчева Н., Микропроцесорна схемотехника – ръководство за упражнения, Русе, Русенски университет 2008 г.

За контакти:

Божидар Петров, Русенски университет "Ангел Кънчев", Специалност "Телекомуникационни системи", e-mail: bozhidarpetrov_@abv.bg

доц. д-р Йоана Русева, Русенски университет "Ангел Кънчев", Катедра „Телекомуникации", тел.: 082-888 673, e-mail: yruseva@uni-ruse.bg

Услуги за информираност за енергопотреблението

автор: Станислав Стефанов
научен ръководител: проф. д-р Никола Михайлов

Abstractl: *BECA services will be offered to 165 tenants, including people from all ages with a medium and high education level, mostly Bulgarian and generally with access to the Internet at home.*

The Resource Use Awareness Services (RUAS) will deliver tenants with direct timely and comprehensible feedback on the impact of their behaviour on a full range of resource uses, thereby enabling tenants to help us all save energy and water and themselves save money.

Key words: *BECA, project, Internet, Ruse, energy, saving, services, dwellings.*

ВЪВЕДЕНИЕ

Изграждането на услуги за информираност за енергопотреблението (Resource Use Awareness Services), е част от проекта – BECA (Balanced European Conservation Approach), финансиран от Европейския съюз. Целта на проекта е мониторинг и намаляване консумацията на електроенергия и вода, в сгради за социално настаняване в няколко страни в Европа. За да се намали пиковата и непълноценно използвана електроенергия и вода, участващите представителите на различните страни, разработват иновативни информационни системи, които следят консумацията водно-енергийните ресурси. Системите са директно насочени, към анализиране на потреблението и изготвяне на съвети към живущите наематели на тези социални жилища. Целта на проекта е намаляване на консумацията на електроенергия и вода до 20%.

ИЗЛОЖЕНИЕ

Описание на услугите

В предлаганата разработка, наемателите ще имат достъп до следните услуги:

- Уеб сайт за потребителите, предоставящ информация за консумацията на електроенергия и вода за всяко жилище;
- Месечни отчети, с препоръки за по-ефективна консумация;
- Графично сравнение на консумацията от предходни периоди и тази на подобни домакинства;

Характеристики и параметри на услугите

Съществена част на разработката е проектиране на мощна информационна система, в която най-важните предоставени услуги са:

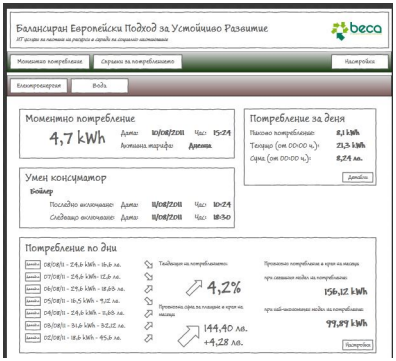
- Обща информация;
- Статистически данни за консумирана електрическа енергия за отопление, битова употреба и студена вода;
- Период на обновяване на данните: 30 min;
- Сравнения с предишни периоди и подобни домакинства;
- Тип на представените данни: Физически единици и парична стойност;
- Задаване на цели: Например, наемателите могат да задават праг на сметката си и дата, на която се очаква да се достигне този праг.
- Прогнози: Порталът прогнозира месечната сметка, на базата на консумацията на ток и вода, статистиката от предходни периоди и референтни стойности от подобни жилища;
- Предупреждения(в портала, чрез e-mail, SMS, телефонно обаждане): Наемателите могат да настроят портала да ги предупреждава чрез посочените методи, когато поставеният праг е достигнат;
- Съвети за пестене: Въз основа на текущото потребление, референтни

стойности и подобни домакинства, системата дава съвети. Съветите за спестяване на енергия при определени обстоятелства, са записани в системата от енергиен експерт и се показват, когато данните за потреблението изпълняват определени условия;

- Известяване по e-mail: Порталът може да бъде настроен да изпраща ежедневно, ежеседмично или ежемесечно данни за консумацията на електрическа енергия и студена вода;
- Енергийни треньори: В случаите, когато автоматичните съвети не дават резултати, с наемателите се свързват експерти, които да им дават съвети как да работят с портала и как да променят поведението си на консуматори.

Имайки в предвид количествата изразходвана електроенергия за едно домакинство и динамиката на електропотреблението, отчитането на консумираната енергия се извършва през 30 min. При отчитане на консумацията на вода интервала е от 1 h. Ако потребителите желаят, могат да получат информация и за външната температура.

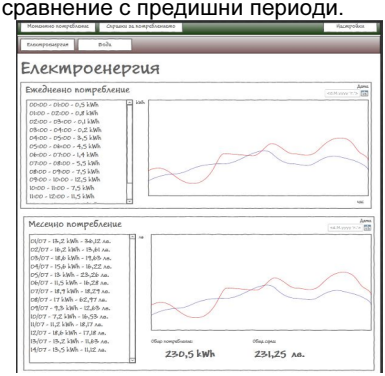
На следващите фигури са представени някои функционални характеристики на портала.



Фиг. 1 – Страница с информация за потреблението на електроенергия

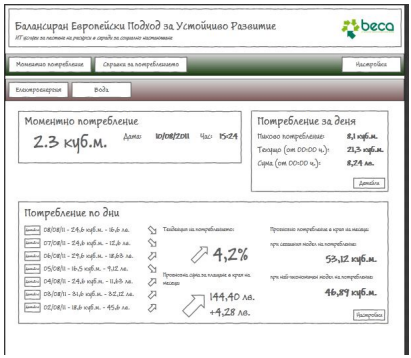
Страниците са два типа:

- с информация за моментното потребление;
- за справка и сравнение с предишни периоди.



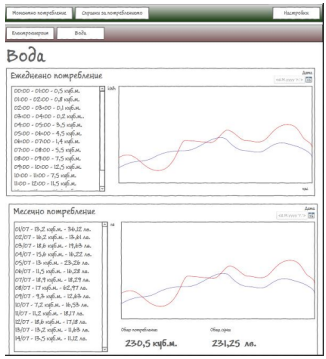
Фиг. 2 – Страница с графика за справки на електропотреблението

Използват се две навигационни ленти - едната служи за преминаване от справки за електроенергия към справки за вода, а втората лента е изградена от 3 бутона.



Фиг. 3 – Страница с информация за потреблението на вода

Първият е за преминаване към страница с моментното потребление, вторият - към справки за предишни периоди, а третият - за преминаване към настройки за потребителя.



Фиг. 4 – Страница с графики за справка на потреблението на вода

В основната част на страницата, показана на фигурите, е разположена статистическа информация за потреблението. За удобство на наемателите информацията е представена и в графичен вид. Използвани са абсолютни измерителни единици - kWh, m3, проценти, лв.

ЗАКЛЮЧЕНИЕ

С реализирането на информационния портал, реално започва мониторинг, контрол, и прилагане на съвети, дадени от енергийните експерти. В следствие на тези действия се очаква намаляване с до 20 % на консумацията на електроенергия и вода. Разработеният портал допълва пакета от електронни услуги.

ЛИТЕРАТУРА

[1] Bembey.P., Kaur.K. Microsoft Visual Basic .NET Professional projects. Premier Press, Inc, 2002

[2] Connell.J., Coding Tehniques for Microsoft Visual Basic .NET. СофтПрес ООД, 2003
[3] DELIVERABLE 1.2 Requirements for BECA services and systems v2
[4] http://beca-project.eu/index.php - Уеб сайт на проекта

За контакти:

Станислав Стефанов, Русенски университет "Ангел Кънчев", Специалност "Компютърни системи и технологии", e-mail: snstefanov@uni-ruse.bg

проф. д-р инж. Никола Михайлов, Русенски университет "Ангел Кънчев", Катедра „Електроснабдяване и електрообзавеждане", тел.: 082-888 843, e-mail: mihailov@uni-ruse.bg

РУСЕНСКИ УНИВЕРСИТЕТ
“АНГЕЛ КЪНЧЕВ”

СТУДЕНТСКА НАУЧНА СЕСИЯ СНС’13

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’12

Под общата редакция на:
доц. д-р Теодор Илиев
ас. Григор Михайлов

Отговорен редактор:
проф. д-р Ангел Смрикаров

Народност българска
Първо издание

Формат: А5
Коли: 7,25
Тираж: 20 бр.

ISSN 1311-3321

ИЗДАТЕЛСКИ ЦЕНТЪР
на Русенски университет “Ангел Кънчев”