ГОДИШНИК

НА ШУМЕНСКИЯТ УНИВЕРСИТЕТ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

ТЕХНИЧЕСКИ НАУКИ

Т. V Е

ANNUAL

OF KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN

Vol. V E

FACULTY OF TECHNICAL SCIENCES

Универистетско издателство
“Епископ Константин Преславски“ 2015

Настоящият годишник съдържа доклади изнасяни през 2014 от преподавателите във Факултета по технически науки

Отговорен редактор: *доц. Атанас Атанасов*
Ред. колегия: *доц. Пламен Чернокожев*
доц. Пламен Михайлов
доц. Николай Досев

ISSN 1311-834X

Съдържание

КВАНТОВИТЕ ТОЧКИ И ПРИЛОЖЕНИЕТО ИМ В ТЕЛЕВИЗИЯТА

Атанас К. Атанасов

THE QUANTUM DOTS AND THEIR APPLICATION IN TELEVISION

Atanas K. Atanasov

ABSTRACT: *This report is referring to the analysis of the possibility of application of the quantum dots in television conductors. The quantum dots as fragments from a semi-conductor with an exact size emit in a particular frequency range, enabling the appearance of a colored image.*

KEYWORDS*: quantum dots, display, CCD matrix, QLED.*

Потребителската част на една телевизионна система е най-динамичната такава, защото позволява да се прилагат нови методи и технологии в областта на обработката и изобразяването на видеоинформацията. При това разходите по разработката, експериментирането и производството на нови модели телевизионни приемници се възстановяват при реализацията им на пазара. Дълго време телевизорите с кинескопи бяха използвани поради възможностите им да формират висококачествено цветно изображение. Но техните основни недостатъци –големи маса и обем, и сложно и скъпо производство на вакуумните тръби ги направи неконкурентно способни по отношение на телевизорите с плоски екрани -плазмени и течнокристални. Основните принципи за изграждане на плоскоекранни телевизори са известни отдавна, но дълго време не можеше да се постигне добра технико-икономическа ефективност при тяхното производство и експлоатация. Благодарение на многобройните изследвания и усъвършенстване на технологията на производство течнокристалните (LCD) телевизори, доминират на пазара на телевизори и монитори. Но те имат съществен недостатък. Сами по себе си течните кристали не светят. А тяхната подсветка, основно

светодиодна, излъчва главно в синята част на видимия спектър, и е по-интензивна от всички останали. Контрастността и интензивността на основните цветове потискат полутоновете и оттенъците. Появата на шлейф усложнява качественото предаване на естествените движения на движещите се обекти. При самото производство или експлоатацията е възможна появата на „мъртви пиксели“. Но те притежават редица преимущества, като ниска работна температура, която изключва прегарянето на екрана, широк зрителен ъгъл, много добри показатели по отношение на контрастността, яркостта и интензивността. Експлоатационният ресурс може да достигне 60000 часа, при това потреблението на енергия е доста икономично. Екранът няма рентгеново излъчване.

Плазмените екрани имат преимущества по отношение на течнокристалните с това че имат голяма излъчваща повърхност, висока контрастност и дълбочина на цветовете особено черния, отлична цветонаситеност и по- естествено изобразяване на движещите се обекти. Наред с това те притежават и редица недостатъци- екранът може да прегори поради високата работна температура и излъчване на голямо количество топлина. При отклонение на ъгъла на обзор се забелязват пикселите, а техният размер не може да бъде намален под 0,4 мм. Ресурсът им е 30000 часа, 9 години при 8 часа работа на ден.

Изследванията в областта на нанотехнологиите позволиха на някои производители на телевизионна техника да постигнат значителни успехи при използването на квантови наноточки за изработване на дисплеи.

Квантовите точки представляват неорганични полупроводникови кристали на CdSe, ZnS, Pbs, InP и други, чийто размери са по малки от радиуса на Бор за екситона на съответния полупроводников материал. Това води до така наречения ефект на квантово ограничение, който се състои в това че във валентната зона и зоната на проводимост на полупроводниковия кристал се формират ясно изразени дискретни електронни нива което обуславя флуоресцентния потенциал на квантовите точки. Енергетичната разлика между поднивата във валентната и проводимата зона на квантовите точки е няколко електронволта (eV). Това обуславя и дискретната флуоресцентна емисия във видимата област на спектъра при възбуждане на нанокристала. При разстояние между нивата 1,7 eV се регистрира емисия в червената област на спектъра, а при 2,4 (eV) в зелената област. Чрез манипулиране на кристалното ядро може да се получат наночастици с желани електронни нива и предсказуем дискретен тесен спектър на емисия. Понастоящем размерите на квантовите точки и техните спектрални

характеристики могат прецизно да бъдат контролирани в хода на тяхното нуклеиране и растеж. Получават се хомогенни дисперсии от наночастици флуоресциращи в различни диапазони на спектъра.

Тъй като квантовите точки са фрагменти от проводник или полупроводник с точно определен размер, и излъчват в определен диапазон, това позволява формирането на цветно изображение. Освен това спектърът на излъчване на всяка точка е строго определен от нейния размер, и той може да бъде настроен доста точно, за разлика от светодиодите, които не могат да бъдат контролирани дори и по принцип.

Колоидните квантови точки са полупроводникови нанокристали с размер 2-10 нанометра и състоящи се от 103-105 атоми създадени на основата на неорганични полупроводникови материали Si, InP, CdSei и други, покрити с монослой от органични молекули играещи ролята на стабилизатор. Колоидните квантови точки обединяват физическите и химически свойства на молекулите с оптоелектронните свойства на полупроводниците. Квантово размерните ефекти имат ключова роля в оптоелектронните свойства на квантовите точки. Енергетическият спектър на квантовата точка принципно се различава от обикновения обемен полупроводник. Електронът в нанокристала се държи като в тримерна потенциална яма. Съществуват няколко стационарни енергийни нива за електроните и дупките с характерно разстояние между тях.

По такъв начин енергетическият спектър на квантовата точка зависи от нейния размер. Аналогично на преходите на атомите между отделните енергийни нива при преминаването на носителите на заряда между енергетическите нива в квантовата точка може да поглъща или излъчва фотон. Честотата на преходите, респективно дължината на вълната при поглъщането или луминисценцията може лесно да се управлява, изменяйки размерите на квантовата точка. По отношение на полупроводниковите материали това може да бъде наречено възможност за контрол на ефективната ширина на забранената зона. Възможността за изменение на дължината на вълната на луминисценцията и сравнително лесното създаване на тънки слоеве на основата на квантови точки дава големи възможности за създаването на светодиоди и плоски екрани. Използването на струен печат е очакван пробив в технологията на органичните телевизионни матрици.

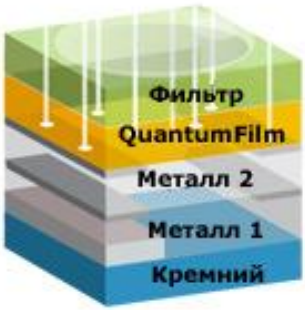
Едно от свойствата по което колоидните квантови точки се различават от обикновените полупроводникови материали е възможността за съществуване във вид на разтвори. Това качество разширява кръга от възможности за манипулация на тези вещества и ги

прави привлекателни за различни технологии. Зависимостта на енергетическия спектър от размера има огромен потенциал за приложение на квантовите точки за практическото им използване. Те могат да намерят приложение в оптоелектронните системи, светодиодите и плоски светоизлъчващи панели, лазери, слънчеви батерии, фотоелектрически преобразователи, в медицината като биологически маркери и изобщо там където са необходими променливи пренастройваеми по дължината на вълната оптически свойства. Основните изисквания към полупроводниковите материали на основата на които се синтезират квантовите точки е на първо място линейният характер на зонния спектър, чрез който се осигурява ефективна луминесценция и малката ефективна маса на носителите на заряд, осигурява квантово- размерните ефекти в достатъчно широк диапазон от размери. По този начин, като се изчислят необходимите размери могат да се създадат светодиоди с червен, оранжев, жълт или зелен цвят. И още едно преимущество на тези устройства – тяхната висока яркост – до 9000 кd/кв.м., докато яркостта на съвременните дисплеи не надвишава 500 кd/кв.м. Способността им да светят, когато са подложени на въздействието на електричество, ги прави приложими при разработването на телевизионни панели от ново поколение-квантови QLED.

Съществуват две направления при използването на квантовите точки в телевизионната техника. Първото, и по-лесно технологически реализуемо, е нанасянето на разтвор от квантови точки върху светодиоди. Оптиката на светодиодите задържа почти 90% от излъчената светлина. Нещо повече, технологията позволява лесно да се увеличи яркостта на светодиодите – само с формирането на няколко квантови точки. Нанасянето на квантови точки върху светодиодите на фоновото подсветяване на течнокристалните дисплеи позволява да се преобразува излъчваната бяла светлина по- ефективно от съвременните цветови филтри. Ако новият дисплей възпроизвежда същите цветове като съвременните дисплеи, то енергопотреблението ще е с 10% по ниско, ще имат по-широк цветови диапазон и ще използват по- голяма част светлината. Съвременните течнокристални панели позволяват да се възпроизведат около 72% от цветовете определени в стандарта NTSC. Прилагането на новата разработка позволява този показател да достигне 103 %.

Ограничението в размерите на CCD матриците използвани във фотоапаратите и телевизионните камери е един от факторите влияещи на реалното качество на картината. Това зависи не само от броя на пикселите, но и от общата ефективност на преобразуване на светлината

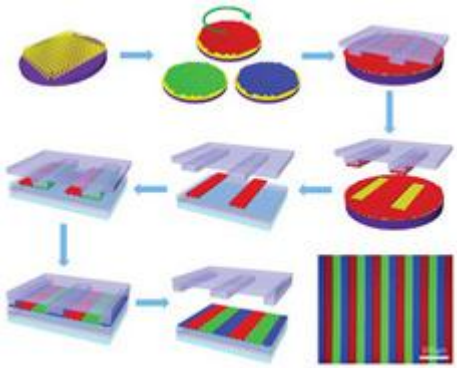
в електрически сигнали. Нанасянето на покритие от квантови точки върху матрицата може да реши този проблем. Квантовото покритие с дебелина около 1.10^{-6} m. се нанася върху матрицата CMOS CCD, а отгоре сее нанасят цветовите филтри за основните цветове. В традиционните матрици около 50% от падащата светлина се губи заради попадането върху проводящите линии и (TFT) транзисторите. Те блокират фотоните, които трябва да попаднат в силициевият слой намиращ се най- отдолу на матрицата. От тези фотони, които все пак достигат до силициевата пластинка, поне половината пропадат поради невисоката квантова ефективност на силиция.



Фиг.1

Филмът от квантови точки покрива 100% от площа на пиксела и не се засенчва от никакви други елементи, а квантовата ефективност на поглъщане е близо до абсолютната (фиг.1). В резултат на това, новата матрица може да прихване до 97% от попадащата върху нея светлина. Тази висока ефективност може да се използва в различни електронни видеоустройства- уеб камери, камери за външно наблюдение и ендоскопи,за технически и за медицински цели.

Реализацията на квантовите точки под формата на течен разтвор позволява и разработването на технология за структуриране на плоски дисплеи.



Фиг.2.

Върху силициева пластина се нанася слой от разтвор на квантови точки от кадмиев селенид и се напръсква с разтворител. След това в този слой с квантовите точки се запресова силициева матрица с гребенчата повърхност, и с нейна помощ се щамповат ивици квантови точки, отговарящи за определен основен цвят върху стъкло или друг прозрачен материал. В цветните дисплеи всеки пиксел съдържа червен, син и зелен субпиксел. Лентите се нанасят непосредствено върху матрица от тънкослойни полеви транзистори (TFT). Транзисторите са от аморфен хафниево-индиево-цинков окис, способен да пропуска по-големи токове и притежаващ по-висока стабилност, отколкото силициевите транзистори. (фиг.2). При прилагане на тази технология дисплеят има субпиксели с размери 50.10^{-6} m и 10.10^{-6} m. Като недостатък може да се отбележи недостатъчният експлоатационен срок-около 10000 часа. За сега тази технология позволява изработването на сравнително малки дисплеи, но положителните качества на квантовите точки са голям стимул за производителите и в скоро време се очаква появата на пълноразмерни квантови дисплеи.

ЛИТЕРАТУРА

1. Румяна А. Желева. Разработване на мултифункционални бионанопроби на основата на квантови точки:структура физикохимични характеристики и приложение за флуоресцентни имиджинг анализи и фотосенсибилизация. Автореферат на дисертация. София.2011 г.
2. Конов К. Телевизионна техника. Издателство ДИОС София, 2005 г.
3. Конов К. Цифрова телевизия. ДИОС София 2001 г.
4. http://www.pctechguide.com/
5. http://www.pcworld.com/

ГЕНЕРАТОР ЗА ИЗСЛЕДВАНЕ НА АМПЛИТУДНО ЧЕСТОТНИ ХАРАКТЕРИСТИКИ

РУМЕН Г. ЦАКОВ

GENERATOR FOR THE STUDY OF MAGNITUDE FREQUENCY RESPONSE

RUMEN G. TSAKOV

***ABSTRACT**: THE magnitude frequency response (MFR) is an important feature for many units and components (amplifiers, RC filters, LC filters, quartz filters, resonators). Lately received development a new class devices - the so-called vector network analyzers for the study of MFR in a complex form or as a module of the transmission coefficient and phase shift for the frequency. But these devices are very expensive and rare measurement tools.*

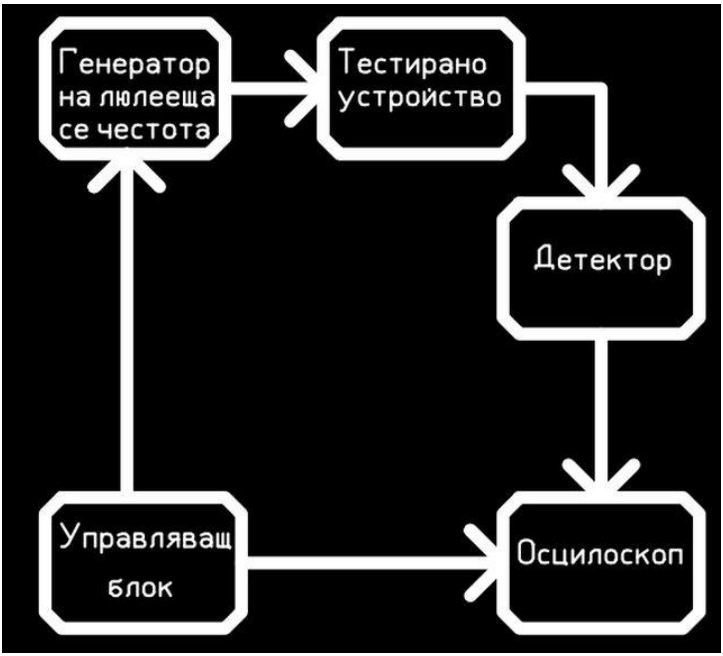
***KEYWORDS**: Sweep generator, MFR, filters.*

Амплитудно честотната характеристика (АЧХ) е важна характеристика за много четириполюсници и компоненти (усилватели, RCфилтри, LCфилтри, кварцови филтри, резонатори и др.). В последно време получиха развитие нов клас устройства – така наречените векторно мрежови анализатори, които позволяват да се снеме АЧХ в комплексна форма или във вид на модул от коефициента на предаване и фазовото изместване от честотата. Но тези устройства са много скъпи и редки инструменти за измерване.

АЧХ представлява зависимостта на модула на коефициента на предаване на тестираното устройство или компонент от честотата. В много случаи е достатъчно да се използват скаларни построители на АЧХ, например на основата на генератор на люлееща се честота (sweep generator), детектор и осцилоскоп (фиг. 1).

Генераторът на люлееща се честота осигурява синусоидален тестов сигнал, чиято честота е пропорционална на управляващото напрежение, което се изменя по линеен, логаритмичен или друг закон. Управляващото напрежение също се подава и на входа на хоризонталния канал на осцилоскопа, а сигналът от тестираното

устройство през детектора се подава към вертикалния канал на осцилоскопа. В резултат на това тестираното устройство се тества със синусоидален сигнал с непрекъснато изменяща се честота, и на екрана на осцилоскопа се изобразява неговата АЧХ.



Фиг. 1. Функционална схема на устройство за снемане на АЧХ с помощта на генератор на люлееща се честота , детектор и осцилоскоп.

Важен параметър на измерителите на АЧХ се явява динамичният диапазон - разликата между максималното и минималното ниво при снемане на АЧХ. При линеен мащаб горе посочените устройства имат динамичен диапазон в рамките на 14-24 dB, тоест той не е висок, и само в логаритмичен мащаб може да достигне до 40db или повече [1].

Преминаването към съвременна елементна база и прилагането на директен цифров синтез на честота (DDS), позволява да се създаде ново поколение генератори с висока честотна стабилност и пренастройка на честотата от хилядни от херца до няколко гигахерца (а понякога и

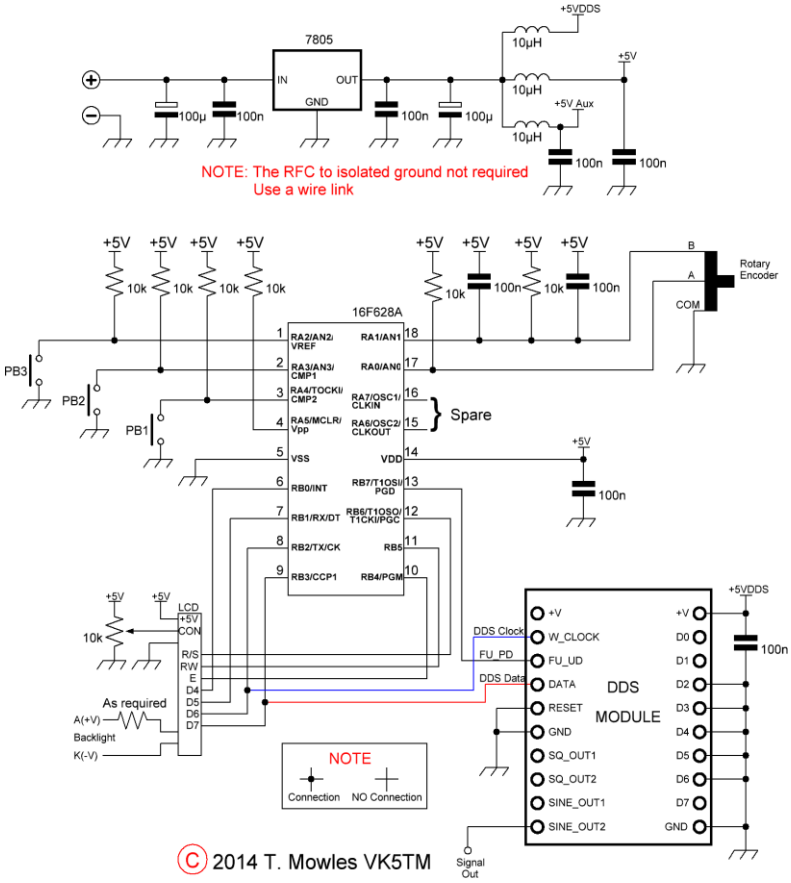
десетки гигахерца). Обикновено, това са малогабаритни прибори с малко тегло и с лесно управление на честотата и нивото.

Използването на детектор е една от пречките за получаване на голям динамичен обхват и точна АЧХ на различни устройства и компоненти. За съжаление, полупроводниковите диоди, които се използват за детектори имат силно нелинейна характеристика.В резултатът на това се наблюдава зона на нечувствителност на детекторите при ниски напрежения и значителни грешки при средно ниво на сигналите. Това води до значително намаляване на динамичния диапазон на измерителите на АЧХ. В някои случаи, например при по-високи честоти от десетки MHz е недостатъчно и бързодействието на диодите.

Тези недостатъци се елиминират чрез премахване на детектора при снемане на АЧХ. При това осцилоскопът трябва да бъде с достатъчно висока честота за директно гледане на изходния сигнал. При максимална честота осцилоскопа обикновено се нормира на -3db (или 0,7 от нивото на ниските честоти). Такъв спад създава неприемливо голяма грешка. За да бъде това е незначително (на нивото на 0,5-1 db), горната гранична честота на осцилоскопа трябва да бъде няколко пъти по висока от тази на тестираното устройството. Тя се определя преди всичко от максималната честота на генератора на люлееща се честота. Налице е тенденция към използване на генератори с директен цифров синтез на честота и генератори с произволна форма [2, 3]. Тяхното приложение позволява да се разшири броят на видовете сигнали, използвани за тестване.

Съобразявайки се с гореизложеното бе изработен генератор на люлееща се честота (sweep generator) на базата на DDS AD9851, микросхема на фирмата ANALOG DIVICES.

Генераторът се управлява от процесор PIC16F628A със специален за целта софтуер (фиг. 2).

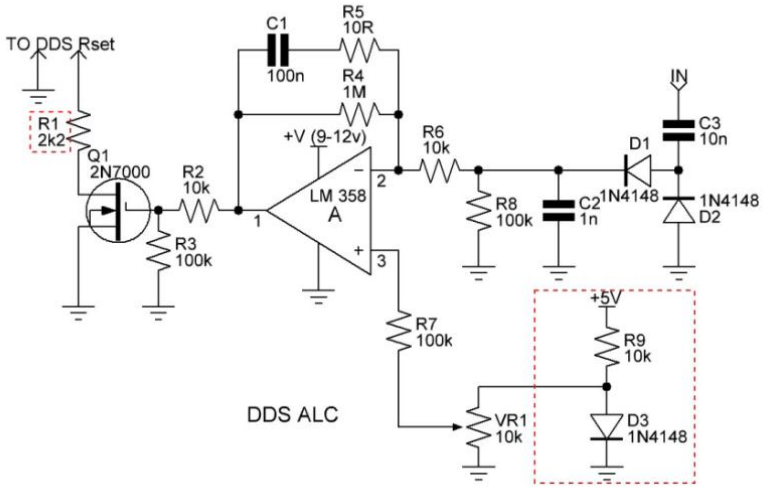


Фиг. 2. Принципна схема на sweep generator

Технически характеристики:

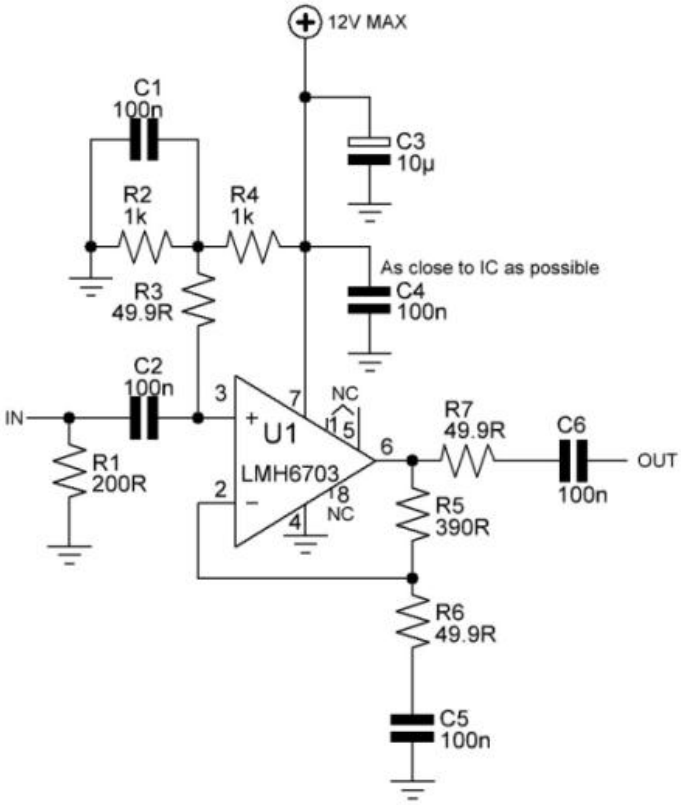
Диапазон на пренастройка:…….0.001 Hz……40,000 MHz
Стъпка на пренастройка:…….0.001 Hz…….10,000 MHz
Напрежение на сигнала върху товар 50 ом…….0,7V

За постигане на постоянна амплитуда на изходния сигнал се използва специална схема (фиг.3) за автоматично регулиране на изходното ниво с помощта на детектор (D1, D2), операционен усилвател (LM358) и полеви транзистор (Q1 – 2N7000).



Фиг. 3. Схема за автоматично регулиране на изходното ниво

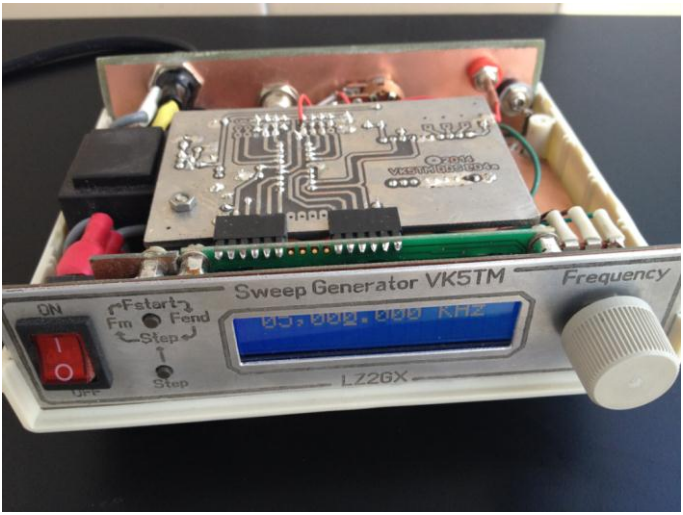
Поради това, че изходното напрежение на DDS AD9851 е доста малко се използва широколентов усилвател с интегрална схема LMH6703 с голяма товароспособност, която осигурява на изхода ВЧ напрежение 0,7V при товар 50 ома (фиг.4).



Фиг. 4. Широколентов усилвател

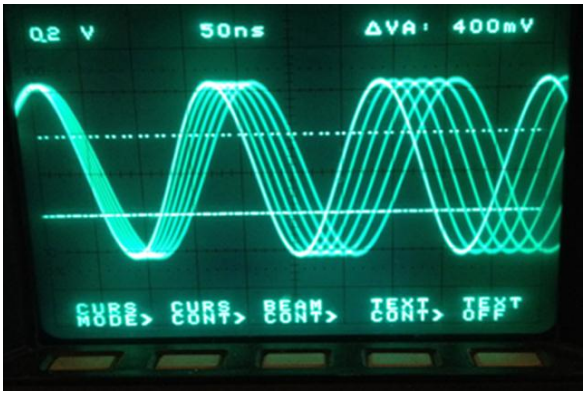
На фиг.5 е показан външният вид на генератора, а на фиг.6 е показан същият генератор със свален горен капак.

Фиг. 5. Външен вид на генератора



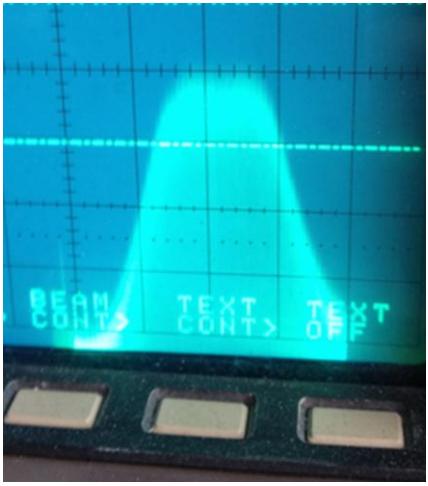
Фиг. 6. Изглед нагенератора със свален горен капак

На фиг.7 е показан изходният сигнал от генератора.



Фиг. 7. Изходен сигнал от генератора

На фиг.8 е показано как изглежда АЧХ на кварзов филтър.



Фиг. 8. АЧХ на кварзов филтър

Литература:

1. Дьяконов В. П. Построитель АЧХ осциллограф или анализатор спектра.
2. http://www.kit-e.ru/articles/oscillograph/2010_12_159.php
3. Дьяконов В. П. Генерация и генераторы сигналов. М.: ДМК-Пресс, 2009.
4. DDS Signal Generator http://www.vk5tm.com/homebrew/dds/dds.php

СТЕПЕННИ ПОСЛЕДОВАТЕЛНОСТИ НА ЯКОБИ С ЕДНО НИВО НА ПЕРИОДИЧНАТА АВТОКОРЕЛАЦИОННА ФУНКЦИЯ

Живко В. Живков, Стефан Ст. Желев, Деница Д. Великова

STEPWISE SEQUENCES OF JACOBI WITH ONE LEVEL OF THE PERIODIC AUTOCORRELATION FUNCTION

Zhivko V. Zhivkov, Stefan St. Zhelev, Denitsa D. Velikova

ABSTRACT: *Has made extensive analysis of stepwise sequences of Jacobi with one level of the periodic autocorrelation function. The results obtained are compared with existing.*

KEYWORDS: stepwise sequences of Jacobi, periodic autocorrelation function, relatively level, coefficient of loss, optimal stepwise sequences.

1. Въведение.

Използването на сложни сигнали в съвременните радиолокационни устройства е актуален въпрос. С тяхна помощ може да се подобри както електромагнитната съвместимост и шумозащитеността, така и качеството на работата. Целта е да се получат импулсни последователности с минимално, или нулево, ниво на страничните листи на импулсната автокорелационна функция.

Целта на настоящия доклад е да се споделят резултатите от проведеното изследване на степенни последователности на Якоби с едно ниво на периодичната автокорелационна функция.

Достатъчно условие за съществуване на N-позиционна степенна последователност (μ) с периодична автокорелационна функция (ПАКФ) с едно ниво е съществуването на разликово множество с параметри $D(N, K^+, \lambda)$ където N са броят на елементите на степенната последователност, K^+ – броят поредни "1" в степенната последователност, а λ – броят на произведенията "1 . 1" в степенната последователност [1].

Известни са няколко, такива семейства от разликови множества [2]. В [1] са дадени само тези от тях, които позволяват да се получи периодична автокорелационна функция с едно ниво:

(1) $D\left(4.x+3,\ \ 2.x+1,\ \ x\right)$, $4.x + 3 = p$, p – просто число.

(2) $D\left(\frac{q^s-1}{q-1},\ \frac{q^{s-1}-1}{q-1},\ \frac{q^{s-2}-1}{q-1}\right)$, $q = p^n$.

(3) $D\left(4.x+3,\ \ 2.x+1,\ \ x\right)$, $4.x + 3 = p.(p + 2)$; $p, p + 2$ – прости числа.

(4) $D\left(4.x+3,\ \ 2.x+1,\ \ x\right)$, $4.x + 3 = 4.y^2 + 27$; $4.y^2 + 27 = p$.

Последователностите, разработени на базата на (3) са известни като "последователности на Якоби".

Определение: *N-позиционни последователности, при които броят на елементите $N = p_1 . p_2$, където p_1 и p_2 са прости числа и $p_2 = p_1 + 2$, се наричат последователности на Якоби с едно ниво на периодичната автокорелационна функция (ПАКФ).*

Правилото за формиране на степенната последователност за $\mu = \{\mu_i: i = 0, 1, 2, \ldots, N – 1\}$, $N = p_1 . p_2$, се формулира [3, 4]:

$$(5)\ \mu_i = \begin{cases} 1, & ако \quad i \equiv 0 (\mathrm{mod}\ N) \\ 1, & ако \quad i \equiv 0 (\mathrm{mod}\ p_2), \quad i \not\equiv 0 (\mathrm{mod}\ p_1) \\ -1, & ако \quad i \equiv 0 (\mathrm{mod}\ p_1), \quad i \not\equiv 0 (\mathrm{mod}\ p_2) \\ \psi_1(i).\psi_2(i), & i \not\equiv 0 (\mathrm{mod}\ p_1), \quad i \not\equiv 0 (\mathrm{mod}\ p_2) \end{cases}$$

В (5) са приети следните обозначения:

$$\psi_1(i) = e^{j\pi u_{i,1}}, \quad i = 1,\ 2,\ ...,\ p_1 - 1,$$

$$(6)\ \psi_2(i) = e^{j\pi u_{i,2}}, \quad i = 1,\ 2,\ ...,\ p_2 - 1,$$

$$u_{i,1} = ind_{\Theta_1} i,$$

$$u_{i,2} = ind_{\Theta_2} i,$$

където Θ_1 е първообразния елемент на полето $GF(p_1)$, а Θ_2 – първообразния елемент на полето $GF(p_2)$.

Още в средата на миналия век е извършен анализ на степенните последователности на Якоби с едно ниво на ПАКФ [1].

Интересно е да се отбележи, че двойката прости числа p_1 и p_2 ($p_2 = p_1 + 2$) са известни в математиката като прости числа-близнаци. Всички те, без (3, 5), са от вида:

(6) $p_i = 6n + z$ ($i = 1, 2$; n – нечетно число; $z = +1, -1$)

По модул от тридесет (30) всички числа-близнаци (без първите две – 3-5 и 5-7) са от вида (11, 13), (17, 19) или (29, 1).

Предполага се, че тези двойки са безкрайно много, но това не е доказано. Най-голямата, известна двойка числа-близнаци е $3\ 756\ 801\ 695\ 685 \cdot 2^{666\ 669} \pm 1$ [5]. Тя е била намерена в рамките на проект "PrimeGrid" [6] на 24 декември 2011 год.

2. Анализ на степенна последователност на Якоби с едно ниво на ПАКФ.

Тъй като мощността на метода е $P = 1$ [1], то търсенето на импулсни последователности с оптимална импулсна автокорелационна функция (ИФА) трябва да се извършва за всяко N чрез циклични премествање на символите на получената последователност, формирана съгласно правило (5).

В литературата [1, стр. 98] е извършен анализ на степенна последователност на Якоби до $N = 323$ (общо 4 двойки прости числа-близнаци). Вследствие на извършения анализ са получени двадесет и две (22) оптимални импулсни последователности.

От приложените резултати [1] се вижда, че с нарастване на броя на елементите в степенната последователност (N), нараства и максималното ниво на страничния лист на ИФА ($\left|\max r_{\mu}(m)\right|$).

Само е отбелязано, че относителното ниво на страничния лист на ИФА (A):

$$(7)\quad A = \frac{\left|\max r_{\mu}(m)\right|}{\sqrt{N}},$$

се намира в рамките на 0,67 – 0,92.

С цел разширяване и подобряване на извършеното изследване беше разработена програма на MATLAB за формиране на степенна последователност на Якоби с едно ниво на периодичната автокорелационна функция (ПАКФ).

Изследването бе извършено до $N = 3600$. Като основни критерии за оценка на резултатите бяха използвани относителното ниво на страничния лист на ИФА (A) и коефициентът на загуби ($K_{\text{заг}}$) вследствие на обработката на сигнала с несъгласуван филтър.

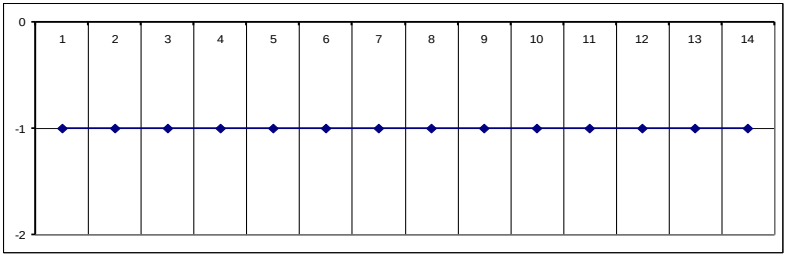
Идеята за използване на несъгласуван, вместо съгласуван филтър, не е нова. Такава обработка позволява да се получи ИФА без странични листи. Разбира се, това довежда до влошаване на отношението

“сигнал/шум” и намаляване на далечната зона на откриване на радиолокационната станция, което характеризира коефициентът на загуби ($K_{заг}$). Анализът на стойностите на $K_{заг}$ показва, че стойности до около 2,5 са приемливи. Те довеждат до приемливо намаляване на далечината на откриване на радиолокационната станция.

Характерно е да се отбележи, че анализ на степенна последователност на Якоби спрямо $K_{заг}$ не е извършвана. Поради това, изследването си постави за цел извършването на такъв анализ. По този начин се цели да се постигне разширяване и обогатяване на знанията за степенната последователност на Якоби.

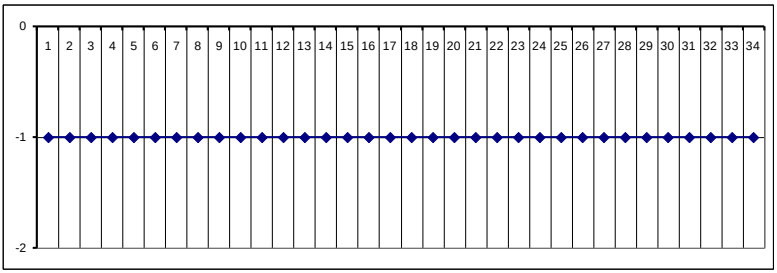
Опитно беше проверена и аналитично изведената зависимост за максималното ниво на страничния лист (фиг. 1, 2) на ПАКФ.

Както се вижда от приложените графики, ПАКФ на последователността на Якоби е с едно ниво със стойност “– 1”.



Фиг. 1. ПАКФ на последователност на Якоби

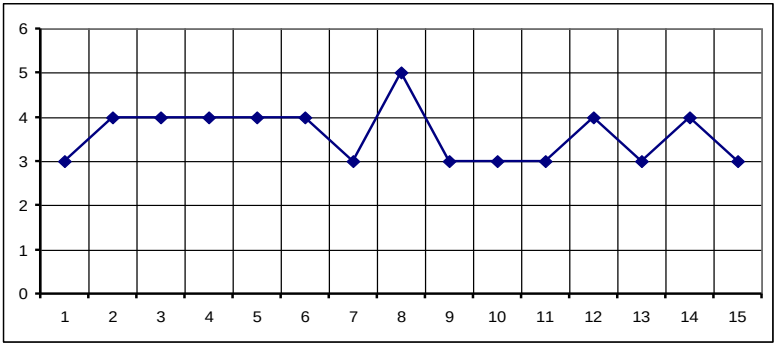
при $p_1 = 3$, $p_2 = 5$, $N = 15$.



Фиг. 2. ПАКФ на последователност на Якоби

при $p_1 = 5$, $p_2 = 7$, $N = 35$.

Бяха проверени и приведените резултати в литературата [1, стр. 98] (фиг. 3, 4). На фигури 3 и 4 е показана абсолютната максимална стойност на страничния лист на импулсната функция на автокорелация при пълно завъртане на степенна последователност на Якоби с $N = 15$ и 30.



Фиг. 3. Максимални стойности на страничния лист

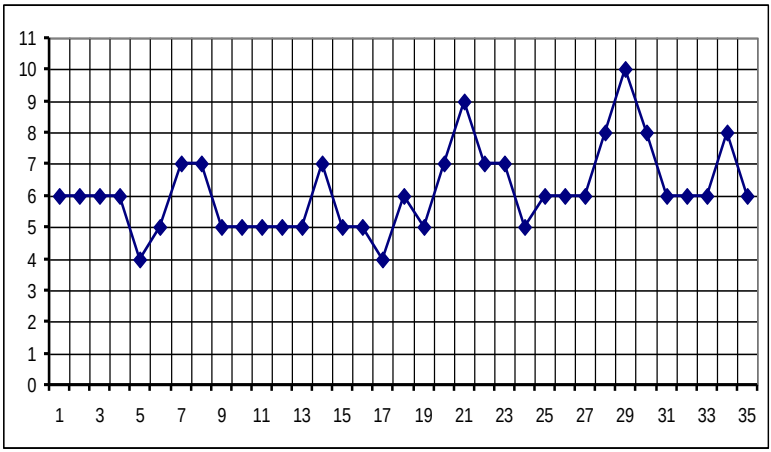
$$\left|\max r_{\mu}(m)\right|$$

при $p_1 = 3$, $p_2 = 5$, $N = 15$.

Тъй като разработената програма завърта циклично импулсната последователност надясно ($L_{ПР}$), а резултатите са показани на базата на циклично изместване наляво (L_O), оптималното изместване се приравнява съгласно:

(8) $$L_O = N - L_{ПР} + 1$$

По този начин се постига съответствие между получените от изследването и декларираните резултати в литературата и се улеснява сравняването на резултатите, което се оказа важно в процеса на работа.



Фиг. 4. ПАКФ на последователност на Якоби

при $p_1 = 5$, $p_2 = 7$, $N = 35$.

Получените резултати, вследствие на изследването за оптимални последователности са показани в Таблица 1. При анализа за всяка степенна последователност е извършено пълно циклично завъртане с последващо търсене на тези последователности, които имат най-ниско ниво на абсолютната максимална стойност на страничния лист на импулсната функция на автокорелация.

Таблица 1

Изследване на последователност на Якоби с едно ниво на ПАКФ и *N* до 3600

p_1	p_2	N	$L_{\text{О ИЗСЛ}}$	$\lvert\max r_\mu(m)\rvert$	Брой последователности
3	5	15	0, 1, 3, 5, 6, 7, 9	3	7
5	7	35	19, 31	4	2
11	13	143	34, 41, 44, 45, 46, 100, 101, 102, 122, 123, 124	11	11
17	19	323	89, 244	16	2
29	31	899	203, 631, 632, 633, 637	29	5
41	43	1763	479, 481, 1427	44	3
59	61	3599	2809, 2810	68	2

Въпреки обявеното в литературата [1], че са изследвани последователностите на Якоби до 1000, не е извършено изследване на последователността при $N = 899$. Има несъответствия между показаните оптимални кодове при $N = 35$ и $N = 143$ и действително получените резултати (Таблица 2).

Таблица 2

Открити несъответствия между публикувани (L_O) и получени резултати ($L_{O\ ИЗСЛ}$) при изследване на степенни последователност на Якоби при N до 323

p_1	p_2	N	L_O	$L_{O\ ИЗСЛ}$	Брой несъответствия
5	7	35	20, 32	19, 31	2
11	13	143	35, 42, **45**, **46**, 47, **101**, **102**, 103, **123**, **124**, 125	34, 41, 44, **45**, **46**, 100, **101**, **102**, 122, **123**, **124**	5

Получените резултати за относителното ниво на страничния лист на ИФА (A) и коефициентът на загуби ($K_{заг}$) са показани на Таблица 3. Наблюдава се нарастване както на A, така и на $K_{заг}$. Характерно е да се отбележи, че въпреки нарастването, в изследвания диапазон коефициентът на загубите остава в приемливи граници. Това позволява да се приеме, че получените степенни последователности могат да се използват в системи за обработка на сигнали с несъгласуван филтър, без това да повлияе негативно на работата на радиолокационното устройство.

Таблица 3

Относително ниво на страничните листи (A) и коефициент на загуби ($K_{ЗАГ}$)

при последователност на Якоби с едно ниво на ПАКФ и N до 3600

p_1	p_2	N	A	$K_{заг}$
3	5	15	0,775	1,8750
5	7	35	0,676	1,9444
11	13	143	0,920	1,9861
17	19	323	0,890	1,9938
29	31	899	0,967	1,9978
41	43	1763	1,048	1,9989
59	61	3599	1,134	1,9994

Анализът на относителното ниво на страничните листи (A) позволява да се конкретизират данните, цитирани в литературата [1], а коефициентът на загуби ($K_{заг}$) позволява да анализира възможността за използване на несъгласуван филтър при обработка на получения сигнал.

3. Заключение.

В доклада са обобщени резултатите от извършеното изследване на степенни последователности на Якоби с едно ниво на периодичната функция на автокорелация.

Получените резултати позволяват се направят следните изводи:

1. извършеното изследване разширява обхвата на степенните последователности на Якоби, взависимост от броя на елементите на степенната последователност (N) – от 323 на 3599;

2. вследствие на изследването са разработени три (3) нови степенни последователности на Якоби и са получени десет (10) нови оптимални степенни последователности;
3. доуточнени са цитираните в литературата [1] известни оптимални степенни последователности;
4. като цяло, с нарастването на броя на елементите на степенната последователност (N), нараства и относителното ниво на страничните листи (A) – 0,775 ÷ 1,134;
5. наблюдава се нарастване и на коефициентът на загуби ($K_{заг}$), като същият остава в приемливи граници – 1,8750 ÷ 1,9994;
6. разработената програма позволява съществено да се намали времето за изчисление и анализ на всяка степенна последователност;
7. не съществува проблем за по-нататъшно разширяване на обема на изследванията за по-голям брой елементи в степенната последователност (N).

Литература:

1. Свердлик М., Б., Оптимальные дискретные сигналы. – М., "Сов. радио", 1975.
2. Холл М. Комбинаторика. Пер. С англ., М., "Мир", 1970.
3. Titsworth R. C., Optimal and minimax sequences. In: International Telemetry Conference. 1963.
4. Brauer A. On a new class of hadamar determinants. – "Math. Z.", 1953, № 58.
5. www.primes.utm.edu/largest.htm#twin; [Електронен документ].
6. www.primegrid.com/forum_thead.php?id=3874; [Електронен документ].

ПРИЛАГАНЕ НА ЛИСТИ ЗА КОНТРОЛ НА ДОСТЪПА С ЦЕЛ ОСИГУРЯВАНЕ НА ПО-ДОБРА ЗАЩИТЕНОСТ НА ТРАФИКА В ДАДЕНА КОМПЮТЪРНА МРЕЖА

ПЕТЪР КР. БОЯНОВ

IMPLEMENTATION OF ACCESS CONTROL LISTS IN ORDER TO ENSURE BETTER PROTECTION OF THE TRAFFIC IN DETERMINED COMPUTER NETWORK

PETAR KR. BOYANOV

ABSTRACT. *Most of the accomplished cyber crimes are based on the flaws and vulnerabilities in computer and network systems. Thereby the most important skills of security network analysts and system administrators are connected with configuring of access control lists. The security network analysts and system administrators use these lists to block traffic or allow only determined traffic while stopping or blocking all other traffic on their networks.*

KEYWORDS: *ACL, COMPUTER NETWORK, CYBER-ATTACKS, LAN, ROUTER, SECURITY, SWITCH, TRAFFIC, VULNERABILITY, WAN*

1. Въведение

Повечето от извършените кибер-престъпления се основават на недостатъци и слаби места в областта на компютърните и мрежови системи. По този начин най-важните умения на мрежовите анализатори по сигурността и системните администратори са свързани с конфигурирането на листи за контрол на достъпа. Мрежовите анализатори по сигурността на мрежите и системните администратори използват тези листи да блокират или позволят само определен мрежов трафик [1],[2],[3],[4],[5],[8],[14],[16],[22],[29],[30].

2. Изложение

Едни от най-важните качества, които трябва да притежава всеки един мрежов и системен администратор, са съвършеното владеене на

листите за контрол на достъпа. Повечето системни администратори използват тези листи да спрат целия мрежовия трафик или да разрешат само определен мрежов трафик през дадената компютърна мрежа. Мрежовите архитекти и дизайнери използват защитните стени да защитят компютърните мрежи от неоторизиран достъп до компютърните ресурси както на големи компании и фирми, така и на обикновените потребители [5],[8],[10],[22],[25],[26],[28],[29],[30]. Защитните стени са хардуерни или софтуерни решения, които подсилват политиките за мрежова сигурност [12],[14]. По този начин защитните стени филтрират неоторизирани и потенциално опасни пакети от цялата мрежа. Листите за контрол на достъпа представляват определена последователност от разрешителни и забранителни команди, които определят каква ще бъде политиката на сигурност в дадената компютърна мрежа. Тези листи осигуряват мощен начин за контрол на трафика в и извън определената мрежа. Конфигурирането на листите за достъп е приложимо за всички рутиращи мрежови протоколи. Най-важната причина за конфигурирането и прилагането на тези листи за контрол на достъпа е свързана с осигуряването на сигурност на цялата мрежа от различи видове злонамерени кибер-атаки, които могат да компрометират дадения хост и информацията в него да бъде или откраднатa, или изтрита [1],[2],[10],[5],[8],[22],[29],[30].

Интересното е, че тези листи могат да забранят или разрешат трафика до определен хост или голяма група от хостове заедно с техните логически мрежови адреси. Тези листи могат да филтрират трафика и по определен TCP (Transmission Control Protocol) порт. В практиката са известни едни от най-важните номера на портове:

- TCP Порт №1863 - MSN Messanger [5],[8],[22],[13],[15],[17],[18],[19],[20].
- TCP Порт №8008 - алтернативен HTTP [5],[8],[21],[23],[24],[25].
- TCP Порт №8080 - алтернативен HTTP [5],[8],[22],[26],[27],[28],[30].
- TCP Порт №21 - файлов протокол за трансфер на информация (FTP).
- TCP Порт №23 - протокол за отдалечен достъп (Telnet).
- TCP Порт №25 - протокол SMTP (Simple Mail Transfer Protocol). Той се използва се за препращане и изпращане на пощенски съобщения между сървъри.
- TCP Порт №80 - уеб базиран протокол HTTP (Hypertext Transfer Protocol).

- TCP Порт №194 - IRC (Internet Relay Chat) [5],[8],[22],[26],[27],[28],[30].
- TCP Порт №443 - HTTPS (Secure HTTP).
- UDP Порт №1812 - RADIUS Authentication protocol.
- UDP Порт №5004 - RTP (Voice and Video Transport Protocol)
- TCP/UDP Порт №53 - DNS (Domain Name Services) и др.

Пакетната филтрация, наречена още статична пакетна филтрация, която има за цел да контролира достъпа към мрежата чрез анализиране на входящите и изходящите пакети в компютърната мрежа [1],[2],[10],[5],[8],[22],[29],[30]. Листите за контрол на достъпа могат да извлекат следната важна информация от пакетния хедър и по този начин да се вземе решение дали да се пропусне или откаже дадения пакет. Всичко тези решения се базират на:

- IP адресът на източника.
- IP адресът на получателя.
- Съобщение от тип ICMP.
- TCP/UDP порт на източника.
- TCP/UDP порт на получателя.

Листите за контрол на достъпа представлява конфигурационен скрипт, който контролира какви решения да взема рутерът. Неговите решения се базират на критерия, намерен в пакетния хедър [5],[8],[10],[15],[18],[20],[22],[25],[26],[28],[29],[30]. По подразбиране маршрутизаторът (рутерът) не притежава никакви конфигурирани листи за достъп като по този начин не може да се филтрира трафика. Трафикът, който навлиза в рутера, се рутира на информацията, въведена в рутиращата таблица. Ако не се използват листи за контрол на достъпа в даден рутер, всички пакети могат да бъдат рутирани свободно от един маршрутизатор към следващия мрежов сегмент.

В практиката листите за контрол на достъпа в компютърните мрежи изпълняват следните важни задачи:

- Ограничаване на мрежовия трафик с цел увеличаване на производителността. Като пример може да се даде ограничаването на видео трафика за сметка на гласовия трафик [5],[8],[10],[15],[18],[20],[22],[25],[26],[28],[29],[30].
- Осигуряване на контрол на трафичния поток. Листите за контрол могат да ограничат доставянето на определени рутиращи обновления. Това се прилага, когато тези обновления не са задължителни и отделно съществуват различни проблеми

по мрежовата връзка [5],[8],[10],[15],[18],[20],[22],[25],[26],[28],[29],[30].

- Осигуряване на базово ниво на сигурност за мрежов достъп. Листите могат да разрешат на даден хост да има достъп до определена част от мрежата и в същото време да забранят на друг хост да има достъп до същата част както предишния хост. Тази политика на достъп често се прилага в големите фирми и университети, където само определени потребители могат да имат достъп до отдел човешки ресурси.
- Вземане на решения за това кой тип от трафик да бъде допуснат или блокиран на дадения интерфейс на рутера. Пример за това може да бъде пропускането на e-mail трафик, но в същото време да бъде блокиран целия Telnet трафик [6],[7],[9],[11],[12].
- Контролиране на областите на достъп, до които даден потребител или клиент може да има достъп [1],[2],[10],[5],[8],[22],[29],[30].
- Прилагане на специални правила, които да разрешат на даден потребител да има или няма достъп до услуги от типа FTP и HTTP.

Най-често се използват два типа листи за контрол на достъпа - стандартни и разширени.

Стандартните листи за контрол на достъпа позволяват да бъде разрешен или забранен мрежовия трафик от IP адреса на източниците. Получателят на пакета, както и съответния порт не се вземат под внимание [5],[8],[10],[15],[18],[20],[22],[25],[26],[28],[29],[30].

Разширените листи за контрол на достъпа филтрират IP пакетите, базирани на няколко атрибута:

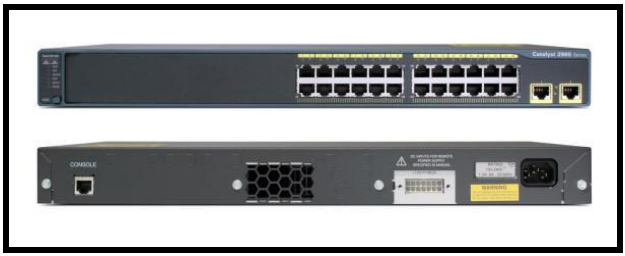
- типа на протокола;
- ip адресът на източника;
- ip адресът на получателя;
- tcp/udp порт на източника;
- tcp/udp порт на получателя и др.

Комуникационната мрежа се състои от следните мрежови елементи:

- 3 броя персонални компютъра;
- 1 брой Web Server [5],[8],[22],[29],[30];
- Кабели от тип Copper Straight-Through UTP cables cat.5e [5],[8],[22],[29],[30];

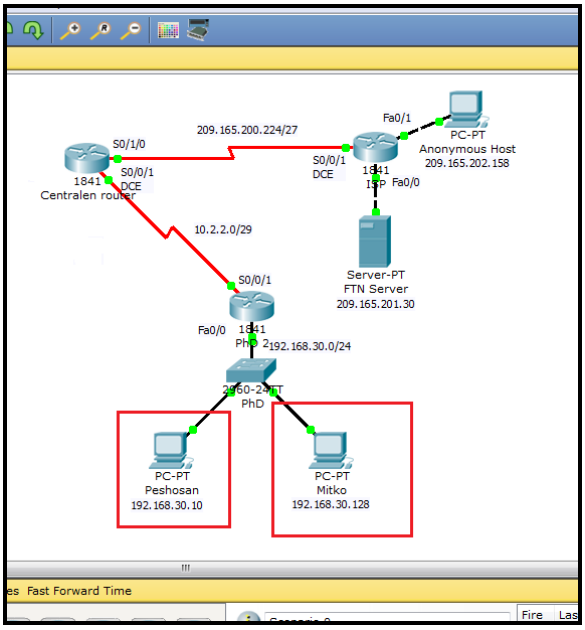
- Кабели от тип Copper crossover cables UTP cat.5e [5],[8],[22],[29],[30];
- Кабели от тип Serial Smart DCE DB60 cable [5],[8],[22],[29],[30];
- 3 броя modular routers - Cisco 1841 Modular Routers (показани на фиг.1);
- 1 броя switch - Cisco C2960-24TT Switches (показан на фиг.2).

Фиг.1. Предна и задна страна на Cisco 1841 Modular Router



Фиг.2. Предна и задна страна на Cisco C2960-24TT Switch

Комуникационната мрежа е симулирана в програмната среда на Cisco Packet Tracer. На фиг.3. е показана общата схема на дадената комуникационна мрежа.



Фиг. 3. Обща схема на комуникационната мрежа

2.1. Комуникационни връзки в мрежата.

Както е известно всеки един рутер притежава определен брой интерфейси. В нашия комуникационен сценарий рутер "PhD 2" има един interface FastEthernet (Fa0/0) с номер на мрежата Net ID 192.168.30.0/24 и един интерфейс interface Serial (Se0/0/1) с номер на мрежата Net ID 10.2.2.0/29 [5],[8],[10],[15],[18],[20],[22],[25],[26],[28],[29],[30].

Мрежата 192.168.30.0/24 се състои от един Cisco 1841 Modular Router, един Cisco C2960-24TT Switch, към който съответно са свързани 2 персонални компютъра. Тази мрежа 192.168.30.0/24 е частна локална мрежа и нейният IPv4 Default Gateway е 192.168.30.1/24 (Това е настроеният мрежови адрес на interface FastEthernet на рутер "PhD 2").

Капацитетът на тази мрежа е 254 хоста. Връзките между комутатора и отделните хостове е осъществена чрез прав кабел - Copper Straight - Through UTP cat.5e cable. Връзката между рутер „PhD 2" и комутатора "PhD" отново е осъществена чрез прав кабел от същия модел [11],[12],[13],[14], [15],[16],[17],[18],[19],[22]. Мрежата 10.2.2.0/29 се състои от 2 мрежови устройства - рутер „PhD 2" и рутер "Centralen router". Връзките между отделните устройства са осъществени по сериен кабел от тип Serial Smart DCE DB60 cable.

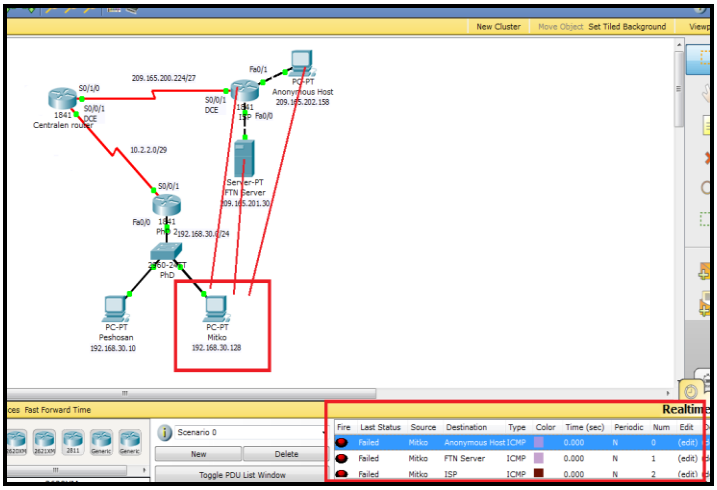
Мрежата 209.165.200.224/27 е публична глобална мрежа. Тя свързва двата рутера „Centralen router" и "ISP" (Internet Service Provider). Връзката между двата рутера е серийна.

Хостът „Anonymous host" с IP адрес 209.165.202.158 е свързан към рутера "ISP" (Internet Service Provider). Хостът Web Server е също свързан към рутера "ISP" (Internet Service Provider). Връзката между тях е по интерфейс FastEthernet като в този случай се използва кръстосан кабел - Copper cross-over UTP cat.5e cable [22],[25],[26],[28],[29].

2.2. Изследване на листите за контрол на достъпа.

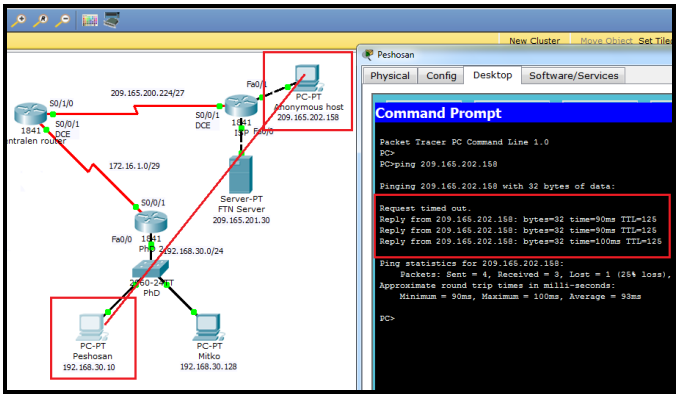
В този доклад ще бъдат изследвани листите за контрол на достъпа в комуникационната мрежа, показана на фиг.3.

Целта на това изследване и тестване е да се разреши само хостът "Peshosan" с частен IP адрес 192.168.30.10 да има достъп навсякъде в комуникационната мрежа, а пък хостът "Mitko" с частен IP адрес 192.168.30.128 да има достъп само в локалната мрежа 192.168.30.0/24 и да няма никакъв достъп извън нея. Резултатът от прилагането на листите за контрол на достъпа за хоста "Mitko" с частен IP адрес 192.168.30.128 са показани на фиг.4. От тях се разбира, че приложените листи функционират правилно и дадения хост няма никакъв достъп извън своята частна локална мрежа. Този тип политика на достъп намира широко приложение в много хотели и държавни институции [5],[8],[12],[14],[22],[29],[30].

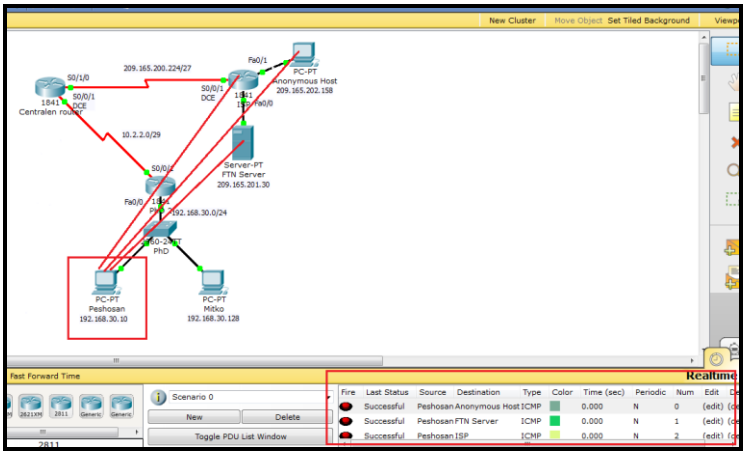


Фиг. 4. Неуспешните опити за връзка от хост “Mitko” към хостове “ISP”, “FTN Server” и “Anonymous Host

Резултатът от прилагането на листите за контрол на достъпа за хоста “Peshosan” с частен IP адрес 192.168.30.10 са показани на фиг.5 и фиг.6.



Фиг. 5. Успешен ping между хост “Peshosan” и хост 209.165.202.158



Фиг. 6. Успешните опити за връзка от хост “Peshosan” към хостове “ISP”, “FTN Server” и “Anonymous Host

3. Изводи и предложения

Изградената стимулационна мрежа ни показва много точно как се прилагат листите за контрол на достъпа както в малка частна локална мрежа, така и в глобална компютърна мрежа. Благодарение на тези приложени политики на сигурност и защита се осигурява по-голяма изправност, надеждност, сигурност и производителност на комуникационните процеси и услуги в дадената компютърна мрежа. Изграждането и поддържането на сигурни листи за контрол на достъпа е от изключително важно значение за запазване интегритета и конфиденциалността на личните данни на потребителите и клиентите. Конфигурирането на листите за контрол на достъпа е препоръчително да бъде изпълнявано от специализирани системни и мрежови администратори с цел защита от различни видове злонамерени кибер-атаки. Тези листи намират изключително приложение в работния процес на много големи и малки фирми, корпорации, държавни институции, университети, училища и др.

This paper is supported by the Project BG051PO00l-3.3.06-0003 “Building and steady development of PhD students, post-PhD and young scientists in the areas of the natural, technical and mathematical sciences”. The Project is realized by the financial support of the Operative Program

“Development of the human resources” of the European social found of the European Union.

ЛИТЕРАТУРА:

1. **Abedin**, Muhammad, Syeda Nessa, Ehab Al-Shaer, and Latifur Khan, "Vulnerability analysis for evaluating quality of protection of security policies." In Proceedings of the 2nd ACM workshop on Quality of protection, pp. 49-52. ACM, 2006.
2. **ADELMAN**, Kenneth Allen, et al. Method and apparatus for a TCP/IP load balancing and failover process in an internet protocol (IP) network clustering system. U.S. Patent No 6,078,957, 2000.
3. **BAKRE**, Ajay; BADRINATH, B. R. I-TCP: Indirect TCP for mobile hosts. In: Distributed Computing Systems, 1995., Proceedings of the 15th International Conference on. IEEE, 1995. p. 136-143.
4. **BHOLE**, Yogesh; POPESCU, Adrian. Measurement and analysis of http traffic. Journal of Network and Systems Management, 2005, 13.4: 357-371.
5. **Calvert**, Peter Sean, Anthony Scott Moran, and Brian James Turner. "Grouped access control list actions." U.S. Patent 7,380,271, issued May 27, 2008.
6. **CASILARI**, Eduardo; GONZBLEZ, F. J.; SANDOVAL, Francisco. Modeling of HTTP traffic. Communications Letters, IEEE, 2001, 5.6: 272-274.
7. **CERF**, Vinton G.; ICAHN, Robert E. A protocol for packet network intercommunication. ACM SIGCOMM Computer Communication Review, 2005, 35.2: 71-82.
8. **Chow**, Sherman SM, Lucas CK Hui, Siu-Ming Yiu, K. P. Chow, and Richard WC Lui. "A generic anti-spyware solution by access control list at kernel level." Journal of Systems and Software 75, no. 1 (2005): 227-234.
9. **CLARK D. D.**, An analysis of TCP processing overhead. Communications Magazine, IEEE, 1989, 27.6: 23-29.
10. **ESTÉVEZ-TAPIADOR**, Juan M.; GARCIA-TEODORO, Pedro; DIAZVERDEJO, Jesús E., Measuring normality in HTTP traffic for anomalybased intrusion detection. Computer Networks, 2004, 45.2: 175-193.
11. **Feit** S, “SNMP, A Guide To Network Management”, McGraw-Hill, 1995
12. **Gold**, Steve. Hacking on the hoof. Engineering & Technology, 2012, 7.3: 80-83.
13. **Hekmat** S, “Communication Networks”, “PragSoft Corporation”, USA, 2005 г.
14. **Hristov** Hr., "A passive strategy for management of counteraction to encroachments on business organization, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, Vol.6, 2014, pp. 187-194

15. **KOZIEROK**, Charles M. The TCP/IP guide: a comprehensive, illustrated Internet protocols reference. No Starch Press, 2005. 50 Association Scientific and Applied Research
16. **Kumar** P. S., & Arumugam S., Establishing a valuable method of packet capture and packet analyzer tools in firewall, International Journal of Research Studies in Computing, 2012 April, Volume 1 Number 1, 11-20
17. **MARKATOS**, Evangelos P. Speeding up TCP/IP: Faster processors are not enough. In: Performance, Computing, and Communications Conference, 2002. 21st IEEE International. IEEE, 2002. p. 341-345.
18. **Marquez**, J. "An Analysis of the IDS Penetration Tool: Metasploit." The InfoSec Writers Text Library, Dec 9 (2010).
19. **MIORANDI**, Daniele; KHERANI, Arzad A.; ALTMAN, Eitan. A queueing model for HTTP traffic over IEEE 802.11 WLANs. Computer networks, 2006, 50.1: 63-79.
20. **MOGUL**, Jeffrey; RASHID, Richard; ACCETTA, Michael. The packer filter: an efficient mechanism for user-level network code. ACM, 1987.
21. **PAPADOPOULOS**, Christos; PARULKAR, Guru M. Experimental evaluation of SUNOS IPC and TCP/IP protocol implementation. Networking, IEEE/ACM Transactions on, 1993, 1.2: 199-216.
22. **Qian**, Jiang, Susan Hinrichs, and Klara Nahrstedt. "ACLA: A framework for access control list (ACL) analysis and optimization." Communications and Multimedia Security Issues of the New Century. Springer US, 2001. 197-211.
23. **RIZZO**, Luigi. Effective erasure codes for reliable computer communication protocols. ACM SIGCOMM computer communication review, 1997, 27.2: 24-36.
24. **Singh** G., & Singh A., Campus Network Security Policies: Problems And Its Solutions, International Journal of Innovative Research and Development, June, 2013, Vol 2 Issue 6, pp.294-306
25. **SO-IN**, Chakchai. A Survey of Network Traffic Monitoring and Analysis Tools. Cse 576m computer system analysis project, Washington University in St. Louis, 2009.
26. **Song**, Yuqian, et al. Towards a framework to support novice users in understanding and monitoring of Home Area Networks. In: Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on. IEEE, 2012. p. 82-87.
27. **Shrestha**, Nishant. "Security Assessment via Penetration Testing: Network and System Administrator's Approach: Security, Network and System Administrator, Penetration Testing." (2012).
28. **STALLINGS**, William; STALLINGS, William. Data and computer communications. New Jersey: Prentice hall, 1997.
29. **Tasheva**, Z. N., Tasheva, A. T. Combining cryptography and steganography in software system for hiding confidential information, International Journal of Science, Education and Innovation, Volume 1, 2013. ISSN 1314-9784, Association Scientific and Applied Research, pp. 84-92.

30. **Wichers**, David, Douglas Cook, Ronald Olsson, John Crossley, Paul Kerchen, Karl Levitt, and Raymond Lo. "PACL's: an access control list approach to anti-viral security." In Proceedings of the 13th National Computer Security Conference, pp. 340-349. 1990.

ДИНАМИЧНИ ТОПОЛОГИИ

Филип И. Любомиров

DYNAMIC TOPOLOGY

Filip I. Lyubomirov

ABSTRACT: The benefits of dynamic topologies include incremental learning system becomes more intelligent as it is exposed to more cases. It is able to cope with uncertainties. The result is that the system can improve the efficiency of the network.

KEYWORDS: Dynamic, topology, network,

Динамични комуникационни мрежи

Динамичните комуникационни мрежи (ДКМ) осигуряват директна връзка между произволна двойка предавател-приемник в паралелния компютър. Това става чрез промяна на комуникационните връзки посредством реконфигурация на активните КЕ. ДКМ и са еднакво подходящи както за схемна комутация, така и за пакетна комутация. ДКМ могат формално да се обозначат като $F:\{N\}\rightarrow\{N\}$, което се тълкува като размяна F на множеството разместванията {N} от N елемента. Класически пример за ДКМ се явява матричния превключвател. Неговият основен недостатък е квадратичното нарастване на броя КЕ в зависимост от броя входове (изходи) на КМ; с други думи става сложно за реализация, дори невъзможно в някои случаи, на мрежа свързваща няколко стотин или хиляди процесора. Едно от възможните решения на този проблем е да се използва многостъпална мрежа.

Многостъпалните мрежи осигуряват пълна система на връзките в рамките на паралелната структура. Те от своя страна се разделят на:

• едностранни

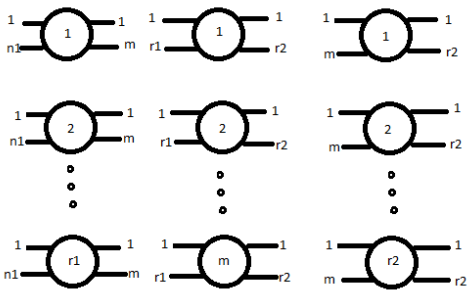
• двустранни.

Едностранните мрежи използват двупосочни ЛВ, а двустранните имат входна страна и изходна страна. Последните от своя страна се разделят на блокиращи, неблокиращи с реконфигурация и напълно неблокиращи. В блокиращите ДКМ е възможно с присъединяването на дадена една двойка предавател-приемник да предизвика конфликт в използването на мрежата за друга двойка предавател-приемник. Най-известни представители на този тип ДКМ са манипулатор, делта, омега, флип и др. Напълно неблокиращите ДКМ, както подсказва името им, не страдат от този недостатък. Примери за такива мрежи са мрежата на Клос и пълносвързаната мрежа. В неблокиращите мрежи с реконфигурация също е възможна реализация на съединенията между произволна двойка предавател-приемник, но за това е необходимо да се измени маршрута на връзките за съединените вече двойки терминали. Примери за такива мрежи са мрежата на Бенес, битоналната мрежа и др. Построяването на многостъпални КМ е свързано с необходимостта от използуване на по-прости (в структурно отношение) КЕ. Това води до увеличен брой стъпала в мрежата, k на брой стъпала в общият случай. Като следствие на това се получава:

• Увеличено време за предаване на съобщенията.

• Усложнен алгоритъм за управление.

Модел на двустранна ДКМ при k=3 стъпала е показан на фиг.1



фиг.1. Обобщен модел на k-стъпална КМ (k=3).

Първото (входно) стъпало се състои от r1 КЕ (комутатора) с размерност n1xm (при това r1xn1=N), междинното стъпало се състои от m КЕ с размерност r1xr2 и последното трето стъпало (изходното) се състои от r2 КЕ с размерност mxr2 (при това r2xn2=N). Връзките между КЕ в различните стъпала се определят от вътрешно системните функции за връзка, които в крайна сметка дефинират и различните видове ДКМ (мрежа на Клос, мрежа на Бенес, омега мрежа, делта мрежа, сигма мрежа, Мемфис мрежа и т.н.).
За оценяване на различните топологии ДКМ се използват най-често следните параметри: Време за предаване. Времето за предаване, с едно първо приближение, може да се счита, че е O(k), т.е. колкото по-малко стъпала има в мрежата толкова по-малки ще бъдат комукационните загуби. Същевременно по-малкият брой стъпала означава, че КЕ в структурно отношение ще бъде по-сложен (за достигане на един и същ брой входове/изходи на мрежата) и по този начин той ще осигурява по-голяма задръжка при преминаване на сигналите през него. Сегментиране. Това е разделяне на ДКМ на независими подмрежи с различни размери. Всяка подмрежа трябва да има всички възможности за връзки на цялата мрежа от същия тип и размер. Ширина на лентата на пропускане. Този параметър се дефинира като очакван брой заявки приети за единица време. Тъй като системната шина не може да осигури широка лента на пропускане за голям брой процесори, а матричния комутатор е скъп, то е интересно и важно да се знае как варира лентата на пропускане при различните ДКМ за различните случаи. Най-често тези оценки се получават с помощта на подходящи имитационни модели.

Литература

1. Tse-yun Feng. A Survey of Interconnection Networks, Computer, Dec., 1981.

2. Howard J. Siegel. The Theory Underlying the Partitioning of Permutation Networks, IEEE Transactions on Computers, vol. C-29, No.9, Sept. 1980.

3. Larry D. Wittie. Communication Structures for Large Networks of Microcomputers, IEEE Transactions on Computers, vol. C30, No4 April 1981.

4. Стоян Марков. Изчислителни системи с висока производителност, С., Техника, 1990.

5. С.О.Степанян Коммуникационные сети в многопроцессорных ЭВМ. Автоматика и вычислительная техника, 1987,Но.3.

6. Goodman J.R., Sequin C.H. Hypertree: A Multiprocessor interconnection topology. IEEE Transactions on Computers, vol. C30, No 12 December 1981.

7. Network topology http://en.wikipedia.org/wiki/Network_topology#See_also

ЕКСПЕРИМЕНТАЛНО ИЗСЛЕДВАНЕ ВЪЗМОЖНОСТТА ЗА СТРЕЛБА С 82 мм МИНОХВЪРГАЧКА НА ДИСТАНЦИЯ ДО 100 м.

Христо Христов

EXPERIMENTAL STUDY THE POSSIBILITY OF FIRING WITH 82 mm MORTAR AT DISTANCES UP TO 100 M

Hristo Hristov

ABSTRACT: *This article discusses the results of the experimental shootings with 82 mm mortar in short distances - up to 100 m. Analyzed the causes of unsuccessful shots. Confirmed is the possibility of conducting training firings of short distances.*

KEY WORDS: *short firing, mortar,*

1.Основни обозначения и термини.

L - разстояние на падане на учебната мина [m];

θ - ъгъл на възвишение, ъгъл на стрелба [град];

средна траектория – траекторията която минава през средата на снопа траектории [4];

център на разсейването (средна точка на попаденията) – точ-ката на пресичането на средната траектория с повърхността на целта [4];

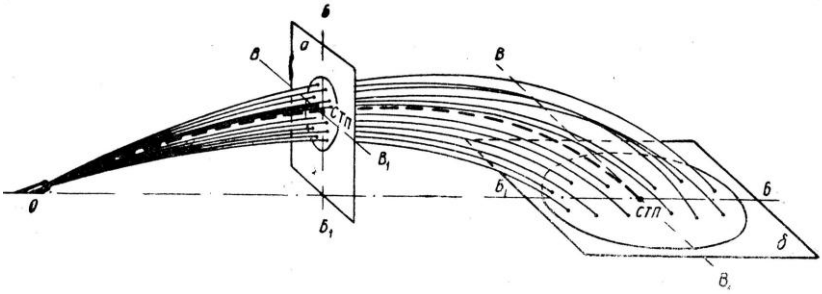
оси на разсейването – взаимно перпендикулярните линии, прекарани през центъра на разсейването [4];

отклонение – разтоянието от точката на срещата (попадението) до осите на разсейването [4];

средно отклонение в дълбочина $B\partial$ - заемащото средно място от всички отклонения в дълбочина $B\partial$, извлечени и подредени по абсолютна стойност (по модул) в низходящ или възходящ ред.[4]

радиус на кръга на попаденията – радиус с начало в центъра на разсейването и обхващащ 50 % (P_{50}) или 100 % (P_{100}) от попаденията

Графична интерпретация на използваните основи обозна-чения и термини е показана на фиг. 1



Сноп траектории, площ на разсейването и ос на разсейването:
а — на вертикална плоскост; *б* — на хоризонтална плоскост; средната траектория е обозначена с пунктирана линия; *СТП* — средна точка на попаденията; BB_1 — хоризонтална (напречна) ос на разсейването; $ББ_1$ — вертикална (надлъжна) ос на разсейването

Фиг.1

1. Експерименти.

За провеждането на експерименталните стрелби бяха направени 20 заряда с подръчни средства. Бяха използвани различни капсули – тип **жевело** и тип **уинчестер**, както и различни гилзи.

През месец октомври 2013 год. на учебен полигон бяха проведени експериментални стрелби с цел да се провери възможността за достверно пресмятане на основния заряд по предложената формула от вида:

(1) $y = a.x^b$

във работи [1], [2]. [3],

както и възможността за стрелба на къси дистанции с учебно-практическа мина с цел използването и в учебния процес.

Бяха извършвани измервания и са отчетени измервания само в едно направление – по разстояние в далечина, т.к. напречните отклоненията се получиха малки (не повече от три дължини на мината).

По време на стрелбата са отчетени:

- 3бр. осечки,
- 5 бр. неправилни възпламенявания на заряда, което води до по-бавно от предвиденото изгаряне на заряда и съответно мнго по-къси траектории.

Таблица 1

№	Ъгъл на стрелба θ [*градус*]	Разто-яние L [m]	Спрямо очаквано средно L [%]	Грешка спрямо очаквана средна L [%]	Неотчетен експеримент
1	45	43	43 %	57 %	груба грешка
2	45	69	69 %	31 %	31 % > 20 %
3	45	79	79 %	21 %	21 % > 20 %
4	45	86	86 %	14 %	
5	45	90	90 %	10 %	
6	45	97	97 %	3 %	
7	45	106	106 %	6 %	
8	45	111	111 %	11 %	
9	45	115	115 %	15 %	
10	45	89	89 %	11 %	
11	45	45	45 %	55 %	Груба решка
12	45	58	58 %	42%	Груба решка
Средно		82,33			
Очаквано средно		100			

Резултатите от експериментите/стрелбите)с пояснения към тях са показани в табл.1 – за стрелба на максимална дистанция.

В табл.2 са показани експериментите /стрелбите за стрелба на минимална дистанция. Вижда се, че при стрелба на къса дистанция грешките в разтояние са малки и се изпълняват условията за техническа

безопасност – минимално разтояние от позицията за стрелба 20 метра. По тази причина са дадени само два изстрела.

Тези отчети показват, че са допуснати **системни грешки** – от гледна точка на статистическите измервания, които се дължат на неправилно направени експерименти (изстрели). Тези груби грешки се откриват лесно, защото резултатите рязко се различават от останалите резултати.

Таблица 2

№	Ъгъл на стрелба θ [*градус*]	Разтояние L [m]	Спрямо очаквано средно L [%]	Грешка спрямо очаквана средна L [%]
1	85	25	98 %	2 %
2	85	27	105 %	5 %
Средно L		26	100 %	
Очаквано средно		25, 50		

Ако използваме за мярка с колко % се различават резултатите – съдържащи системни грешки, то този процент е по-голям или равен на 20 %.

2. Анализ на експерименталните резултати.

От опита при предишни експериментални стрелби може уверено да се твърди, че при стойности на далечина под 80 метра при ъгъл на стрелбата 45 градуса се дължат на неправилно възпламеняване на заряда, съпроводено с относително бавното му изгаряне. Понякога това се чува като шипене. Освен това всички данни с отклонения по големи 20 % от очакваната средна далечина – 100 м, се считат за неточни, поради недопустимо отклонение.

По тази причина данните с поередни номера 1, 2, 3, 11, 12 няма да бъдат отчетени, тъй като са нарушени горните две условия: да не се отчитат в експерименталните резултати **системните грешки** и да няма

отклонения по големи от 20 % в далечина. След обработка данните са представени в табл. 3. Бяха определени също **отклоненията в дълбочина**, **средно отклонение в дълбочина** $B\partial$ и **радиус на кръга на попаденията.**

Таблица 3

№	Ъгъл на стрелба θ [*градус*]	Разтояние *L* [m]	Спрямо чаквано средно *L* [%]	Грешка спрямо очаквана *L* [%]
1	45	86	86,00 %	14 %
2	45	90	90,00 %	10 %
3	45	97	97,00 %	3 %
4	45	106	106,00 %	6 %
5	45	111	111,00 %	11 %
6	45	115	115,00 %	15 %
7	45	89	89,00 %	11 %
Средно		**99,14**	99,14 %	**10 %**
Очаквано средно		**100,00**		
Макс.отклон. „къс”		14	14 %	
Макс. отклон.„дълъг”		15	15 %	

При стрелба на близки разтояния **площта на разсейването** във вертикалната равнина има форма на кръг, който се проектира върху хоризонталната равнина приблизително като кръг или елипса, чиито оси са почти равни [4]. Резултатите са показани в табл. 4

Таблица 4

№	Ъгъл на стрелба θ [*градус*]	Разтояние L [m]	Отклонение в дълбочина $B\partial$ [m]
1	45	86	13,14
2	45	90	9,14
3	45	97	2,14
4	45	106	6,86
5	45	111	11,86
6	45	115	15,86
7	45	89	
Средно L		**99,14**	
Средно отклонение в дълбочина $B\partial$			**9,14**
радиус на кръга на попаденията P_{50}			**9,14**
радиус на кръга на попаденията P_{100}			**15,86**

3. Изводи.

Осечките (не произвеждането на изстрел), се дължат на:

- ползваните различни видове гилзи и капсули.

- лошото закрепване (кернирane) на капсулите към гилзите

Неправилното възпламеняване и изгаряне на основния заряд се дължи на:

- лошото закрепване на капсулите към гилзата, което води до нееднаквост на процеса на възпламеняване;

- различната дебелина на картонената част на гилзата, което води до нееднаквост на изгаряне на основния заряд, процеса на горене се подчинавяа на различни закони на горене.

За да се отстранят посочените недостатъци е необходима унификация на зарядите с които ще се произвеждат изстрелите, която е възможно да бъде постигната в заводски условия.

5. Заключение.

На основата на гореизложеното може да се направи закллючение, че с помоща на щатна 82 мм батальонна минохвъргачка е възможно:

- да се произвеждат изстрели с учебно- практически мини и
- да се провежда обучение с тях при стриктно спазване мерките за безопасност.

Литература

1. Христов Хр. **Определяне на количеството барут на основния заряд при свръх къси дистанции на стрелба с 82 мм батальонен миномет.** Сборник научни трудове. Част 1. стр.35 – 39, ISSN 1314-1953, НВУ „ В. Левски”, 2010

2. Христов Хр**. Обобщен математичен модел на връзката начална скорост – енергия**. MATTEX 2012 стр. 101 – 107, ISSN 1314-3921, Шумен, 2012

3. Христов Хр. и Ц. Цонев. **Алгоритъм за изчисляване заряда на минохвъргачките при къси дистанции на стрелба.** Сборник научни трудове. Част 1. стр.123 – 129, ISSN 1313-7433, НВУ „ В. Левски”, 2013

4**. Наставление по стрелково дело**. ДВИ при МНО, 1958 год.

ТЕХНИЧЕСКИЕ ВСПОМОГАТЕЛЬНЫЕ СРЕДСТВА ДЛЯ ДЕТЕЙ С ДЕТСКИМ ЦЕРЕБРАЛЬНЫМ ПАРАЛИЧЕМ И СПИНОМОЗГОВЫМИ ЗАБОЛЕВАНИЯМИ

Вера Лаврецка, Иван Цонев

TECHNICAL ACCESSORIES FOR CHILDREN WITHCHILD CEREBRAL PARALYSIS AND SPINE-BRAIN DISEOSES

Vera Lavrozhka, Ivan Zhonev

ABSTRACT: *The report is a justification of technical equipment necessary for the treatment of children with infantile cerebral paralysis. With these funds as a result of many efforts of the patient and his relatives can achieve good results.*

KEYWORDS: *child cerebral palsy, corset reciprocal orthosis, robotic orthosis, bionics, simulator*

Введение.

ДЦП, дефицит мышечной активности, дисбаланс мышечного тонуса, дислокации и контрактуры в суставах, выраженные функциональные нарушения становятся причиной гиподинамии, возникновения хронических заболеваний внутренних органов, остеопороза и патологических переломов. Дети теряют способность сидеть, стоять и передвигаться, требуют дополнительного ухода, что приводит к изоляции от общества[1].

Большинство специалистов в мире мотивированно считают ДЦП – собирательным понятием, объединяющим группу синдромов, возникающих в результате недоразвития и/или повреждения мозга в пренатальный или ранний постнатальный периоды и в дальнейшем проявляющихся неспособностью сохранять позу и выполнять произвольные движения. Детский церебральный паралич (ДЦП) –

заболевание ЦНС, характеризующееся патологической двигательной активностью и аномальными постуральными нарушениями [4].

Отсутствие движения и нагрузки в течение продолжительного времени приводят к формированию контрактур суставов, деформации конечностей и позвоночника, нарушению статики и локомотив вплоть до полной утраты возможности передвигаться и самообслуживания. Длительная гиподинамия является причиной воспалительных заболеваний органов пищеварения, нарушения минерального обмена, развитию остеопороза, прогрессированию скелетных деформаций, ведущих к полному обездвиживанию, формированию сердечно-легочной недостаточности, что является препятствием в общении, ведет к стрессу, депрессии и еще более усугубляет вышеупомянутые расстройства [7].

Технические вспомогательные средства для ДЦП И СМЗ

Средства бывают пассивными и активными (роботизированные системы).

Пассивные ТВС

В начале 90-х лет был модифицированный и адаптирован к применению у пациентов с детским церебральным параличом костюм Адели".

Устройство воздействует на тонические рефлексы, которые лежат в основе формирования патологических мышечных заимодействий у больных и обуславливает преодаление действия силы тяжести деферентным путем.

По методу биодинамической проприоцептивной коррекции движений (Козявкин, 1991 год) [8] все занятия программы проводятся с костюмом - биодинамический корректор "Спираль". Он представляет собой систему эластичных упругих тяг, которые спиралевидно накладываются на туловище и конечности и прикрепляются к специальным опорным элементам - жилету, шортам, наколенникам, налокотникам, полуперчаткам и сапожкам.

К ортопедическим средствам, позволяющим компенсировать отсутствующую функцию опороспособности и ходьбы у пациентов с выраженным дефицитом мышечной силы и дефицитом координации движений, относятся:

- Устройства, позволяющие сохранять положение тела в пространстве: параподиумы, вертикализаторы, опоры для сидения, ползания, умывания, туалета;

Фото 1а. Папаподиум. [7]

Фото 1 б. Вертикализатор.

- Корсеты ортопедические,
- Туторы: устройства ограничения подвижности суставов
- Аппараты ортопедические: для нижних конечностей, верхних конечностей, на все тело (AFO, HAFO, SAFO, SMO);

Фото 3. Тутор[7]

Фото 4. Ортезная система[7,9]

Фото 5. Аппарат ортопедический [7]

Фото 6 Корсет мягкий. [7]

- Аппараты RGO: реципрокные ортезы (RGO — reciprocating gait orthosis), обеспечивающие возвратно-поступательную ходьбу, эквивалентную естественной: HGO (hip guidans orthosis, parawalker), ARGO (advanced RGO), IRGO (isocentric RGO) [5,6].

Фото 7. РОС[9]

Фото 8. REHA-STIM

Активные ТВС

Роботизированные комплексы для клиничного и домашнего применения реализуют императивную локомоцию как метод лечения.

Роботизированная система REHA-STIM придерживает пациента при помощи костюма над платформой, а ноги крепятся лентами к педалям. При запуске системы стопы ног совершают антропоморфные движения, описывая естественную траекторию движения при локомоторном режиме. Тренажер подает команды и оценивает походку пациента. А похожий на снаряжение космонавта костюм «Атлант», внутри которого находятся надувные камеры, сжимающие мышцы и активизирующие центральную нервную систему, помогает удерживать тело в вертикальном положении, скорректировать осанку, сформировать "Рефа Стим" правильный изгиб позвоночника, отрегулировать движения. Может использоваться только клинически из-за габаритов, с обязательным участием ассистента.

Роботизированная система «LOKOMAT»

В процессе работы на комплексе «Локомат», пациента вертикализуют при помощи приспособлений по типу альпинистских обвязок, закрепляют ноги в специальные тренажеры (ортезы), работу которых контролирует сложная компьютерная программа, и помещают пациента на беговую дорожку

Фото 9. Локомат

Может использоваться только клинически из-за габаритов, с обязательным участием ассистента.

Единственными в мире роботизированными системами, использующимися в домашних условиях, и запускающимися только мамой являются комплексы БИОНИКА[2, 3]. Бионика 1 используется для плавания, ползания и передвижения на четвереньках.
Бионика 2 применяется для восстановления или приобретения навыков двуногой ходьбы как в состоянии бодроствования, так и в состоянии дневного сна.

Фото 10. Бионика 1[2,3]

Фото 11 Бионика II[2,3]

Оба робота реализуют императивные локомоции при помощи метода компенсации дефицита мышечной и управляющей активности

внешней энергией., осуществляя полный цикл бионической абилитации и реабилитации.

Литература:

[1]. Чернышева, И.Н. Особенности ортезирования детей с нервно-мышечными заболеваниями // «Ортопедия, травматология и протезирование» - 2010, - №1, С.124–132

[2]. Дюкенджиев, Е. Бионика в реабилитации церебрального паралича и спиномозговых заболеваний - И-во РТУ, Рига - 2010, Том I.

[3]. Дюкенджиев, Е. Бионика в абилитации церебрального паралича и спиномозговых заболеваний - И-во РТУ, Рига - 2013, Том II.

[4]. Бадалян, Л.О. Детские церебральные параличи, // Л.О.Бадалян, Л.Т.Журба, О.В.Тимонина,- Зоровья, Киев,- 1988г.,-324с.

[5]. Pat. 13100B Latvijas Republikas. Civeka Kustibu vadisanas reciprokalas pienemiens un reciprokala ortozu sistema visam kermenim / E. Dukendjiev. — № 13100B. 19.06.2002.

[6]. Robert R. Reciprocat. Gait Orth. (RGO) [Электронный ресурс] / R.R. Madigan, K.D. Fillauer. Режим доступа: http://www.fillauer com/education/ED RGO.html.

[7]. Протезно-ортопедическое обеспечение детей с детским церебральным параличом. Prosthetic & Orthotics providing children with cerebral palsy. А.А. Стеклов, М.В. Паршиков, В.И. Горбунов, В.В. Мельник. 10.Baltic-Bulgarian Conference On BIONICS and PROSTHETICS BIOMECHANICS and MECHANICS MECHATRONICS and ROBOTICS. Латвия, Лиепая, 2014 г. июнь.

[8]. В. Лаврецкая, С. Хоботов Сравнительный анализ неинвазивных методов лечения церебральных параличей и других спинальных заболеваний и повреждений. V.International Conference On BIONICS and PROSTHETICS BIOMECHANICS and MECHANICS MECHATRONICS and ROBOTICS. Варна, Болгария, 2006 г. июнь.

ПРОЕКТИРАНЕ И СИМУЛИРАНЕ НА УЧИЛИЩНА ЛОКАЛНА КОМПЮТЪРНА МРЕЖА

И. Цонев, В. Атанасов

DESIGN AND SIMULATION OF LOCAL SCHOOL COMPUTER NETWORK

I.Tsonev, V. Atanasov

abstract. *В доклада е описана методика за създаване проект за изграждане на локална компютърна мрежа в училище. Обосновани са изискванията към компютърната мрежа на средно училище. Предложени са структурата и стандарта за изграждане на мрежата.*

keywords: *school, network, ethernet, wireless, router, switch.*

Планирането на една компютърна мрежа е сложен процес, който в никакъв случай не може да се ограничи в рамките на няколко дни. Ако сравним един компютър с една сграда, то изграждането на компютърна мрежа можем да сравним с изграждането на един квартал. Изключително важно, за качествената компютърна мрежа, е нейното планиране. Тук трябва да се има предвид не само броя на компютрите, а и много добре да се прецени риска от заплахи, както външни, така и вътрешни, възможности за разширяване и управление, както и независимостта на топологията.

Изборът на техническото и приложно програмно осигуряване се осъществява в зависимост от конкретните дейности, за които то ще се използва. Всяко обсъждане, свързано с техническото и програмно осигуряване за локалната мрежа, започва с проучване на съществените потребности.

За да се проектира компютърната мрежа е необходимо да се направи проучване за следните параметри:

- трафикът от данни;
- дължина на съобщенията;
- средно и пиково натоварване;

- скорост на предаваните съобщения;
- разположение на помещенията;
- разположение на персоналните компютри;
- отдалеченост на компютри и сървъри.

Отчитат се ограниченията по отношение на времето за отговор и секретност. След анализа на потребностите се определят изискванията към локалната мрежа. Следващата стъпка е планиране на конкретни технически средства.

Определя се топологията на мрежата, процедурата за достъпа до съобщителната среда, методът на предаване. Необходимо е също така да се отчете съвместимостта със съществуващите стандарти и ограничения при реализация на локалната мрежа. Потребителското програмно осигуряване се определя от конкретните задачи на абонатите на мрежата. Удачно е използване на пакети приложни програми, решаващи тези задачи, като се обърне внимание на съвместимостта.

Проектирането на училищна локална мрежа в много от случаите се пренебрегва. Инсталират се компютри и периферни устройства, като се акцентира повече на операционната система, отколкото на комуникацията между отделните устройства. От гледна точка на сигурността се допускат сериозни грешки, които могат да доведат до сериозни проблеми, причинени от зловредни действия.

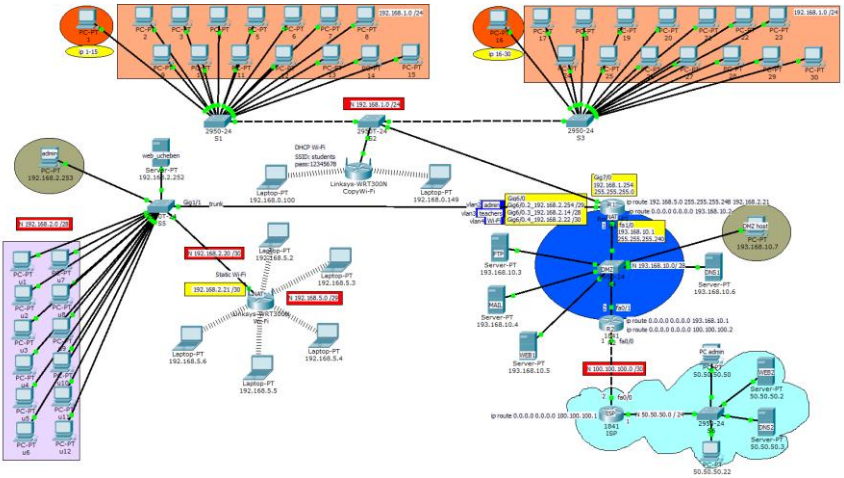
Необходимо е проектиране и симулиране училищна

мрежа с представено пълно описание на конфигурирането на отделните

мрежови и хардуерни устройства.

На Фиг.1 е показана структурната схема и мрежовата топология на

училищна локална компютърна мрежа.



Фиг.1

Функциите и услугите, предлагащи се в мрежата налагат избор на подходящи мрежови устройства от активен и пасивен тип – маршрутизатори, комутатори (суичове) , кабели и други.

С цел повишаване на сигурността на мрежата и вследствие анализа на съществуващите комуникационни среди, приложими в локалните компютърни мрежи, за нуждите на настоящия проект е избрана кабелна свързаност на мрежовите устройства със задаване на статични и динамични настройки.

На базата на анализ на основните международни стандарти за изграждане на локална компютърна мрежа е избран стандарт IEEE 802.3 (Ethernet), поради добрата надеждност, сигурност и пълната съвместимост на стандарта със съществуващите мрежови операционни системи и устройства.

Анализа на съществуващите класификации и топологии на локалните компютърни, наложи избора на хетерогенна топология, включваща мрежа с равноправен достъп и мрежа от тип „клиент-сървър”.

С цел повишаване на функционалността на мрежата са добавени безжични устройства, работещи в стандарт IEEE 802.11.

С цел ефикасното администриране на мрежата е извършено

конфигуриране на участващите мрежови устройства. На рутерите са дефиниране контролни листи, които според изискванията на ръководството на училището, налагат следните ограничения:

Ученическата мрежа (192.168.1.0 /24) е изградена от 28 компютъра, разположени в две стаи по 14, като във всяка стая има по един учителски компютър, от който е достъпна учителската мрежа, с цел всеки учител да може да достъпи споделената информация на компютъра си в учителската стая. Учениците от своя страна имат достъп до вътрешния сървър **"web_ucheben**, пълен достъп до интернет и съответно до сървърите в ДМЗ;

Ученическата безжичната мрежа (192.168.0.0 /24) - с възможност за получаване на 50 адреса по DHCP за достъп от мобилни устройства (телефони, таблети, преносими компютри);

Учителската мрежа (192.168.2.0 /28) - има пълен достъп до интернет, мрежата на учениците, вътрешния WEB сървър;

Безжичната мрежа (192.168.5.0 /29) - с четири преносими компютъра със статични адреси за административния персонал и един за директора;

Гранична мрежа ДМЗ (193.168.10.0 /28) - Демилитаризирана зона, в която са поставени четирите училищни сървъра (FTP, MAIL,WEB1,DNS1), достъпни от Интернет. Тук е поместен и един компютър (ДМЗ хост), през който системният администратор да може да достъпва локалната мрежа от интернет;

Интернет – симулиран с WEB2 сървър, DNS2 сървър, администраторски компютър и клиентски компютър.

Изводи:

1. Проведените симулационни тестове показаха пригодността на предложеният проект за мрежа, от гледна точка на свързаността между потребителите и гарантиране на услугите в мрежата;
2. Предложената структура на мрежата дава възможност за надграждане при нужда, като приложените защитни механизми гарантират надеждността на данните, потребителите и системата.

Литература:

1. Цонев И., Предавне на данни и компютърни комуникации, Шумен, 2012
2. Ганчев И., Компютърни мрежи и комуникации, Пловдив, 1999
3. Станев Ст.,Смит П., Захариев Ф., Компютърни системи и мрежи, Шумен, 2002
4. Тужаров Х., Компютърни мрежи, Велико Търново, 2000
5. Попов М., Калбанов М., ISDN Нова мрежова и информационна технология, Велико Търново, 2004

СРАВНИТЕЛЕН АНАЛИЗ НА ГЕОДЕЗИЧЕСКИ СИСТЕМИ БГС 2000 И БГС 2005

Събин И Иванов

COMPARATIVE ANALYSIS OF GEODETIC SYSTEM 2000 BGS AND BGS 2005

Sabin I Ivanov

ABSTRACT: *This report will examine the properties of conformal conical (Lambert) projection, Gaussian cross-cylindrical projection and its modification - the universal cross-cylindrical Mercator - UTM, which are used in introducing Bulgarian Geodetic System 2000 (Lambert) and Bulgarian Geodetic System 2005 (UTM).*

KEYWORDS: *projection, geodetic system, function, ellipsoid, meridian, parallel*

УВОД

Картата е умалено, генерализирано изображение на земната повърхност по даден математически закон върху равнина, показваща природните и обществено-политическите явления и процеси. Действителната физична земна повърхнина е с неправилна форма, затова при съставянето на карти е необходимо да се премине към друга, правилна повърхнина.

Обработката на измерванията става в подходящо избрана координатна система. Поради кривината на Земята координатната система не може да се приложи за големи територии (формата на Земята се приема за ротационен елипсоид). От тази гледна точка въвеждането

на равнинни координати ще бъде възможно след изобразяване на част от референтния елипсоид върху равнина (образна, проекционна) по определен математически закон. Елипсоида се явява повърхнина с гаусова кривина, различна от нула (K≠0), и всяко негово изображение е свързано неминуемо с деформации. Тези деформации в най-общия случай са в дължини, в ъгли и в площи.

При геодезическите и картографските проекции законите на изображението са същите, но те се различават по вида на основните координатни линии, които се изобразяват. При картографските проекции тези линии са паралелите и меридианите от географската координатна система.

При геодезическите проекции освен условието за непрекъснатост на изображението и за взаимно еднозначно съответствие на точките от елипсоида (оригинални точки) с тези от проекционната равнина (образни точки) се изискват още:

1. Дължините, ъглите и площите, които се измерват да се изобразяват с възможно най-малки деформации върху равнината, така че при работа с картата да са в границите на нейната графическа точност. Конформните изображения са за предпочитане, за да се получат ъглите във вярната им стойност, т.е. мащабът на изображението в околността на дадена точка да е един и същ.
2. За да се преминава бързо и точно от елементи върху елипсоида към съответните им елементи в равнината, деформациите трябва да се изчисляват лесно.
3. Поради горните две изискванията не е възможно да се използва само една координатна система, както е при големите държави, като въведените координатни системи трябва да бъдат напълно еднообразни.

Основното предимство на конформните проекции се явява обстоятелството, че мащабът на изображението не зависи от посоката, а само от мястото на точката.

Основните построения върху земната повърхнина, с помощта на които се предават единни координати за определени територии, са триангулацията и полигонометрията. От положенията на точките в тях върху земната повърхнина се преминава към положенията им върху повърхността на референтния елипсоид и след това и в проекционната равнина. Върху елипсоида точките се съединяват с геодезически линии,

а в равнината с прави линии, които не са обаче изображение на геодезическите линии. Въз основа на това се налага въвеждането на подходящи редукции в дължините и в посоките освен заради деформациите, дължащи се на геодезическата проекция, и заради прехода към друга съединителна линия в равнината.

В този доклад ще разгледам качествата на конформната конична (Ламбертова) проекция, Гаусовата напречно-цилиндрична проекция и нейната модификация – универсалната напречно-цилиндрична проекция на Меркатор – UTM, които са използвани при въвеждането на Българска геодезическа система 2000 (Ламбертова) и Българска геодезическа система 2005 (UTM).

Основният критерий по който ще се направи оценка на качествата на двете проекции ще бъде изчислените стойности на частните мащаби. Колкото частните мащаби са по-близки до единица, толкова проекцията ще бъде по-качествена.

ТЕОРЕТИЧНА ПОСТАНОВКА

1.Класификация на картографските проекции.

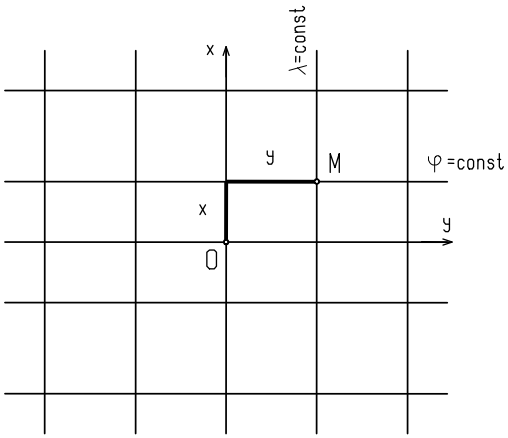
1.1.Класификация по вида на образите на меридианите и паралелите от основната мрежа (класификация на нормалните проекции).

1.1.1.Цилиндрични проекции.

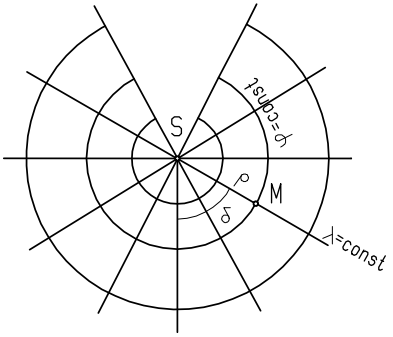
При нормалните цилиндрични проекции меридианите се изобразяват като равно отдалечени успоредни прави, а паралелите – като успоредни прави, перпендикулярни на образите на меридианите (фиг.1). При подходящо подбрана декартова правоъгълна координатна система в картната равнина дефиниционните уравнения на цилиндричните проекции са

(1) $x = f(\varphi), \qquad y = C.\lambda, \qquad C = const.$

Където φ, λ са елипсоидни географски координати Видът на функцията $f(\varphi)$ и константата C характеризират отделните цилиндрични проекции.



Фиг.1



Фиг.2

1.1.2.Конични проекции.

При нормалните конични проекции паралелите се изобразяват като дъги от концентрични окръжности, а меридианите – като лъчи, които излизат от центъра на окръжностите и сключват ъгли, по-малки

от оригиналните ъгли между меридианите (фиг.2). Аналитичната дефиниция на коничните проекции при полярна координатна система в картната равнина е

(2) $\rho = f(\varphi), \qquad \delta = \alpha.\lambda, \qquad \alpha = const.$

Функцията $f = (\varphi)$ и константата $\alpha < 1$ характеризират отделните конични проекции.

1.2.Класификация на проекциите според характера на изображението.

Според характера на изображението картографските проекции се делят на конформни, еквивалентни, равнопромеждутъчни и произволни.

При конформните проекции, наричани още равноъгълни, се изобразяват без деформации ъглите. При тези проекции се явява подобие в безкрайно малкото.

При еквивалентните проекции, наричани още равноплощни, се изобразяват без деформации площите. При тези проекции площният мащаб p е повсеместно константен.

При равнопромеждутъчните проекции се изобразяват без деформации или меридианите, или паралелите.

Към произволните проекции се отнасят проекциите, при които не се запазват нито ъглите, нито площите, нито разстоянията.

1.3.Класификация на проекциите според положението на нормалната мрежа спрямо основната.

Според положението на нормалната мрежа спрямо основната картографските проекции се делят на три групи:

1.3.1.Нормални или директни проекции, при които нормалната и основната мрежа съвпадат, т.е. $\varphi_0 = 90^0$.

1.3.2.Трансверзални или напречни проекции, при които полюсите на нормалната мрежа лежат в екватора на основната мрежа, т.е. $\varphi_0 = 0^0$.

1.3.3.Наклонени или коси проекции, при които полюсите на нормалната мрежа заемат общо положение в основната мрежа, т.е. $0^0 < \varphi_0 < 90^0$.

Освен тези признаци картографските проекции могат да се разделят на групи и по други признаци. Например при азимуталните, коничните и цилиндричните класове проекции, като подкласове се явяват перспективните и неперспективните проекции.

2. Оценка на качествата на ламбертова и Гаусова проекции.

От гледна точка на математиката при всички проекции имаме, най-общо казано, “изображение”.

Една от важните характеристики на дадена проекция се явява мащабният фактор m на изображението, който е мярка за деформацията на проекцията и в общия случай зависи от мястото и посоката. За дадена картографирана област мащабът m трябва да бъде близък до единица. Минималната разлика на мащаба от единица е важен белег за оптималност, но важно е също трансформацията от образните (картните) координати (x, y) към елипсоидните географски координати (φ, λ) да се извършва лесно и удобно.

Друг важен качествен показател е простотата на закона за изобразяване.

Важен въпрос, който може да се постави е да бъде ли проекцията конформна? При конформната проекция ъглите се запазват недеформирани при изобразяването. В днешно време се изтъкват съображения, според които се измерват повече разстояния, отколкото ъгли, което налага запазването на техните истински стойности. При изработването на кадастрални карти и в някои устройствени дейности е от значение запазването на площите на отделните области, т.е. употребява се еквивалентна (равноплощна) проекция, която не е конформна. Трябва да се подчертае и следното качество на

конформната проекция, че мащабът зависи само от мястото, но не и от посоката. Следователно предпочитанието за конформност на изображението се запазва.

2.1. Ламбертова проекция.

Нормалната конформна конична проекция се свързва с името на немския математик и философ Йохан Хайнрих Ламберт Поради това разглежданата проекция се нарича още конична проекция на Ламберт, или Ламбертова проекция. В по-късен етап проекцията е намерила приложение в страни като Белгия и Франция и в някои щати на САЩ. В България Ламбертовата проекция е намерила заслужено място както в учебната литература, така и при създаването на Българската геодезическа система 2000 (БГС 2000).

При коничната Ламбертова проекция избраният централен меридиан не съвпада по смисъл с централния меридиан на Гаусовата (а също и на UTM) проекция, а обикновено се определя от средната елипсоидна географска дължина λ_0 на изобразяваната територия.

Следователно за разликата в дължините l ще имаме

(3) $l = \lambda - \lambda_0$,

радиусът на паралела е

(4) $r = \dfrac{a.\cos\varphi}{\left(1 - e^2.\sin^2\varphi\right)^{1/2}}$,

където φ и λ са елипсоидните географски координати, λ_0 е географската дължина на избрания централен меридиан.

Изометричната ширина ще бъде равна на

(5) $q = \dfrac{1}{2}\ln\left[\dfrac{\left(1+\sin\varphi\right)}{\left(1-\sin\varphi\right)}\right] + \dfrac{1}{2}e.\ln\left[\dfrac{\left(1-e.\sin\varphi\right)}{\left(1+e.\sin\varphi\right)}\right]$.

Дефиниционните уравнения на проекцията са

(6) $x = X_0 - \rho.\cos(\alpha.l)$, $y = Y_0 + \rho.\sin(\alpha.l)$,

където (x, y) са равнинните образни координати, а радиус-векторът ρ ще се определи по формулата

(7) $\rho = C.\exp(-\alpha.q)$.

Дефиниционните параметри се явяват α <1 и C >0.

Константата X_0 може да се избере по такъв начин, че абсцисите да са положителни, например при условие $X_0 > \rho$.

Мащабът m се определя по формулата

(8) $m = \dfrac{\alpha.C.\exp(-\alpha.q)}{\rho}$.

2.2. Гаусова и UTM проекции.

Към Гаусовата проекция може да се присъедини и известната напоследък UTM (Universal Transverse Mercator) проекция. Те са еднотипни цилиндрични проекции различаващи се само по наименованието. Начало на координатната система се взема пресечната точка на екватора с някой от меридианите, наречен основен за конкретната система. Мащабът по целия основен меридиан за дадена система има константна стойност, който е равен на единица или на стойност, близка до единица. С отдалечаване от основния меридиан, деформациите в изображението ще нарастват.

Земята се разделя на триградусови и шестградусови гаусови координатни системи (ивици, зони), които се простират от полюс до полюс и имат мащаб по основния меридиан $m_0 = 1$. При триградусовите ивици основния меридиан е отдалечен по на $1,5^0$ на изток и на запад. Ивиците са номерирани без прекъсване, като номер $n = 1$ има ивицата с основен меридиан $L_0 = 3^0$, номер $n = 2$ –

ивицата с основен меридиан $L = 6^0$ и т.н. При шестградусовите ивици основния меридиан е отдалечен по на 3^0 на изток и на запад, ивиците също са номерирани без прекъсване, като номер $n = 1$ има тази с основен меридиан $L_0 = 3^0$, номер $n = 2$ – ивицата с основен меридиан $L = 9^0$ и т.н. Връзката между номера на координатната система и централния меридиан $L = L_0$ е показана на фиг.38. От графиката се вижда, че всеки втори основен меридиан на триградусовите ивици, съвпада с основния меридиан на шестградусовата ивица.

Абсцисата X е по направление на основния меридиан, а ординатата Y започва от оста X – на изток е положителна, на запад отрицателна. За да не се получават ординатите отрицателни, е възприето предложението на Баумгарт да се прибавят към тях 500 000 m = 5.10^5 m, а като милионна цифра да идва последната цифра от номера на координатната система, т.е. $n.10^6$ m. Следователно гаусовите координати на една точка се записват във вида

(9) $X = x,\ Y = Y_0 + y = \left(n.10^6 + 5.10^5\right) + y.$

От начина на записване на ординатата Y се проличава разположението на дадена точката по отношение на основния меридиан. Ако цифрата, следваща след милионната цифра, е по-малка от 5, точката има отрицателна ордината y, считана от основния меридиан, и се намира следователно на запад от него, а ако е 5 и над 5 – тя има положителна ордината y и лежи на изток от него.

Територията на България се обхваща от:

а) две 3^0-ови гаусови координатни системи с основни меридиани $L_0 = 24^0$ и $L_0 = 27^0$ и съответно номера 8 и 9;

б) две 6^0-ови гаусови координатни системи с основни меридиани $L_0 = 21^0$ и $L_0 = 27^0$ и с номера 4 и 5. Мащабът е равен на

единица по основния меридиан и расте на изток и на запад от него. Вижда се, че меридиан с дължина $L_0 = 27^0$ се повтаря.

Общоприето е картите в мащаб 1:5000 и плановете в мащаб 1:2000 и по-едър да се свързват с 3^0-овите гаусови координатни системи, а тези в мащаби 1:500 000, 1:200 000, 1:100 000, 1:50 000, 1:25 000 и 1:10 000 в зависимост от графическата им точност с 6^0-овите гаусови координатни системи.

3. Връзка на координатните системи 2000 и 2005 с 1970 и 42-83

3.1 Българска геодезическа система 2000.

За нуждите на кадастъра, а и не само за него, се е наложила необходимостта от въвеждането на нова геодезическа система. Направените предпоставки за въвеждане на подходяща геодезическа система в България са:

3.1.1.Въведена и материализирана е системата EUREF на територията на България посредством 15 точки, избрани, стабилизирани и определени в система ETRF-89, наречени в последствие Булреф (BULREF).

3.1.2.Включването на територията на страната в Европейската височинна система, чрез Европейската височинна мрежа EUVN. А също така се свързва и първокласната прецизна нивелачна мрежа на страната с UELN – към Европейската височинна референтна система EVRS.

3.1.3.Създадените осем гравиметрични станции в рамките на проекта UNIGRACE.

3.1.4.Реализиран е и Европейски геоид, съвместим както с ETRS-89, така и с EVRS.

БГС 2000 се въвежда да послужи за отправно начало на всички национални геодезически измервания. Обновяването и усъвършенстването на геодезическата основа в страната ще се извършва на базата от 15-те български точки (BULREF). Основното изискване, което е поставено към БГС 2000 е да има минимални линейни деформации.

3.2 Българска геодезическа система 2005.

На 29 юли 2010 г. се въвежда „Българска геодезическа система 2005” за територията на Република България. Създаването на нова Държавна GPS мрежа се инициира от Министерството на регионалното развитие и благоустройството (МРРБ) и Министерство на отбраната. През периода 2003 – 2005 г. Военногеографската служба (ВГС) създава Държавната GPS мрежа, определена в Европейската координатна система.

За Държавната GPS мрежа се въвеждат понятията основен клас и второстепенен клас, към основния клас са включени 112 точки. Общият брой на точките на държавна мрежа е 473 точки, към които са включени и мареографните станции в Бургас и Варна. Обработката на мрежата се извършва в Централната лаборатория по висша геодезия (ЦЛВГ) със специализиран софтуер Bernese.

4. Приложения от изследванията.

С въвеждането на „Българска геодезическа система” в страната ще се осигурят условия за по-лесно и по-ефективно приложение както на технологиите на измерване, така и на информационните технологии. Ще отпадне необходимостта да се търсят точки от старата геодезическа мрежа, които в повечето случаи са трудно достъпни, повредени, унищожени или точността им не е ясна. Ще се избегне трудната трансформация към съществуващите системи, при която се деформират принудително високоточните GPS измервания. Трансформацията от GPS координати във желаната проекция и обратно ще се извършва по строго определени и затворени формули. Координатната система ще е единна за цялата страна, което ще направи възможно изграждането на общи информационни системи за цялата страна. Разграфката и номенклатурата ще са в съответствие с международните стандарти. Референтната рамка за координатите, височините и гравиметрията ще е обединена с тази на Европа.

ЗАКЛЮЧЕНИЕ

От сравнението на Гаус-Крюгеровата, UTM и коничната конформна проекция могат да се направят следните изводи относно аналитичната форма на изображението: коничната конформна проекция ще има решаващо предимство, дори и при посоченото рационализиране на изчислението на Гаус-Крюгеровата проекция (UTM се явява само нейна модификация).

Относно разпределението на деформациите, като се има предвид, че точките от територията на страната ни имат ширини малко повече от 41^0 (за южната част) и малко повече от 44^0 (за северната част), предимство, макар и слабо изразено, ще има коничната проекция. Тази проекция ще има обаче и друго предимство: на $\varphi = const$ съответства $m = const$, докато мащабът при Гаус-Крюгеровата проекция се изменя както с дължината λ, така и (макар и слабо) с φ. Най-съществено предимство обаче се проявява в следното: поради географските особености на нашата страна (размери и местоположение) при коничната проекция е достатъчна само една образна координатна система – единна за цялата страна. При Гаус-Крюгеровата проекция (съответно UTM) това няма да бъде възможно. За нашата сравнително малка по размери страна неподходящо би било да има две или повече системи (ивици или зони) с неизбежните трансформации между тях за граничните точки.

„Система 1970" трябва да се изостави поради своите недостатъци, а също поради необходимостта от преход към европейската референтна система.

И така, като се вземе в предвид формата и размерите на страната, най-подходяща геодезическа проекция се оказва конформната конична (Ламбертова) проекция. Предпоставките за това са следните:

1. Проекцията е единна за територията на страната и ще осигури същото качество за правоъгълните равнинни координати (x, y), с което се избягва необходимостта от преобразуването им при преминаване от една ивица (зона) в друга.

2. По форма територията на страната е близка до правоъгълник с основа успоредна на паралелите и почти два пъти по-дълга от височината. Разположена в пояса на средните географски ширини ($41^0 10` – 44^0 15`$), което ще позволява да се приложат варианти с един или два стандартни паралела $x_0 = const$, в близост до които координатите ще са локално декартови. При два стандартни паралела, мащабът по които е единица, разстоянието (s) до най-отдалечените от тях точки се дава около 50 km. По формулата за изчисление на линейната деформация:

$$(10)\ \delta s = \frac{s\left(x - x_0\right)^2}{2R^2},$$

където R е средният земен радиус, е установено, че една дължина от 10 km се проектира с максимална деформация 30,8 cm. За сравнение с Гаусовата проекция, където формулата е:

$$(11).\ \delta s = \frac{s\left(y - y_0\right)^2}{2R^2},$$

дори при ширина на ивицата 3^0, се установява, че тази стойност ще достига 1,5 m. При ширина на ивицата 6^0 (както е при UTM) тази стойност ще достига 6 m.

3. Ламбертовата проекция е конформна, без ъглови деформации. За редица приложения е важно площните деформации да бъдат минимални, т.е. проекцията да е еквивалентна. Тези изисквания ще се съчетаят добре в този случай, защото при минимална линейна деформация и конформност е естествено и площната деформация да бъде малка.

4. Формулите на проекцията са прости и в затворен вид.

За нуждите на отбраната и други държавни учреждения може да е по-целесъобразно да се търси друг тип проекция, с оптимални показатели не само за територията на страната, а и за райони, разположени в различни краища на света. Такива са напречните

цилиндрични проекции, които неслучайно намират широко приложение в много страни и международни организации, а също така и при въвеждането на новата геодезическа система за територията на нашата страна под наименованието „Българска геодезическа система 2005” – UTM проекция.

ЛИТЕРАТУРА:

1. ст.н.с. I ст. д-р инж. Г. Милев, проф. д-р инж. Г. Вълев, доц. д-р инж. М. Минчев, М. Матова, К. Василева, П. Гъбенски – Европейската референтна система в България, София, 2006.

2. проф. д-р инж. М. Даскалова, доц. д-р инж. И. Здравчев – Математическа геодезия, София, 2005.

3. ст.н.с. д-р И. Йовев – GPS технологиите и създаване на условия за тяхното ефективно приложение в България, статия, сп.”География`21”, бр.5, 2007.

4. инж. В. Коритарова – Българска геодезическа система 2005 – история и бъдеще, статия, сп.”Геомедия”, бр.5, 2010.

5. доц. д-р инж. А. Аврамов. Възможности на равноъгълните конични проекции за създаване на едромащабни карти на територията на България – Сборник трудове на Научна сесия `95. Част VII – ВВУАПВО, Шумен, 1995 г.

6. доц. д-р инж. М. Андреев – Математическа картография, София, 1980.

АЛГОРИТЪМ ЗА ОЦЕНЯВАНЕ ЧЕСТОТАТА НА ПРИРОДНИТЕ БЕДСТВИЯ ЧРЕЗ ПОЛИНОМ НА ЧЕБИШЕВ

Борислав Й. Беджев, Доника В. Диманова

ALGORITHM FOR ASSESSING THE INTENSITY OF NATURAL DISASTERS BY CHEBYSHEV POLYNOMIALS

Borislav Y. Bedzhev, Donika V. Dimanova

ABSTRACT: *Essential in the work of the responsible authorities is the rapid and timely response to heavy snowfalls, floods, earthquakes, landslides, fires and storms. For this reason, the report justifies the thesis that in order to improve the efficiency of government officials involved in the protection of the population and prevention from natural disasters, it is necessary to make scientifically based estimates of the incidence and causes of their occurrence in the next few years. Addressing this important practical task is possible by developing an algorithm for assessing the frequency of natural disasters.*

KEYWORDS: *algorithm, model, Chebyshev polynomials*

Въведение

Зависимостта на хората от природните явления би могла да бъде със съдбоносни за съществуването им измерения, особено когато се наблюдават големи отклонения от нормалните стойности на метеорологичните елементи – температура и валежи. Природните бедствия нанасят значителни поражения на стопански, жилищни и инфраструктурни обекти. Част от тях обхващат значителна територия от страната, продължават денонощия, проявяват се многократно, ангажират значителни човешки, материални и финансови ресурси.

В тази връзка целите на доклада са:

1. Да се изследва тенденцията за увеличаване на едно от природните бедствия – наводнения в България;

2. Да се обосноват мерки за подобряване на работата на държавните органи, ангажирани с предотвратяването или ликвидирането на вредните последствия при извънредни ситуации.

Хипотеза се обосновава чрез разработване на Алгоритъм за оценяване честотата на природните бедствия.

Изложение

Докладът е структуриран по следния начин:

1. Изследва се тенденцията и причините за увеличаване на наводнения в България.

2. Приема се хипотезата, че предприеманите дейности за намаляване риска от възникването на наводнения не са достатъчни и е нужна политика на цялостно управление на риска.

3. Описан е алгоритъм за синтез на модел на честотата на екстремни климатични явления със сума от ортогонални полиноми на Чебишев.

Изследванията за България **показват**, че се увеличава честотата на наводненията. Едни от основните причини са изменението на климата, интензивното социално – икономическо развитие, урбанизацията, остарялата инфраструктура на отводнителните системи, речни прииждания вследствие на обилни валежи от дъжд, от обилно снеготопене и значително покачване на нивото на водата на големи реки и язовири, от аварии на хидротехнически съоръжения или неправилно управление на язовирите, повишаване нивото на морето в резултат на урагани и земетресения и др. Особено опасни са наводнения от интензивни валежи за селищните райони, където водонепропускливите улични настилки създават условия за големи скорости на водата, бърза концентрация и почти никакви загуби от инфилтрация в почвата. На фигура 1 са представени данни от НСИ за наводненията в България за периода 2003 – 2014 г, като данните за 2014г. са до м. юли [4]. От

фигурата е видно, че годините с най – голям брой наводнения са 2005 и 2013.

Фиг.1 Наводнения на територията на България за 2003 – 2014г.

Фиг.2. Съотношение годишния брой наводнения към общия брой природни бедствия

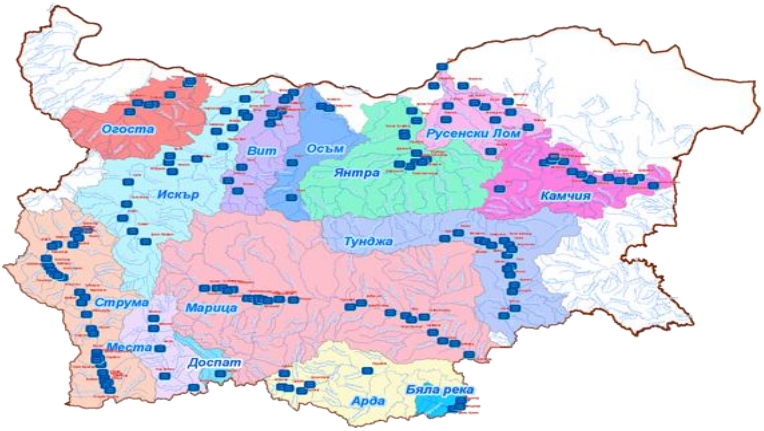
Наводненията се различават от другите природни бедствия по това, че в значителна степен се поддават на прогнозиране. Общо 30 % от бедствията, сполетели България в периода 1974 – 2006 г., са наводнения [4]. Това се потвърждава и от фигура 2.

Наводненията причиняват големи щети на инфраструктурата и големи разходи за икономиката и обществото. Най – засегнати могат да бъдат селско стопанство, лесовъдство, енергетика, туризма и други отрасли.

Нанесените щети от наводнения през последните години са показател, че не сме достатъчно подготвено да се противопоставим на този нарастващ риск. Прилаганите досега дейности за намаляване на риска от възникването на наводнения не са достатъчни и е нужна политика на цялостно управление на риска.

Оценката и управлението на риска от наводнения в Република България са регламентирани с Европейската Директива 2007/60/ЕО от 26.11.2007 г. [2]. Съгласно нея и Закона за водите (2010 г.), управлението на риска от наводнения се извършва на басейнов принцип и включва три основни етапа [1]:

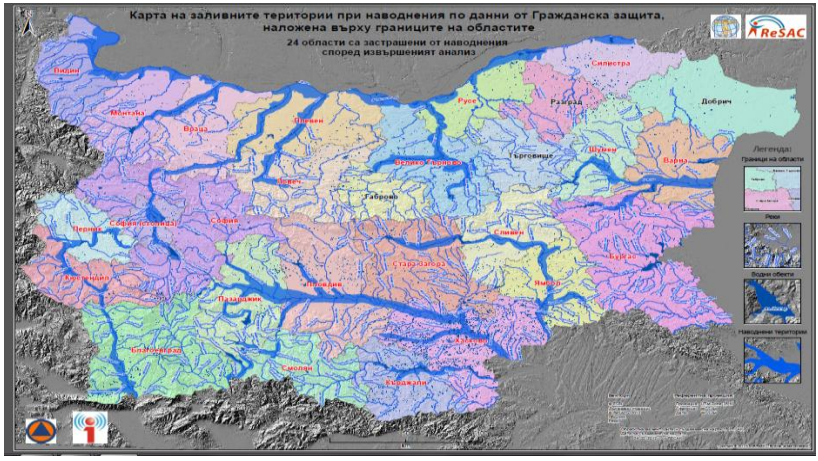
- извършване на предварителна оценка на риска от наводнения (ПОРН);
- изготвяне на карти на районите под заплаха от наводнения и с риск от наводнения в срок до края на 2013 г. (РЗПРН);
- разработване на планове за управление на риска от наводнения в срок до края на 2015г.



Фиг. 3 Райони с готови симулационни модели за наводнения

На фигура 3 е представена карта на районите с готови симулационни модели за наводнения на територията на Р. България [5]. До момента са изготвени 163 симулационни модели. Представените графични материали са свързани с опростени модели за симулиране на заливните територии от евентуални наводнения. Симулационните модели са опростени и включват основно в себе си модел на релефа, изграден на база топографски карти, спътникови изображения с висока разделителна способност и анализ на земно покритие / земеползване. Картите са изготвени от специалисти от Център за приложение на спътникови изображения (РЕСАК), Агенцията за устойчиво развитие и евроинтеграция (АУРЕ), специалисти от Софийски университет "Св. Климент Охридски" и Националния институт по метеорология и хидрология.

На фигура 4 е показана карта на заливни зони на основните български реки по данни на ГД – ПБЗНБА към МВР.



Фиг. 4. Карта на заливни зони на основните български реки

За намаляване риска от природни бедствия, в случая наводнения, е целесъобразно използването на програми от мерки, насочени към прогнозирането и оценка на въздействието върху всички фактори, влияещи върху появата им. Тази оценка може математически да се обоснове чрез използването на различни методи за моделиране и

симулация на природните бедствия. Тези модели могат да бъдат важен инструмент при анализ на процесите при бедствени ситуации и да подпомогнат вземането на решения от отговорните органи.

За да се направи анализ на честотата на природните бедствия се приема хипотезата, че количеството наводнения за една година се описва със сума от ортогонални полиноми на Чебишев [3]:

$$L(t) = \sum_{j=0}^{s} \hat{C}_n . Z_n(t). \qquad (1)$$

Тук $\hat{C}n, n = 0,1, \dots, s$ са статистически оценки на коефициентите, $Z_n(t)$ е ортогонален полином на Чебишев от n – ти ред, дефиниран върху множеството $\{ t_1, t_2, \dots, t_N \}$.

При анализа е използван следният алгоритъм за синтез на модел на честотата на екстремните климатични явления.

Алгоритъм за синтез на модел за честотата на природните бедствия

Стъпка 1: Намиране на оптимална степен на полинома $L(t)$ от (1).

За определяне оптималната степен s на полинома, описващ тенденцията на изследваното явление, е необходимо:

1.1. Да се изчислят оценките на коефициентите $\hat{C}_0, \hat{C}_1, \hat{C}_2, \dots$ и H_j за разглеждания брой години N.

1.2. Да се намерят стойностите на полиномите $Z_0(t), Z_1(t), Z_2(t), \dots, Z_n(t)$.

1.3. Да се изчисли сумата от квадратите на отклоненията S_n, представляваща обективна оценка на дисперсията относно изгладената крива.

За оптимална се приема тази степен s на полинома, при която стойността на дисперсията σ^2 практически престава да намалява.

Значенията на аргумента са с постоянна стъпка $h = 1$година и тежест $w = 1$, тъй като наблюденията на различни метеорологични станции са равноточни.

След заместване в [3]:

$$Z_0(t) = 1, Z_1(t) = t,$$

$$Z_{j+1}(t) = t\,Z_j(t) - \frac{H_j}{H_{j-1}} Z_{j-1}(t) \quad (j = 1, 2, \dots), \qquad (2)$$

отчитане на отношенията:

$$\mathrm{H_j} = \frac{(\mathrm{j!})^2(\mathrm{N+j})(\mathrm{N+j-1})\dots(\mathrm{N-j})}{4^{\mathrm{j}}[(2\mathrm{j-1})]^2(2\mathrm{j+1})}, \quad \frac{\mathrm{H_j}}{\mathrm{H_{j-1}}} = \frac{\mathrm{j}^2(\mathrm{N}^2-\mathrm{j}^2)}{4(2\mathrm{j-1})(2\mathrm{j+1})} \ (\mathrm{j} = 1,2,3, \dots) \quad (3)$$

и конкретните данни за разглежданото явление, се получават стойностите на полиномите на Чебишев $Z_0(t), Z_1(t), Z_2(t), \dots, Z_n(t)$ от $n-$ ти ред, дефиниран върху множеството $\{ t_1, t_2, \dots, t_N \}$.

Оценките на изгладените регресионни коефициенти $\hat{C}_0, \hat{C}_1, \hat{C}_2, \dots$ на полинома (1), се получават от формула [3]:

$$\hat{C}_j = \frac{1}{H_j} \sum_{i=1}^{N} v_i Z_j(t_i) \quad (j = 0, 1, \dots, s; s < N) \qquad (4)$$

при съответната стойност на N, където:

$$H_j = \sum_{i=1}^{N} Z_j^2(t_i),$$

v_i – брой екстремни събития (дни) в i-та година,

N – броя на разглежданите години,

а $t_i = \frac{x_k - \bar{x}}{h}$ приема само цели стойности $0, \pm 1, \pm 2, \dots, \pm(N-1)$ при нечетно N, или полуцели значения $0, \pm 1/2, \pm 2/2, \dots, \pm(N-1)/2$ при четно N, като тук $\bar{x} = \frac{1+2+\cdots+N}{N}$.

За изчисляване на дисперсията относно изгладената крива е необходимо да се намери сумата от квадратите на отклоненията S_n по формула [3]:

$$S_n = \sum_{i=1}^{N} w_i\, {v_i}^2 - (\hat{C}_0^2 H_0 + \hat{C}_1^2 H_1 + \cdots + \hat{C}_n^2 H_n). \qquad (5)$$

Отношението:

$$\frac{S_n}{N-s-1} = \frac{1}{N-s-1} \sum_{i=1}^{N} w_i [\, v_i - \sum_{j=0}^{s} \big(\hat{C}_j\big)_e Z(t_i)]^2 \qquad (6)$$

за обективна оценка на дисперсията σ^2.

Добавянето на всеки нов член $\hat{C}_{n+1}Z_{n+1}(t)$ в сумата (4) на ортогоналните полиноми $Z_j(t)$ намалява отклонението S_n с величината $\hat{C}_{n+1}^2 H_{n+1}$.

Всяко значение на S_n изчислено по (5) трябва да се раздели на числото $N-s-1$ и полученото отношение (6) да се сравни с предходното значение на това отношение. Трябва да се повишава степента на полинома (1) дотогава, докато отношението (6) престане чувствително да намалява. Това значение $n=s$, след което отношението (6) практически престава да намалява, дава оптималната степен на полинома [3].

Така търсения полином се записва във вида:

$$L(t) = \sum_{j=0}^{s} \hat{C}_j Z_j(t) = \hat{C}_0 Z_0(t) + \hat{C}_1 Z_1(t) + \ \ldots + \hat{C}_n Z_n(t) \quad (7)$$

Стъпка 2: Изчисляване на изгладените и екстраполираните стойности.

След заместване в [3]

$$\hat{L}(t_j) = \sum_{n=0}^{s} \hat{C}_n \hat{Y}_n(t_i) \quad (8)$$

могат да се изчислят изгладените стойности на изследваното екстремно явление. Аналогично екстраполираното значение на явлението X в момента t_e се намира по формулата:

$$x_{(m)e} = \hat{L}(t_e) = \sum_{n=0}^{s} \hat{C}_n \frac{Z_n(t_e)}{\sqrt{w_e}} \quad (9)$$

Стъпка 3: Извеждане на статистическия модел на екстремното явление.

Като се заместят получените значения във формула (7) и се разкрият скобите се получава търсеният полином.

След направените изчисления и преобразувания може да се запише в окончателен вид статистическият модел за оценяване честотата на изследваното явление, представен чрез полиномите за Чебишев и да се представи в графичен вид.

Заключение

Използването на ортогонални полиноми на Чебишев (1) за оценка честотата на природните бедствия в сравнение с класическия метод има следните предимства:

1) статистическите оценки на коефициентите $\hat{C}_n$ в (1) се получават направо от резултатите на измерванията;

2) тъй като грешките на последователните измервания на честотата на природните бедствия с интервал на отчитане 24 часа са независими, то в този случай и оценките на коефициентите $\hat{C}_n$ в (1) са независими в съвкупност;

3) ако се окаже, че при използването на сума от полиноми от ред $s-$ ти точността на изглаждане не е достатъчна, е необходимо само да се изчислят значенията на полинома $Z_{s+1}(t_i),\ i = 1,2,\dots,N$ и коефициента $\hat{C}_{s+1}$ (оценка на C_{s+1}). Последното предимство опростява значително много разработването на модели на екстремни климатични явления.

Въпреки своите важни положителни свойства, изглаждането с помощта на ортогонални полиноми за сега не е намерило широко приложение при оценяване честотата на природните бедствия, защото коефициентите $\hat{C}_n$ нямат физически смисъл на скорост, ускорение и т.н. По тези причини досега те са използвани за решаване на тесен кръг задачи и теорията им не е напълно разработена. В настоящия доклад е показано, че поради еднозначно обратимо съответствие между алгебричните полиноми $L_L(t) = \sum_{n=0}^{s} \frac{b_n}{n!}$ и (1) преходът от коефициентите $\hat{C}_n$ към скорост, ускорение и т.н. не представлява никаква трудност.

Неудобствата, които произтичат от малко нетрадиционната форма многократно се компенсират от ускоряването и опростяването на изчислителните процедури при разработването на екстремни природни явления.

ЛИТЕРАТУРА:

[1] Национална програма за защита при бедствия 2014 - 2018
[2] Стратегия за намаляване на риска от бедствия 2014-2020
[3] Рушимский Л.З., Математическая обработка результатов эксперимента, Москва 1971
[4] www.nsi.bg
[5] http://bsdi.asde-bg.org/floods.php#Map

МОДЕЛ ЗА ЧЕСТОТАТА НА ЕКСТРЕМНИ ТЕМПЕРАТУРИ

Доника В. Диманова, Христо Л. Лалев

MODEL ABOUT THE FREQUENCY OF EXTREME TEMPERATURES

Donika V. Dimanova, Hristo L. Lalev

ABSTRACT: *As climate change is real and we cannot stop the anomalies in temperature, rainfall and sea level rise, a global challenge is to enable the responsible authorities to manage climate risks when necessary. Climate change is a long process. While short-term changes may be less extreme than anticipated changes in the next 100 to 200 years, and the risks can be significantly different from today. Flexibility is therefore necessary to adapt to the risks associated with climatic extremes and the formulation of strategies for dealing with them.*

KEYWORDS: *climate change, statistical model, extreme temperatures.*

Въведение

През последните години температурите отбелязват рекордни нива. Несъмнено планетата търпи затопляне през последния половин век. Освен това всяко десетилетие на Земята от 1980г. насам е по – горещо от предходното [8, 9]. Един от основните изводи в аналитичният доклад на британския икономист Никалъс Стърн [7], публикуван през октомври 2006 г. е, че бездействието спрямо климатичните промени би струвало на човечеството 5% от световния брутен вътрешен продукт годишно, като акумулираните вреди може да наложат разходи в размер на 20% от глобалния БВП. В сравнение с това, предприемането на действия за намаляване и смекчаване на последствията от глобалното затопляне се оценява на 1% от световния БВП.

Глобалните проблеми свързани с климатичните промени и екстремните температури с особена актуалност засягат и нашата страна. В тази връзка целите на доклада са:

3. Да се изследва тенденцията за увеличаване на екстремно ниските и екстремно високите температури в България.

4. Да се обосноват мерки за подобряване на работата на държавните органи, ангажирани с предотвратяване и намаляване риска от екстремни температури.

Хипотеза се обосновава чрез разработване на модел за оценяване честотата на екстремните температури.

Изложение

Докладът е структуриран по следния начин:

4. Изследва се тенденцията и причините за увеличаване на екстремните температури в България.

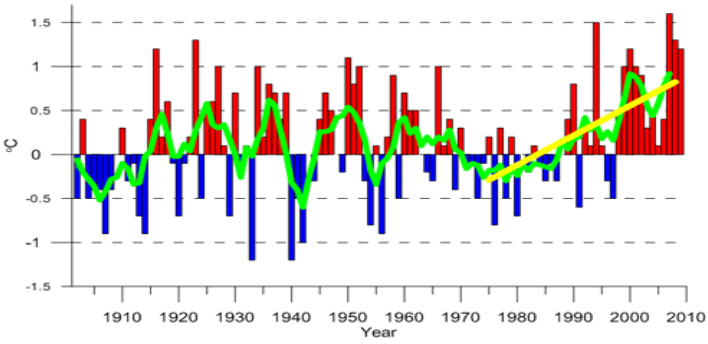
5. Приема се хипотезата, че предприеманите дейности за намаляване риска от екстремни температури не са достатъчни и е нужна политика на цялостно управление на риска.

6. Описва се модел за синтез на честотата на екстремни климатични явления със сума от ортогонални полиноми на Чебишев.

Според Кристалина Георгиева, европейски комисар по международно сътрудничество, хуманитарна помощ и реакции при кризи, най-големият риск пред света и пред Европа днес са климатичните изменения. „ … защото те са вече реалност и за съжаление природните системи не са линейни системи. Ние вече виждаме по – чести наводнения, горски пожари в Европа, по света – урагани и бедствия, които надминават въображението... В този свят на климатични изменения ние имаме задължението първо да се опитаме да намалим рисковете, да намалим причината и второ, да се адаптираме към тях. Защото, ако не направим това днес, ще платим много висока цена утре“ [2].

Промените в климата може да доведат до по – чести и по – силни бури и градушки, наводнения, свлачища, пожари, снегонавявания, дълготрайни засушавания и екстремни температури. Те всъщност са в резултат на опасни метеорологични явления. Като опасни могат да се

определят тези явления, които предизвикат финансови щети и застрашат здравето и живота на хората. Според Световната метеорологична организация (СМО) опасни явления са всички атмосферни условия, които са потенциално разрушителни или рискови за хората. Прогнозирането на опасните явления и условията за тяхното формиране изискват развитието на модели за предвиждане на тяхното местоположение и честота. Това е жизнено важно, тъй като предварително могат да бъдат известни засегнатите области и по този начин да се избегнат човешки жертви.



Фиг.1: Аномалии на температурата на въздуха в България спрямо периода 1961 – 1990,°C

На фигура 1 са представени аномалиите на температурата на въздуха в България спрямо периода 1961 – 1990г., °C, по данни от НИМХ към БАН [4]. В червено са отбелязани положителни аномалии на средната годишна температура спрямо климатичната норма на периода 1961 – 1990г. В синьо – отрицателни аномалии на средната годишна температура спрямо климатичната норма на периода 1961 – 1990г. В зелено – вариациите в аномалиите на средната годишна температура, а в жълто – линейния тренд в аномалиите на средната годишна температура за периода 1971 – 2010 г.

Екстремните температури [5] са от една страна аномално ниски температури в пролетния, есенния и зимния период – студове, от друга – аномално високи температури през лятото – горещини. Те затрудняват

ежедневната дейност на човека, но и причиняват различни аварии и кризисни ситуации. Степента на отрицателното им въздействие зависи от останалите метеорологични характеристики – влажността на въздуха, скоростта на вятъра и други. През последните години се наблюдават необичайни явления като високи температури в зимния период и сравнително ниски температури през лятото.

Екстремните горещини могат да вземат човешки жертви и да са предпоставка за възникването на горски пожари и значителни засушавания. Екстремно ниските температури може да причинят заледявания и обледявания, в резултат на което да предизвикат сериозни щети на енергопреносната мрежа. В критични ситуации могат да изпаднат и редица производства.

Една от основните задачи на Националният институт по метеорология и хидрология (НИМХ) при БАН е информационна защита на обществото. На сайта на института се предлага най – актуална информация за потенциално опасни метеорологични явления в реално време и за близко бъдеще на територията на страната, последни спътникови и радарни снимки, измервания на температурата, налягането, валежите както и информация за облачността. Опасните явления са разграничени в четири цветови кода – зелен, жълт, оранжев и червен, в зависимост от опасността на проявлението им [10, 11].

На база характеристиките на цветовите кодове за опасни явления, данните за района на Шумен [12] в периода 1990 – 2013 за настъпили екстремно ниски и екстремно високи температури са обобщени в таблица 1.

Таблица 1

година	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001
бр.опасни температури	27	39	53	72	33	62	50	50	54	38	63	56
година	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
бр.опасни температури	37	84	52	47	63	43	60	45	56	57	86	38

От данните в таблици 1 и чрез Алгоритъма за оценяване честотата на природните бедствия [1] може да се изведе модел за честотата на опасно екстремните температури. За да се направи анализа

се приема хипотезата, че броя на екстремните температури за една година се описва със сума от ортогонални полиноми на Чебишев от вида [6]:

$$L(t) = \sum_{j=0}^{s} \hat{C}_n . Z_n(t). \qquad (1)$$

Модел за честотата на опасно екстремни температури

Модел 1: Прави се изследване на опасни температури на територията на област Шумен за периода 1991г. – 2013г. и тенденцията на развитие за следващите пет години. Използват се данните в таблица 1 и алгоритъма за оценяване честотата на природните бедствия [1]. Значенията на аргумента са с постоянна стъпка $h = 1$ година и тежест $w = 1$, тъй като наблюденията на различни метеорологични станции са равноточни.

За полиномите на Чебишев $Z_0(t), Z_1(t), Z_2(t), \dots, Z_n(t)$ от n – ти ред, дефиниран върху множеството $\{ t_1, t_2, \dots, t_N \}$ се получава следната система [1, 6]:

$$Z_o(t) = 1;$$

$$Z_1(t) = t^1;$$

$$Z_2(t) = t\, Z_1(t) - \frac{H_1}{H_0} Z_1(t) = t^2 - 44;$$

$$Z_3(t) = t\, Z_2(t) - \frac{H_2}{H_1} Z_2(t) = t^3 - 79\, t;$$

$$Z_4(t) = t\, Z_3(t) - \frac{H_3}{H_2} Z_3(t) = t^4 - 112.43\, t + 1470.92; \quad (2)$$

$$Z_5(t) = t\, Z_4(t) - \frac{H_4}{H_3} Z_4(t) = t^5 + 145\, t^3 + 4043.95\, t\ ;$$

$$Z_6(t) = t\, Z_5(t) - \frac{H_5}{H_4} Z_5(t) = t^6 - 176.82\, t^4 + 7621.47\, t^2 - 46804.67;$$

$$Z_7(t) = t\, Z_6(t) - \frac{H_6}{H_5} Z_6(t) = t^7 - 207.85 t^5 + 11852.57 t^3 + 164807.13 t;$$

като отношенията [6]:

$$\mathrm{H_j} = \frac{(\mathrm{j!})^2(\mathrm{N+j})(\mathrm{N+j-1})\ldots(\mathrm{N-j})}{4^{\mathrm{j}}[(2\mathrm{j-1})]^2(2\mathrm{j+1})}, \frac{\mathrm{H_j}}{\mathrm{H_{j-1}}} = \frac{\mathrm{j}^2(\mathrm{N}^2-\mathrm{j}^2)}{4(2\mathrm{j-1})(2\mathrm{j+1})} \qquad (3)$$

за $j = 1, 2, \ldots, s$; $N = 23, s < N$, имат следните стойности: $\frac{H_1}{H_0} = \frac{N^2-1}{12} = 44$; $\frac{H_2}{H_1} = \frac{N^2-4}{15} = 35$;

$\frac{H_3}{H_2} = \frac{(N^2-9)9}{140} = 33.43$; $\frac{H_4}{H_3} = \frac{(N^2-16)16}{252} = 32.57$; $\frac{H_5}{H_4} = \frac{(N^2-5^2)5^2}{396} = 31.82$; $\frac{H_6}{H_5} = \frac{(N^2-6^2)6^2}{572} = 31.03.$

Оценките на изгладените регресионни коефициенти $\hat{C}_0, \hat{C}_1, \hat{C}_2, \ldots$ на полинома (1), са дадени в таблица 2 и се получават от формула [6]:

$$\hat{C}_j = \frac{1}{H_j}\sum_{i=1}^{N} v_i Z_j(t_i) \quad (j = 0, 1, \ldots, s; s < N) \qquad (4)$$

при съответната стойност на N, където:

$H_j = \sum_{i=1}^{N} Z_j^2(t_i)$,

v_i – брой екстремни събития (дни) в i-та година,

N – броя на разглежданитегодини,

а $t_i = \frac{x_k - \bar{x}}{h}$ приема само цели стойности $0, \pm1, \pm2, \ldots, \pm(N-1)$ при нечетно N, или полуцели значения $0, \pm1/2, \pm2/2, \ldots, \pm(N-1)/2$ при четно N, като тук $\bar{x} = \frac{1+2+\cdots+N}{N}$.

Таблица 2:

Резултати от изчисленията на изгладените регресионни коефициенти с Модел 1

n	0	1	2	3	4	5	6	7
$\hat{C}_j$	53.8261	0.3389	−0.0097	0.0014	−0.0010	$8.46 * 10^{-6}$	$-1.419 * 10^{-4}$	$-1.31 * 10^{-5}$

В таблица 3 са обобщени изчисленията за опасно екстремни температури.

Таблица 3:

Резултати от изчисленията за опасно екстремни температури с Модел 1

t	v	$(v-\widehat{Co})^2$	Z_1	$v*Z_1$	Z_2	$v*Z_2$	Z_3	Z_4	Z_5	Z_6	Z_7
1	39	156.75	-11	-429	77	3003	-462	2 508.00	-12 540.00	58 140.00	-250 449.23
2	53	703.31	-10	-530	56	2968	-210	228.00	4 560.00	-52 854.55	387 057.90
3	72	2 072.07	-9	-648	37	2664	-18	-1 074.86	10 260.00	-58 140.00	204 913.01
4	33	42.51	-8	-264	20	660	120	-1 628.57	9 120.00	-21 141.82	-113 840.56
5	62	1 261.67	-7	-434	5	310	210	-1 637.14	4 620.00	19 750.91	-281 605.59
6	50	553.19	-6	-300	-8	-400	258	-1 280.57	- 720.00	45 065.45	-248 052.59
7	50	553.19	-5	-250	-19	-950	270	- 714.86	-5 220.00	48 845.45	-82 261.26
8	54	757.35	-4	-216	-28	-1512	252	- 72.00	-7 920.00	33 970.91	109 857.90
9	38	132.71	-3	-114	-35	-1330	210	540.00	-8 460.00	8 198.18	237 902.10
10	63	1 333.71	-2	-126	-40	-2520	150	1 037.14	-6 960.00	-19 080.00	254 114.69
11	56	871.43	-1	-56	-43	-2408	78	1 359.43	-3 900.00	-39 354.55	160 363.64
12	37	110.67	0	0	-44	-1628	0	1 470.86	0.00	-46 800.00	0.00
13	84	3 308.55	1	84	-43	-3612	-78	1 359.43	3 900.00	-39 354.55	-160 363.64
14	52	651.27	2	104	-40	-2080	-150	1 037.14	6 960.00	-19 080.00	-254 114.69
15	47	421.07	3	141	-35	-1645	-210	540.00	8 460.00	8 198.18	-237 902.10
16	63	1 333.71	4	252	-28	-1764	-252	- 72.00	7 920.00	33 970.91	-109 857.90
17	43	272.91	5	215	-19	-817	-270	- 714.86	5 220.00	48 845.45	82 261.26
18	60	1 123.59	6	360	-8	-480	-258	-1 280.57	720.00	45 065.45	248 052.59
19	45	342.99	7	315	5	225	-210	-1 637.14	-4 620.00	19 750.91	281 605.59
20	56	871.43	8	448	20	1120	-120	-1 628.57	-9 120.00	-21 141.82	113 840.56
21	57	931.47	9	513	37	2109	18	-1 074.86	-10 260.00	-58 140.00	-204 913.01
22	86	3 542.63	10	860	56	4816	210	228.00	-4 560.00	-52 854.55	-387 057.90
23	38	132.71	11	418	77	2926	462	2 508.00	12 540.00	58 140.00	250 449.23
S_n	**1238**	**4281.3**	-	**343**	-	**-142**	-	-	-	-	-
H	-	-	**1020**	-	**35420**	-	**1184040**	**11.0188*10^6**	**1227.096*10^6**	**3.4001*10^{16}**	**1.2433*10^{20}**

За изчисляване на дисперсията относно изгладената крива е необходимо да се намери сумата от квадратите на отклоненията S_n по формула [6]:

$$S_n = \sum_{i=1}^{N} w_i \, v_i{}^2 - (\hat{C}_0^2 H_0 + \hat{C}_1^2 H_1 + \cdots + \hat{C}_n^2 H_n). \qquad (5)$$

и отношението:

$$\frac{S_n}{N-s-1} = \frac{1}{N-s-1} \sum_{i=1}^{N} w_i [\, v_i - \sum_{j=0}^{s} (\hat{C}_j)_e Z(t_i)]^2 \qquad (6)$$

за обективна оценка на дисперсията σ^2.

Стойностите на дисперсията σ^2 за различните степени са дадени в таблица 4.

$$\sigma^2 \approx \frac{S_0}{N-1} \approx \frac{S_1}{N-2} \approx \frac{S_2}{N-3} \approx \frac{S_3}{N-4} \approx \frac{S_4}{N-5} \approx \frac{S_5}{N-6} \approx \frac{S_6}{N-7} \approx \frac{S_7}{N-8}$$

Таблица 4:

Резултати от изчисленията на дисперсията при различните степени на полинома

n	0	1	2	3	4	5	6	7
σ^2	194.60	179.09	177.94	176.85	174.06	173.05	138.72	129.16
$\Delta\sigma_n^2$ $-\Delta\sigma_{n+1}^2$	-	15.51	1.15	1.09	2.79	1.01	34.33	9.56

От таблица 4 се вижда, че σ^2 практически престава да намалява при $n_0 = 3$:

$$1.15 = \frac{S_2}{N-2-1} \approx \frac{S_3}{N-3-1} = 1.09$$

и $n_0 = 3$ може да се приеме за оптимална степен на полинома (2.18).

Но преди да се запише емпиричната формула в окончателен вид е желателно да се оценят грешките в определянето на коефициентите $\hat{C}_j$ и да се закръглят намерените значения на параметрите като се вземат предвид тези грешки. Грешките η_k в измерените значения на функциите v_k предизвикват грешки β_j при определяне на коефициентите $\hat{C}_j$. Грешките β_j ще са независими и ще бъдат разпределени нормално с център 0 и дисперсии $\frac{\sigma^2}{H_j}$ $(j = 0, 1, \ldots, n)$.

В разглеждания модел дисперсията σ^2 на резултатите от измерванията се оценява с величината $\sigma^2 \approx \frac{S_3}{19} = 176.85$. Затова

средноквадратичните грешки при определяне регресионните коефициенти $\hat{C}_0, \hat{C}_1, \hat{C}_2,$ и $\hat{C}_3$ се оценяват съответно с величините:

$\sigma(\hat{C}_0) = \sqrt{\frac{\sigma^2}{23}} \approx 7.6891$; $\sigma(\hat{C}_1) = \sqrt{\frac{\sigma^2}{1020}} \approx 0.1734; \sigma(\hat{C}_2) = \sqrt{\frac{\sigma^2}{35420}} \approx 0.0050$; $\sigma(\hat{C}_3) = \sqrt{\frac{\sigma^2}{1184040}} \approx 1.49 * 10^{-4}$

Намерените по – горе значения на коефициентите $\hat{C}_j$ се закръглят, като се съобразява броя цифри след десетичната запетая на грешките. След заместване в [6]:

$$\hat{L}(t_j) = \sum_{n=0}^{s} \hat{C}_n \hat{Y}_n(t_i), \quad (7)$$

могат да се изчислят изгладените стойности на изследваното екстремно явление.

Аналогично екстраполираното значение на явлението X в момента t_e се намира по формула:

$$x_{(m)e} = \hat{L}(t_e) = \sum_{n=0}^{s} \hat{C}_n \frac{Z_n(t_e)}{\sqrt{w_e}} \quad (8)$$

Като се заместят получените значения във формула (1) и се разкрият скобите се получава търсеният полином. Следователно моделът на изменение на дните с опасно екстремни температури на територията на област Шумен чрез полиномите за Чебишев за период от 23 години има следния вид:

$$\hat{L}(t_j) = \hat{C}_0 Z_0(t_1) + \hat{C}_1 Z_1(t_2) + \cdots + \hat{C}_n Z_n(t_n) = \hat{C}_0 + \hat{C}_1 t + \hat{C}_2(t^2 - 44) + + \hat{C}_3(t^3 - 79\, t) = 54.2529 + 0.2283t - 0.0097t^2 + 0.0014t^3$$

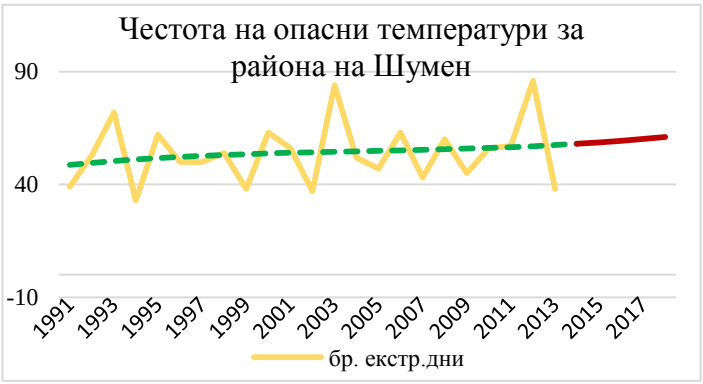
Изчислените стойности на $\hat{L}(t_j)$ за всяка от изследваните години и екстраполираните стойности за следващите пет години са показани в таблица 5.

Таблица 5:

Резултати от изчислени и екстраполирани стойности на честотата на опасни температури с Модел 1

година	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**
Бр. екстр.дни	39	53	72	33	62	50	50	54	38	63	56	37	84	52
$\hat{L}(t)$; s=3	48.71	49.60	50.39	51.08	51.69	52.22	52.69	53.09	53.44	53.74	54.01	54.25	54.48	54.69
година	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Бр. екстр.дни	47	63	43	60	45	56	57	86	38					
$\hat{L}(t)$; s=3	54.90	55.11	55.34	55.58	55.86	56.18	56.54	56.96	57.44	**57.99**	**58.62**	**59.34**	**60.15**	**61.07**

Следователно статистическият модел на опасно екстремни температури на територията на област Шумен, с отчетена тенденция за следващите пет години има визуализацията от фигура 2. От фигурата и изчисленията на модела в таблица 5 е видно, че тенденцията на дните с опасно екстремните температури е към повишаване.



Фиг. 2: Модел за честотата на опасно екстремните температури за периода 1991 – 2013

Модел 2: Прави се изследване на опасни температури на територията на област Шумен за периода 1991г. – 2013г. и тенденцията

на развитие за следващите пет години. Използват се данните в таблица 1, като за оптимална степен на полинома се избира $n_0 = 4$.

След направени преобразувания, моделът на изменение на дните с опасни температури на територията на област Шумен чрез полиноми за Чебишев за период от 23 години има следния вид :

$$\hat{L}(t_j) = \sum_{j=0}^{4} \hat{C}_j Z_j(t) = \hat{C}_0 + \hat{C}_1 t + \hat{C}_2(t^2 - 44) + \hat{C}_3(t^3 - 79\,t) + \hat{C}_4(t^4 - 112.43\,t^2 + 1470.92) = 51.9284 + +0.2283t - 0.1027t^2 + 0.0014t^3 - 0.0010t^4$$

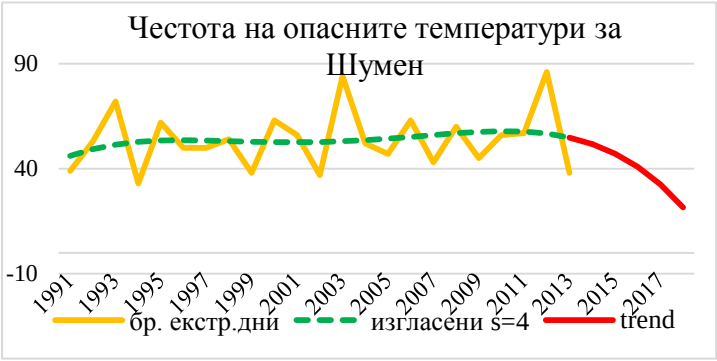
(10)

Изчислените стойности на $\hat{L}(t_j)$ за всяка от изследваните години и екстраполираните стойности за следващите пет години са показани в таблица 6.

Таблица 6:

Резултати от изчислени и екстраполирани стойности на честотата на опасни температури с Модел 2

Години (t)	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**
бр.дни с опасни темп.	39	53	72	33	62	50	50	54	38	63	56	37	84	52
$\hat{L}(t_j)$,s=4	46.12	49.37	51.50	52.77	53.38	53.55	53.43	53.16	52.88	52.67	52.61	52.74	53.07	53.62
Години (t)	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
бр.дни с опасни темп.	47	63	43	49.62	45	56	57	86	38					
$\hat{L}(t_j)$,s=4	54.34	55.18	56.07	56.91	57.55	57.86	57.65	56.72	54.85	**51.78**	**47.23**	**40.91**	**32.48**	**21.60**



Фиг. 3: Модел на интензивността на опасно екстремните температури за периода 1990 – 2012

Следователно статистическият модел на опасни температури за територията на област Шумен с отчетена тенденция има вида от фигура 3. От фигурата илюстрираща модела с полином от четвърта степен, се вижда тенденция на намаляване броя на дните с опасни температури за една година.

Заключение:

Като цяло анализът на обоснованите в доклада статистически (фигура 2 и 3) за честотата на опасните температури се вижда, че в краткосрочен план има стабилизиране на дните с опасни температури и тенденцията е към намаляване.

Първият модел (модел 1, фигура 2), изразен с полином от трета степен на Чебишев, може да се приеме за песимистичен. При него се отчита тенденция на повишаване, въпреки че кривата на нарастване на дните с опасни температури е плавна.

Вторият модел (модел 2, фигура 3), изразен с полином от четвърта степен може да се приеме за оптимистичен. При него кривата на нарастване на дните с опасни температури е плавна и при изчисляване на тенденцията за следващите пет години се наблюдава намаляване на броят дни с опасни температури.

Както бе посочено в началото на доклада е необходима адаптация към рисковете свързани с климатични крайности. Адаптацията по същество представлява промяна на съществуващите практики за намаляване отрицателните въздействия от изменението на климата. Стратегиите свързани с изменението на климата трябва да се интегрират със стратегиите за управление на риска от бедствия. Чрез намаляване на уязвимостта в райони, застрашени от бедствия, хората ще бъдат по – добре адаптирани към изменението на климата и неговото въздействие. Важно е да се осигури навременна и ефективна защита на инфраструктура.

Ключовите области, които могат да бъдат засегнати от изменението на климата са: водните ресурси, екосистемите, селското стопанство, използването на земята и горското стопанство,

крайбрежието, човешкото здраве, инфраструктурата, икономиката, енергетиката, застрахователното дело, туризма, промишлеността и транспорта.

Поради това за преодоляването на извънредни ситуации от екстремни явления, са необходими действия на всички нива – държавно, регионално и местно [3]. Тези действия, включват широк кръг от превантивни, защитни, териториално устройствени, правно – административни, организационни и др. мерки. Превантивните и защитните дейности подробно са описани в Националната програма за защита при бедствия 2014 – 2018, Стратегията за намаляване на риска от бедствия 2014 – 2020, Закона за защита при бедствия и други нормативни документи.

ЛИТЕРАТУРА:

[1] Беджев Б., Диманова Д., Алгоритъм за оценяване честотата на природните бедствия чрез полином на Чебишев

[2] Георгиева К., изказване във ВА „Г.С.Раковски" при връчването ѝ на почетно звание „Доктор хонорис кауза"

[3] Димитров Д., Предизвикателства и перспективи пред някои елементи от националната сигурност на съвременния етап , НК на факултет „А, ПВО и КИС“ гр.Шумен 2013г

[4] Климатични промени, НИМХ - БАН, 2010

[5] Стратегия за намаляване на риска от бедствия 2014 – 2020

[6] Рушимский Л.З., Математическая обработка результатов эксперимента, Москва 1971-16

[7] Трети национален план за действие по изменение на климата за периода 2013-2020

[8] Changnon, Stanley A., The Climate Event of the Century. London, Oxford University Press, 2000

[9] Jones, Phil.Global Temperature Record, University of East Anglia

[10] http://www.weather.bg

[11] http://info.meteo.bg/opasni/

[12] http://www.stringmeteo.com

СОФТУЕРНА СИСТЕМА ЗА АВТОМАТИЗИРАНО СИНТЕЗИРАНЕ НА МОДЕЛИ ЗА ЧЕСТОТА НА ПРИРОДНИ БЕДСТВИЯ

Доника В. Диманова

SOFTWARE SYSTEM FOR AUTOMATED SYNTHESIS OF MODELS FOR THE FREQUENCY OF NATURAL DISASTERS

Donika V. Dimanova

ABSTRACT: *The basis for making scientifically based decisions in the management of crises caused by natural disasters is existence of a sufficiently reliable and precise forecasts for the development of the crisis. That is why in the world today are carried out intensive applied research aimed at the development of mathematical models of different types of crises. However, these problems are very complex and despite intensive work on them takes some common patterns can be specified for the geographical regions so as to maximize the accuracy of the forecasts for the development of crises.*

KEYWORDS: *software system, algorithm, model, disasters.*

Въведение

В предстоящите десетилетия се очаква промените в климата да доведат до нарастване на честотата и мащаба на природните бедствия. По-честите и по-силни бури и градушки, наводнения, свлачища, дълготрайни засушавания и екстремни температури, опустошителни горски пожари, могат да окажат значително вредно въздействие върху обществото [2], [3]. Поради това е необходима адаптация към рисковете свързани с климатични крайности и правилно идентифицираните и дефинирани рискови фактори и заплахи.

Увеличаването на различните по характер извънредни ситуации вследствие на природни бедствия на територията на страната, поставя все по-категорично въпросите за ефективността на прогнозирането и планирането на национално, институционално, областно и обектно ниво. В условията на развитие на бедствена ситуация, разглеждането на

всички възможни варианти е практически невъзможно. Това поражда необходимостта от използването на математически методи за анализ и синтез, което е предпоставка за вземане на оптимално решение и намаляване на риска [1].

В тази връзка целите на доклада са:

5. Да се състави универсална компютърна програма, работеща в средата на Матлаб, която осигурява използването на Алгоритъм за модел на честотата на природните бедствия.

Изложение

Докладът е структуриран по следния начин:

7. Разработена е софтуерна система за автоматизирано синтезиране на модели за честотата на поява на природни бедствия.

8. Съставена е блок-схема, описваща работата на универсалната компютърна програма, работеща в средата на Матлаб.

Намаляване риска от бедствия е не само национален, но и световен приоритет. Предвид актуалността на проблема, се разработват статистически модели на честотата на поява на природни бедствия, чието приложение в работата на националния и областните кризисни щабове може да доведе до повишаване положителния ефект при провежданите превантивни, спасително-неотложни и аварийно-възстановителни мероприятия. Като основен статистически метод за изследване на зависимости, при който факторните и резултативните променливи са количествени признаци се използва регресионният анализ. При него величината, която следва да бъде прогнозирана за бъдещ период от време, се представя с математическа функция на времето, наречена изглаждаща функция, чиито параметри се определят чрез точкови статистически оценки на базата на данни в минали моменти от време. Много често се избира изглаждащата функция да бъде полином от s – та степен. Удобно е да се използва ортогонален полином на Чебишев, т. к. процедурата по съгласуване на степента на полинома с емпиричните данни се осъществява много лесно [6]. При анализ с класическия метод, ако избраната степен на полинома не се съгласува с емпиричните данни, всички направени до момента изчисления трябва да бъдат повторени като се използва полином от по-

висока степен. Това е причината да се разглежда и анализира честотата на природните бедствия чрез ортогонални полиноми на Чебишев.

За улеснение на процеса при разработване на модел на честотата на природните бедствия, се използва специално разработен софтуер на системата. Както е известно Матлаб е програмна среда, която интегрира в себе си възможности за аналитични преобразувания, числени пресмятания и графично представяне на получените резултати. Ориентирана е към работа с масиви от данни - вектори, матрици, многомерни масиви, масиви от клетки и масиви от записи [5].

Алгоритъма се състои от универсална компютърна програма, работеща в средата на Матлаб, който осигурява практическото използване на модела на честотата на природните бедствия.

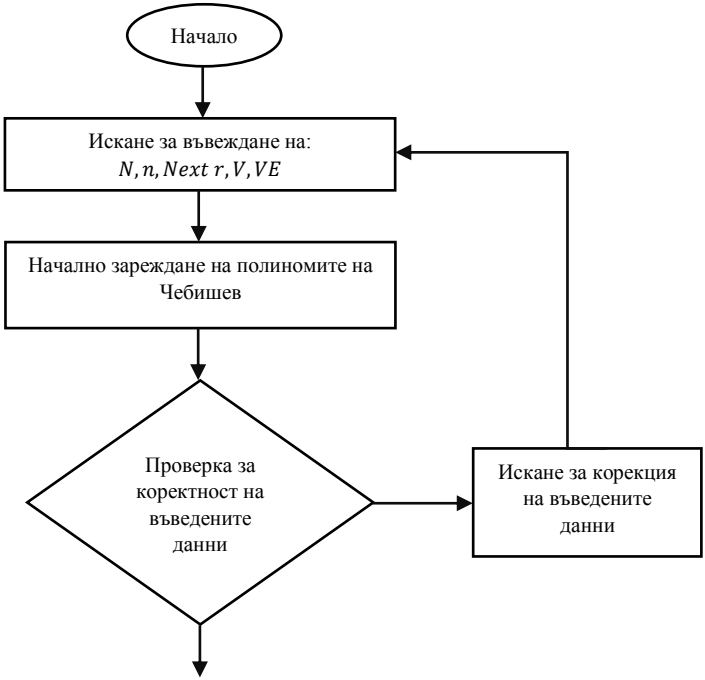
Работата на програмата се пояснява с блок-схемата от фигура 1 и може да се опише както следва.

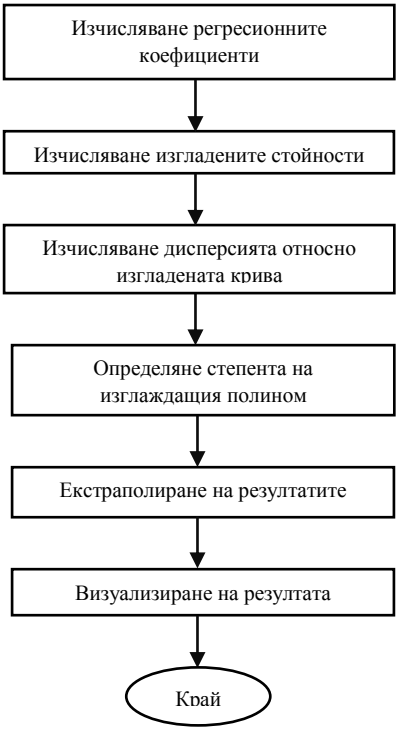
1) В началото на програмата се задават стойностите на параметрите:

- N – броя на изследваните години, които при изчисляване моделите в могат да бъдат стойности $N = 1, 2, \dots, m$;
- n – степента на полинома на Чебишев, която трябва да бъде просто число;
- $Next\ r$ – екстраполираните стойности. При изчисляване на моделите може да се изчисли тренда за следващите години, $Next\ r = 1, 2, \dots, m$;
- NE – общ броя на годините, като $NE = N + Next\ r$.

2) Следващата стъпка е въвеждане данните за изследваното явление:

- V – брой природни събития (дни) за всяка от разглежданите години, които приемат различни стойности в зависимост от изследваното природно явление;


Начало
Искане за въвеждане на:
$N, n, Next\ r, V, VE$
Начално зареждане на полиномите на Чебишев
Проверка за коректност на въведените данни
Искане за корекция на въведените данни



Фиг. 1: Блок-схема на универсална програма, реализираща алгоритъм за синтез на модел за честотата на природните бедствия

- VE – брой екстраполирани природни събития (дни) за всяка от разглежданите години, които приемат различни стойности в зависимост от изследваното природно явление и изчисленията;
- t_{sr} – средна стойност на разглежданите години с природни бедствия;
- t_{srex} – средна екстраполирана стойност на природните бедствия на разглеждания период;

t_{sr} и t_{srex} приема само цели стойности $0, \pm 1, \pm 2, \dots, \pm(N-1)$ при нечетно N, или полуцели значения $0, \pm 1/2, \pm 2/2, \dots, \pm(N-1)/2$ при четно N.

3) Следва зареждане полиномите на Чебишев [6]:

- $Z_0(t),\ Z_1(t),\ Z_2(t), \dots,\ Z_n(t)$ са полиноми на Чебишев.

Стойностите на ортогоналните полиноми на Чебишев с първи коефициент равен на единица се задават със следната рекурентна формула [6]:

$$Z_0(t) = 1,$$

$$Z_1(t) = t,$$

$$Z_{j+1}(t) = t\,Z_j(t) - \frac{H_j}{H_{j-1}} Z_{j-1}(t) \quad (j = 1, 2, \dots),$$

- А – отношения на коефициентите $\frac{H_j}{H_{j-1}}$, при изчисляване стойностите на полиномите, които се определят с формулата:

$$\mathrm{H_j} = \frac{(\mathrm{j!})^2(\mathrm{N+j})(\mathrm{N+j-1})\dots(\mathrm{N-j})}{4^{\mathrm{j}}[(2\mathrm{j}-1)]^2(2\mathrm{j}+1)}, \qquad \frac{\mathrm{H_j}}{\mathrm{H_{j-1}}} = \frac{\mathrm{j}^2(\mathrm{N}^2-\mathrm{j}^2)}{4(2\mathrm{j}-1)(2\mathrm{j}+1)} \quad (\mathrm{j} = 1,2,3,\dots) \tag{2}$$

4) Следва проверка за ортогоналност на полиномите на Чебишев. Ако полиномите са ортогонални два по два, тяхното векторно произведение е равно на нула. Ако изчислените стойности за полиномите не са нула или близки до нула, се прави корекция на въведените данни.

5) Изчисляване на регресионните коефициенти $\hat{C}_j$ при $j = 1,2,\dots,n$ – оценка на изгладените регресионни коефициенти се изчислява по [6]:

$$\hat{C}_j = \frac{1}{H_j}\sum_{i=1}^{N} v_i Z_j(t_i) \quad (j = 0, 1, \dots, n_0; n_0 < N) \tag{3}$$

6) Изчисляване изгладените стойности $Vizgl(I)$ на изследваното природно явление по [6]:

$$\hat{L}(t_j) = \sum_{n=0}^{s} \hat{C}_n\, \hat{Y}_n(t_i) \tag{4}$$

където: $\hat{C}_n = \frac{\sum_{i=1}^{m} v_i . Y_n(t) . w_i}{\sum_{i=1}^{m} Y_n^2(t_i)},\ n = 0,1,\dots,s$ и

$Y_n(t_i) = \frac{Z_n(t_i)}{\sqrt{w_i}}, n = 0, 1, \dots, s$ и $w_i = \frac{\sigma_0^2}{\sigma_i^2}$ е обобщение на полином

7) Изчисляване дисперсията относно изгладената крива $-Dis$. Дисперсията σ^2 служи за определяне оптималната степен на полинома. Трябва да се повишава степента на полинома до тогава, докато отношението:

$$\sigma^2 \approx \frac{S_{n_0}}{N-n_0-1} \approx \frac{S_{n_0+1}}{N-n_0-2} \approx \cdots \tag{5}$$

престане чувствително да намалява. Тук S_n е сумата от квадратите на отклоненията, представляваща обективна оценка на дисперсията относно изгладената крива и се изчислява по формула [6]:

$$S_n = \sum_{k=1}^{N} w_k \, v_k{}^2 - (\hat{C}_0^2 H_0 + \hat{C}_1^2 H_1 + \cdots + \hat{C}_n^2 H_n) \quad (6)$$

Това значение $n = n_0$, след което отношението (5) практически престава да намалява, дава оптималната степен на полинома.

8) Екстраполиране на резултатите [6]:

• $VizglE(I)$ – екстраполирано значение на явлението X в момента t_{e} и се намира по:

$$\hat{L}(t_e) = \sum_{n=0}^{r} \hat{C}_n \frac{Z_n(t_e)}{\sqrt{w_e}} \quad (7)$$

9) Визуализация на резултатите:

- изчертаване развитието на разглежданото явление;
- изчертаване на изгладената крива;
- изчертаване на екстраполираната крива;

Следва да се отбележи, че след като се определи оптималната степен на полинома, програмата се преработва за $n = n_0$ и се отчитат изгладените и екстраполираните стойности на изследваното природно явление. На тази база може да се изчисли и визуализира търсения полином.

Заключение

С навлизането на по-нови технологии, при по-широкото използване на спътникова информация и съвременни математични модели се правят по-достоверни сезонни прогнози. В света съществуват над 20 центрове, които се занимават с моделиране на глобалния и регионалния климат.

В тази връзка все повече се обръща внимание на разработените програми под ръководството на ЕС и Европейската космическа агенция, свързани с наблюдение на Земята (ESA), географските информационните системи (ГИС), глобалната позиционираща система (GPS) и дистанционното сондиране, унификацията на базите от данни, методиките и др. Страните от ЕС все повече си сътрудничат в областта на сигурността, като си предоставят информация, свързана с рискове от кризи и подпомагат спасителните действия при възникнали природни бедствия [2], [3], [4].

Въпреки това, практиката показва определена неподготвеност в България за посрещане на по-големи природни бедствия и аварии. Причините най-вероятно са в:

- ограничените и разпръснати данни за бедствията;
- недостатъчната информираност на населението относно дейностите по намаляване риска от бедствия, както и реакциите им при възникнало бедствие;
- координацията между отговорните институции на национално, областно, общинско и обектно ниво;
- дългосрочното планиране на управлението на риска при бедствия.

Затова е необходима цялостна политика за управление на риска от възникване на природни бедствия.

ЛИТЕРАТУРА:

[1] Атанасов Б., Количествени методи в управлението на бизнеса, кн.1, Варна 1994г.
[2] Национална програма за защита при бедствия 2014 - 2018
[3] Стратегия за намаляване на риска от бедствия 2014-2020
[4] Христов Х., Подходи за идентифициране на източниците на заплаха на организацията", НК –„Наука, образование, иновации", Шумен, 2014
[5] Дьяконов В., Круглов В., Матлаб. Анализ, идентификация и моделирование систем, Санкт Петербург 2002
[6] Рушимский Л.З., Математическая обработка результатов эксперимента, Москва 1971

ФИРМЕНОТО КОНТРАРАЗУЗНАВАНЕ В ДЕЙСТВИЕ

ХРИСТО А. ХРИСТОВ

COMPANY SECURITY SERVICE IN ACTION

HRISTO A. HRISTOV

ABSTRACT: *Encroachments on company security are possible through usage of conspiratorial ways and means and methods. With the purpose to counteract against them successfully, the counteracting itself must be materialized by usage of similar identical ways and means and methods, which are counter-intelligence, by nature. In connection to this, the present report is going to examine the practiced counter-intelligence by business organizations' security services.*

KEYWORDS: *company security system, turbulence, security environment, management, business organization, protection, in- and outside factors, encroachments, counteraction.*

Посегателствата срещу фирмената сигурност се извършват с използване на конспиративни средства и методи. За да бъде успешно противодействието, то трябва да се извършва с използването на идентични средства и методи, а те по своята същност са контраразузнавателни (оперативни). „В действителност службите за сигурност на бизнес организацията осъществяват контраразузнавателна дейност. Тя се изразява в „наблюдение, разкриване, предотвратяване и пресичане на замислени, подготвени или осъществявани посегателства срещу фирмената сигурност, подпомагане на наказателното и административно производство и превантивна дейност." [4].

„Оперативното разкриване представлява дейността на службите за фирмена сигурност по събирането, анализа и оценката на информация, която се отнася до извършващи се посегателства срещу сигурността на икономическия субект." [4]. Тази дейност изяснява кои организации, групи и лица извършват посегателства срещу фирмената сигурност и в какво конкретно се изразяват те. Така събраната и оценена информация може да се използва в няколко насоки:

- Да се информира фирменото ръководство за нея, като се посочат и причините и условията, които благоприятстват извършването на посегателства.

- Да се предприемат мерки за предотвратяване и пресичане на престъпления и нарушения, нанасящи вреди на сигурността на бизнес организацията.
- Да се предприемат мерки за подпомагане на бъдещото наказателно или административно производство.
- Да се предприемат допълнителни мерки за засилване на ефекта от превантивната дейност.

„В процеса на събирането на информация за посегателства срещу фирмената сигурност контраразунавателните служби анализират и отсяват информацията, даваща основание да се подозира или да се направи изводът, че се извършва конкретно посегателство срещу бизнес организацията. Тази информация се нарича оперативна информация." [8].

Най-често получаваната оперативна информация е описателна и се изразява в устно или писмено обяснение на участник или очевидец на дадено събитие. Освен това тя може да бъде материално фиксирана или пък да бъде във вид на следи. Носители на информация са също писма, счетоводни документи, договори, а също книги, списания, вестници. Средствата, чрез които се осъществяват престъпленията, също дават определена информация за престъпни посегателства.

Характерът на информацията подсказва какви могат да бъдат и нейните източници. Това са доверени лица, доброволни заявители, очевидци, участници. Това са писмени документи. Това са предмети и вещи, върху които са фиксирани следи от извършените престъпления или са носители на информация за тях.

Способите, които използва фирмената служба за сигурност, за да събира оперативна информация зависят основно от два фактора.

Първият е характерът на посегателството, т.е. дали то е престъпление, противозаконна дейност, административно нарушение или друга форма на посегателство. Когато става въпрос за евентуална престъпна дейност, много важно е да се определи видът на престъплението. Това ще определи до голяма степен и тактиката за получаване на информация за нея.

Вторият фактор е състоянието на силите и средствата, които ще се използват за разкриване на тази антифирмена дейност. Колкото по-големи са възможностите на фирмената служба за сигурност като щатен състав, сътруднически апарат, техническо оборудване, толкова по-големи ще бъдат и нейните възможности за прилагане на повече и по-разнообразни способи.

Контраразузнавателните органи на фирмата използват следните **способи** за разкриването на престъпления срещу фирмената сигурност**:**

Оперативен разпит – това е разговор, при който лице, което е участник или очевидец на престъпления, на противоправно деяние, на нарушение, се подбужда да съобщи съзнателно факти за тях. Лицето може да се е явило по собствено желание, а може и да бъде извикано на този разговор. Разпитът може да се проведе и извън служебните помещения на бизнес организацията.

Извършване на справки – за лице, което се подозира или има данни, че подготвя, извършва или е извършило престъпление, може да се извършват два вида справки:

Вземане на образци за сравнително изследване – това е дейност за получаване на материали, които да се използват за оперативно изследване от експерти специалисти. Такива образци могат да бъдат почеркът на дадено лице, негов запис върху аудионосител, фотография, дактилоскопни отпечатъци, коса, кръв. Могат да бъдат също и образци на писмени и печатни документи, на вещи и предмети, на оръжие и др. Или на образци за идентификация и възстановяване на родова принадлежност на трупове с неизяснена самоличност, на животни, вещи и предмети. Тези образци позволяват да се изясни дали са идентични на намиращите се или открити от контраразузнавателните органи оригинали.

Изследване на предмети и документи – това са предмети и документи, използвани като средство за извършване на престъплението. Или върху тях има следи от престъплението. Или изясняват обстоятелства, свързани с престъплението.

Разпознаване на лица и предмети, имащи отношение към престъпната дейност (идентифициране) – в практиката този способ се използва като допълващ момент на разпита. То е възможно, когато в хода на разпита даден очевидец или доброволен заявител сподели, че е видял лице или предмет, които имат отношение към престъплението.

Наблюдение – при него скрито се фиксират външните прояви на дадено лице по време, когато то е в движение на открито или в обществено достъпни помещения или се намира в закрити помещения, жилища, кабинети, хотелски стаи и др., с цел да се установяват негови престъпни действия, да се разкриват вещи, предмети и документи, използвани за извършване на посегателства, да се откриват връзки и съучастници, да се установява неговото местонахождение и т.н. Възможно е да се наблюдава и стационарен обект – сграда, автомобил, открита площадка, с цел да се изясни кои са посетителите, да се открие издирвано лице или да се изучи обстановката, с оглед осъществяване на дадено мероприятие.

Подслушване – при подслушването се засичат и документират (записват) разговори, проведени от контролираното лице устно или по телефона. Подслушването позволява да се разкриват планове и намерения за извършване на посегателства, да се установяват връзките на подслушваните лица, местонахождението на укривани материали, а също на укриващи се извършители на престъпления.

Събиране на информация от технически канали за комуникации – става въпрос преди всичко за фиксиране с технически средства на информацията, предавана или получавана чрез компютърната мрежа от лица, групи и организации, които се занимават с престъпна дейност. Това позволява да се получат факти и данни, свързани с тяхната престъпна дейност, с техни замисли и планове.

Секретен оглед – *ц*елта е да се открие местонахождението на материалните носители на тази информация и те да се фиксират с технически средства (фотоапарат, видеокамера) или да се опишат.

Белязване на обекти и предмети – използва се често за разкриване на кражби, когато има данни, че предстои да се извърши ново посегателство на пари, вещи и документи, при което те ще бъдат пипани от престъпника. Използва се също за белязване на пари с цел документиране на такива престъпления като подкуп, измама и др.

Оперативна беседа – тя може да се провежда законспирирано или открито.

Законспирираният разговор- провежда се от служители на звеното за фирмена сигурност, действащи под прикритие или от доверени лица на фирмената служба за сигурност. При него може да се разговаря както с очевидци, така и с извършители на посегателства.

Откритият разговор – провежда се от служители на фирменото контраразузнаване, които не крият своята принадлежност.

Събиране на информация „на тъмно” – това е разговор, при който участник или очевидец на посегателства се подбужда да сподели несъзнателно известни му факти за тях. Може да се провежда от представител на контраразузнавателното звено, от такъв действащ под прикритие или от доверено лице.

Оперативният експеримент – представлява способ за наблюдаване поведението на изучаваното лице, което е поставено в обстановка, изкуствено създадена от контраразузнавателните органи. При него фактически лицето се поставя в условия, които са възникнали с активната намеса на тези органи и без да се оказва въздействие върху него, се наблюдава каква ще бъде реакцията му.

Открити източници – при събирането на факти и данни за посегателства срещу фирмата, осъществявани от дадено лице, група и

организация, могат да се използват и открити източници като вестници, списания, книги, радио и телевизионни предавания, документални филми, статистически и други отчети, архиви на ведомства, официална служебна документация, бюлетини, справочници и пр.

Анализът на оперативната информация е важен етап в цялостната оперативна дейност. Той цели преди всичко да се даде отговор на въпроса дали изучаваното лице се занимава или не с престъпна или друга дейност, нарушаваща сигурността на икономическия субект.

Анализът на получената оперативна информация относно изучаваните прояви на дадено лице, група или организация се извършва от служители на контраразузнавателното звено. При всички случаи те трябва да използват общите методи на мисловната дейност, които позволяват да се получат нови знания [7] .

Формиране на изводи и издигане на версии – когато събраната информация за дейността на дадено лице, група или организация е анализирана и оценена, пред контраразузнавателните органи възниква задачата да формират и издигнат съответни изводи и версии.

Може да се направи категоричен извод, че обектът не извършва престъпна дейност. Друг извод може да бъде, че обектът е в процес на подготовка, опит или в момента извършва престъпна дейност. Или пък данните категорично да сочат, че той вече е извършил престъплението. Или че извършва посегателство, което не е престъпление.

Предотвратяване и пресичане на престъпления – в теорията на контраразузнаването тези две понятия може да се обобщят и с понятието „неутрализиране". „Предотвратяването и пресичането е вид оперативно-издирвателна дейност, при която с помощта на оперативни сили, средства и методи не се допуска извършването на отделни действия или продължаването на дейността от страна на дадено лице, група или организация, вършещи посегателства срещу фирмената сигурност".[1]

Когато тези оперативни мерки не дават възможност лицето да извършва отделни действия, става въпрос за предотвратяване. Когато обаче довеждат лицето до невъзможност да продължи престъпната си дейност, говорим за пресичане.

Някои от способите за предотвратяване и пресичане на престъпления са:

Склоняване към прекратяване на конкретното престъпление – при склоняването се оказва въздействие върху съзнанието и волята на обекта по такъв начин, че той да се откаже от своите престъпни

[1]Асенов, Б., Кипров, П., Теория на контраразузнаването, Труд, 2000, с.114.

замисли, планове и действия. То може да води лицето до отказване от извършване на конкретно действие или до окончателно прекратяване на неговата дейност.

Затрудняване действията на обекта – затрудняването е един от най-често ползваните методи за неутрализиране на престъпна дейност, извършвана от дадено лице, група или организация. При него пред обекта се създават пречки за осъществяване на неговите конкретни действия. Обикновено затрудняването води до неосъществяване на дадено действие, но не и до отказ от тази дейност.

Оперативната практика познава различни варианти на създаване на препятствия, които могат да се обобщят в следните основни групи:

- Лишаване от възможността да се получи достъп до обекта на действие.
- Създаване затруднение на обекта да се снабди с оръдия и средства за престъпна дейност.
- Недопускане конспиративното осъществяване на противоправни действия. Този метод се основава на факта, че този, който извършва такава дейност в повечето случаи прави това конспиративно, скрито, замаскирано. Когато този характер на неговата дейност е нарушен, той ще предпочете да се откаже от нея, за да не се разконспирира. Затрудняването е по-широко използван метод, защото може да се осъществява не само с оперативни сили и средства, но и да се използват и административни мерки за постигане на неговите цели (например засилване на охраната на дадена сграда).

Лишаване от оръдия за извършване на престъпления – за извършване на редица престъпни действия и постигане целите на престъплението понякога е необходимо използването на специални оръдия (средства). Те могат да бъдат оръжие, взривни материали, приспособления за отваряне на брави и каси и др. Когато се получи информация за подобни намерения, един от методите, който може да се използва за недопускане извършването на престъпление е да не се даде възможност на обекта да се снабди с това оръдие. Това ще се осъществи като се създадат затруднения за снабдяването му с тях. Ако обаче това не е направено или обектът е бил вече снабден с оръдието, пред службата се поставя въпросът за лишаването му от възможността да го ползва. Това може да стане по следните начини:

- Да се изземе оръдието.
- Да се повреди оръдието по начин, който ще стане известен на обекта.
- Да се приведе оръдието в негодно състояние, без това да се разбере от обекта. Вариантите за това са два. Първият е да се

извърши невидимо изменение в неговите свойства, което го прави неизползваемо. И вторият е да бъде заменено с друго, негодно оръдие, което външно да прилича на първото.

Отвличане върху негодна цел – при този метод вниманието на контролираното лице (лица) и неговите усилия за извършване на дадено действие се насочват към негодна цел. В обекта се създава впечатлението, че той е осъществил своя замисъл, но реално това не отговаря на действителността.

Компрометиране – това е способ, при който се цели да се пресече окончателно възможността на дадено лице да провежда престъпна дейност. Той е възможен тогава, когато това лице се намира в зависима връзка с ръководството на група или организация, към която то принадлежи и по чиито указания извършва тази дейност. Например участник в дадена престъпна организация действа съгласно указанията на нейното ръководство и спазва правилата, създадени в нея. Това поддържа и организационната връзка между него и намиращото се над него независимо звено.

При компрометирането тази организационна връзка между тях се нарушава чрез разбиване на доверието, което ръководното звено има към съответния член на организацията. За целта фирменото контраразузнаване събира и довежда до знанието на независимото звено компрометиращи данни, които трябва да го убедят, че по-нататък е невъзможно, опасно и противоречащо на неговите правила използването на това лице в тяхната дейност.

Разобличаване – в известен смисъл е близко до компрометирането, тъй като става въпрос също за разпространяване на данни и факти за дадено лице, които са компрометиращи за него. Но докато в първия случай тези данни се довеждат до знанието на неговите ръководители, то при разобличаването тези данни се разпространяват сред неговото обкръжение. И докато в първия случай се цели да се снеме доверието към него от страна на ръководителите му, то в този случай се цели той да изгуби своя авторитет и влияние сред своите връзки, които евентуално би използвал за осъществяването на престъпните си намерения. Тук се разчита на различията във възгледите на обекта на разобличаване и средата, сред която той действа.

Разлагане на групи и организации – използва се за неутрализиране на групи и организации. То се изразява в нарушаване на организационната връзка между участниците в групата и организацията. Известно е, че всяка група или организация обединява в себе си хора съмишленици или поне лица, преследващи еднакви цели. Това им дава възможност те да провеждат организирана дейност. Когато се наруши

тази организационна връзка, те не могат реално да осъществяват дейността, заради която са обединили своите сили.

Някои от най характерните открити способи за предотвратяване и пресичане на престъпления са:

Провеждане на превантивни индивидуални беседи - когато има данни, че дадено лице възнамерява да извърши посегателство или е започнало подготовка за това, с него може да се проведе беседа, с която да бъде предупредено за последствията от неговите действия.

Задържане – фактически в тези случаи ще се пресече окончателно престъпната дейност на лицето.

Проверки в помещения – фирменото контраразузнаване има право да извършва проверки в помещения на бизнес организацията, когато имат данни, че в тях предстои да се извърши или вече се извършва дадено посегателство или в тях се укрива лице, извършило престъпление. Целта на проверката е да се предотврати предстоящото или започнало посегателство или да се задържи престъпникът.

Използване на технически средства за явно наблюдение – при него се поставя визуална техника пред сгради и входове, в магазини и на други публични места. Тяхното поставяне и ползване се огласява. Този факт оказва възпиращо влияние върху лица, които имат намерение да извършат престъпления и нарушения.

Въвеждане на временни ограничения за извършване на дейности – това става със заповед на собственика на икономическия субект, когато има данни, че може да се извършат посегателства на определени места във фирмата, с цел да се предотврати тяхното извършване.

Подпомагане на наказателното и административно производство има за основна цел на всяка служба за фирмена сигурност е да разкрива, предотвратява и пресича посегателства срещу фирмената сигурност. Когато по оперативен път се установи, че това лице (лица) действително се е ангажирало с престъпна дейност и е консумирало състава на дадено престъпление, се поставя въпросът за откритото пресичане на тази му дейност чрез предприемане на наказателни мерки по отношение на него. Ако се установи, че то е извършило дейност, която не представлява престъпление, но е в нарушение на административни разпоредби, спрямо него могат да се предприемат административни или дисциплинарни мерки. В такива случаи пред фирменото контраразузнаване възникват две задачи. Първата е да уведоми писмено органите на досъдебното производство (прокурора) за подготовката, извършващото се или извършено престъпление и това да послужи като законен повод за започването на наказателното производство. Ако се касае за административни нарушения, трябва да се уведоми писмено

фирменото ръководство с цел да вземат административноправни и дисциплинарни мерки по отношение на лицето.

Цялата тази дейност, която се извършва в рамките на досъдебното и съдебното производство и която е обединена в т.нар. наказателно производство, цели да се пресече открито престъпната дейност, извършвана от дадено лице, което става чрез неговото осъждане и лишаване от възможностга да я продължи.

„Подпомагането на досъдебното и съдебно производство от службите за фирмена сигурност се изразява в издирване, установяване, фиксиране и съхраняване на фактически данни и предмети, свързани с престъплението, които могат да се използват като доказателства в наказателното производство или да съдействат за тяхното събиране и проверка.” [4].

Друга група оперативни данни са тези, с които се съдейства на органите на наказателното производство в събирането и проверката на доказателства. Фирмените служби за сигурност може да подпомагат тези органи в събирането и проверката на доказателства, които те извършват чрез разпит, експертиза, оглед, изземване, задържане и разпознаване на лица и предмети.

При подпомагане на наказателното и административно производство органите на фирмена сигурност трябва да спазват няколко важни изисквания:

- Строго спазване на закона за частната охранителна дейност и конкретно на Наказателно-процесуалния кодекс и на Закона за специалните разузнавателни средства.
- Органите на наказателното и административното производство са водещи при доказване на престъплението и нарушението. Фирмените служби за сигурност ги подпомагат в тази им дейност.
- Събирането на доказателствата за подпомагане на наказателното и административно производство да става чрез използването на онези способи, които ще имат най-ефективно въздействие върху техния ход.
- Използването на доверени лица като свидетели трябва да бъде само по изключение и при липса на други възможности, поради реалното нарушаване на конспиративния характер на отношенията с тях.

„Превантивната дейност представлява система от организационни, възпитателни, правни и оперативни мерки, осъществявани от органите на фирменото контраразузнаване за

недопускане извършването на посегателства срещу фирмената сигурност.” [4].

Органите на фирменото контраразунаване имат за основна задача да разкриват, предотвратяват и пресичат престъпления и да подпомагат наказателното и административно производство. Наред с това обаче те отделят важно място на премахването на причините и условията, които ги пораждат или играят благоприятна роля за тяхното извършване, на своевременното възпиране на лица от престъпни действия. Важността на тази задача оформя дейността на фирменото контраразузнаване по нейното осъществяване като отделен вид, наричан превенция.

Превантивната дейност се съобразява и подчинява на общите принципи и постановки, установени от науката за същността, формите, методите и организацията на превенцията. Сред тях може да се посочат законност, хуманизъм, публичност, комплексност, координираност, целенасоченост, системност.

Съществуват различни варианти за класифициране на превантивната дейност. Може да бъде обща, групова и индивидуална превенция. Съществува и разделението ѝ на първична, вторична и третична превенция. В зависимост от времето, когато се извършва индивидуалната превенция, тя може да бъде ранна, текуща и последваща.

Когато се говори за превантивна дейност на фирменото контраразузнаване, обикновено тя се представя като обща и частна. Основният критерий за това деление е насочеността на превантивните мерки, т.е. дали те се отнасят за целия състав, или за групи на бизнес организацията, или за отделни служители.

Превантивна дейност на общо равнище – има конкретен и целенасочен характер. Тук става въпрос за разкриване и премахване на причините и условията, които пораждат или благоприятстват извършването на посегателства в конкретния икономически обект.

Превантивната дейност на това равнище включва системата от възпитателни мерки към работещите в бизнес организацията, които се осъществяват от органите на фирмено контраразузнаване и целят да се създаде правилна позиция в личния състав на фирмата по отношение на проблемите на фирмената сигурност и да го направят активен участник в тяхната защита. Към тези мерки може да се включи и разпространяването на информация сред състава, разкриваща състоянието, тенденциите и общественоопасния характер на престъпленията срещу тях. Може да се разобличават конкретни прояви, представляващи посегателства на личността, на собствеността, на правата и свободите на гражданите, с оглед оказване въздействие върху

съзнанието на личния състав и засилване на неговата отговорност към тези проблеми.

Превантивна дейност на индивидуално равнище – се изразява в организирането и провеждането на беседи с лица, за които са получени данни, че замислят, подготвят или извършват престъпни действия. Целта на беседата е тези лица устно или писмено да бъдат предупредени да прекратят тези си прояви или да се откажат от своите замисли, за да не извършат посегателства срещу фирмената сигурност.

Практиката показва, че най-често обекти на такава профилактика са следните групи лица:

- Лица, които се включват в дейността на организации и групи, извършващи посегателства срещу фирмената сигурност.
- Лица, за които има достоверни данни, че възнамеряват, крият планове и са склонни към извършване на престъпление или друго действие, застрашаващо фирмената сигурност.
- Лица, които са започнали приготовления за извършване на дадено престъпление, ако тези приготовления не са обявени за престъпления.

При провеждането на индивидуални превантивни беседи могат да се използват два методаза оказване на въздействие върху дадено лице – убеждение и принуждение.

Убеждението е предпочитаният метод. При него на лицето се разяснява характера на постъпката, разкриват се неговите заблуди, осъждат се неговите възгледи и поведение, подчертава се отговорността и опасността от действията му и се предупреждава за последствията, ако продължи тази си дейност. Целта е да се окаже въздействие върху неговото съзнание и то само да се убеди, че е необходимо да прекрати общественоопасната си дейност.

Принуждението е метод, който се използва след като не са постигнати целите на убеждението. То се изразява в предприемане на административноправни мерки спрямо лицето по предложение на службата.

Индивидуалните превантивни беседи се извършват под две форми – *устна или писмена.*

При *устната форма* с лицето се провежда разговор, в който се предупреждава да не се ангажира по-нататък с действия, които може да прераснат в престъпления или нарушения на фирмената сигурност.

При *писменото предупреждение* се съставя протокол, с който лицето се предупреждава за отговорността, която ще носи при извършване на съответното престъпление или нарушение. В зависимост

от това кой провежда превантивната беседа тя може да бъде открита и засекретена.

Откритата форма представлява беседа от страна на представител на фирменото контраразузнаване, в рамките на която той убеждава и разобличава съответното лице за неговата дейност и го предупреждава за последствията. Служителят не крие своята принадлежност към контраразузнавателната структура на фирмата.

Засекретената форма на провеждане на беседа с дадено лице се предпочита при няколко фактора: стремеж да се прикрие оперативният интерес към лицето; получените данни за неговото поведение не могат да се легализират и има опасност от разкриване на източника им; откритата беседа може да има обратен ефект; лицето е връзка на обект; с оглед запазване авторитета на лицето; когато има оперативни възможности за такава беседа, и др. Тя може да се извърши от служител на контраразузнаването под прикритие, от доверено лице, което е съмишленик, приятел, роднина, колега на лицето. В тези случаи оказването на необходимото положително въздействие върху лицето може да се осъществи и чрез еднократна беседа, и чрез продължителни разговори.

Анализът на съдържанието на доклада позволява да бъдат изведени следните заключения:

- Противодействието на посегателства срещу бизнес организацията от службите за фирмена сигурност се осъществява чрез видовете контраразузнавателна дейност, изразяваща се в разкриване, предотвратяване и пресичане на замислени посегателства срещу фирмената сигурност, подпомагане на наказателното и административно производство и превантивна дейност.
- Като компонент на националната система за сигурност, бизнесът се нуждае от приемане на нормативна уредба, регламентираща функциите, целите, задачите и дейността на фирмените звена за сигурност, правните им възможности за ползването на средствата и методите на ОИД за защита на фирмената сигурност и взаимодействието със специализираните държавни институции.

ЛИТЕРАТУРА

1. Сандев, Г., Стратегии за сигурност на фирмата, Университетско издателство „Еп. Константин
Преславски", Шумен, 2005.
1. Василев, Ем., Фирмена сигурност, Труд, 2000. С.
2. Сандев, Г., Сигурност на организациите, Университетско издателство „Еп. Константин Преславски" Шумен., 2012, ISBN 978-954-577-621-2.
3. Асенов, Кипров, Теория на контраразузнаването, София, Труд, 2002.
4. Асенов, Б., Основи на оперативно- издирвателната дейност, ВСУ „Черноризец Храбър", ISBN 978-954-715-432-2, 2009.
5. Сандев, Г., Национална сигурност, Издателство „Фабер", 2008.
6. Начев, Й., Конкурентно разузнаване, Сиела, 2007.
7. Гетова, И, Дигиталната грамотност в новите информационно-образователни технологии, // Сборник / Информационна грамотност – модели за обучение и добри практики: Изд. „За буквите .- О`писменех", София, с. 243-247, 2012.
8. Boyanov, P. Analysis and assessment of several security vulnerability databases, THIRD INTERNATIONAL SCIENTIFIC CONFERENCE SCIENCE, EDUCATION, INNOVATION, DEDICATED TO THE 145TH ANNIVERSARY OF BULGARIAN ACADEMY OF SCIENCES AND TO THE 35TH ANNIVERSARY OF GEORGI IVANOV'S FLIGHTISSN, ISBN 978-954-577-969-5, vol. II, Shumen, Bulgaria, 21-23 May 2014, pp. 118-122

ПОДХОДИ СВЪРЗАНИ С ИЗСЛЕДВАНЕ СИГУРНОСТТА НА ОРГАНИЗАЦИЯТА - ФИРМАТА

Христо А. Христов

APPROACHES CONNECTED WITH STUDYING SECURITY OF ORGANIZATION – THE COMPANY

Hristo A. Hristov

ABSTRACT: *The security is becoming more and more main problem for each person and social organizations as well as main object of scientists' study researches. Security is one of the most frequently used polysemantic matter of speaking. Its public side is widely discussed and at the same time it is often covered with mysticism and secrecy. Because of this, getting a clear picture of security is an important prerequisite for correct rationalization of problems, strategy (conception) and system of company security. This term of matter is a question of present interest and also captivating because it concerns fundamental problems about surviving of business organizations.*

KEYWORDS: *security, social organization, business organization, company security, standards of security, levels of security, subjective and objective security, security as condition and process.*

В настоящият доклад са представени няколко възможни подхода и разбирания за обединяване на широките теоретични възгледи и перспективи, относно проблематиката на сигурността на организациите.

За всяка жива система е естествен стремежът към повече сигурност. Затова за В. Проданов: „Сигурността е характеристика на всяка система и тя е в нейната способност да се съхрани при промяна на средата, условията и обстоятелствата, от които зависи, да функционира и се развива оптимално, т.е. при най-малък разход на ресурси да осъществяват заложените в нея закономерности и цели"[1].

Арнолд Уолфърс различава „Субективна и обективна сигурност, като обективната сигурност се свързва с отсъствието на заплаха (за ценностите на системата), а субективната – с отсъствието на страх от заплаха (че тези ценности ще бъдат атакувани). За да има истинска сигурност, трябва да са налице и обективната, и субективната сигурност" [2].

Според Иля Пригожин: „В равновесието материята е сляпа, а извън равновесието, тя проглежда. В несигурността, за разлика от сигурността, винаги преобладава не статиката, а динамиката; нелинейността, а не линейността. Тя поражда импулси за действие, съпротивлява се срещу статуквото, срещу пряката и непреодолима връзка между причина и следствие" [3].

Като анализира сигурността Георги Стефанов пише: „Понятието „сигурност" има много широк обем и е многоаспектно. Така е, защото проблемът дали сигурността е налице, дали липсва или е недостатъчна, възниква всякога и навсякъде, където се съчетават условията: *с*състояние, представляващо ценност за субекта; неопределеност на бъдещето; връзка между тези два елемента, при която бъдещето на състоянието зависи от неопределеното развитие" [4].

В своята монография „Равнища на сигурност", Димитър Йончев разглежда „Сигурността като състояние на присъствие, при което е налице задоволителен контрол от страна на присъстващия над въздействията върху него" [5].

За Г. Сандев, „Понятието сигурност има многостранни измерения и означава увереност, положителност, липса на тревожност, безопасност и защитеност. Сигурността е понятие, с което се описва състоянието на обект, който контролира факторите на своето присъствие, т.е. не е възможна абсолютна и непрекъсната сигурност. Терминът, отнесен към личността, организацията и държавата, се разбира като безопасност и защитеност на тези субекти" [6].

Анализирайки сигурността, Георги Стефанов пише: "Сигурността е първостепенна ценност, която се стремят да постигнат или да запазят ръководителите на бизнес организациите" [4].

Н.Слатински свързва разкриването на същността, смисъла и съдържанието на категорията „Сигурност с четири условия"[7].

- Първо, това е разглеждането на свързаните с обекта явления и свойства в система. По този начин те няма да бъдат анализирани разпокъсано и хаотично.
- Второ, обектът трябва да бъде възприеман като процес. Така ще се изучава развитието му във времето, вместо само някакво негово моментно състояние.
- Трето, във всички действия, връзки и отношения, на които обектът е функция, в които той встъпва и които поражда, е нужно да се търси съдържащата се в тях логика.

- Четвърто, необходима е определена степен на абстракция, т.е известно отделяне на съществено от несъществено, откъсване от емпириката и конкретиката, с цел чрез аналогия и хомоморфизъм да се достигне до същността на явлението.

Сигурността, като аксиоматично, парадигмално понятие, е смисъла и стремежа в избора на поведение на една система и е главният движещ мотив, който придава целенасоченост и рационалност в съществуването, оцеляването и просперирането на системата и в реализирането на заложените в тази система мисия и цели. Сигурността може да се определи като мярата за това как системата, чрез своята сила, е защитила интересите си в конфликта. Логическата линия на разсъждения е следната: Различност ↔ Различни Интереси → Конфликт → Сила → Сигурност. Сигурността на системата е състояние, при което е гарантирано нейното съществуване и са надеждно защитени нейните жизненоважни интереси [7].

При изясняването на всички системни и структури подходи, приоритети и проблеми, свързани с управлението на сигурността, е необходимо да бъдат определяни и анализирани няколко изключително съществени неща: Първо, на кого трябва да бъде гарантирана сигурността (индивиди, организация, общество, държава, регион, алианс). Второ**,** какво трябва да се защитава (ценности, идентичност, ресурси, структури, идеи, социална тъкан на обществото, обществен ред, суверенитет, политически, напр. интеграционен, избор). Трето, от какво се защитаваме (риск, опасност, заплаха, посегателство). Четвърто, от кого се защитаваме (държави, организирани престъпни мрежи, различни бедствия, аварии, катастрофи и т.н.). Пето, кой определя заплахите и как определя заплахите, с какви приоритети, по какви методи и с какви процедури). Шесто, кои са най-ефективните мерки за въздействие и по какъв начин.

Една от класификациите на сигурността е свързана с потенциала на основните рискове и предизвикателства, заплахи и опасности, пред които е изправена системата и нейната способност да им противодейства. При тази класификация сигурността бива абсолютна безопасност, защитена безопасност, относителна сигурност и трансформационна сигурност.

При „абсолютната безопасност" става дума за напълно хипотетична, идеална ситуация, при която системата не е изложена на никакви въздействия.

При „защитената безопасност" съществуващите въздействия върху системата, макар реални и оказващи влияние върху нея, не са в състояние да се отразят съществено върху нейната сигурност.

При „относителната сигурност” се говори за въздействия, носещи в себе си потенциал за значително нарастване, но системата е в състояние да блокира това развитие или да го държи под контрол, така че критичната точка, след която тя напуска равновесното положение, да не бъде достигната.

При „трансформационната сигурност” се подразбира, че въздействията са над критичната точка за системата, но тя извършва определени структурни трансформации, с които усилва потенциала си и съумява да ги неутрализира и управлява успешно. Една фирма може да постигне подобна трансформация, като предприема извънредни усилия, нетипични за своето нормално функциониране, например като създаде звено за сигурност, приемане на стратегия за сигурност, увеличаване на бюджета за сигурност; създаване на нова нормативна уредба и сключване на договори с агенция за сигурност.

Анализираната от Н.Слатински „Схема на Трите вълни на сигурността успява адекватно да схване и опише т.нар. „времева протяжност” на съвременното схващане за сигурността” [7].

Първата вълна на сигурността е вълната на безопасността, при нея всички усилия на системата (държавата, корпорацията) са насочени към защита на безопасността, като се подчертае, че: -Безопасността е състояние; Безопасността се защитава; Целта е постигане на абсолютна (пълна) сигурност; Стратегията е ресурсно ориентирана.

Втората вълна на сигурността е вълната на сигурността**,** всички усилия на системата са насочени към гарантиране на сигурността, като се подчертае, че: -Сигурността е хибридно съчетаване на състояние и процес; Сигурността се гарантира; Целта е постигане на относителна (приемлива) сигурност; Стратегията е ресурсно ориентирана.

Третата вълна е вълната на риска. При вълната на риска терминът „риск” се разбира като въздействие на несигурността върху целите на системата, т.е. това са възможни, имащи голяма степен на неопределеност, събития или процеси, които могат да въздействат върху визията, мисията, стратегията и ресурсите на системата. Всички усилия на системата вече се насочват към управление на риска: -Общуването с риска е процес; Рискът се управлява (приема, избягва, споделя, ограничава); Целта е постигане на минимизирани рискове; Стратегията е целево ориентирана, т.е. базира се на целите, които системата се стреми да постигне.

Ако дадена система е в неравновесие или в такова неустойчиво равновесие, при което най-малкото въздействие върху нея може да я извади необратимо от него, логично не може да се говори за сигурност на тази система, по-скоро сигурността й достига своя минимум, а

несигурността й – своя максимум. Ако, обаче, системата е в устойчиво равновесие, така че при всяко въздействие тя, дори да се отклони от равновесното си положение, след кратки колебания отново се връща в него,.то тогава сигурността й е в своя максимум, а несигурността й – в своя минимум. В този смисъл сигурността е мярка за устойчивостта на равновесното положение на системата.

Ако разглеждаме бизнес организацията като система, то сигурността на системата е състояние, при което е гарантирано нейното съществуване и са надеждно защитени жизненоважните й интереси. Съществува ли заплаха за тези интереси, системата изпитва дефицит на сигурност, т.е. тя се намира в състояние на несигурност. За защита на жизненоважните интереси се жертват огромни ресурси. И така се постъпва винаги, когато само по този начин системата може да гарантира своето съществуване и развитие.

Разбирането на проблематиката на сигурността изисква познаване и прилагане както на дескриптивни, така и на теоретични подходи[8].

Дескриптивният подход на анализ предполага интегриране на картината на обстановката (ситуацията) и на възможните алтернативи на решения от различни документи, данни, факти, изследвания на обществено или експертно мнение и т.н. и поради това, той се реализира предимно чрез емпирични или индуктивни методи (извличане на теория от фактите).

Теоретичния подход, в същия контекст, се свързва с използване на компютърни модели и симулации или обикновени логико-математически методи на дедукция (т.е. на прогнозиране сбъдването на събития на основата на теория). На тази база се генерират изводи и се извличат тенденции.

Стратегическият подход представлява анализ и оценка на ситуациите и заплахите, прогнозиране, синтез на концептуален модел, изработка на варианти на целенасочени поведения (решения) и подпомагане избора на най-подходящ измежду тях.

Обект на стратегическия подход са ситуациите в реалния свят, съдържащи практически проблеми (текуща социална практика).

Предмет на стратегическия подход е разкриването на връзката между същността и съдържанието на тези ситуации, от една страна, и резултата от решаването (по определен начин с определени инструменти) на възникналите в тях проблеми, от друга страна.

Целта на стратегическия подход е откриването на условията, факторите и .механизмите, определящи успеха на начинанията и

гарантиращи постигането на ефективно организационно поведение (т.е. изработка на адекватни делови решения).

Системният подход се основава на принципите на общата теория на системите и динамиката им и е свързан със системния анализ и синтез. Прилагането му се регламентира от разбирането, че проблематиката на сигурността обхваща:

- социална система – тази на междуфирмените отношения;
- специфична за всяка бизнес организация (фирма) социална система;
- сложни социални процеси.

В съответствие с този подход, изследването на обект, какъвто е сигурността на бизнес организацията, трябва да отговаря на следните условия:

- Да се анализират, свързаните с обекта „фирмена сигурност", явления, структури и свойства в комплекс, а не разпокъсано и хаотично.
- Точно определяне на системообразуващите елементи на обекта „фирмена сигурност", както и връзките между тях.
- Обектът „фирмена сигурност" да се разглежда като процес, като се изучава развитието му във времето, вместо някакво негово моментно състояние.
- Във всички действия, връзки и отношения, на които обектът е функция, да се въведе определена степен на абстрактност, т.е. отделяне на съществено от несъществено, откъсване от емпиричното и конкретното, за да се хвърлят мостове към други области на познанието и да се използват идеи от тях.

Системните изследвания са съвкупност от научни и технически теории, концепции и методи, в които обекта на изследването или моделирането се разглежда както система.

Кръгът на значение на понятието „система" в гръцкия език е доста обширен: съчетание, организъм, устройство, организация, съюз, строй, ръководен орган.

Централна концепция в теорията на системите, системния анализ и цялата систематология е понятието система. Редица автори са анализирали това понятие и са развивали определението за система до определена степен на формализация.

Например Гиг дава кратко определение – „Системата е съвкупност или множество от свързани между себе си елементи"

[9]. Постепенно, като развива това понятие, той определя системата като съвкупност от живи и неживи елементи.

Акоф дефинира „Системата като множество от взаимосвързани елементи, всеки от които е свързан пряко или косвено с всеки друг елемент и две, какви да е, подмножества на това множество, не могат да бъдат независими”[10].

Понятието „система” е неразривно свързано с понятието „цел на системата”. Терминът „системен анализ” включва две понятия „система” и „анализ” и означава разбор по части, следователно „системния анализ” е разделяне на целите на системата на подцели и разделяне на системата на подсистеми със задачата – да се изясни какви са подсистемите и защо могат или не могат да изпълнят поставените пред тях цели. Следователно прилагането на „системния анализ” изисква разбиване на целите на системата на подцели (йерархия на целите) и разделяне на самата система на подсистеми (йерархия от системи), с намерение да се изясни какви подсистеми и защо могат (или не могат) да изпълняват поставените пред тях цели (подцели**).**

Определящи признаци на понятието „система” са нейните елементи, които се намират в определена взаимовръзка помежду си и са обединени за постигане на единна цел, т.е. елемента (материален, енергиен или информационен) е най-малката неделима функционална част от изследваната система.

На база на казаното дотук, в теорията на системите и системния анализ се определят някои основни принципи.

Като първи принцип се обособява цялостност на системата с нейните две страни: 1) свойствата на системата (цялото) не е сума от свойствата на елементите й; 2) свойствата на системата (цялото) зависи от свойствата на елементите й, като изменението в една част води до изменение в цялата система. Свойството цялостност е свързано с целта, за изпълнението на която е предназначена системата.

Вторият принцип е комуникативност. Този принцип стои в основата на определението за система и е подчинено на факта, че системата образува единство със средата. Всяка изследвана система е елемент от система от по-висок ранг, а елемент от изследваната система се явява система от по-нисък ранг, т.е

системата не е изолирана, тя е свързана с множество комуникации, както със средата, така и със собствените си елементи, което пък създава изисквания и ограничения за изследваната система. Основно съдържание на системния анализ е определянето на структурните, функционалните, информационните, пространствено-времеви връзки.

Третият основен принцип е свързан със свойството на системата „ефективност". Теоретично е доказано, че винаги съществува функция – ценност на системата, която зависи от нейната структура и функциониране. Процесът на изменение на състоянието на елемента (системата) се оценява по степента на постигане на целите, свързани с нейното функциониране.

Като четвърти принцип се определя управляемостта на системата. Всяка система съдържа елементи (системи) за управление, които контролират съответствието между резултата на действие на системата и поставената цел. Елементите изпълняват, или са длъжни да изпълняват, целта точно колкото е зададена отвън – нито повече, нито по-малко (не малко или много, а оптимално), по принципа: „необходимо и достатъчно". Елементите на управление следят за изпълнението на целта.

Следователно системата се характеризира с:

- цел (определя предназначението на системата);
- йерархия (определя взаимоотношенията между всички елементи на системата без изключение);
- изпълнителните елементи;
- блок на управлението (следи за правилното протичане на действията за достигане на целта).

Не на последно място е принципа изоморфизъм. Той се състои в наличие на еднозначно или частично съответствие на структурата на една система на структурата на друга, което дава възможност да се моделира една или друга система с помощта на подобна на нея система" [11]..

Методът на системния инженеринг в най-пълна степен удовлетворява изискванията за комплексност и дълбочина при изследване проблематиката на сигурността. Прилагането на системния анализ дава възможност да се осветяват и разглеждат различни свойства на тези системи, техни особености и канали на проявление в различни условия на обстановката. Така не само

анализаторите, а и лицата, вземащи решения, придобиват представа за мащабите на „цялото” и особеностите на „частното”. Системният синтез дава възможност да се изследва взаимодействието между елементите в различните организации, да се прогнозира тяхното поведение и да се предвиждат възможните резултати (ефекти) от използването на различни инструменти на политиката за сигурност в различни ситуации и за постигането на различни цели.

Интегрирайки базовите характеристики на формулираните подходи за анализ на проблематиката на сигурността, могат да се направят следните изводи:

- Сигурността е всеобща същност на всички форми на съществуване и проявление на материалния и духовния свят. Няма явление, процес, дейност, които да не съдържат като същностен и градивен елемент сигурността, която може да се отнесе към комплекса от категории като: пространство, време, движение, енергия.
- Сигурността изразява количествената и качествената определеност на всяка система, на нейното съществуване и развитие в съответствие със същността ѝ и собствените ѝ параметри. Това е обективен закон, чието подценяване или отричане закономерно води до хаос и разпадане на всяка система.
- Системата „сигурност” винаги е елемент на дадена природна и социална система. Извън, встрани и над природните и социалните системи няма и не може да има система за сигурност. Тя е техен градивен елемент и същностна функция, което дава основание да се разглежда, като относително самостоятелна система.
- Системата „сигурност” гарантира пълноценно, стабилно и възходящо функциониране и развитие на организацията, като своевременно открива и неутрализира всички възможни опасности и заплахи за нейната същност и съществуване.
- Сигурността като система, е в непрестанно движение, промяна и развитие, има начало, върхове, падения и свой край. Всичко това протича по силата на нейни специфични закономерности, произтичащи от особеностите на дадената обективна реалност.

За да бъде теоретичната конструкция на обекта (системата) „Фирмена сигурност” издържана от гледна точка на анализа и синтеза при изследването, е целесъобразно:

а) да се идентифицират детерминантите на сигурността на системите (организациите) и те да се корелират с архитектурата и

функциите на бизнес организациите. На тази база могат да се определят характеристиките на системата на фирмена сигурност:

- стратегически цели;
- обща и специализирана архитектура;
- основни функции.

б) взаимодействието на системата на фирмена сигурност със средата, с цел изграждане и поддържане на синергетиката и устойчивостта й, да се осъществи на базата на диагностициране на най-важните фактори, които могат да въздействат на бизнес организациите.

в) технологиите за генериране на сигурност да се формират на основата на управлението на екстремни (кризисни) ситуации, конфликти и изграждането и изпълнението на концепции за устойчиво развитие на различните бизнес организации.

На базата на казаното дотук, може да се приеме, че сигурност за една социална система (човек, организация, общност, общество, държава, общност от държави) има тогава, когато основните идеали, ценности, потребности и интереси на системата не са подложени на никакви въздействия (абсолютна безопасност) или незастрашени от съществуващи въздействия, които социалната система да не е в състояние ефективно да неутрализира (защитена безопасност), контролира (относителна сигурност) или управлява (трансформационна сигурност).

За гарантиране на сигурността истинското мениджърско предизвикателство е да се намери онова, изискващо възможно най-малък преразход на ресурси, състояние на устойчивост, в което бизнес организацията намира оптималния си баланс между несигурност и безопасност.

Литература:

1. Проданов, В. ”Вътрешна сигурност и националната държава”. Военен журнал, София, с.16.
2. Wolfers, Arnold. National Security as an Ambiguous Symbol. Political Science Quarterly, 1952, Vol. 67, No 4, p. 485.
3. Пригожин, Илья. Философия нестабильности.//Вопросы философии, 1991, № 6, с. 50.
4. Стефанов,Г.”Теория на международната сигурност”. Сиела, 2005.
5. Йончев, Д. Равнища на сигурност, С.: Нов български университет, 2008, с. 34.
6. Сандев,Г.„Система и политика на националната сигурност”, Университетско издателство „Епископ Константин Преславски”, Шумен, 2007, с.75.

7. Слатински, Н.”Същност, смисъл и съдържание на сигурността”. „Военно издателство” ЕООД http://www.vi-books.com -2011.
8. Сандев, Г. „Национална сигурност”, Издателство „Фабер”, 2008, с.15.
9. Гиг Дж., Ван. „Прикладная общая теория систем”—М.:Мир,1981.с.145.
10. Дегтерев А.С., Ерыгин Ю.В., Лобков К.Ю. Оптимизация портфеля инновационных проектов на машиностроительном предприятии ОПК в условиях конверсии / Конверсия в машиностроении, 2004, № 3. с.64.
11. Диманова Д., "Рискови фактори и заплахи за сигурността в България". Трета международна научна конференция “Наука, образование, иновации”, 21 – 23 май 2014 г. Шумен.

ПОДХОДИ ЗА СЪЗДАВАНЕ НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ФИРМЕНА СИГУРНОСТ

Христо А. Христов

APPROACHES ABOUT CREATING A SYSTEM FOR MANAGING COMPANY SECURITY

Hristo A. Hristov

ABSTRACT: *This report examines the approaches about creating a system for managing company security and it claims that this is extremely important stage in the process of business' organization management that is thought as a prerequisite for achieving and creating conditions for rationality of the process itself at the stage of organizing the counteraction against encroachments on company security.*

KEYWORDS: *company security system, turbulence, security environment, management, business organization, protection, in- and outside factors, encroachments, counteraction.*

С развитието на съвременните глобални предизвикателства, заплахи и посегателства, нараства необходимостта от оптимизиране на подходите за своевременното им надеждно разкриване, неутрализиране и минимизиране на негативните последици от въздействието им върху бизнес организациите.

Дефинирането на противодействието на посегателства срещу фирмената сигурност и прилагането на подхода на управление на противодействието в организацията е един от възможните механизми за повишаване ефективността на процеса по защита сигурността на бизнес организациите от съвременните посегателства. В тази връзка, в доклада ще бъдат изследвани, подходите за създаване на система за управление на фирмената сигурност,като изключително важен етап в процеса на управление на бизнес организацията, разглеждан като предпоставка за постигане и създаване на условия за рационалност на процеса на организиране на противодействието.

Защитата на фирмената сигурност е функция на бизнес организацията като цяло и тя се осъществява от нейните структури за сигурност, в рамките на тяхната компетентност и в съответствие с възложените им функции и предоставените им сили, средства и методи на дейност.

На формите на видовете посегателства, съответства системата за фирмена сигурност, като конкретна, практически проявена форма на абстрактното родово понятие „фирмена сигурност". Системата за фирмена сигурност в едно търговско предприятие е всъщност видово определената вече фирмена сигурност[1].

Системата за фирмена сигурност е единствена форма за противодействие на различните форми на видовете посегателства. В този смисъл, службата за фирмена сигурност, като материален израз в действителността на системата за фирмена сигурност, се явява общото средство за противодействие на всички възможни посегателства.

Службата за сигурност на едно търговско предприятие е организационната структура на системата му за фирмена сигурност, тя е материалният еквивалент на фирмената сигурност, като система. Тя има за основна цел да защитава фирмената сигурност, като използва своите специфични средства, методи и способи за превенция, разкриване, неутрализиране и подпомагане пресичането на дейността на онези вътрешни и външни сили, които извършват посегателства срещу бизнес организацията [1].

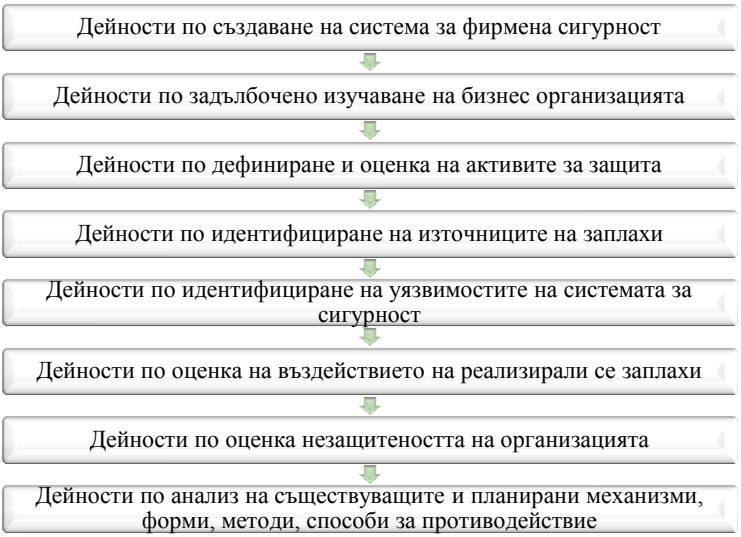
Организацията на противодействието на посегателства срещу сигурността на фирмата е изключително важен етап в процеса на управление на бизнес организацията, характеризиращ се със сложна съставна същност и включващ определени взаимно свързани дейности и процедури. Комплексното и прецизно осъществяване на всяка една от дейностите е предпоставка за постигане на висока степен на обективност на анализа и оценката на незащитеността на организацията и създаване на условия за рационалност на процеса на организиране на противодействието.

Организацията на противодействието на посегателства срещу фирмената сигурност в методологически аспект, включва дейности,представени на фиг. 1:

- създаване на система за управление на фирмена сигурност;
- задълбочено изучаване на социалната организация;
- дефиниране и оценка на ценностите и активите за защита на организацията –кои и какви ресурси трябва да се защитят;
- идентифициране на източниците на заплаха на дефинираните активи –от какво трябва да се защитят ценностите и активите и каква е вероятността конкретната заплаха да се реализира;
- идентифициране на уязвимостите на системата за сигурност на организацията – уязвимите места, които могат да бъдат атакувани;
- оценка на въздействието, което реализирали се заплахи оказват на организацията – какви могат да бъдат последиците за организацията

при реализиране на дадена заплаха (несанкциониран достъп, промишлен шпионаж, разкриване на конфиденциална информация), включително и последствия за организацията от реализацията на дадена заплаха в дългосрочен план (загуба на имидж, загуба на доставчици и пазари, финансови и материални загуби, фалит и др);

- оценка на незащитеността на организацията, чрез използване на количествени и качествени способи;
- анализ на съществуващите и планирани механизми, форми, методи и способи за противодействие и защита.



Фиг. 1. Методология на организацията за противодействие срещу фирмената сигурност

Комплексното разглеждане на посочените дейности са задължително условие за извършването на надеждно противодействие на посегателствата за организацията. Подценяването на някой от компонентите или непълното му характеризиране не би позволило извършването на надеждно идентифициране на посегателствата и би възпрепятствало осъществяването на последващите етапи от процеса на организация на противодействието.

Създаване на система за управление на фирмена сигурност (СУФС)

*„Системата за управление на фирмената сигурност*е част от общата система за управление на организацията, цели изграждането, внедряването, действието, наблюдението, прегледа и подобряването на фирмената сигурност.*Тя включва организационната структура, политики, дейности по планирането, отговорности, практики, процедури, процеси и ресурси”[5]*.

При изграждането, внедряването, действието, наблюдението, прегледа и подобрението на СУФС на организацията се насърчава използването на процесния подход. Този подход се препоръчва по следните съображения. За да може ефективно да функционира една организация, тя трябва да идентифицира и управлява много дейности. Всяка дейност, която използва ресурси и се управлява с цел превръщането на входните елементи в изходни, може да се счита за процес. Често изходните данни от един процес се явяват входни данни за следващия. Прилагането на система от процеси в организацията, заедно с идентифицирането и взаимодействието на тези процеси и тяхното управление, се нарича процесен подход.

Процесният подход за управление на фирмената сигурност, съдейства на тези, които го прилагат да осъзнаят важността от:

а) Разбирането на изискванията за сигурност на организацията и необходимостта от създаване на политика и цели за фирмена сигурност.

б) Внедряването и прилагането на различни начини на контрол в контекста на управлението на противодействието срещу посегателства на организацията.

в) Наблюдението и прегледа на действието и ефективността на СУФС.

г) Непрекъснато подобрение, основано на обективни измервания.

„Четирите основни процеса в СУФС и тяхното съдържание са показани в табл. 1” [5].

Изграждането на СУФС изисква разработване на политика по фирмена сигурност, която да демонстрира ангажимента на организацията за опазването на сигурността на фирмата. Разработването и внедряването на такава система е сложен и всеобхватен процес, който зависи от предмета на дейност на организацията, характера на процесите в нея и произтичащите уязвимости и заплахи.

*Подчерта се, че с*игурност за една социална система има тогава, когато основните идеали, ценности, потребности и интереси на системата не са подложени на никакви въздействия (абсолютна безопасност) или не са застрашени от съществуващи въздействия, които социалната система да не е в състояние ефективно да неутрализира

(защитена безопасност), контролира (относителна сигурност) или управлява (трансформационна сигурност).

За да се осигурят тези характеристики, се изгражда*система за сигурност.* Всяка система за сигурност има за основна цел да обезопаси ценностите на системата.

Основните понятия, които се използват в сектора за сигурност, свързани с противодействието на посегателства срещу фирмената сигурност, са: предотвратяване, превенция, разкриване и неутрализиране на различни заплахи и форми на посегателства. Тяхната същност и съдържание не са изложени в настоящото изследване.

Таблица 1.Основни процеси в СУФС

Планиране **(създаване** на СУФС)	Създаване на политики, цели, процеси и процедури на СУФС във връзка с управлението на противодействието за подобряването на фирмената сигурност за постигането на резултати в съответствие с общата политика и цели на организацията.
Действие *(*внедряване и действие *на СУФС)*	Внедряване и действие на политиката, контролите, процесите и процедурите на СУФС.
Проверка *(*наблюдение и преглед *на СУФС)*	Оценка и, където е приложимо, измерване на изпълнението на процесите спрямо политиката по сигурността, целите и практическия опит и докладване на резултатите пред ръководството за преглед.
Изпълнение (поддържане и подобряване на СУФС)	Предприемане на коригиращи и превантивни действия, базирани на прегледа от ръководството, за да се постигне непрекъснато подобрение на СУФС.

*Първото, с което трябва да се започне при разработването на системата, е*да се определят и обосноват мястото, целите, обхватът и политиката на СУФС.

„Политиката на СУФСна организацията може да включва”[5]:

- рамка на целите и принципите за реализиране на фирмената сигурност;
- кои законови, стандартизационни, бизнес изисквания и договорни задължения за сигурност ще удовлетворява;

- на какъв стратегически контекст за управление на противодействието на посегателства ще отговаря;
- по кои показатели и критерии ще се оценява незащитеността на организацията.

Тази политика се одобрява от ръководството на организацията (от стратегическото ниво за управление).

Целта на политиката за фирмена сигурност може да се дефинира като необходимост да осигури насоки и подкрепа на ръководството по отношение на фирмената сигурност, в съответствие с изискванията на бизнеса и съответните закони и разпоредби. Ръководството следва да даде ясна посока на политиката, в съответствие с целите на бизнеса и да демонстрира подкрепа и ангажираност по отношение на фирмената сигурност чрез публикуването и поддържането на политика за фирмена сигурност в цялата организация.

Препоръчва се документът за политиката по фирмена сигурност да съдържа следните постановки [5]:

- дефиниция на фирмена сигурност, нейните общи цели и обхват и важността на противодействието за организацията;
- изявление за намерението на ръководството в подкрепа на целите и принципите на фирмата, в съответствие със стратегията и целите на бизнеса;
- общата рамка за определяне на цели и механизми за контрол, включващи структурата за оценка и управление на противодействието;
- кратко обяснение на политиките за сигурност, принципите, стандартите и изискванията за съответствие, които касаят организацията, включващи:
  - ✓ законовите, нормативни и договорни изисквания за съответствие;
  - ✓ изискванията за образование, обучение и съзнание по отношение на сигурността;
  - ✓ изискването за управляване на непрекъснатостта на бизнеса;
  - ✓ последствията при нарушаване на политиката по фирмена сигурност;
  - ✓ дефиниране на общите и специфични отговорности за управление на фирмената сигурност, включително и за докладване на инциденти по сигурността;
  - ✓ препратки към документи, подкрепящи тази политика, като например по-подробни политики и процедури за специфични дейности или правила за сигурност, с които потребителите трябва да се съобразяват.

Тази политика за фирмена сигурност трябва да бъде разпространена до потребителите в организацията във форма, която е подходяща, достъпна и разбираема за читателите, за които е предназначена [9].

Политиката за фирмена сигурност може да бъде оформена като отделен документ в организацията, както може да е и част от общия документ за политиката на организацията. Ако документът на политиката по фирмена сигурност ще се разпространява извън организацията, трябва да се внимава да не се разкрива чувствителна информация.

Проблемите на фирмената сигурност в България са свързани с липсата на достатъчно професионалисти в областта и отношението на мениджърите. Те подценяват проблема, ограничават по различни съображения сферата на дейност на звеното за сигурност, тъй като те виждат как харчат пари за сигурност, а не виждат пряка възвращаемост. В тази връзка е необходимо обучение. Мениджърите са свикнали да вземат решения и, при добра основа и адекватно информационно осигуряване, бързо ще се ориентират в проблемите на сигурността. Тяхната основна задача, обаче е да ръководят и да „правят" бизнеса, затова е необходимо да могат да разчитат на специалисти професионалисти.

Л и т е р а т у р а:

1. Василев,Ем. „Фирмена сигурност". Труд, 2000. С.
2. Сандев, Г. Сигурност на организациите. Университетско издателство „Еп.Константин Преславски" Шумен.2012. ISBN 978-954-577-621-2.
3. Станев, С, С. Железов. Компютърна и мрежова сигурност. Шумен: Университетско издателство, 2002.
4. Владимиров, П. Управление на специалните служби. С., 2002, СБ. с.164-190.
5. Млеченков,М. „Методика за разработване на система за информационна сигурност", НВУ „В.Левски", Факултет „Артилерия,ПВО и КИС" Шумен.2010.
6. Асенов, Кипров. Теория на контраразузнаването. София : Труд, 2002.
7. Асенов. Основи на оперативно – издирвателната дейност. ВСУ „Черноризец Храбър" . ISBN 978-954-715-432-2, 2009.
8. Сандев, Г. „Национална сигурност", Издателство „Фабер", 2008,
9. Диманова Д., "Кризата като социално явление и фактор, влияещ върху състоянието на националната сигурност". Годишник ШУ, декември 2013г.

СЪВРЕМЕННИ МЕТОДИ И ТЕХНИКИ НА ПРЕПОДАВАНЕ ПО МЕХАНИКА

Христо Христов, Пламен Дянков

MODERN METHODS AND TECHNIQUESTEACHING OF ENGINEERING MECHANICS

Hristo Hristov, Plamen Djankov

ABSTRACT: *This article discusses modern methods and techniques of teaching mechanics at university. The tiny school hours for lectures and exercises require the active use and their combinations in the learning process.*

KEYWORDS: *METHOD, TECHNIQUES OF TEACHING*

1. В съвременните условия за обучение във ВУЗ кредитната система служи за основа при разработване на учебните програми. В тях от своя страна е планиран и съгласно тях се реалзира и провежда учебния процес по съответната учебна дисциплина.

При разработването на учебните програми за нуждите на учебия процес са залегнали два основни аудиторни начина (метода) за обучение:

- лекции;

- упражнения (семинарни и лабораторни).

Самостоятеланата работа на студентите е единствения метод за обучение - от неаудиторните методи за обучение, който е включен в учебните програми по съответната дисциплина. Много често този метод

за обучение е подценяван и като резултат неизползван достатъчно ефективно.

От методическа гледна точка така разработените учебни програми са много несъвършенни, защото формално не дават възможност за използването на другите известни методи за обучение.

Това води до еднообразие, материала който се преподава изглежда скучен и неинтересен. В резултат студентите губят интерес към дисциплина МЕХАНИКА и ТЕХНИЧЕСКА МЕХАНИКА, а понякога и към обучнието си във Факултета по Технически Науки като цяло.

В същото време в учебния процес по общо техническите инженерни дисциплини могат да се прилагат допълнително добре известните „класически" методи за преподаване – разказ, беседа, дискусия, презентация и т.н.

Включването на допълнителни методи на преподаване / обучение води до по–голямо ранообразие, засилване интереса на обучаемите към съответната дисциплина.

По надолу ще бъде предложена една примерна класифи-кация за приложение на методите за обучение. Тя може да се използва при разработване на програмите по дадена дисциплина от групата на общо техническите с цел повишаване ефектив-ността на учебния процес.

2. Методи итехники, приложими в аудиторни условия, за преподаване на нови знания.

ЛЕКЦИЯ - изнася се от преподавателя и се използва за предаване на голям по обем и сревнително труден по характер, аналитичен материал. Особеност в структурата на лекцията е ползването на **метода на теоретичното доказателство**. Да се владее този метод означав да се владее от преподавателя *доказателството* като логическо средство както на равнището на формалната, таки и на равнището на диалектическата логика.Това предполага:

- ясно и точно формулиране на теоретичното положение, чиято истинност или неистинност ше се доказва;

- строг научен подбор на фактологичния материал на аргументите, които трябва да имат безспорна доказателствена стоиност;

- подходящо ползване на формите на доказателството – индуктивни, дедуктивни, традуктивни;

- формиране на изводи, точно произтичащи от приведените аргументи.

РАЗКАЗ - една от най популярните форми за монологично изложение на учебния материал. Заема съществено място в обучението по философският цикъл. Разказът има предимно описателен характер предоставяики информация за същноста и особеностите на почти всички явления от живота. Съдържа потенциали за силно емоционално и интелектално въздеиствие върху студентите чрез възможностите за образно разкриване на изучаваните факти. Ролята на метода не се ограничава само със съобщаването на нови знания, той може да се използва като:

- изходна предпоставка за създаване на проблемна ситуация за решаване на нови познавателни задачи

- за систематизиране на определен обем знания и за достигане но значими изводи.

Значението му в обучението по общотехническите дисциплините е толкова по-голямо, колкото в по-голяма степен обслужва теоретичните доказателства в изложението на преподавателя.

БЕСЕДА - един от основните методи също с широко приложение в обучението. Реализира се като фронтално поставяне в определена последователност на въпроси от преподавателя към студентите. Обикновенно те са свързани с новото учебно съдържание, но основното им предназначение е да се реализира обмен на информацията между всички страни в акта на обучение. Главната цел на беседата е да се постиген по задълбочено осмисляне на учебното съдържание и да се разкрият реалните посоки в които то може да бъде приложено. Предимство на метода е възможноста за активно включване в мисловната дейност на цялата група/поток.

Изисквания към въпросите:

-да бъдат логически свързани така че сравнително пълно да търсят съответните отговори.

-да бъдат формулирани ясно,точно и не многословно;

-да небъдат подсказващи или внушаващи

- беседата да бъде управляем процес, т.е. отговорите да се следят от всички и своевременно да се коригират и допълват при необходимост.

Има два типа беседа:

= ЕВРИСТИЧНА, когато се извлича ново знание въз основа на миналият опит на студентите;

= КОНТРОЛНА/проверовачна, когато преподавателят има за цел да установи степента на усвоеност на съответният вече преподаден материал.

ПРЕЗЕНТАЦИЯ - изнася се от преподавателя, използва се за представяне на тема или идея. Студентите трябва да си водят бележки и да участват активно в обсъждането. Ползването на интерактивни средства е желателно/задължително.

ВОДЕНЕ НА БЕЛЕЖКИ ПОД РЪКОВОДСТВОТО НА ПРЕПОДАВАТЕЛЯ - той предава някакъв обем информация като показва /инструктира обучаемите как да си водят бележки.

ДИСКУСИЯ - характерът на учебното съдържание и особенстите на младежката възраст са добри предпоставки за широкото и приложение. В практиката на обучението най-често се реализират импровизирани дискусии по време на семинарни упражнения, те бързо приповдигат тонуса на учебната работа, но като явление трудно поддаващо се на ръководене не оказват съществено влияние върху съдържателният аспект на обучението.

По целесъобразно е прилагането на ръководената от преподаватеял дискусия, което предполага предварителна организация от страна на преподавателя и студентите. Целесъобразно е да се ползва в хода на лекциите, разказите, беседите и презентация.

3. Аудиторни методи за затвърждавене на знания.

СЕМИНАР ПОД РЪКОВОДСТВОТО НА ПРЕПОДАВАТЕЛЯ/СЕМИНАРНО УПРАЖНЕНИЕ - съдържа набор от практически упражнения, които се провеждат след изнасянето на теоретичния материал по дадена тема. Целта е да се приложат теоретичните знания и да се формират съответните алгоритми за решаване на практически инженерни задачи. Препоръчва се свободно общуване, дискусия между преподавател и студенти, както и водене на бележки от страна на студентите.

ДИСКУСИЯ - В практиката на обучението най често се реализират импровизирани дискусии по време на упражнение - те бързо приповдигат тонуса на учебната работа. Удачно е прилагането на ръководена от преподавателя дискусия по дадената тема за упражнение, което изисква предварителна подготовка от страна студентите.

АКТУАЛИЗАЦИЯ - чрез подходящ набор от въпроси преподавателят цели да актуализира в оперативната памет на студентите по-рано усвоени знания.

УПРАЖНЕНИЯ ЗА ЗАПОМНЯНЕ - предлагат се задачи, които са специално насочени към затвърждаване, запомняне и превръщане на даден обем от информация в част от дълготрайната памет.

МОЗЪЧНА АТАКА – преподавателят задава въпрос и задължително записва всички отговори след това те се обсъждат, сравняват, обобщават и приемат с консенсус.

ИЗУЧАВАНЕ НА КАЗУС/ЗАДАЧА - на студентите се представя някакъв казус чието решение изисква от тях да демонстрират определени деиствия или идеи.

ФОРМАЛЕН ДЕБАТ - реализира се чрез дебатиране по предварително установени правила върху зададена тема.

4. Неаудиторни методи. Методи за самостоятелна работа.

САМОСТОЯТЕЛНО УЧЕНЕ - на студентите се дават конкретни указания и инструкции за самостоятелна работа по определени теми/задачи.

КУРСОВА ЗАДАЧА – тя представлчва част от технически проект. Необходимо е да бъде направена/решена самостоятелно. Нейното изработване и написване/отпечатване трябва да бъде съобразно действащите БДС. Накрая трябва да бъде дискутирана и „защитена" пред преподавателя.

5. Изводи и заключения.

В настоящата работа са показани и предложени за работа класически методи на обучение във ВУЗ, които да бъдат използвани в обучението по дисциплините Механика, Техническа механика. Правилнот изплзване и прилагане на предложените методи за обучение дава възможност за:

- повишаване заинтересоваността на обучаемите / студен-тите;

- повишаване качеството на усвояване на материала по дисциплините Механика, Техническа механика;

- възможност за намаляване аудиторната натовареност на судентите в разумни граници – 10 макс. 20 % намаляване на часовете за аудиторна заетост по дисицплините Механика, Техническа механика;

Литература:

1. **Джиджева В.С.** Методика на обучението по техническите дисциплини. Издателство на ВМЕИ „В.И.Ленин". София. 1982 год.

2. **Такворян-Солакян Б.Л.** Иновационни образователни техно-логии и подходи. ISBN 978-954-549-109-0. ИК „Феномен". София. 2012 год.

3. Новите технологии в образованието и професионалното обучение. Научно-практическа конференция с международ-но участие. София. 2003 год.

ПОСТИГАНЕ ВИСОКИ ПОКАЗАТЕЛИ НА ПРЕДАВАНЕ НА ДАННИ В МОБИЛНИТЕ КОМУНИКАЦИИ

Драгомир Василев, Иван Цонев

HIGH DATA RATES IN MOBILE COMMUNICATION

Dragomir Vasilev, Ivan Tsonev

ABSTRACT: *Evolution of mobile communication provide the possibility for significantly higher end user data rates compared to what is achievable with, for example, the first releases of the 3G standards. This includes the possibility for higher peak data rates but, even more so the possibility for significantly higher data rates over the entire cell area, also including, users at the cell edge.*

KEYWORDS*: Data rates, White noise, Interference, Time dispersion*

Въведение

Една от основна цели за развитието на мобилните комуникации е да се осигури възможност за по-високи скорости и възможности за предаване на данни до крайния потребител в сравнение с това, което се предлага например с първите версии на стандартите 3G. Това включва и възможността за значително по-високи скорости на трансфер над цялата площ на клетките, които да включват и потребителите в периферията на клетката. В доклада се излагат съществените ограничения по отношение на това, как може да бъде постигната висока скорост на предаване на данни в различни условия.

Основни ограничения за постигане на високи скорости.

След основен преглед на всевъзможните многонивови и многофазови методи, за кодиране, Шенон дава един от основните теоретични инструменти отнасящи се до пропускателната способност (капацитета) на канала *C*, т.е. теоретичната горна граница за скоростта

на предаване на данни, които може да се предадат със зададена средна мощност на сигнала *S* през комуникационен канал, който е под въздействие на адитивен бял гаусов шум (AWGN) с мощност *N* [1],[2].

$$C = BW \cdot \log_2\left(1 + \frac{S}{N}\right),$$

(1)

Където *BW* е свободната честотна лента. От уравнението става ясно, че два от основните фактори, ограничаващи постигане на висока пропускателна способност е съотношението: мощност на сигнала / мощност на шума *S/N*, и наличната честотна лента. За да се изясни допълнително как и кога тези фактори ограничават пропускателната способност трябва да предположим, комуникация с определена скорост *R*. Мощността на приетия сигнал може да бъде изразено, като

(2) $S=Eb.R$

където *Eb* е енергия на бит. Освен това силата на шума може да бъде изразена, като

(3) $N=N0.BW$

където *N0* е едностранната спектрална плътност на адитивния бял гаусов шум постъпващ на входа изразен във *W/Hz*.

Ясно е, че скоростта на предаване не може да надхвърля капацитета на канала. Заедно с по-горе дадените изрази за мощността на сигнала и мощността на шума можем да изведем неравенството:

$$R \le C = BW \cdot \log_2\left(1 + \frac{S}{N}\right) = BW \cdot \log_2\left(1 + \frac{E_b \cdot R}{N_0 \cdot BW}\right)$$

(4)

или, чрез определяне на съотношението на използване на радио честотна лента $\gamma=R/BW$,

$$\gamma \le \log_2\left(1 + \gamma \cdot \frac{E_b}{N_0}\right).$$

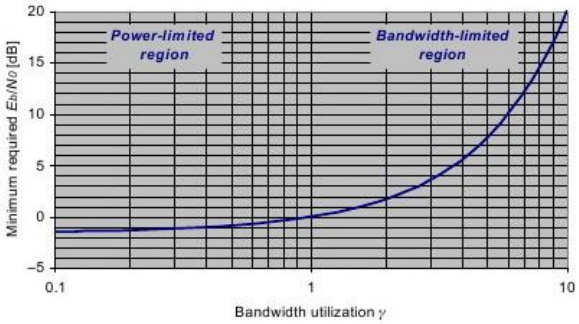
(5)

Това неравенство може да бъде преформулирано за осигуряване на по-ниска граница на необходимата енергия на бит, нормализирана до мощността на плътността на шума за използваната честотна лента.

$$\frac{E_b}{N_0} \geq \min\left\{\frac{E_b}{N_0}\right\} = \frac{2^\gamma - 1}{\gamma}.$$

(6)

Минимума, изискван в приемника, като функция на степента на използване на честотната лента *E*b/*N*0 може да видим във Фиг. 1.



Фиг. 1

Използваната честотна лента е значително по-малка от 1, това е много по-малко от необходимия минимум *Eb/N0* и е относително постоянна, независимо от γ. Следователно за дадена плътност на мощността на шума, всяко увеличение на скоростта на предаване предполага подобно относително нарастване на минималната необходима мощност на сигнала $S=Eb.R_в$ на приемника. От друга страна, за използван трафик по-голям от 1, минимумът изискван *Eb/N0* се увеличава бързо с γ. По този начин, когато имаме предаване със скорост от същия порядък, това оказва влияние на всяко следващо увеличаване на скоростта, без да се увеличава наличната честотна лента, се получава относително нарастване на минималната изисквана мощност на получения сигнал [1],[2].

Постигане на високи скорости за предаване на данни при ограничаване на шума

Един от основните проблеми по отношение на достигане на по-високи скорости за предаване на данни в мобилните комуникационни системи се явява, когато шумът е фактор при увреждане на радио връзката:

1. Стойностите на скоростта, които могат да бъдат осигурени при такива случаи винаги се ограничават от свободната мощност на получения сигнал или от съотношението мощност на приемания сигнал и мощност на шума. Освен това всяко увеличение на скоростта на трансфер в дадена честотна лента ще изисква едно и също относително увеличение на мощността на сигнала. В същото време, ако се осигури достатъчно мощност на получения сигнал може да се постигне и висока скорост за предаване на данни.
2. В случай на използване на тясно честотна лента, увеличението на скоростта на предаване изисква приблизително същото относително увеличение на мощността на получения сигнал.
3. В случай на използване на високо честотна лента, при всяко последващо увеличаване на скоростта на предаване, се изисква много по-голямо увеличение мощността на сигнала. Това е така освен ако честотната лента не се увеличава пропорционално на увеличението на скоростта на предаване.

Мощността на приетия сигнал може винаги да се увеличи, чрез намаляване на разстоянието между предавателя и приемника. По този начин се намалява затихването на сигнала от предавателя към приемника. При ограничаване на шума теоретично е възможно да се увеличи скоростта на предаване. Когато намаляване разстоянието предавател - приемник говорим за намален обхват, в мобилна комуникационна система, това би било равносилно на намаляване размера на клетките и по този начин възникване на нуждата от сгъстяване на мрежата с повече клетъчни сайтове за покриване на същата обща площ. Това по-специално, осигурява същата или по-висока скорост от наличната честотна лента и изисква значително намаляване размера на клетките. Така високите скорости са достъпни само за потребители в центъра на клетката, а не по цялата и площ и особено в периферията на клетката.

Друг начин за увеличаване на общата мощност на получения сигнал за постигане на дадена предавателна мощност е използването на допълнителни антени към приемника. Множество приемни антени могат да бъдат интегрирани в клетъчната структура за осигуряване на

високи стойности на предаване uplink - downlink. Постигането на по-високи стойности, чрез използване им е ефективно до определено ниво, което се определя от мощността на сигнала и честотната лента. След това ниво, средата започва да се насища и всяко по-нататъшно увеличаване броя на предавателни или приемани антени, ще осигури само незначително увеличение. Това насищане може да бъде избегнато, чрез използване на антени в предавателя и приемника, позволяващи така нареченото пространствено мултиплексиране MIMO (Multiple-Input Multiple-Output) [1],[2].

Постигане на по-високи скорости за предаване при ограничаване на интерфернцията.

В действителните мобилни комуникации, смущения възникнали от предавания излъчвани в две съседни клетки се нарича междуклетъчни смущения. Този вид смущения са често доминиращ източник на увреждане на радио връзката. Те влияят повече от тези в следствие на шума. Явлението се получава основно в случай на използване на малки клетки, които поемат висок трафик. Междуклетъчното смущение в някои случаи може да бъде и смущение от други предавания в рамките на текущата клетка (смущения в рамките на клетката).

В много отношения интерференцията при радио връзка е подобна на смущенията възникнали при шум. Практически може да се определят следните основни принципи при увреждане на радиовръзката:

- Максималната скорост на данни, която може да бъде постигната в дадена честотна лента е ограничена от съотношението мощност на сигнала и мощност на смущенията;
- При шум се увреждa доминиращата радио връзка. Намаляването размера на клетката, както и използването на многоантенни техники са ключови средства за повишаване скоростите за предаване на данни и ограничаване на интерференцията:

Намаляване на размера на клетката очевидно ще намали броя на потребителите и респективно трафика през нея, но така се намалява и относителното ниво на интерференция и по този начин има възможност за по-високи скорости на трансфер.

Ако ограничим нарастването на съотношението сигнал - шум, правилната комбинация и увеличаване броя на антените намаляват интерференцията при получените сигнали. Правилното използването на формираните диаграми на предавателните антени може да увеличи предавателната мощност в посока на приемника, което води до намаляване на интерференцията възникнала от други излъвания, като по този начин се подобрява и общото съотношение в системата.

Една важна разлика между интерференция и шум е, че шума обикновено има определена структура, която го прави поне до известна степен предвидим и по този начин е възможно да се подтисне или дори да се премахне напълно, докато при интерфернцията проблема може да пристигне от неопределена посока и единствената намеса може да се окаже коригиране или напълно премахване, чрез пространствена обработка, използваща антените при приемника [1],[2].

Високи скорости за предаване в рамките на ограничена честотна лента.

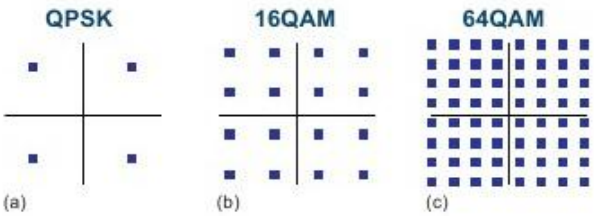
Предаването на данни със скорост по-голяма от наличната честотна лента е основно неефективно. Изисква непропорционално високи стойности на съотношенията сигнал/шум и интерференция в приемника. При тези условия мобилните комуникационни системи трябва да бъдат проектирани така, че бъдат в състояние да предложат много високи скорости на трансфер в рамките на ограничена честотна лента, когато условията на разпространение на радио вълните го позволяват.

Един от начините да се предложи по-високи скорости на трансфер в рамките на дадена честотна лента е използването на по - висока модулация.

Такъв тип е QPSK модулацията, използвана в първите версии на мобилни комуникационни стандарти 3G (WCDMA и CDMA2000). Състои се от четири различни сигнални алтернативи. Тези четири алтернативи сигнали могат да бъдат илюстрирани както четири различни точки в двумерна равнина. С четири различни сигнални алтернативи, QPSK дава възможност да се съобщават до два бита информация по време на всеки интервал модулация (символ). Както в GSM мрежата, за да се намали ширината на честотния канал, в CDMA мрежата (в правия, Downlink канал) се използва предварително филтриране на информационния сигнал. Така се стеснява честотната

лента на модулирания сигнал, но се влошава фазовата картина на QPSK сигнала [1],[2].

Значително повишаване на шумоустойчивостта на предаваните модулирани комуникационни сигнали се получава при едновременно въздействие на амплитудата и фазата на носещия сигнал. Така се получава т. нар. m-QAM (m – цяло число; броят на различните амплитудни и фазови състояния на сигнала), при което се предават едно-временно log2m бита. Този тип модулация има подобни характеристики на 16-PSK модулация, но показва по-добра шумозащитеност, защото съседните фазови състояния се различават и по амплитуда. С разширяване на 16QAM модулация се образуват 16 различни сигнални алтернативи. Използването на 16QAM по този начин дава възможност за до 4 бита информация съобщена на символ интервал. Допълнително удължаване до 64QAM дава възможност за до 6 бита информация съобщена на символ интервал. В същото време, на честотната лента на предавания сигнал е най-малка и скоростта основно зависи от използваната модулация. Максимално използване на честотната лента, изразена в bits/s/Hz, за 16QAM и 64QAM една и съща, но предадената информация е няколко пъти повече в сравнение с QPSK модулацията е илюстрирано на Фиг. 2.



Фиг.2

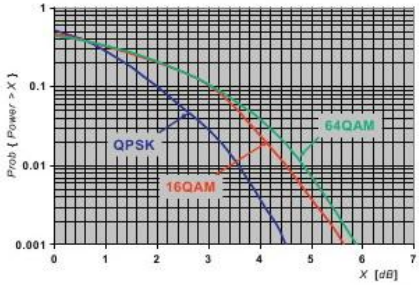
Прилагането на модулация осигурява възможност за по-добро използване на честотната лента, в резултат на което се достигнат по-високи скорости на трансфер в рамките на определен трафик. Въпреки това, пълното използване на честотната лента е за сметка на намалената устойчивост на шум и интерференция. Схеми за модулация по-висок ред, като 16QAM или 64QAM, изискват по-високо съотношение Eb/N0 в приемника иначе се повишава вероятността за битова грешка, в сравнение с QPSK [1],[2].

Схеми с по-висок порядък модулация като 16QAM и 64QAM изискват, сами по себе си, по-високи стойности на Eb/N0 в приемника. В комбинация с кодиране използването на по-висок порядък модулация е по-ефективно и изисква по-ниска стойности на Eb/N0 за дадена скорост. Това може да се постигне с кодиране на канала при ограничена честотна лента и прилагане на модулация, и може да доведе общо подобрение на ефективността в сравнение с използването на QPSK.

Например ако използваме честотната лента в близост до 2 информационни бита на модулационен символ, QPSK модулация ще даде възможност за много ограничено кодиране на канала. От друга страна, използването на 16QAM модулация ще даде възможност за по-добро шумоустойчиво кодиране. По същия начин, ако се използва лента в близост до 4 информационни бита на модулационнен символ, използването на 64QAM може да бъде по-ефективно от 16QAM модулация, като се отчита възможността за по-ниска натовареност на канала и съответното достигане на по високи нива на кодиране при 64QAM [1],[2],[3] .

Вариации в моментната предавателна мощност.

Общ недостатък на схемите по-висок ред модулация като 16QAM и 64QAM, където информацията се кодира в моментната амплитуда на модулирания сигнал, е че модулирания сигнал има по-големи вариации, следователно възникват по-големи пикове в моментната мощност. На Фиг. 3 е показано разпределението на моментната мощност за QPSK, 16QAM, 64QAM. Ясно се вижда, че големи пикове в моментната мощност възникват при по-висок порядък модулация.



Фиг. 3.

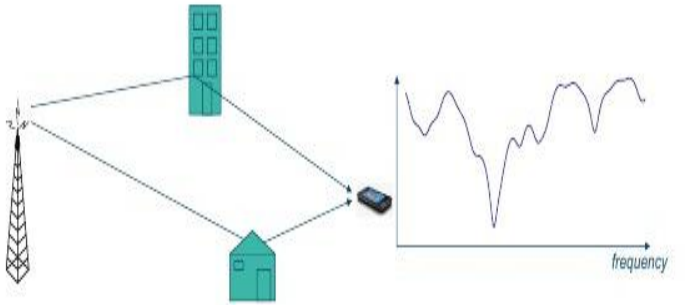
По-големи пикове в моментната мощност на сигнала означават, че усилвателя на предавателя трябва да бъде преоразмерен, за да се избегне нелинейност при усилване, появяваща се при високи нива на моментна мощност, което води до срив при предаване на сигнала.

Модулация с много носещи честоти

При тесно - лентови сигнали с еднакви или близки по честота носещи могат да интерферират и това се оказва сериозен проблем в повечето комуникационни системи. При широколентовите комуникации се наблюдава честотно-селективен фадинг. Идеята за модулация на цифров сигнал с помощта на много носещи е излъчваният поток от битове да се раздели на субпотоци и да се "носи" от много субносещи. Битовата скорост на всеки субканал е много по-ниска от общата; съответно честотната лента на всеки субканал е много по-тясна от общата. Броят на субносещите се избира така, че всеки субканал да има честотна лента, която е по-малка от кохерентната лента и може да се наблюдава само "плосък фадинг" и силно подтисната междусимволна интерференция ISI. Много по-ефективно използване на спектъра се постига с "ортогонални" субносещи, чиито спектри се припокриват, но поради ортогоналността си сигналите си влияят минимално. За ефективна модулация броят на субносещите трябва да е голям.

По - специфични теоретични проблеми свързани с предаване на много носещи честоти е влошаването на излъчвания сигнал дължащо се на време-дисперсия на радиоканала. Време дисперсия се получава, когато предавания сигнал се разпространява към приемника по множество посоки с различни закъснения. Това може да доведе до сривове в целостта на честотата на излъчвания сигнал, което ще доведе до високи нива на грешки и нарушения в съотношението шум / смущения [1],[2].

Радиочестотният спектър на канала зависи също от околната среда, разпределението на сградите в градовете и разпределението на клетките. При гъсто разположени малки клетки в градска среда се наблюдава намаляване на време дисперсията в сравнение с рядко разположени големи (мощни) клетки. В случая сградите се явяват, като потенциални рефлектори отразяващи сигнала. На Фиг.4. е показано схематично два случая на влиянието на сградите при разпространяване на сигнала към приемника чрез множество пътеки с различни закъснения [1],[2].



Фиг. 4

Един от най-ефективните методи за използване на радиочестотния спектър е Ортогоналната модулация (OFDM, (Orthogonal Frequency Division Multiplexing Access). Това се явява и най-простият тип многочестотна модулация. В доклада не се разглеждат подробно математическите основи на метода. Нека да разполагаме с N незастъпващи се канала, всеки с ширина $2BN$ и носеща честота $fn = fc + 2nBN$, $n = 0, 1,\ldots,N\text{-}1$ (fc е честота в обхвата на дадена мрежа) [1],[2].. Така в рамките на всеки бит с ширина TN може да се разложи общия сигнал $S(t)$ по базовите функции. Това може да стане с бърза Фурие трансформация. Връзката "TN -BN" се дава от израза $TN = 0.5(1+\beta)/BN$, където β е фактор на формата на спектъра на суб-носещите ($\beta = 0$ за правоъгълен сигнал или $\beta = 1$ за положителната 1/2 част от косинусоидален сигнал). Ако се използват правоъгълни сигнали, те не трябва да се застъпват. Ако, обаче, се използват 1/2 части от косинусоудални сигнали $\cos(2\pi j/TN)$, $j = 1, 2\ldots$, ($TN = 1/BN$), те образуват ортогонална база от функции в интервала 0, 1/ fn и техните спектри могат да се застъпват. Геометрично това се изразява с факта, че максимума на спектъра на дадена суб-носеща съвпада с нулите от спектъра на близките съседни субносещи. Днес OFDM модулацията е един от най-ефективните методи за ползване на спектъра. Като пример за реализация на OFDM модулацията можем да посочим: Излъчваният цифров поток с битова скорост R се разделя на N субпотока със скорости $RN = R/N$. Всеки от тях се модулира линейно в съответния теснолентов субканал (напр. чрез mPSK или mQAM модулации, m – ниво на модулация. Приемането става по обратен път. Съвременната OFDM-модулация е дискретна (DMT, discrete multitone modulation). При

нея общият поток се модулира с QAM модулатор и се получава комплексен символ X. Той се разделя на N паралелни QAM символа Xn по субносещите, които са дискретните честотни компоненти на изходния сигнал. Чрез инверсна IFFT Фурие трансформация от тези дискретни честотни компоненти се получава времевата форма на сигнала без никаква между-символна интерференция ISI. Това се постига, чрез "cyclic prefix": непоследователна честотно - времева матрица, т. е. Честотните канали не са последователни (съседни) [1],[2].

Заключение:

В заключение може да се обобщи:

- По-високочестотните сигнали се разпространяват с по-малки загуби, както в свободното пространство, така и в т. нар. предавателни линии. При предаване на много високочестотни сигнали е необходима пряка видимост между приемно-предавателните станции, а при по-ниски честоти се получава ефект на дифракция.
- При по-високи честоти могат да се поместват повече на брой широколентови канали. Първото е свързано с осигуряване на по-висок трафик, а второто – на по-висококачествени комуникационни услуги и по-бързо предаване на информацията в bits/s.
- При по-високи честоти антените са по-малки по размери поради по-малката дължина на вълната. Освен това антените имат по-висока насоченост, поради което се използват предаватели с по-ниска изходна мощност.

Литература:

1. **Цонев**, И. Предаване на данни и компютърни комуникации. – Шумен., Университетско издателство, 2012.
2. **Dahlman** E**., Parkvall** S**., Sköld** J**.** 4G LTE/LTE-Advanced for Mobile Broadband. – UK., Academic Press is an imprint of Elsevier, 2011.
3. **Цонев, И. Станев, С**т. Компютърни мрежи и комуникации. УИ, ШУ, 2008.

ГОДИШНИК

НА ШУМЕНСКИЯТ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

ТЕХНИЧЕСКИ НАУКИ

Т. V Е

Формат 16/80/84

ISSN 1311-834X

Универистетско издателство
“Епископ Константин Преславски“ 2015