

**ГОДИШНИК**  
**НА ШУМЕНСКИЯТ УНИВЕРСИТЕТ**  
**„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“**  
**ТЕХНИЧЕСКИ НАУКИ**

**T. VI E**

---

**ANNUAL**  
**OF KONSTANTIN PRES LAVSKI**  
**UNIVERSITY OF SHUMEN**

**Vol. VI E**

---

**FACULTY OF TECHNICAL SCIENCES**



Университетско издателство  
“Епископ Константин Преславски“ 2016

Настоящият годишник съдържа доклади изнасяни през 2015 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**

©Шуменски университет, Факултет по технически науки 2016

©Университетско издателство „Епископ Константин Преславски“

## Съдържание

|                                                                                                                                                                                                                         |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <b>Огнян М. Фетфов, ЗАЩИТА НА ИНФОРМАЦИЯТА В ГРУПОВИТЕ РАДИОМРЕЖИ TETRA</b> .....                                                                                                                                       | 5   |
| <b>Атанас К. Атанасов, ПСИХОФИЗИЧЕСКИ ОСНОВИ НА КЛАСИФИКАЦИЯТА НА СЕНЗОРИТЕ В СИГНАЛНО-ОХРАНИТЕЛНАТА ТЕХНИКА</b> .....                                                                                                  | 12  |
| <b>Тихомир С. Трифонов, СИНТЕЗ И АНАЛИЗ НА 5-ЛЕНТОВ ЦИФРОВ ЕКВАЛАЙЗЕР</b> .....                                                                                                                                         | 18  |
| <b>Румен Г. Цаков, ПРИБОР ЗА ИЗМЕРВАНЕ НА АМПЛИТУДНО ЧЕСТОТНИ ХАРАКТЕРИСТИКИ ЧРЕЗ ПЕРСОНАЛЕН КОМПЮТЪР</b> .....                                                                                                         | 29  |
| <b>Цветослав С. Цанков, Доника В. Диманова, КОМПЮТЪРНА ДИДАКТИЧНА ПРОГРАМА ЗА КОД НА ХЕМИНГ</b> .....                                                                                                                   | 38  |
| <b>Доника В. Диманова, Цветослав С. Цанков, АНАЛИЗ СЪСТОЯНИЕТО НА КРИТИЧНАТА ИНФРАСТРУКТУРА ЗА РАЙОН ШУМЕН</b> .....                                                                                                    | 45  |
| <b>Доника В. Диманова, МАТЕМАТИЧЕСКИ МЕТОДИ ЗА ВЗЕМАНЕ НА УПРАВЛЕНСКИ РЕШЕНИЯ ПРИ БЕДСТВИЯ</b> .....                                                                                                                    | 55  |
| <b>Драгомир И. Василев, Иван К. Цонев, ПЛАНИРАНЕ НА ЧЕТВЪРТО ПОКОЛЕНИЕ МРЕЖИ (WLAN, ALL-IP, OFDM)</b> .....                                                                                                             | 95  |
| <b>Драгомир И. Василев, Иван К. Цонев, ПЛАНИРАНЕ И ОПТИМИЗАЦИЯ НА ПРЕНОСА В МРЕЖИТЕ ЧЕТВЪРТО ПОКОЛЕНИЕ</b> .....                                                                                                        | 102 |
| <b>Огнян М. Фетфов, Петър Кр. Боянов, Жанета Н. Ташева, Тихомир Сп. Трифонов, АНАЛИЗ НА СЪВРЕМЕННИТЕ ВИДОВЕ УЯЗВИМОСТИ И ЕКСПЛОЙТИ В КОМПЮТЪРНИТЕ МРЕЖИ И СИСТЕМИ</b> .....                                             | 112 |
| <b>Огнян М. Фетфов, Петър Кр. Боянов, Жанета Н. Ташева, Тихомир Сп. Трифонов, СРАВНИТЕЛЕН АНАЛИЗ НА СЪВРЕМЕННИТЕ ВИДОВЕ АНТИВИРУСНИ ПРОГРАМИ</b> .....                                                                  | 123 |
| <b>Огнян М. Фетфов, Петър Кр. Боянов, Иван О. Николов, Жанета Н. Ташева, Тихомир Сп. Трифонов, СРАВНИТЕЛЕН АНАЛИЗ НА СЪВРЕМЕННИТЕ ВИДОВЕ БЕЗЖИЧНИ IP ВИДЕОКАМЕРИ В КОМПЮТЪРНИТЕ МРЕЖИ ЗА НАБЛЮДЕНИЕ И КОНТРОЛ</b> ..... | 134 |
| <b>Петър Кр. Боянов, Иван О. Николов, Жанета Н. Ташева, Тихомир Сп. Трифонов, ИЗСЛЕДВАНЕ НА СИГУРНОСТТА НА БЕЗЖИЧНА ЛОКАЛНА КОМПЮТЪРНА МРЕЖА</b> .....                                                                  | 143 |
| <b>Димитър С. Димитров, СИТУАЦИОНЕН ЦЕНТЪР ЗА УПРАВЛЕНИЕ НА СИСТЕМАТА ЗА СИГУРНОСТ НА ОРГАНИЗАЦИЯТА</b> .....                                                                                                           | 150 |
| <b>Христо А. Христов, ГРАЖДАНСКИ КОНТРОЛ НА СЕКТОРА ЗА СИГУРНОСТ</b> .....                                                                                                                                              | 161 |

|                                                                                                                                                                                                              |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Христо А. Христов, ОБЩЕСТВЕН КОНТРОЛ НАД СЕКТОРА ЗА СИГУРНОСТ .....</b>                                                                                                                                   | <b>174</b> |
| <b>Добротмир Ж. Добрев, ДЪЛГИЯТ ПЪТ НА ТУРЦИЯ КЪМ ЕВРОПА .....</b>                                                                                                                                           | <b>190</b> |
| <b>Добротмир Ж. Добрев, МУЛТИКУЛТУРНИ ПРОБЛЕМИ В ЗАПАДНИЯ СВЯТ .....</b>                                                                                                                                     | <b>201</b> |
| <b>Добротмир Ж. Добрев, СБОРНИКА «ВЕХИ» И РУСКАТА ИНТЕЛИГЕНЦИЯ .....</b>                                                                                                                                     | <b>209</b> |
| <b>Христо А. Христов, Цоню Г. Цонев, КОНСТРУКТИВНИ ИЗМЕНЕНИЯ НА ОСНОВНИЯ ЗАРЯД НА 82 ММ УЧЕБНО-ПРАКТИЧЕСКА МИНА, ПРЕДНАЗНАЧЕНА ЗА ТРЕНАЖОР ЗА ОБУЧЕНИЕ НА МИНОХВЪРГАЧНИТЕ РАЗЧЕТИ .....</b>                  | <b>220</b> |
| <b>Христо А. Христов, Цоню Г. Цонев, ОПРЕДЕЛЯНЕ АНОРМАЛНИТЕ ИЗСТРЕЛИ ПРИ ЕКСПЕРИМЕНТАЛНИ СТРЕЛБИ С 82 ММ УЧЕБНО-ПРАКТИЧЕСКА МИНА, ПРЕДНАЗНАЧЕНА ЗА ТРЕНАЖОР ЗА ОБУЧЕНИЕ НА МИНОХВЪРГАЧНИТЕ РАЗЧЕТИ .....</b> | <b>227</b> |
| <b>Георгиев С., Колев Х., Георгиев Н., Пехливански В., УСТРОЙСТВО ЗА ЗАЩИТА НА СЕИЗМИЧЕН СЕНЗОР ОТ СМУЩЕНИЯ В БЛИЗКАТА ЗОНА .....</b>                                                                        | <b>236</b> |
| <b>Николай Л. Георгиев, ОБОБЩЕНИ ПОКАЗАТЕЛИ ЗА ЕФЕКТИВНОСТТА НА ЕДИН КЛАС СЕНЗОРИ ОТ СИСТЕМИ ЗА ЗАЩИТА .....</b>                                                                                             | <b>249</b> |
| <b>Христо Л. Лалев, Явор И. Спасов, ПРИЛОЖЕНИЕ НА WAVELET ФУНКЦИИТЕ ЗА СЕГМЕНТАЦИЯ НА ВИДЕОИЗОБРАЖЕНИЕ .....</b>                                                                                             | <b>273</b> |
| <b>Красимира Кирилова, Андрей Андреев, КОСМИЧЕСКИ ГРАВИТАЦИОННИ МИСИИ ШАМП, GRACE И GOCE- ЕДНА НОВА ЕРА НА СПЪТНИКОВА ГРАВИМЕТРИЯ .....</b>                                                                  | <b>285</b> |
| <b>Кирил Янчев, Андрей Андреев, РЕЗУЛТАТИ ОТ ГЕОДЕЗИЧЕСКИ ИЗМЕРВНИЯ И ИЗСЛЕДВАНИЯ С ИЗПОЛЗВАНЕТО НА ГНСС В РАЙОНА НА СТРУМСКАТА РАЗЛОМНА ЗОНА - СТРУМСКИЯ И КРУПНИШКИЯ РАЗЛОМ.....</b>                       | <b>297</b> |

# ЗАЩИТА НА ИНФОРМАЦИЯТА В ГРУПОВИТЕ РАДИОМРЕЖИ TETRA

Огнян М. Фетфов

## SECURITY IN THE TETRA NETWORKS

Ognyan M. Fetfov

**ABSTRACT:** *This paper discusses the methods of data encryption in TETRA standard.*

**KEYWORDS:** *TETRA (Terrestrial Trunked Radio), DCK (Derived Cipher Key), SCK (Static Cipher Key), CCK (Common Cipher Key)*

### 1. Увод

TETRA (Terrestrial Trunked Radio) е отворен стандарт за цифрова клетъчна комуникация, сертифициран от ETSI (European Telecommunications Standards Institute) [1,3], който дава възможност различни обществени организации от сферата на сигурността (полиция, армия, пожарна безопасност, спасителни служби и пр.), държавната администрация, големите производствени и транспортни компании да получават професионална мобилна комуникация с най-висока степен на сигурност и бързина на обмена на данни.

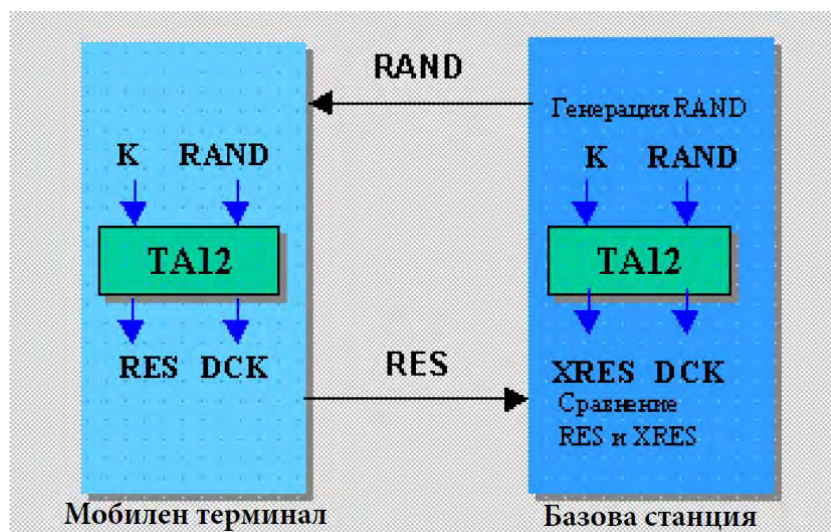
Предвид спецификата на абонатския профил на потребителите на тази услуга, защитеността на предаваната информация от несанкциониран достъп е от съществено значение. В настоящия доклад се разглеждат технологията и процедурите за автентификация, шифриране и защита идентификацията на абонатите.

### 2. Автентификация

Автентификацията е съвкупност от механизми за проверяване автентичността на абоната и мобилния терминал при опит за достъп до системата и за отхвърляне опитите за достъп до

ресурсите на системата на неупълномощени потребители [3]. Използва се протокол “поискване – отговор - резултат” (challenge-response-result protocol), за да автентифицира както мобилния терминал, така и инфраструктурата.

В стандарта TETRA се използва сравнително нова концепция за автентификация чрез шифриране. За целта, в текста на предаваното съобщение се вгражда код, чиято структура може да е постоянна или променлива в зависимост от предаваните съобщения.



Фиг. 1. Обобщен алгоритъм за автентификация в стандарта TETRA

За изпълнение на процедурата се използват записаните в SIM-картата на абоната индивидуален ключ за автентификация и контролер за изпълнение на алгоритъма за автентификация.

Алгоритъмът за проверка на автентичността на абоната се реализира по показания на Фиг. 1 начин. Базовата станция изпраща случайно число RAND към мобилния терминал. В мобилния терминал се извършва криптографска операция (TA12), в резултат

на която чрез индивидуалния ключ на абоната К се изчислява резултатът RES, който се изпраща към базовата станция. В базовата станция се сравняват стойностите на изчисления в мобилния терминал резултат RES и очаквания резултат XRES, получен от същия алгоритъм TA12 и същото случайно число RAND. При съвпадение на двата резултата RES и XRES, инфраструктурата предоставя достъп до системата. В случай, че отговорът е некоректен, инфраструктурата отхвърля опита за достъп до системата.

Освен изчисленият резултат RES, от случайното число RAND и индивидуалния ключ на абоната К се генерира и произведен шифровъчен ключ DCK (Derived Cipher Key), който се ползва при шифрирането на въздушния интерфейс.

Недостатък на описания алгоритъм за автентификация е необходимостта в базовата станция да се съхраняват индивидуалните ключове на всички абонатите. Този недостатък е преодолян чрез използване на йерархична система, при която вместо ключа за автентификация на абоната К се използва друг сеансов ключ KS, генериран от криптографски алгоритъм TA11 на базата на ключа К и случайна поредица RS. Разпределението на сеансовите ключове KS по базовите станции се поддържа от център за автентификация по защитени трасета.

### **3. Шифриране**

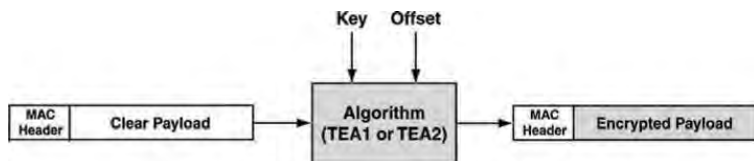
Стандартът поддържа два типа шифриране – шифриране на радиоинтерфеса AIE (Air Interface Encryption) и шифриране от типа „от краен потребител до краен потребител“ E2EE (End to End Encryption).

При шифрирането на радиоинтерфейса, процесът обхваща участъка от абонатните терминали до свързаната базова станция като се използват специални алгоритми за шифриране TEA (TETRA Encryption Algorithm). Обменът между елементите вътре в архитектурата на TETRA-мрежата е открит.

Шифрирането на въздушния интерфейс осигурява сигурност на радиообмена между инфраструктурата и мобилните терминали. За целта се използва общ ключ за криптиране CEK (Common Encryption Key) както в свързаната базова станция, така

и в абонатния терминал. По този начин устройствата криптират и декриптират трафик едно от друго. Шифрирането на въздушния интерфейс се прилага при каналите за контрол, гласовия трафик и трафика на данни.

Предаващият терминал използва ключа и начална (offset) стойност в алгоритъм за криптиране на трафичния поток. Приемащия терминал използва същият ключ и начална (offset) стойност за декриптиране на трафичния поток. MAC - хедърът за пакетите остава ясен през целия процес на криптирането. Реализацията на този процес е показана на фиг. 2.



*Фиг. 2. Шифриране на трафичния поток*

Сертифицирани са следните нива за шифриране:

TEA1: за използване от публичния сектор в Европейския съюз;

TEA2: за използване от службите за сигурност в Европейския съюз;

TEA3: за използване от службите за сигурност извън Европейския съюз;

TEA4: за използване от публичния сектор извън Европейския съюз.

При шифрирането E2EE „от край до край“, сигурността на трафика се осигурява чрез криптиране на връзката, използвайки стандартни или допълнително вградени от потребителя алгоритми.

Процесът на шифриране се активира само след успешна автентификация на абоната и оборудването и защитава потребителските трафични канали и каналите за контрол.

Шифрирането на речта се реализира под формата на обработка на нискоскоростен цифров поток, използвайки алгоритми с висока криптоустойчивост без влошаване на



качеството на възстановената реч. Зависимостта на скоростта на цифровия поток (Kb/s) от нивото на защита на канала е показано в Таблица 1:

Таблица 1

| Ниво на защита | Брой на използваните времеинтервали |      |      |      |
|----------------|-------------------------------------|------|------|------|
|                | 1                                   | 2    | 3    | 4    |
| Без защита     | 7,2                                 | 14,4 | 21,6 | 28,8 |
| Ниско ниво     | 4,8                                 | 9,6  | 14,4 | 19,2 |
| Високо ниво    | 2,4                                 | 4,8  | 7,2  | 9,6  |

Стандартът TETRA ползва поточно шифриране, предвид предимствата на този метод по отношение на мултиплицирането на грешките при дешифриране в канали със смущения.

При шифрирането на радиоинтерфейса се ползват следните ключове:

- Производен шифровъчен ключ DCK (Derived Cipher Key);
- Статичен шифровъчен ключ SCK (Static Cipher Key);
- Общ шифровъчен ключ CCK (Common Cipher Key).

Производният ключ за шифриране (DCK) се генерира като резултат от процеса на автентификация и осигурява уникален ключ за криптиране за мобилния терминал. След автентификация, мобилният терминал съхранява своя изчислен резултат за DCK, като копие от DCK се запазва в базата данни на опорната инфраструктура. За криптиране и декриптиране на трафика помежду си, базовата станция и мобилният терминал използват уникалния DCK и началната (offset) стойност. DCK не се използва за групови повиквания. Въпреки това, DCK поддържа услуги по групови повиквания, като осигурява криптиране на Общия шифровъчен ключ (Common Cipher Key, CCK), който се изпраща към мобилните терминали за групови повиквания. DCK може да бъде използван само когато в клъстера е инсталирана и активирана автентификация. Всеки отделен DCK съществува за времето, през което мобилния терминал е регистриран и автентифициран в

системата. При всяко ново автентифициране на мобилния терминал в системата се генерира нов DCK.

Базовите станции и мобилните терминали са разполагат с 32 статични шифровъчни ключа (SCK). Всеки път системата въвежда един SCK и изпраща номера на SCK ( $SCKN\ 0 \div 31$ ), който към момента се използва в системата към мобилните терминали. Мобилният терминал избира съответния SCK (от предоставения й списък с ключове) за декриптиране на трафика от инфраструктурата. Базовата станция и мобилния терминал използват SCK заедно с началната (offset) стойност за криптиране и декриптиране на трафика между тях. SCK се използва преди мобилният терминал да бъде автентифициран от системата и когато поддържаният сайт е в режим „транкинг в сайт” (и е неспособен да разработи произведен шифровъчен ключ – Derived Cipher Key, DCK). SCK се използва също така, когато опцията за автентификация не е инсталирана или активирана.

Общият шифровъчен ключ (ССК) се използва за криптиране на трафик за групови повиквания. Всички регистрирани към системата мобилни терминали поделят един и същи ССК за групови повиквания по всяко време. Когато автентифицирана мобилен терминал направи заявка за групово повикване, инфраструктурата изпраща текущия ССК (потвърден с DCK) към абонатите, включени в груповото повикване. Мобилните терминали декриптират ССК, като използват собствената локална калкулация за DCK (от автентификацията) и използват ССК за криптиране и декриптиране на трафика от инфраструктурата. Базовата станция и мобилният терминал използват ССК, заедно с началната (offset) стойност, за криптиране и декриптиране на трафика помежду си. Системата всеки ден променя ССК.

#### **4. Защита идентификацията на абонатите**

За защита от несанкционирана идентификация на абонат чрез прихват на съобщения по радиоканала в стандарта TETRA се използват временни идентификационни номера на абонатите, които се ползват след първоначалната регистрация на абоната в мрежата с уникалния му идентификационен номер. При всяка следваща регистрация тези временни номера мога да бъдат

подменяни. Освен това, индивидуалният и временният номер се защитават допълнително по процедурите на шифриране на радиоинтерфейса. Процесът на осигуряване на скритост на абоната се поддържа и при преминаването му от клетка в клетка, като за целта служебния обмен между базова станция и мобилен терминал е чрез размяна на временни идентификационни номера на абонатите без възможност за установяване принадлежността им към конкретен абонат.

### **ЛИТЕРАТУРА:**

1. <http://www.etsi.org/index.php/technologies-clusters/technologies/tetra>
2. <http://www.tandcca.com/>
3. [http://www.tandcca.com/Library/Documents/About\\_TETRA/stdnrd\\_crptgrphy\\_algrth\\_ms\\_ed4.pdf](http://www.tandcca.com/Library/Documents/About_TETRA/stdnrd_crptgrphy_algrth_ms_ed4.pdf)

# ПСИХОФИЗИЧЕСКИ ОСНОВИ НА КЛАСИФИКАЦИЯТА НА СЕНЗОРИТЕ В СИГНАЛНО-ОХРАНИТЕЛНАТА ТЕХНИКА

Атанас К.Атанасов

## PSYCHOPHYSICAL BASICS OF THE CLASSIFICATION OF THE SENSORS IN THE PROTECTIVE SIGNALING INSTALLATION

Atanas K.Atanasov

**ABSTRACT:** *This report refers to the psychophysical characteristics of a person and his interaction with the environment. On that basis, an attempt was made for classification of the sensors used in the technical means of protection.*

**KEYWORDS:** *technical means of protection, sensors, psychophysical characteristics*

Решаването на задачите по осигуряване на безопасността на различните обекти все повече се опира на широкото използване на технически средства за охрана и сигнализация. Техническо средство за охрана, това е основно понятие с което се обозначава апаратура, използвана в състава на комплекс от технически средства използвани за охрана на обекти от несанкциониран достъп. То е предназначено за използване от охраната на обекта с цел повишаване на ефективността на откриване на нарушителите и осигуряване на контрол на достъпа до охраняемия обект.

При избор и внедряване на технически средства за охрана и сигнализация (ТСОС) на обектите, отделя се особено внимание на постигане на висока защитеност на апаратурата от нейното преодоляване. Производителите на ТСОС предлагат различни начини за реализация на тази задача: контрол на отваряне на различните блокове, автоматична проверка на изправността на средствата за откриване и на каналите за предаване на

информацията, защита на достъпа до управлението на апаратурата с помощта на кодове, архивиране на всички възникнали събития, защита на информационните потоци между съставните части на ТСОС чрез маскиране и шифриране и др. По принцип съвременните ТСОС имат едновременно няколко степени на защита.

Всяко средство за откриване, което е едно от основните части на ТСОС, се базира на определен физически принцип, на основата на който работи неговият чувствителен елемент. **Чувствителен елемент (сензор) - това е първичният преобразовател, който реагира на въздействието върху него от обекта на откриване (нарушителя) и възприемащ изменението на окръжаващата среда.**

При своето движение човекът- нарушител оставя множество различни следи на своето движение или местонахождение, които могат да бъдат фиксирани от различни прибори. Действително, човекът притежава напълно определени параметри като: геометрични размери, маса, температура на тялото, мирис, електрически биомеханични и биодинамични характеристики, скорост на движение, честота на крачката, инфрачервено излъчване и др.

При своето движение човек възбужда звукови и ултразвукови колебания в атмосферата и обкръжаващите го предмети, а също и сеизмически колебания в почвата и строителните конструкции. В процеса на изпълнение на едни или други действия човек оказва непосредствено силово въздействие върху предметите представляващи интерес за него, а също и динамическо въздействие върху електромагнитните и акустични полета, предизвиквайки нарушаване на тяхната пространствена структура.

Движението на човек предизвиква генериране на свръхнискочестотни електрически полета възникващи като следствие на пренасянето на индуцирания в резултат на триенето на обувките в пода и взаимното триене на частите на тялото и дрехите електростатичен заряд.

Освен това в процеса на физическата дейност си дейност човек излъчва електромагнитни сигнали в много широк спектър от

честоти, а дихателните органи и кръвообращението генерират акустични колебания. Потните жлези на човек отделят в обкръжаващата атмосфера продукти, в състава на които има десетки химически вещества, някои от които се явяват характерни само за човека. В процеса на проникване в помещение нарушителят отваря врати и прозорци, понякога е принуден да изрязва или избива стъкла, или да прави отвори в тавани на пода или стените. Вътре в помещението той премества предмети, части от обстановката, опитва се да отвори метални шкафове или сейфове, да фотографира документи или различни изделия. За да извърши тези действия той може да има при себе си фотоапаратура, различни инструменти, оръжие или взривни вещества. Посочените фактори притежават самостоятелни информативни характеристики, даващи възможност за откриване на присъствието на човека в охраняваното помещение, едновременно с това увеличавайки обема от информация за него. Намиращото се в нарушителя оръжие или инструменти притежават определени физически параметри и наличието им може да доведе до изменение на напрегнатостта на магнитното поле и честотата на облъчващия го свръхвисокочестотен сигнал. Използването на механичен инструмент за отваряне на врати и метални шкафове, разбиване на отвори в стените и подовите се съпровожда с възбуждането на характерни колебания и акустични вълни във въздушната среда на помещението.

При използване на газова горелка съществува топлинно излъчване на пламъка, изменя се температурата на подложения на въздействието от страна на нарушителя обект, появява се специфичният мирис на горивна смес, който както и при използване на взривни вещества води до изменение на химическия състав на въздуха.

По такъв начин появата на нарушител в охраняваното помещение може да бъде открито по голям брой физико-химически явления. Това откриване става с помощта на технически средства, построени на базата на най-различни принципи на регистрация на изменението на състоянието на средата. Основните типове чувствителни елементи

осъществяващи взаимодействие с външната среда и нарушителя могат да бъдат използвани за построение на системите за охрана.

Вероятността за откриване съществено зависи от тактико-техническите характеристики на сензорите, които са заложили в съответствие от условията за тяхното използване и вземайки в предвид нивото на необходимата защита и съответно необходимите разходи по изграждането на техническото средство за охрана за конкретния обект.

**Основата на комплекса от технически средства за охрана се състои от:**

- сензори;
- технически средства за наблюдение;
- система за събиране, обработка изобразяване и документиране на информацията;
- средства за контрол на достъпа;
- спомогателни средства и устройства.

Освен това при извънредни обстоятелства могат да бъдат използвани и специални средства за защита на информацията, претърсване за откриване на подслушвателна и техника за наблюдение, а също специални средства за откриване и обезвреждане на диверсионно-терористични средства. Много важно значение за безопасността на обекта има използването на средства за пожарна сигнализация.

По принцип в инженерната практика могат да бъдат класифицирани следните типове сензори:

-по начина на привеждане в действие сензорите се подразделят на автоматични и автоматизирани;

-по назначение сензорите се подразделят на такива за затворени помещения и такива за открити площадки и периметри на обектите;

- по вида на зоната контролирана от сензорите-точкови, линейни, повърхностни, обемни;

-по принципа на действие -механични, електромагнитни безконтактни, магнитометрични, капацитивни, индуктивни, хидроакустични, акустични, сеизмични, оптико-електронни, радиовълнови, радиолъчеви, олфактронни, комбинирани.

-според броя на зоните на откриване, създавани от сензорите се подразделят на еднозонни и многозонни;

-според разстоянието на действие ултразвуковите, оптико-електронните и радиовълновите се подразделят на такива с малък радиус на действие до 12 м, със среден радиус на действие -повече от 12 м-до 30 м; голям радиус на действие-повече от 30 м.;

- по разстояние на действие оптико-електронните и радиовълновите сензори за открити площадки и периметри на обектите, се подразделят на такива с малък радиус на действие -до 50 м., със среден радиус на действие -повече от 50 и до 200 м, с голям радиус на действие –повече от 200 м.

-според конструктивното изпълнение ултразвуковите, оптико-електронните и радиовълновите сензори се подразделят на- еднопозиционни -един или повече предаватели и приемникът са съвместени в един блок, двупозиционни-предавателят и приемникът са изпълнени като отделни блокове, многопозиционни- в повече от два блока;

Различните подходи за класифициране притежават определени недостатъци -недостатъчна пълнота, в различни класове съществуват едни и същи типове сензори, др.

Априорно е ясно че, изборът на конкретен сензор е свързано със съответствието на неговите тактико-технически характеристики с условията на използване. Това означава че сензор с определени тактико-технически характеристики може да се използва само при определени условия. Сензорът трябва да бъде поставен в такава среда, характеристиките на която в максимална степен удовлетворяват неговите възможности, определяни от тактико-техническите му характеристики. Ако няма такава възможност, то се разработва и се произвежда нов сензор, в тактико-техническите характеристики на който се задават изисквания удовлетворяващи условията на експлоатация, т.е. множество фактори, като -климатически, биологически, геологически, механични, електромагнитни полета и лъчения, акустични колебания, ниво на радиоактивност, ниво на осветеност, режими на работа на апаратурата, условия за електрозахранване, ниво на квалификация на обслужващия персонал, цена и др.



Изхождайки от едни или други фактори обуславящи използването на сензорите, интерес представляват следните основни тактико-технически характеристики:

- характеристики на зоната за откриване;
- вероятност за откриване с определен модел на нарушител;
- ниво на лъжливо сработване;
- чувствителност на сензорите;
- параметри на входните и изходни сигнали;
- горна и долна граница на скоростта на преместване на нарушителя;
- време за готовност на сензорите след включване на захранващото напрежение;
- време за възстановяване на дежурния режим след завършване на сигнала за сработване;
- изисквания към параметрите на електрозахранването;
- показатели за надеждност.

Общо взето в структурата на техническите средства за охрана може да се отбележи наличието на три основни компонента:

- средства за откриване(сензори);
- линии за предаване на сигналите за тревога;
- блокове за индикация, регистрация и обработка на получения сигнал.

Освен това съществуват и спомагателни средства -блокове на резервно захранване, средства за говорна комуникация, пряка телефонна линия за връзка с полицията и др.

Съществуват различни подходи за класификация на сигнално-охранителните системи, като се имат в предвид тяхната структура, назначение, физическите принципи на действие на използваните сензори, типовете и схемите на линиите за предаване на сигналната информация, и редица други характеристики.

При избор на сензор за конкретна сигнално-охранителна система определящи са тактико-техническите характеристики на сензорите, предвидени за използване. За особено важни обекти е желателно вероятността за откриване да бъде близка до 0,98, а наработката до лъжливо сработване да е в границите на 2500-3500 часа.

# СИНТЕЗ И АНАЛИЗ НА 5-ЛЕНТОВ ЦИФРОВ ЕКВАЛАЙЗЕР

Тихомир С. Трифонов

## DESIGN AND ANALYSIS OF 5-BAND DIGITAL EQUALIZER

Tihomir S. Trifonov

**ABSTRACT:** *A method for design and analysis of 5-band graphic digital equalizer is presented in this paper. The method is based on the properties of the classic analogue schematic using operational amplifiers. The designed equalizer can be implemented in a digital signal processor or it can be used as a part of a sound processing subsystem in an every sound playing device.*

**KEY WORDS:** *Graphic Equalizer, Digital Signal Processing, Frequency Response, Phase Response, Gain, Attenuation, Quality Factor, Digital Filter, Pass-band Filter.*

### Въведение

Еквалайзерът представлява устройство, използвано в системите за обработка и възпроизвеждане на звук, предназначено за корекция на амплитудно-честотната характеристика (АЧХ) на звуковия канал. Необходимостта от корекция на АЧХ се дължи на следните фактори:

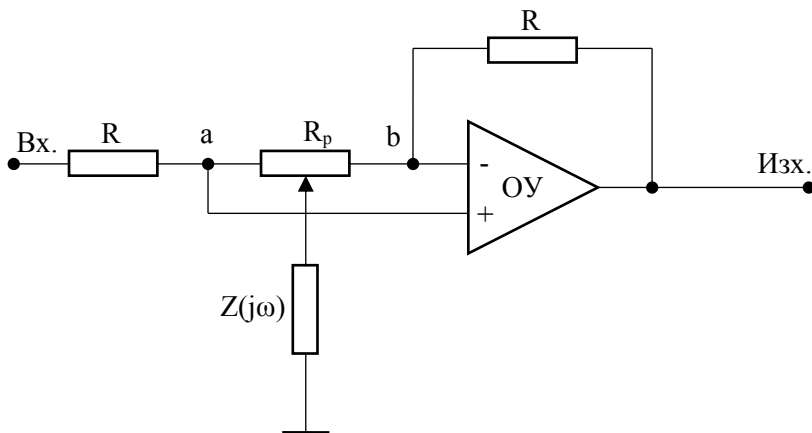
- неравномерна чувствителност на човешкия слух в звуковия честотен диапазон;
- неравномерна честотна характеристика на високоговорителите и озвучителните тела;
- влияние на акустичните свойства на помещението върху характеристиките на възпроизвеждащата система;
- индивидуални субективни предпочитания на слушателя.

Тъй като чувствителността на човешкия слух е по-ниска в областта на ниските и високите честоти, най-често в практиката се използват тонкоректори с възможност за повдигане на нивата на НЧ и ВЧ сигналите с цел компенсация и по-добро възприятие на звуковата картина. В повечето случаи предварително заложените характеристики на тонкоректорите не могат да компенсират точно неравномерностите на честотните характеристики на отделните компоненти на звуковата система. Еквалайзерът всъщност представлява тонкоректор, но с по-големи възможности за настройка на АЧХ. Най-често използваните еквалайзери биват параметрични и графични. Параметричният еквалайзер представлява комбинация от филтри с възможност за регулиране на нивата на повдигане (потискане) на всеки филтър, както и на неговата срязваща честота. Крайната АЧХ се получава чрез сумиране на отделните АЧХ на филтрите. По-големи възможности за настройка имат графичните еквалайзери, при които целият звуков диапазон е разбит на няколко честотни ленти, които могат да се регулират по ниво. Наименованието „графичен еквалайзер“ произлиза от факта, че най-често регулировката на нивата на класически аналогов еквалайзер се осъществява чрез линейни потенциометри, подредени вертикално, като техните органи за управление описват графика по честотната ос. В аналогово изпълнение многолентовите еквалайзери представляват сравнително несложни схеми, но с много голям брой дискретни елементи (резистори, кондензатори, бобини, операционни усилватели, потенциометри и др.). Освен това, точността на честотните свойства зависи от толерансите на пасивните компоненти, които особено за кондензатори и бобини са големи ( $> \pm 10\%$ ) и, следователно, за направата на качествен аналогов многолентов еквалайзер се изисква подбор на компоненти. В съвременните системи за възпроизвеждане на звук, където се използва цифрова обработка на сигналите, тонкорекцията най-често се реализира като алгоритъм в дискретната област и сигналите на изходите на цифрово-аналоговите преобразуватели (ЦАП) вече са коригирани. По такъв начин с малко усложняване на алгоритъма за обработка на сигнала могат да се реализират не само тонкоректори за ниски и високи честоти, но и параметрични

или графични еквалайзери с повече ленти. В настоящата публикация се предлага вариант за разработка на цифров графичен еквалайзер с пет ленти. Методът може да се използва и при разработката на еквалайзер с повече ленти.

## 1. Основна схема на аналогов графичен еквалайзер

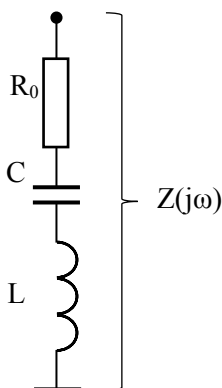
Като основа при разработката на цифровия еквалайзер е използвана класическа схема на аналогов еквалайзер на базата на операционен усилвател, потенциометри и последователни RLC резонансни вериги [1]. При стерео изпълнение е необходима още една такава схема за другия канал.



Фиг. 1. Основна схема на графичен еквалайзер

На Фигура 1 е показана основната схема на графичен еквалайзер. Честотно зависимото съпротивление  $Z(j\omega)$  определя централната честота на еквалайзера. Импедансът на  $Z(j\omega)$  трябва да бъде нисък за централната честота и висок за останалите честоти. Ако  $Z(j\omega)$  се замени с късо съединение, се вижда, че лявата част на потенциометъра  $R_p$  образува атенюатор, през който входният сигнал се подава към неинвертиращия вход на операционния усилвател, чието усиление се определя от дясната половина на  $R_p$ . Ако  $Z(j\omega)$  се замени с отворена верига,  $R_p$  е свързан само между двата входа на ОУ, които са с еднакъв потенциал и на

практика  $R_p$  не участва във веригата. Чрез включване на повече от една верига потенциометър- $Z(j\omega)$  паралелно между точките а и b, могат да се реализират много честотни ленти. За всяка от тях плъзгачът на потенциометъра трябва да бъде свързан към различно съпротивление  $Z(j\omega)$ . Поставянето на плъзгача на потенциометъра в средно положение определя коефициент на усилване на схемата, равно на единица. В крайно ляво положение се получава максимално затихване, а в крайно дясно – максимално повдигане на сигналите за дадената честотна лента. Честотно определящото съпротивление  $Z(j\omega)$  представлява или последователна RCL верига (Фиг. 2) или т. нар. жиратор.



Фиг. 2. Последователна RCL верига

За последователната RCL верига  $Z(j\omega) = R_0 + j(X_L - X_C)$ , където  $X_L = \omega L$ , а  $X_C = \frac{1}{\omega C}$ . При резонанс  $X_L = X_C$  и  $Z(j\omega_0) = R$ . Централната честота за всяка лента се определя от стойностите на кондензатора и бобината  $f_0 = \frac{1}{2\pi\sqrt{LC}}$ , а ширината на честотната лента зависи от качествения фактор (Q- фактора) на веригата  $Q = \frac{1}{R_0} \sqrt{\frac{L}{C}}$ .

Коефициентът на усилване на схемата от Фиг. 1 за централната честота на лентата се определя от съотношенията между съпротивления на резисторите  $R$ ,  $R_0$  и на потенциометъра  $R_p$ :

$$A_U = \frac{U_{изх}}{U_{вх}} = \frac{(R + (1 - \beta)R_p)\beta R_p}{(R + \beta R_p)(1 - \beta)R_p}, \quad \alpha \leq \beta \leq (1 - \alpha), \quad \alpha = \frac{R_0}{R_p}.$$

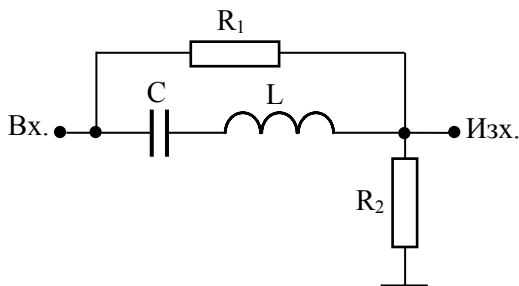
Основен недостатък на използването на RCL верига в качеството на честотно зависимо съпротивление е трудността при изработката на бобините за всяка от лентите. Техните индуктивности, особено за ниски честоти, се получават от порядъка на няколко милихенри, което означава много голям брой навивки. Друга голяма трудност при реализация на схемата е, че при необходимост от промяна на Q-фактора на веригата трябва едновременно да се променят стойностите и на капацитета на кондензатора, и на индуктивността на бобината. При голям брой на лентите анализът на схемата с цел получаване на еквивалентната ѝ АЧХ, която всъщност представлява интерес, е много труден. Задачата на анализа още повече се усложнява, ако е необходимо да се изследва АЧХ на еквайзера при различни положения на потенциометрите. Ето защо в настоящата статия се предлага възможност за използване на характеристиките на схемата от Фиг. 1 за реализация на еквайзер чрез използване на средствата на цифровата обработка на сигналите.

## 2. Синтез на цифров еквайзер

При синтеза на цифров еквайзер са използвани цифрови лентови филтри и регулатори на усилването за всеки от филтрите. При проектиране на филтрите се цели получаване на амплитудно-честотни характеристики, близки до тези на схемата от Фиг. 1, тъй като тя се е доказала в областта на аналоговата схемотехника. Проектирането на цифров филтър с характеристики като на аналогов по принцип е възможно, но само за рекурсивните филтри. Освен това съществува и аналогия между реда на цифровия филтър и броя на реактивните елементи в електрическата верига на аналоговата схема. В случая всеки филтър трябва да бъде

лентов от втори ред. С цел опростяване на анализа на аналоговия еквалайзер се изследва пасивна схема (Фиг. 3) със същата форма на АЧХ, както на схемата от Фиг. 1, състояща се от една лента и потенциометър, поставен на максимално усилване.

Фиг. 3. Схема на аналогов лентов резонансен филтър



Тъй като схемата е пасивна, тя може да внася само затихване. Коефициентът на предаване на схемата за централната (резонансната честота) е единица  $A(f_0) = 1$ , а за честоти, клонящи към нула и към безкрайност, е  $A(f_0 \rightarrow 0, f_0 \rightarrow \infty) = \frac{R_2}{R_1 + R_2}$ .

Затихването, което внася схемата, може да се компенсира чрез усилвател с коефициент на усилване  $K = \frac{R_1 + R_2}{R_2}$ . Например, ако  $R_1 = 3,3k\Omega$ ;  $R_2 = 1k\Omega$ , затихването ще бъде равно на  $A(f \rightarrow 0, f \rightarrow \infty) = 0,2326$ . По формулата за затихване в dB се получава  $N_A = 20 \lg(0,2326) = -12,67dB$ .

Централната честота на филтъра ще съвпада с резонансната, т.е  $f_0 = \frac{1}{2\pi\sqrt{LC}}$ . Качественият фактор Q, от който зависи

широчината на честотната лента, се определя по формулата  $Q = \frac{1}{R_{екв}} \sqrt{\frac{L}{C}}$ ,

$$\text{където } R_{екв} = \frac{R_1 R_2}{R_1 + R_2}$$

Тъй като  $R_1$  и  $R_2$  вече са зададени, за  $R_{екв}$  се получава  $R_{екв} = 767,44\Omega$ . Следователно, ако се задават стойности на  $f_0$  и  $Q$ , ще трябва да се изчислят стойностите на капацитета  $C$  и индуктивността  $L$ . Решавайки системата уравнения спрямо  $L$  и  $C$ , се получава:  $L = \frac{QR_{екв}}{2\pi f_0}$ ,  $C = \frac{1}{2\pi f_0 QR_{екв}}$ .

Чрез специално разработена програма на MATLAB се изследва АЧХ на филтъра и се търси цифров филтър с максимално близка характеристика.

### **Програма за синтез на цифров филтър:**

```
clear all;close all;pause(.5);
n=1:.005:log10(24000);
f=10.^n;
f0=200;
Q1=9;
w=2*pi*f;
R1=3300;R2=1000;Re=(R1*R2)/(R1+R2);
C=1./(f0*2*pi*Q1*Re);L=(Q1*Re)./(f0*2*pi);
XL=w*L;XC=1./(w.*C);
Z=j*XL-j*XC;
ZR=(R1.*Z)./(R1+Z);
K=R2./(ZR+R2);
K1=abs(K);KL=20*log10(K1);
Q=sqrt(L./C)/(Re);
semilogx(f,KL+12.6694);title(['Q= ',num2str(Q)]);pause(.5);
sss=5000;p=1;
for i=1:675,
    f1=f(i);
    for j=i+2:677,
        f2=f(j);
        [b,a]=butter(1,[f1/24000 f2/24000],'bandpass');
        H=freqz(b,a,f,48000);H1=20*log10(abs(H*(1-
        .2326)+.2326)));
        err=sum((H1-KL).^2);
```

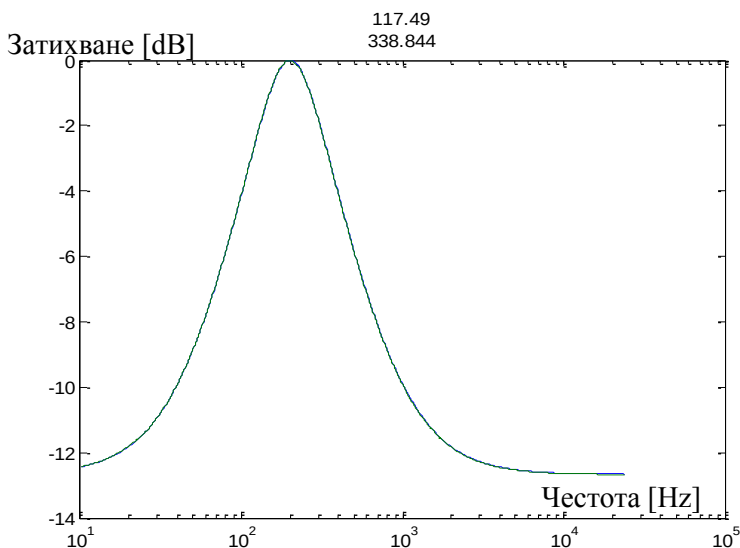


```

    if err<sss,
        sss=err;
        xx(1,:)=b;
        xx(2,:)=a;
        p=p+1;
        semilogx(f,KL,f,H1);title([f1 f2]);
        pause(.01);
    end
end
end

```

Експериментът доказва, че цифров лентов филтър на Батървурт от втори ред при подходящо подобрени срязващи честоти  $f_{c1}$  и  $f_{c2}$  и с известна адаптация поради разликата в затихванията, напълно съпада по АЧХ с аналоговия (Фиг. 4).



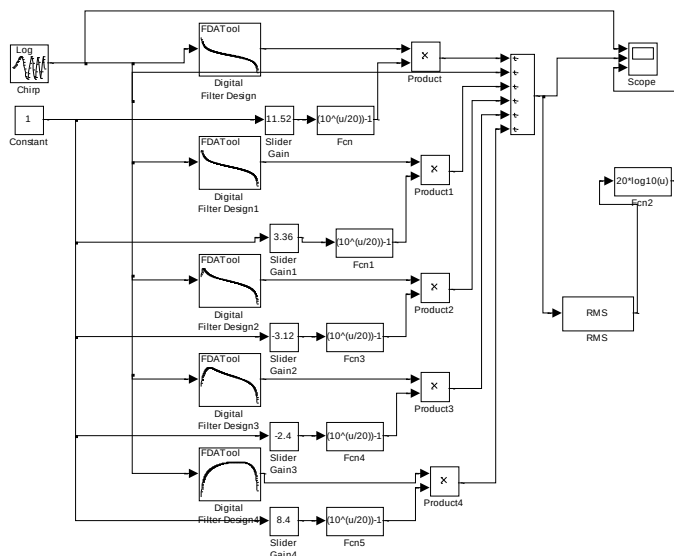
Фиг. 4. АЧХ на аналоговия и на цифровия филтър

По такъв начин дизайнът на цифровия еквайзер се свежда до проектиране на цифровите филтри чрез задаване на централните честоти и Q-фактора. Централните честоти се избират през равни коефициенти, така че да покриват желания честотен

диапазон. Например, в автомобилните медия плейъри на фирмата Pioneer от сериите DEH-1500UB, DEH-1600UB, MVH-150, MVH-160, MVH-170 се използва вграден 5-лентов еквалайзер с централни честоти 80; 250; 800; 2,5k и 8k Hz. Тези честоти, дори и с по-широки ленти на пропускане на филтрите, не биха могли да покрият целия звуков диапазон за качествено възпроизвеждане. На базата на експерименти при разработката на еквалайзера са избрани следните централни честоти: 50; 200; 800; 3,2k и 12,8k Hz. Разликата между честотите е 2 октави (4 пъти). Друг възможен вариант на разпределение на централните честоти е: 63; 250; 1k; 4k и 16k Hz, също през 2 октави.

Друг важен параметър е Q-факторът. От него зависи широчината на честотната лента на всеки филтър. При разработката на филтрите се използва един и същ Q-фактор за всички филтри. При тесни ленти се получават големи неравномерности в АЧХ на еквалайзера, а при широки ленти – значително застъпване между съседните честоти и обезсмисляне на повечето ленти. Експериментално е установено, че добри резултати за конкретния случай се получават при стойности на Q в интервала от 0,8 до 1. На Фиг. 5 е показан симулационният модел на еквалайзера в MATLAB Simulink. Конкретната конфигурация е за тестване на АЧХ на еквалайзера чрез сигнал с логаритмично изменение на честотата. На третия канал на осцилоскопа се наблюдава зависимостта на амплитудата на изхода, преизчислена в dB. Показаният симулационен модел лесно може да се тества с музикален файл, като изходният цифров сигнал се подава на звуковата карта на компютъра. Така в реално време могат да се настройват нивата на отделните честотни ленти и да се прослушва крайният резултат.

Моделът съдържа пет цифрови лентови филтъра на Батървурт с безкрайна импулсна характеристика от втори ред. Освен това съдържа плъзгачи, чрез които се задават нивата в dB, и блокове, в които се преизчисляват нивата в коефициенти на усиление. Преминалите през филтрите сигнали се умножават по коефициентите, сумират се с входния сигнал и така се формира изходният.



Фиг. 5 Симулационен модел на 5-лентов еквайзер.

## Заклучение

Предложеният модел може да се реализира чрез цифров сигнален процесор с цел получаване на относително самостоятелно устройство. Също така алгоритъмът може да се използва за подобряване на възможностите за честотни корекции на звука в различни цифрови възпроизвеждащи устройства (медия плейъри, музикални уредби, мобилни устройства и др.).

## **ЛИТЕРАТУРА**

1. [http://mysite.mweb.co.za/residents/cyb00746/audiodocs/Analog\\_EQ.htm](http://mysite.mweb.co.za/residents/cyb00746/audiodocs/Analog_EQ.htm)
2. Дьяконов В., Абраменкова И. MATLAB обработка сигналов и изображений. Специальный справочник. Питер, 2002 г.

# ПРИБОР ЗА ИЗМЕРВАНЕ НА АМПЛИТУДНО ЧЕСТОТНИ ХАРАКТЕРИСТИКИ ЧРЕЗ ПЕРСОНАЛЕН КОМПЮТЪР

РУМЕН Г. ЦАКОВ

## DEVICES FOR MEASURING OF MAGNITUDE FREQUENCY RESPONSE VIA PC

RUMEN G. TSAKOV

**ABSTRACT:** *The use of generators with direct digital synthesis Direct Digital Synthesizer (DDS) allows you to create a new generation of generators with high frequency stability and readjustment of parts of hertz to several gigahertz. On the basis of DDS was developed instrument designed to measure and monitor in real time on a computer screen the magnitude frequency response (MFR) of different quadripoles and components at frequencies between 100 kHz and 70 MHz.*

**KEYWORDS:** *Direct Digital Synthesizer (DDS), MFR, filters.*

Важна характеристика за много устройства и компоненти (усилватели, RC филтри, LC филтри, кварцови филтри, резонатори и др.) е тяхната амплитудно честотната характеристика (АЧХ). Това е зависимостта на модула на коефициента на предаване на тестираното устройство или компонента от честотата. В последно време получиха развитие нов клас устройства – така наречените векторно мрежови анализатори, които позволяват да се снее АЧХ в комплексна форма или във вид на модул от коефициента на предаване и фазовото изместване от честотата[1].

Използването на генератори с директен цифров синтез (Direct Digital Synthesizer (DDS), позволява да се създаде ново поколение генератори с висока честотна стабилност и пренастройка от части на херца до няколко гигахерца.

На основата на DDS бе изработен прибор предназначен за измерване и наблюдение в реално време на екрана на компютър АЧХ на различни четириполусниции компоненти на честоти между 100 KHz и 70 MHz. Функционалната и принципната [3] схема на прибора са показани на фигури 1 и 2.

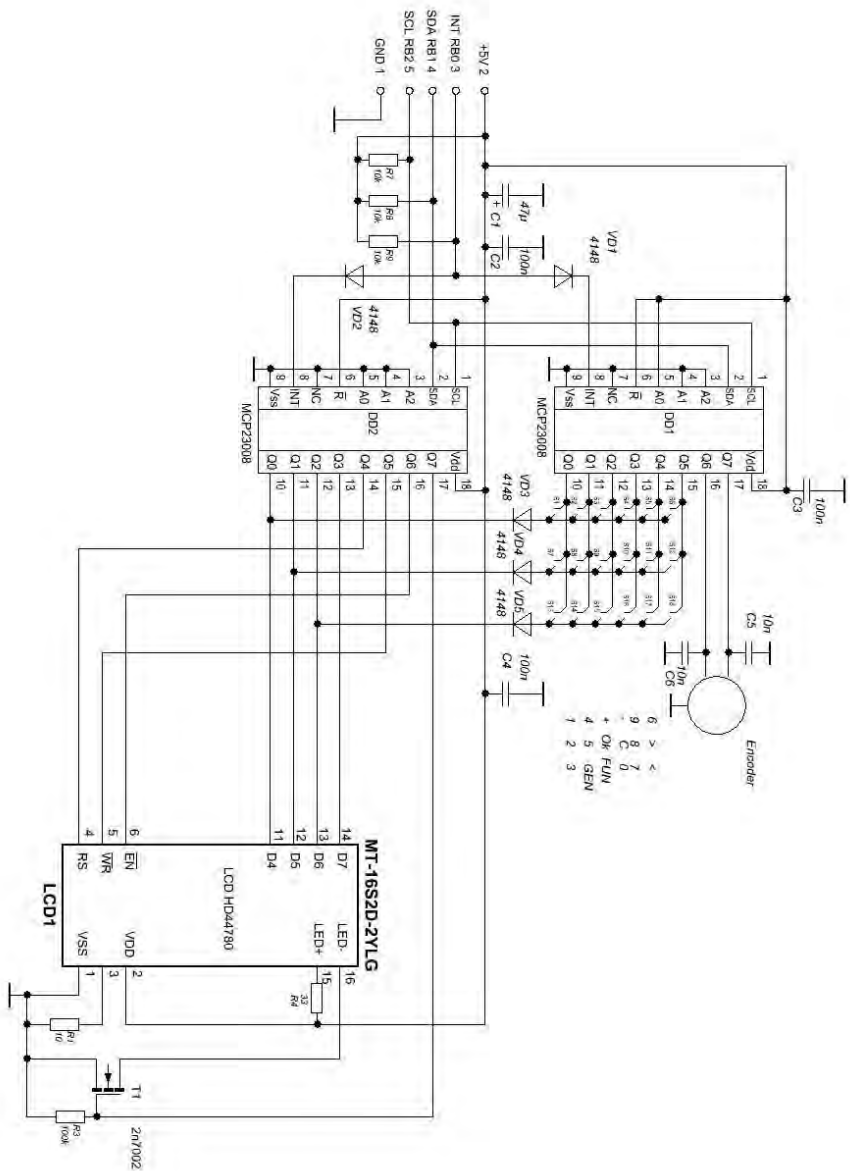
**Фиг. 1. Функционална схема**



За управление на прибора се използва програмния продукт WinNWT. Изходната честота на AD9851 се задава програмно от компютъра. Този сигнал се подава на изследваното устройство. Информацията за управление на прибора постъпва от персоналния компютър чрез USB конвертора FT232RL и галваничното развързване с интегрална схема ADUM1201 в микроконтролера PIC2525. Той обработва приетите команди, преобразува ги във формат DDS и ги предава на AD9851. От изследваното устройство чрез логаритмичен или линеен детектор сигналът се подава на аналогово цифрови преобразователи в микроконтролера PIC2525. От тук сигналът постъпва обратно в персоналния компютър, където става обработка на сигнала и изобразяване на информацията върху екрана на компютъра.

При отсъствие на персонален компютър приборът може да работи автономно, като за целта е добавена платка (фиг.3) с двуреден индикатор, бутони и енкодер, които позволяват да се работи с прибора автономно без използване компютър. Допълнителната платка работи по протокол I2C и се включва към свободните изводи на микроконтролера на основната платка[3].





При съвместна работа с персонален компютър приборът може да работи като:

- Генератор на люлееща се честота (sweep generator);
- Хетеродин с отчитане изместването по междинна честота;
- Измерител на мощност с протоколиране на резултатите

от измерването.

При автономна работа приборът може да работи като:

- генератор на сигнали;
- Измерител на мощност;
- Измерител на коефициента на стояща вълна (КСВ);
- Измерител на импеданс.

## **Технически характеристики**

### **1. Параметри на генератора с AD9851:**

- Честотен диапазон от 50 KHz до 70 MHz при неравномерност не повече от 3dB;
- Стъпка за пренастройка на честота 1 Гц;
- Затихването на вътрешния атенюатор е от 0 до -50dB със стъпка 10dB;
- Ниво на изходния сигнал +13 дБм;
- Изходно съпротивление 50 ома.

### **2. Режим измерване на АЧХ при използване на програмен продукт WinNWT:**

- Честотен диапазон от 25 KHz до 90 MHz при неравномерност не повече от 4dB;
- Динамичен диапазон от 80 dB до 90dB;
- Неравномерност на измерването в диапазона от 0 до -80dB не повече от 4 dB.

### **3. Режим измерване на нивото на сигнала - Логаритмичен детектор:**

- Динамичен диапазон от -75 dBm до +16dBm;
- Честотен диапазон до 400 MHz;
- Входно съпротивление 50 ома.

4. Режим измерване на нивото на сигнала - Линеен детектор:

- Динамичен диапазон от -20 dBm до +10dBm;
- Честотен диапазон до 2000 MHz;
- Входно съпротивление 50 ома.

5. Режим измерване на КСВ:

- Честотен диапазон от 200 KHz до 70 MHz;
- точност +/- 0,2 при КСВ до 2х;
- точност +/- 0,3 при КСВ повече от 2х;
- Калибровката на измерителя на КСВ става по 350 точки.

6. Измерване на импеданс:

- Честотен диапазон от 200 KHz до 70 MHz;
- Точността зависи от точността на измерване на КСВ.

На фиг.4 е показан външният вид на прибора заедно с ПК при изследване на АЧХ на елементарен трептящ кръг. На фиг.5 и 6 е показан същият прибор със свален горен капак.



**Фиг.4** Външен вид на прибора заедно с ПК.



**Фиг. 5. Изглед на прибора със свален горен капак**



**Фиг. 6. Изглед на прибора със свален горен капак**

## **ЛИТЕРАТУРА:**

1. Дьяконов В. П. Построитель АЧХ осциллограф или анализатор спектра.
2. [http://www.kit-e.ru/articles/oscillograph/2010\\_12\\_159.php](http://www.kit-e.ru/articles/oscillograph/2010_12_159.php)
3. Sobol Home Site - UB3TAF <http://www.asobol.ru/>

# КОМПЮТЪРНА ДИДАКТИЧНА ПРОГРАМА ЗА КОД НА ХЕМИНГ

Цветослав С. Цанков, Доника В. Диманова

## COMPUTER DIDACTIC TOOL FOR HAMMING CODE

Tsvetoslav S. Tsankov, Donika V. Dimanova

**ABSTRACT:** *The training in universities and secondary schools underwent major changes dictated by the current state of technology and the interests of the students. In the proposed tool for training is provided theory of the training material submitted with attracting interest.*

**KEY WORDS:** *Computer didactic tool, Hamming code, Teach Yourself, Learning through play*

### Въведение

В съвременните условия на живот е все по-неподходящо преподаването на учебния материал по класическите методи в учебните заведения. Черната/бялата дъска в редица уроци/лекции се заменя с интерактивни дъски или просто с екран и прожекционен апарат. Представени в слайдове, лекциите имат стегнат и приятен вид: схемите са начертани безупречно, текста е лесно четим, могат да се използват много допълнителни мултимедийни възможности. При използването на тези предимства е малка вероятността за отклоняване на вниманието или загубата на интерес от студентите към учебния материал.

В търсене на нови и интересни дидактични материали, в настоящия доклад е представен кодът на Хеминг за единична грешка. Теорията по извеждане на правила е преплетена със своеобразна игра, ангажираща вниманието на обучаемите.

След натрупването на достатъчен брой подобни дидактични материали следва да се проведе педагогическо изследване с изследователски метод – педагогически експеримент.

### *Теоретична обосновка*

Кодът на Хеминг е един от най-известните систематични кодове за коригиране на единични грешки и има минимално кодово разстояние  $d_{min}=3$  (това е броят на разрядите, по които се различават две последователни разрешени кодови комбинации). Кодът на Хеминг се строи по такъв начин, че към началните информационни разряди се добавят известен брой контролни разряди, които се формират преди предаване на информацията на базата на определяне на четността на сумата на единиците в съответни групи информационни разряди [1, 3].

След приемане на информацията контролната апаратура образува от получените информационни и контролни разряди т.нар. коригиращо число на базата на аналогично преброяване на единиците. При липса на грешка коригиращото число е равно на нула. При грешка стойността му посочва мястото на грешката – двоичния номер на грешния разряд в думата. Грешният разряд автоматично се коригира чрез инвертиране на стойността му.

Ако кодовата дума не съдържа грешки, коригиращото число трябва да бъде равно на нула. Ако в младшия разряд на коригиращото число се появи единица, това означава, че има грешка в един от тези разряди на думата, поредните номера на които в двоичното си представяне имат единица в младшия разряд (това са всички нечетни номера) [2, 4].

Въвежда се първият контролен разряд и му се присвоява нечетен пореден номер. Този контролен разряд се получава чрез сумиране по модул 2 на всички нечетни разряди. Тази сума трябва да бъде равна на нула. Описаната операция може да се запише по следния начин:

$$E_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{11} \oplus a_{13} \oplus a_{15} \oplus \dots = 0, \quad (1)$$

където  $a_1, a_3, a_5, a_7, a_9, a_{11}, a_{13}, a_{15}, \dots$  са двоични стойности, записани в разрядите с поредни номера 1, 3, 5, 7, 9, 11, 13, 15 и т.н.

Появата на единица във втория разряд на контролното (коригиращото) число означава грешка в онези разряди на думата, чиито поредни номера в двоичното си представяне имат единици във втория разряд (отдясно наляво). Това са номерата от вида 2, 3,

6, 7, 10, 11, 14, 15, ... . Така се въвежда вторият контролен разряд, който се получава чрез сумиране по модул 2 на съответните разряди:

$$E_2 = a_2 \oplus a_3 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} \oplus a_{14} \oplus a_{15} \oplus \dots = 0 \quad (2)$$

От аналогични разсъждения се получават и останалите необходими контролни разряди чрез изпълнение на операциите:

$$E_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_{12} \oplus a_{13} \oplus a_{14} \oplus a_{15} \oplus \dots = 0, \quad (3)$$

$$E_4 = a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{13} \oplus a_{14} \oplus a_{15} \oplus \dots = 0 \quad (4)$$

...

След предаване и приемане на кодовата дума (заедно с формираните контролни разряди) се изпълняват същите операции за преброяване, с чиято помощ се получени контролните разряди. Образуваното число  $E = E_k.E_{k-1} \dots E_3.E_2.E_1$  се нарича коригиращо число.

Когато при предаването не е била открита грешка. При наличие на грешка няма да бъдат равни на нула онези негови разряди (суми)  $E_i$ , в образуването на които е участвал грешният разряд.

Мястото на контролните разряди във всяка от групите се определя по такъв начин, че контролните разряди да участват само веднъж в операциите по определяне на четността. Така процесът на кодирането се опростява. Ако се разгледат изразите за  $E_1$ ,  $E_2$ , ... се забелязва, че такива позиции са разрядите с номера, представляващи цели степени на числото две, т.е. 1, 2, 4, 8, 16, ... .

Следва да се определи броят на контролните разряди:

$$k = n - m, \quad (5)$$

където  $n$  е дължината на кодовата дума, а  $m$  е броят на информационните битове. Коригиращото число с дължина  $k$  разряда може да опише  $2k$  състояния, които съответстват на отсъствие на грешка и на поява на грешка в  $i$ -тия разряд. Следователно трябва да е изпълнено условието:



$$2^k > n + 1, \quad (6)$$

откъдето може да се изведе Таблица 1:

**Таблица 1:** Брой на контролните разряди в кода на Хеминг

| Диапазон на $m$ | $k_{\min}$ |
|-----------------|------------|
| 1               | 2          |
| 2 – 4           | 3          |
| 5 – 11          | 4          |
| 12 – 26         | 5          |
| 27 – 57         | 6          |

**Компютърна дидактична програма за код на Хеминг за  
единична грешка**

Изготвянето на нагледна дидактична програма е нелека задача и често пъти не може да се изпълни целта на преподавателя за по-лесно усвояване на учебния материал. Изготвянето на настоящата дидактична програма е в табличен вид, т. к. възприемането на информацията е значително по-улеснено в графичен и табличен вид, отколкото в описателен текст.

При спазване на всички условия от теоретичната част на настоящия доклад се построява таблица, поясняваща кода на Хеминг за дума с 11 информационни символа. Като се има предвид Таблица 1 и формула 6, се определя броя на контролните разряди – в този случай могат да бъдат 4.

На Фиг. 1 е даден общият вид на дидактичната програма, онагледяващо кода на Хеминг за единична грешка с 11 ( $I_1 - I_{11}$ ) информационни и 4 ( $P_1 - P_4$ ) проверочни разряда.

Формулите в таблицата са скрити при работа в потребителски режим. След няколко примерни упражнения с таблицата може да се отключи до режим на „разузнаване“.

За още по-лесно възприемане са оцветени клетки, които са съпоставими едни с други в еднакви цветове и със съответната индикация. Нанесени са номерата на всички битове и са изнесени и в двоична бройна система. Инициирани са информационни и проверочни битове с техните номера.

|    | A                                                | B     | C     | D     | E     | F     | G     | H     | I     | J     | K        | L        | M        | N        | O        | P        |
|----|--------------------------------------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|----------|----------|----------|
| 1  | Код на Хеминг за дума с 11 информационни символа |       |       |       |       |       |       |       |       |       |          |          |          |          |          |          |
| 2  | бит №                                            | 1     | 2     | 3     | 4     | 5     | 6     | 7     | 8     | 9     | 10       | 11       | 12       | 13       | 14       | 15       |
| 3  | бит в двоична                                    | 0001  | 0010  | 0011  | 0100  | 0101  | 0110  | 0111  | 1000  | 1001  | 1010     | 1011     | 1100     | 1101     | 1110     | 1111     |
| 4  | проверочен/информационен                         | $P_1$ | $P_2$ | $I_3$ | $P_4$ | $I_5$ | $I_6$ | $I_7$ | $P_8$ | $I_9$ | $I_{10}$ | $I_{11}$ | $I_{12}$ | $I_{13}$ | $I_{14}$ | $I_{15}$ |
| 5  | за $P_1$                                         | 0     |       | 0     |       | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |
| 6  | за $P_2$                                         |       | 0     | 0     |       | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |
| 7  | за $P_3$                                         |       |       | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |
| 8  | за $P_4$                                         |       |       | 0     |       | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |
| 9  | кодова дума                                      | 0     | 0     |       | 0     |       |       |       | 0     |       |          |          |          |          |          |          |
| 10 | кодвата дума с единична грешка                   | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |
| 11 | бит в двоична                                    | 0001  | 0010  | 0011  | 0100  | 0101  | 0110  | 0111  | 1000  | 1001  | 1010     | 1011     | 1100     | 1101     | 1110     | 1111     |
| 12 | проверочен/информационен                         | $P_1$ | $P_2$ | $I_3$ | $P_4$ | $I_5$ | $I_6$ | $I_7$ | $P_8$ | $I_9$ | $I_{10}$ | $I_{11}$ | $I_{12}$ | $I_{13}$ | $I_{14}$ | $I_{15}$ |
| 13 | 0                                                | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |
| 14 | 0                                                | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |
| 15 | 0                                                | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |
| 16 | 0                                                | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        | 0        | 0        | 0        | 0        |

**Фиг. 1:** Код на Хеминг за дума с 11 информационни символа

Първият проверочен разряд се получава от (1) при сумиране по модул 2 на всички нечетни разряди:

$$P_1 = \text{MOD}(D5 + F5 + H5 + J5 + L5 + N5 + P5; 2)$$

За получаване на втория проверочен бит при спазване на (2) се сумират битове 2 през 2 (проверочния се прехвърля от другата страна на равенството):

$$P_2 = \text{MOD}(D6 + G6 + H6 + K6 + L6 + O6 + P6; 2)$$

Съответно за третия проверочен бит при спазване на (3) се сумират битове 4 през 4 (проверочния се прехвърля от другата страна на равенството):

$$P_3 = \text{MOD}(F7 + G7 + H7 + M7 + N7 + O7 + P7; 2)$$

По (4) се сумират информационните битове от  $I_5$  до  $I_{11}$ , като също проверочния от осмorkата битове е прехвърлен отляво на равенството:

$$P_4 = \text{MOD}(\text{SUM}(J8:P8); 2)$$

Коригиращото число  $E$  се получава в инвертиран вид на редовете 13, 14, 15, и 16 по формулите (1), (2), (3) и (4) при съответните суми по модул 2:

$$E1 = \text{MOD}(B13 + D13 + F13 + H13 + J13 + L13 + N13 + P13; 2)$$

$$E2 = \text{MOD}(C14 + D14 + G14 + H14 + K14 + L14 + O14 + P14; 2)$$

$$E3 = \text{MOD}(E15 + F15 + G15 + H15 + M15 + N15 + O15 + P15; 2)$$

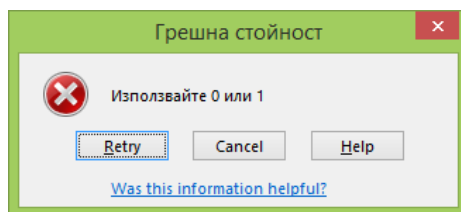
$$E4 = \text{MOD}(\text{SUM}(I16:P16); 2)$$

При първоначална работа с таблицата в потребителски режим се използват упътванията на триколюрния панел вдясно на таблицата (Фиг. 2):

| Код на Хеминг за дума с 11 информационни символа |       |       |       |       |       |       |       |       |       |       |       |       |       |          |          |
|--------------------------------------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|
| Бит №                                            | 1     | 2     | 3     | 4     | 5     | 6     | 7     | 8     | 9     | 10    | 11    | 12    | 13    | 14       | 15       |
| бит в двоична                                    | 0001  | 0010  | 0011  | 0100  | 0101  | 0110  | 0111  | 1000  | 1001  | 1010  | 1011  | 1100  | 1101  | 1110     | 1111     |
| проверочен/информационен                         | $P_1$ | $P_2$ | $I_1$ | $P_3$ | $I_2$ | $I_3$ | $I_4$ | $P_4$ | $I_5$ | $I_6$ | $I_7$ | $I_8$ | $I_9$ | $I_{10}$ | $I_{11}$ |
| за $P_1$                                         | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| за $P_2$                                         | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| за $P_3$                                         | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| за $P_4$                                         | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| кодова дума                                      | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| кодвата дума с единична грешка                   | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| бит в двоична                                    | 0001  | 0010  | 0011  | 0100  | 0101  | 0110  | 0111  | 1000  | 1001  | 1010  | 1011  | 1100  | 1101  | 1110     | 1111     |
| проверочен/информационен                         | $P_1$ | $P_2$ | $I_1$ | $P_3$ | $I_2$ | $I_3$ | $I_4$ | $P_4$ | $I_5$ | $I_6$ | $I_7$ | $I_8$ | $I_9$ | $I_{10}$ | $I_{11}$ |
| 0                                                | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| 0                                                | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| 0                                                | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| $\text{MOD}(\text{SUM}(I16:P16))$                | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |

Фиг. 2: Таблицата за код на Хеминг, заедно с триколюрния панел

Новият потребител е поканен да въведе желани информационни символи от кодовата дума в белите клетки срещу белия цвят на триколюра, като не може да сгреша и да попълва в жълтите проверочни, а също не може да въвежда стойности различни от 0 и 1 (Фиг. 3):



Фиг. 3: Грешка – недвоично въвеждане

Напътствието Тук променете произволен бит след изпълнение се променя на Има един променен, или съобщение

Променихте повече от един

Нека грешката да е  
само една

заедно с , когато е превишен броя на грешките.

Когато е въведена само една грешка, съобщението е Грешката е в бит № , а след него в прав двоичен вид е изписан номера на сгрешения бит.

Стойностите на проверочните битове се проектират върху кодовата дума и реда в който е с грешката.

### **Заключение**

В доклада е предложена компютърна дидактична програма, която значително улеснява възприемането на конкретен учебен материал. Целта е чрез учебна игра да се усвоява кода на Хеминг.

### **ЛИТЕРАТУРА:**

[1] Досев Д., Илиев С., Христов Х., „Възможности за използване на стеганография в социалните мрежи Facebook и Google+“, Трета международна научна конференция – „Наука, образование, иновации“, посветена на 145 годишнината на БАН и 35 годишнината от космическия полет на Георги Иванов, 21-23-05. 2014г. Шумен.

[2] Фадеева Т. и др., Технологичното обучение – реалност и перспективи за развитие, УИ „Епископ К. Преславски“, Шумен, 2002.

[3] Цонев И., Предаване на данни и компютърни комуникации, УИ „Епископ К. Преславски“, Шумен, 2012.

[4] Bott E., C. Siechert, Microsoft Office Inside Out 2013 Edition, Microsoft Press, California, 2013.

# АНАЛИЗ СЪСТОЯНИЕТО НА КРИТИЧНАТА ИНФРАСТРУКТУРА ЗА РАЙОН ШУМЕН

Доника В. Диманова, Цветослав С. Цанков

## ANALYSIS OF THE STATE OF CRITICAL INFRASTRUCTURE FOR THE AREA SHUMEN

Donika V. Dimanova, Tsvetoslav S. Tsankov

**ABSTRACT:** *Critical infrastructure is increasingly fitting into the geopolitical, geo-economic and geo-energy risks. Encroachment on such an object can cause enormous damage to politics and economics. Therefore, risk management of critical infrastructure is among the top priorities of our national security.*

**KEY WORDS:** *critical infrastructure, security, protection, analysis, hazardous facilities.*

### Въведение

Защитата на критичната инфраструктура и обектите, свързани със сигурността на България заемат централно място в Стратегията за национална сигурност. Наред с гарантирането на правата, свободите, сигурността и благосъстоянието на гражданите и обществото; запазването на суверенитета, териториалната цялост на България и единството на нацията; защитата на конституционно установения ред и демократичните ценности; изпълнението на интеграционните задължения на страната в рамките на евро-атлантическата (НАТО) и европейската общност (ЕС), в чл. 15 и чл.19 на Стратегията е записано, че защитата на населението и критичната инфраструктура при кризи, бедствия, аварии, катастрофи и други рискове и заплахи е една от главните цели на съвременната политика за национална сигурност. Изрично е посочено, че защитата ѝ е „Жизненоважен интерес“ за страната [5, 6].

Критичната инфраструктура все повече се вписва в гео-политически, гео-икономически и гео-енергийни контексти и

рискове. Посегателството срещу такъв обект може да не доведе до разрушения, жертви на населението и екологични катастрофи, но да нанесе огромни щети на политиката и икономиката. Поради това критичната инфраструктура се превръща в стратегически ресурс, управлението на рисковете за който е сред водещите приоритети на националната ни сигурност.

В тази връзка целите на доклада са:

1. Да се анализира състоянието на критичната инфраструктура в България.
2. Да се направи оценка и анализ на критична инфраструктура за района на област Шумен.

### **Изложение**

Докладът е структуриран по следния начин:

1. Направен е анализ на критичната инфраструктура в България.
2. Определени са значимите критични места за територията на област Шумен.
3. Направена е категоризация на опасностите за района на Шумен по степен на уязвимост, важност и риск за населението.

Понятието „критична инфраструктура” е дефинирано в Закона за защита при бедствия и други нормативни документи, според които "критична инфраструктура" е система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни негативни последици за Република България в резултат на невъзможността да се запазят тези функции [2, 3].

### ***Състояние на критичната инфраструктура в Република България***

С въвеждане на Директивата за европейските критични инфраструктури в Закона за защита при бедствия [1, 2, 3, 6], е разработена нормативната уредба за защита от бедствия на обектите, представляващи националните и европейски критични инфраструктури, оценка на риска и мерките за подобряване на тяхната защита. *Обектите* срещу които могат да бъдат насочени

някои от рисковете и заплахите за сигурността са практически във всички области (фиг. 1).



**Фиг. 1.** Потенциално опасни обекти на територията на Р. България

Изпълнявайки ангажиментите по Директива 2008/114/ЕО, България включва възможности за съвместна дейност между публичния и частния сектор, базирани на взаимен интерес и експертни умения на партньорите за гарантиране защитата на обществените интереси и потребности чрез ефективно разпределение на средствата, рисковете и ползите в този процес [5].

Защитата на критичната инфраструктура включва създаване на регистър, в който са вписани секторите и стратегически обекти като: АЕЦ, ТЕЦ и ВЕЦ, заводи за производство на стратегическа продукция, язовирни стени, тесни и уязвими участъци от пътища и жп линии, виадукти, тунели и др.

Секторите с критична инфраструктура в Република България са енергетика, транспорт, информационни и комуникационни технологии, околна среда, земеделие и храни, здравеопазване, отбрана, културно наследство и др. (таблица 1). Те са регламентирани в приложение 1 на Наредбата за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях (ДВ. бр.81/23.10.2012г.).

**Таблица 1: Списък на секторите с критична инфраструктура в Република България**

| <b>Сектор</b>                                  | <b>Подсектор</b>                                      | <b>Отговорно ведомство</b> |
|------------------------------------------------|-------------------------------------------------------|----------------------------|
| I. Енергетика                                  | 1. Електроенергия                                     | МИЕТ                       |
|                                                | 2. Нефт                                               | МИЕТ                       |
|                                                | 3. Газ                                                | МИЕТ                       |
|                                                | 4. Топлинна енергия                                   | МИЕТ                       |
| II. Транспорт                                  | 1. Автомобилен транспорт и пътна инфраструктура       | МРРБ, МТИТС                |
|                                                | 2. Железопътен транспорт и железопътна инфраструктура | МТИТС                      |
|                                                | 3. Въздушен транспорт и летища                        | МТИТС                      |
|                                                | 4. Воден транспорт и пристанища                       | МТИТС                      |
| III. Информационни и комуникационни технологии | 1. Електронни съобщителни мрежи                       | МТИТС                      |
|                                                | 2. Информационна и комуникационна инфраструктура      | МТИТС                      |
| IV. Пощенски и куриерски услуги                |                                                       | МТИТС                      |
| V. Околна среда                                | 1. Околна среда                                       | МОСВ                       |
|                                                | 2. Води, водоснабдяване и канализация                 | МОСВ, МРРБ                 |
| VI. Земеделие и храни                          | 1. Земеделие                                          | МЗХ                        |
|                                                | 2. Храни                                              | МЗХ                        |
|                                                | 3. Гори и ловни стопанства                            | МЗХ                        |
| VII. Здравеопазване                            | 1. Медицинска и болнична помощ                        | МЗ                         |
|                                                | 2. Лекарствени средства                               | МЗ                         |
| VIII. Финанси                                  |                                                       | МФ                         |
| IX. Икономика                                  |                                                       | МИЕТ                       |
| X. Спортни обекти и съоръжения                 |                                                       | МФВС                       |
| XI. Образование, наука и технологии            |                                                       | МОМН                       |
| XII. Природни ресурси                          |                                                       | МИЕТ, МОСВ                 |
| XIII. Туризм                                   |                                                       | МИЕТ                       |
| XIV. Регионално развитие и благоустройство     |                                                       | МРРБ                       |
| XV. Отбрана                                    | 1. Отбранителна промишленост                          | МО                         |
|                                                | 2. Военна инфраструктура и                            | МО                         |



| Сектор                                     | Подсектор                      | Отговорно ведомство |
|--------------------------------------------|--------------------------------|---------------------|
|                                            | военни формирования            |                     |
| XVI. Правосъдие, обществен ред и сигурност |                                | МП, МВР, ДАНС       |
| XVII. Държавно и социално управление       |                                | МВР, МТСП           |
| XVIII. Защита при бедствия                 |                                | МВР                 |
| XIX. Културно наследство                   | 1. Недвижими културни ценности | МК                  |
|                                            | 2. Движими културни ценности   | МК                  |

Както вече бе споменато, установяването на критичните инфраструктури и обектите им, както и оценката на риска за тях, се извършват с цел намаляване на риска от бедствия и защита на населението. Самата процедура по установяването е законова регламентирана и включва следните *три етапа* [3]:

*На първия етап* се прави се първоначален подбор на инфраструктурите и обектите им, включени в съответните сектори. Работни групи от компетентни министри и държавни служители извършват проверка дали инфраструктурите отговарят на определението за критична инфраструктура и дали загубата на услуги от нея ще има значително въздействие. Определените като потенциални критични инфраструктури преминават към следващия етап от процедурата.

*Във вторият етап* се извършва оценка на негативните последици от разрушаването на инфраструктурите или от нарушаването на нормалното им функциониране и сравняват тези негативни последици с критериите: потенциален брой пострадали, потенциални икономически последици, потенциални обществени последици. При оценката на негативните последици се отчитат и времето за възстановяване и наличието на алтернативи на инфраструктурите.

*В третия етап*, потенциалните критични инфраструктури и обектите им, определени във втория етап, се включват в списъка на установените критични инфраструктури и обектите им, който се утвърждава от министъра на вътрешните работи, други компетентни министри или държавни органи.

Едновременно с установяването и опазването на критичната инфраструктура - енергийна, транспортна, комуникационна, екологическа - трябва да се заделят средства за тяхното поддържане и развитие. Финансирането е от бюджета на държавата и общините и се разглежда като предпоставка за превенция и ефективно управление на кризи.

Ефективното реагиране се постигат чрез комплексен подход към изграждане на интегрирана, гъвкава и устойчива национална система за управление. Изгражда се капацитет за превенция, ранно предупреждение и управление при кризи на основата на информация и възможност за обмен на данни и чрез използване на космически и други високи технологии. За ефективно управление при кризи се развиват интегрирани военни и граждански способности за действие в страната и в рамките на ЕС. Под ръководството на областните управители и кметовете на общини се поддържат и предоставят способности за подкрепа на населението и защита на националната критична инфраструктура при предотвратяване и ликвидиране на последствията от бедствия и аварии;

Съгласно Наредбата за установяване на критичните инфраструктури и обектите им и оценка на риска за тях, областните управители събират и обобщават необходимата информация за потенциалните критични инфраструктури и обектите им на територията на областта, като предоставят информация на министъра на вътрешните работи. Кметовете на общини събират необходимата информация и я предоставят на областните управители. В областта се изготвят плановете за защита при бедствия на общините, категоризирането на населените места в зависимост от броя на потенциално засегнатото население съгласно Закона за защита при бедствия, ежегодните доклади за дейността по защита при бедствия и др.

### ***Критична инфраструктура за района на област Шумен***

Критичната инфраструктура за района на област Шумен се определя съгласно областния план за защита при бедствия. Планът се изготвя съгласно Закона за защита при бедствия от служителя по ОМП и защита на населението и се утвърждава от Областния управител и Министъра на вътрешните работи. Осъществяването

на плана се подпомага от главен експерт по „ОМП и сигурност на информацията” в Областна администрация- Шумен, началника на Областно управление ППЗН, военни формирования, в който има модули за защита на населението при бедствия, директор на ОД на МВР-гр. Шумен, директор на РЗИ-гр. Шумен, директор на ЦСМП-гр. Шумен, директор на БАБХ-гр. Шумен, директор на ОПУ-гр. Шумен, началник сектор-гр. Шумен в басейнова дирекция за Черноморски район-гр. Варна и др.

Целта на плана [4] е :

- Създаване оптимална организация в областта за осигуряване защитата на населението, инфраструктурата и националното стопанство при възникване на бедствия.

- Изготвяне на анализ за възможните бедствия и прогноза за въздействието им върху територията на областта.

- Осигуряване организация за провеждане на ефективни мероприятия по осигуряване на защитата и дейности за възстановяване нормалното функциониране на засегнатите райони.

- Създаване на организация за действие и взаимодействие на отговорните институции, реализиращи мероприятия по защитата при бедствия.

### ***Значими критични места за територията на област Шумен [4]***

#### ***1. Язовири и корекции на реки***

Критични места са селищата по поречието на р. Камчия - с. Хан Крум, с. Ивански, с. Янково и с. Бял бряг и коригираните участъци по течението.

Потенциално опасни обекти са: яз. ”Тича”, р. Камчия.

#### ***2. Съоръжения на „ВиК”***

Критични места са: магистрален водопровод от яз. ”Тича”, охранващ общини Велики Преслав, Шумен и Търговище през поречието на р. Камчия и основни помпени станции.

Потенциално опасни обекти са: магистрален водопровод от яз. ”Тича”, помпена станция „1300” за гр. Шумен и съседни села, помпена станция „Изгрев”.

### 3. Съоръжения от електропреносната и електроразпределителната мрежа

Критични места:

- въздушна линия „Отечество” - 400 кV
- подстанция „Мадара” - 220/110 кV
- въздушна линия „Волов” – 220 кV
- въздушна линия „Тича” – 220 кV

#### 4. Републиканска пътна инфраструктура

Участъци от РПМ създаващи критична ситуация на територията на областта при снегонавяване: Път I-2 " Русе - Варна", Път I-4 " Коритна - Белокопитово", Път I-7 " Силистра - Шумен - Ямбол", Път II-73 "Шумен - Карнобат", Път II-74 " Велики Преслав - Търговище", Път III-207 " Нови пазар - Тодор Икономово", Път III-731 "Радко Димитриево - Друмево", Път III-3203 " Преслав - Смядово", Път III-3204 " Ивански - Жълъд", Път III-3205 "Мътница - Мадара", Път III-3206 "Шумен - Златна нива", Път III-3208 " Венец - Борци - Ясенково", Път III-3210 "Изгрев - Каолиново - Тодор Икономово", Път III-3211 " Струйно - Хитрино", Път III-3023 "Косово - Марково - Мадара".

#### 5. Критични места от горския фонд

На територията на област Шумен, средната площ на участъците от горския фонд които при възникване на пожар застрашават територията на повече от една община е около 700-800дка.

#### 6. Промислени обекти, работещи с рискови вещества и материали

Обектите, работещи с ОВ (съхраняват амоняк) с най-големи потенциални опасности в гр. Шумен са: "Родопа Шумен 1882 " ЕООД; "Ваком МП" ООД; "Карлсберг България" АД, Пивоварна Шумен; ЕТ „Николай Неделчев” с. Кочово, община Велики Преслав; ЕТ „Николай Неделчев”, база гр. Велики Преслав; „Винекс – Преслав” АД, гр. Велики Преслав; „Винарска изба – Хан Крум” АД, с. Хан Крум, община Велики Преслав.

На територията на област Шумен са разположени и обекти работещи със суровини и материали, които при възникване на промишлена авария, съпроводена с пожар могат да образуват токсични вещества. Тези обекти са: "Августа мебел" АД, "Мебел

джен” АД, „Максам България” АД, завод гр. Смядово, „Херти” ООД, „Нафтекс Петрол” ЕООД, гр. Варна, Петролна база Каспичан, "Алкомет" АД, ДР "Зърнобаза" Шумен, “Ризов” ООД – Мелница, „ВиК” ООД, „Крис ойл 97” ООД,

***Категоризация на опасностите по степен на уязвимост, важност и риск за населението [4]***

1. *Опасност от земетресения – нисък риск* на опасност, при максимална степен на труса за територията на областта по прогноза – частични, изключване на трафопостове, вероятна възможност за възникване на пожари разрушения на сгради.

2. *Опасност от наводнения – висок риск* на опасност, при голямо наводнение следствие проливни дъждове, интензивно снеготопене и/или скъсване на язовирни стени I и II категория.

3. *Опасност от авария в АЕЦ*, трансграничен пренос на радиоактивни частици – *среден риск* на опасност, в зависимост от посоката на вятъра и големината на аварията.

4. *Опасност от промишлени аварии* в обекти работещи с ОВ – *нисък риск* на опасност, според оценката по „Севезо”.

5. *Опасност от възникване на пожари – среден риск* на опасност, малка вероятност за обхващане на две общини – само при масови горски пожари.

6. *Опасност от снегонавяване и обледявания – нисък риск* на опасност, обхваща частични участъци от републиканската и общинска пътна мрежа.

7. *Опасност от терористични действия – среден риск* на опасност - на територията на областта няма инфраструктура и големи промишлени обекти засягането ,на които ще се отрази цялостно на нормалния стереотип на живот.

От направения анализ на възможните опасности, прогнозата за тяхното въздействие, значимите критични места и потенциално опасни обекти и определената критична инфраструктура в област Шумен може да се направят следния извод. На територията на областта тежка обстановка, засягаща повече от една община може да възникне при земетресение, наводнение, снегонавяване и обледяване, авария в АЕЦ и горски пожари. Като най-тежка ситуация може да се създаде след възникване на земетресение,

наводнение вследствие скъсване стената на яз. "Тича" и обилни валежи и снегонавявания.

### **Заклучение**

Установяването на критичните инфраструктури и обектите им, и оценката на риска за тях се извършват с цел намаляване на риска от бедствия и защита на населението. Оценяването на изискванията за сигурност за подобни инфраструктури следва да се извърши съгласно минимален общ подход. За ефикасното установяване на рисковете, заплахите и уязвимите места в съответните сектори се изисква комуникация между собствениците и оператори на критична инфраструктура, централни и местни държавни органи и структури на гражданското общество.

### **ЛИТЕРАТУРА**

1. Директива 2008/114/ЕО относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита
2. Закона за защита при бедствия, ДВ, бр. 53 от 27.06.2014г.
3. Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях, ДВ, бр.81 / 23.10.2012г.
4. Областен план за защита при бедствия, област Шумен, 2012г.
5. Стратегия за национална сигурност на Република България, 2011г.
6. Hristov H., „Approaches about evaluation on threats' influence upon social organization”, Journal Science education innovation, vol. 3, 2014

# МАТЕМАТИЧЕСКИ МЕТОДИ ЗА ВЗЕМАНЕ НА УПРАВЛЕНСКИ РЕШЕНИЯ ПРИ БЕДСТВИЯ

Доника В. Диманова

## MATHEMATICAL METHODS FOR MANAGEMENT DECISION MAKING DISASTER

Donika V. Dimanova

**ABSTRACT:** *In recent years, the policy of reducing the risk of disasters is a top priority for many countries in the world, including Bulgaria. A key factor in solving issues related to disaster risk reduction, is the existence of political commitment at all levels. In terms of the development of the emergency situation, the examination of all possible options is virtually impossible. That is why in the world today are carried out intensive applied science researches aimed at the development of mathematical models of various natural disasters. Through them, may be chosen the best optimal solution which in the given conditions is the most effective.*

**KEY WORDS:** *risk, mathematical methods, management, disaster situations*

### Въведение

Важна част от работата на органите на изпълнителната власт е бързото и своевременно реагиране при природни бедствия. Базата за вземане на научно-обосновани решения при управлението на природни бедствия е наличието на достатъчно надеждни и прецизни прогнози за развитието на кризата.

В тази връзка целите на изложението са:

1. Да се анализират на методите за моделиране честотата на възникване на природни бедствия.
2. Да се избере метод за статистическа обработка при изследване честотата на природните бедствия.
3. Да се представи общ алгоритъм на модел за честотата на природни бедствия.
4. Да се представи модел за честотата на възникване на интензивни валежи за района на Шумен, на база направено изследване с полином на Чебишев.

5. Да се представи прогноза за честотата на поява на природни бедствия за района на Шумен за следващите пет години.

### **Изложение**

В социалната и природната област явленията имат масов характер и поради това тяхното опознаване и управление може да се анализира само чрез статистическия подход. Закономерностите, които се откриват чрез статистическото изучаване, са жизнено необходими при разработването и прилагането на статико-математическите модели на разглежданите процеси. Изучавайки миналото и настоящето на явленията дава възможност да се прогнозира бъдещото развитие и с достатъчна точност да се предвиждат очакваните последствия от едни или други управляващи въздействия. По този начин могат да се вземат най-целесъобразните и ефективни управленски решения.

### **Анализ на методите за моделиране на честотата на възникване на природни бедствия**

Както вече бе споменато, важна част от работата на органите на изпълнителната власт е бързото и своевременно реагиране при природни бедствия. При формирането на стратегическите и тактическите решения, органа за управление трябва да отчита множеството взаимно противоречиви съображения, от които да търси вариант, който при дадените условия е най-ефективен. Този най-ефективен вариант за вземане на управленско решение се нарича оптимален вариант. Следователно при наличието на няколко възможни варианта при изграждане на стратегии за управление, трябва да се разгледат всички възможни решения и да се избере най-доброто измежду тях, което се нарича оптимално решение. В условията на развитие на бедствена ситуация, разглеждането на всички възможни варианти е практически невъзможно. Това поражда необходимостта от използването на методи за моделиране и симулации на бедствени ситуации, което е предпоставка за вземане на научно обосновани решения в управлението [1].

Една от най-важните задачи при изследването е построяване на модели на изучаваните обекти. Дейността по построяването, анализирането и проверката на модела се нарича *моделиране*.



Основно понятие при моделирането е понятието „модел”. Под модел се разбира някаква опростена система, имаща материално-веществен или абстрактен характер, която отразява само отделни, но важни свойства на изучавания обект, наричан „оригинал” [1]. Често когато се казва думата "модел" се иска да се подчертае разликата между реалният обективно съществуващ и въображаемия абстрактен моделен свят, който е продукт на нашият разум, и който "съществува" във вид на твърдения, формули, математически символи и връзки, схеми и някои други средства.

Съществуват няколко вида моделиране, които могат да се групират в две основни групи [8]:

1. Материално-веществено моделиране – моделът е реализиран като материален обект (опитна уредба, устройство, машина и т.н.);
2. Абстрактно-логическо моделиране – моделите се представят чрез средствата на математиката.

Познати са следните методи на моделиране [8]:

- Физическо моделиране-моделите възпроизвеждат изучаваното явление в натура, като се запазва неговата физическа природа. За тази цел се използват специално построени физически модели, на които се провеждат експериментите. Степента и характера на подобие между модела и оригинала се осъществява чрез така наречените критерии на подобие.
- Математическо моделиране-моделите се строят със средствата на математиката и представляват отделни уравнения или системи уравнения (алгебрични, диференциални, интегрални и др.).

Математическите модели могат да се класифицират по следните признаци [1,8]:

- Според вида на ограничителните условия и целевата функция, математическите модели биват *линейни и нелинейни*. Почесто срещаните математически модели са линейни, тъй като намирането на оптимална програма на линейните модели е значително по-лесно. За намирането на решения на нелинейните модели съществуват приближени или итеративни методи, които

водят до решения близки до оптималните. Въпреки това, в много от случаите, получаваните резултати от нелинейните модели значително по-реално отразяват разглеждания процес.

- Според характера на предварителната информация, моделите се разделят на детерминирани и стохастични. Детерминирани са тези модели, в които с пълна точност се формулират както ограничителните условия, така и критериите за оптималност. Стохастични са тези модели, при които съществува неопределеност, т.е. изходните данни на модела имат вероятностен характер. При тях следва да се изследват законите за разпределение на съответните случайни величини, което не винаги е възможно. Детерминираните модели са значително по-прости от стохастичните. Затова много често вместо стохастичен се разглежда детерминиран модел, като се игнорира случайният характер на използваните величини.

- Математическите модели могат да се разделят още на статични и динамични. Изграденият математически модел е статичен, ако се изследва процес в точно определен период от време, без да се отчитат настъпващите изменения във времето. Динамичните модели отчитат динамиката в развитието на процеса.

Съществуват две групи методи за построяване на математически модели-аналитични и експериментални.

- При аналитичните методи, моделът се построява чрез законите описващи процесите в изучавания обект. Правят се редица допускания, чрез които се отчита относителната важност на величините, определящи изучавания обект. Някои коефициенти и зависимости се получават по експериментален път. Математическият модел се проверява за адекватност чрез специално поставени експерименти и с помощта на специални числени критерии.

- В основата на експерименталните методи за математическо моделиране лежи така нареченият принцип на „черната кутия”. Обектът на изследването се представя формално като затворена част от околната среда-черна кутия, в която протичат неизвестни за изследователя процеси. Обектът взаимодейства с околната среда чрез редица входни въздействия-фактори и множество изходни параметри-реакции, определящи

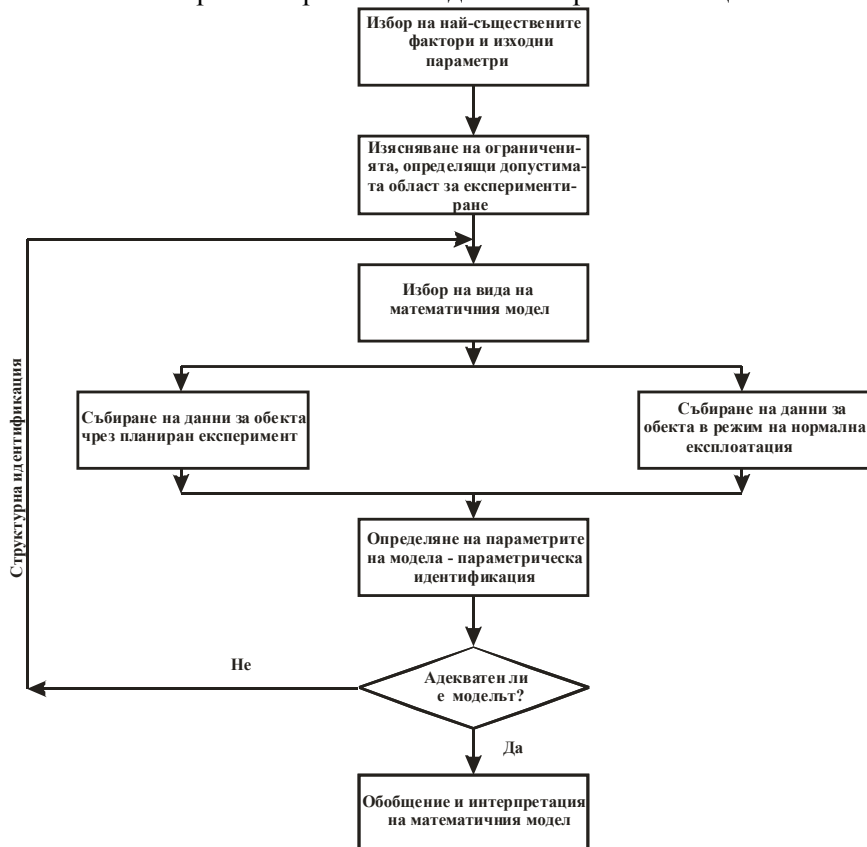
неговото функциониране и състояние. На основата на експериментална информация за входните фактори и изходните параметри се получава достатъчно пълна информация за обекта без да се познава вътрешната му структура. Чрез тази информация се построява моделът, обвързващ входните фактори и изходните параметри. Факторите имат различна природа и се разделят на управляеми и неуправляеми.

Етапите при построяване на математически модели чрез аналитични методи са показани на фигура 1, а по експериментален път са показани на фигура 2. Моделите, построени по тази схема са валидни само за условията, при които са построени опитите.



Фиг. 1 Математически модели чрез аналитични методи

Частен случай на математическото моделиране е *имитационното моделиране*. Имитационното моделиране е изследователски метод, при който системата на изследване е заменена от модела с достатъчна точност. Целта е да се експериментира с модела, за да се набави информация за реалната система. Експериментирането с модела се нарича имитация.



Фиг. 2 Математически модели на базата на експериментални данни

Имитационният модел е формализирано описание на изучаваното явление в цялата му пълнота. Най-често представлява общо логико-математическо представяне на дадена система или операция, запрограмирано за решаване от компютърна система.

Един от недостатъците на имитационното моделиране е, че полученото решение винаги носи частен характер, отговаряйки на фиксирани значения на параметрите на системата, входната информация и началните условия. Независимо от това, имитационното моделиране е най-ефективният метод за изследване на сложни системи (понякога и практически единствено достъпното средство за получаване на необходимата информация за поведението на системата).

Друг недостатък е, че построяването на имитационен модел на дадена система е твърде сложен и трудоемък процес, изискващ освен това висока и разностранна квалификация.

В социалната и природната област явленията имат масов характер и поради това тяхното опознаване и управление може да се анализира само чрез статистическия подход. Закономерностите, които се откриват чрез статистическото изучаване, са жизнено необходими при разработването и прилагането на статикоматематическите модели на разглежданите процеси. Изучавайки миналото и настоящето в развитието на явленията и отчитайки обстоятелството, че в достатъчно голям брой наблюдения се установяват трайни причинно-следствени връзки и тенденции, дава възможност да се прогнозира бъдещото развитие на явленията и с достатъчна точност да се предвиждат очакваните последиствия от едни или други управляващи въздействия. По този начин се откриват нови идеи и подходи към управлението и могат да се вземат най-целесъобразните и ефективни управленски решения.

### **Статистическо изследване на връзките и зависимостите при природни бедствия**

Изследването на връзките и взаимодействията между явленията и процесите при природни бедствия е една от най-важните и сложни задачи, която стои пред научното познание. Чрез анализиране на връзките и зависимостите се разкриват и опознават закономерностите на състоянието и развитието на явленията и процесите. Анализът на причините за дадено състояние или за настъпилите изменения, дават възможност да се посочат мерки за регулиране на управленския процес. За да се

предприемат мерки за отстраняване на смушаващите фактори (грешки), е необходимо да се проучи и анализира въздействието им в конкретните условия. Разкриването на различните фактори и причините обуславящи отклоненията от нормалния ритъм на работа се извършват чрез специално организирани изследвания. Чрез статистическият анализ се изследват количествените зависимости между въздействащите фактори и резултатите.

Най-общо зависимостите могат да се класифицират от гледна точка на различни категории признаци:

- В зависимост от характера си зависимостите биват причинно-следствени и не причинно-следствени.
- Според начина на проявление зависимостите биват функционални и корелационни.
- Според броя на включените в анализа фактори, корелационните зависимости биват единични и множествени.
- Според формата и модела, чрез които се представят, зависимостите биват линейни и нелинейни.
- Зависимостите могат да бъдат еднопосочни и разпосочни.

Конкретните задачи при изследване на връзки и зависимости са:

- Да се изследва дали интересуващата ни връзка между явленията обективно съществува и как се проявява в практиката. Тук при изследването намират приложение методите за проверка на хипотезите.
- Да се моделират съществуващите зависимости. Закономерностите, на които е подчинена зависимостта, се представят чрез математически израз.
- Да се намерят количествените съотношения, които се пораждат от изследваните връзки и зависимости.

#### *Статистически оценки и техните свойства*

Нека в резултат на експеримент е получена извадката от опитни данни  $V = \{v_1, v_2, \dots, v_m\}$ , разпределението на която има известна математическа форма, но съдържа някои неизвестни параметри. По принцип съществуват безкрайно много функции от извадката, които могат да се предложат като оценки на

интересуващите ни параметри. Ето защо възниква проблемът за избор на най-точна оценка. При това трябва да се има предвид, че тъй като всяка оценка е функция от извадката, то тя е наблюдавано значение на една случайна величина. Затова не може да се предскаже индивидуалното значение на оценката в дадения частен случай и за качеството на оценката трябва да се съди само по разпределението на нейните значения, което се проявява в дълъг ред от изпитания.

Следователно:

$$\hat{a}_j = R_j(V), \quad j = 1, 2, \dots \quad (1)$$

като тук  $\hat{a}_j$  е оценката, получавана чрез функцията  $R_j$  от извадката  $V$ , а " $a$ " е точката, чиито стойности са интересуващите ни истински значения на параметрите.

За сравняване на оценките, получени с различните статистически методи, са въведени следните основни характеристики на оценките [2, 3, 4, 5, 7].

1. **Неизместеност.** Нека с  $M[\hat{a}_j]$  означим математическото очакване на случайната величина  $\hat{a}_j$ . Ако  $M[\hat{a}_j] = a$ , то оценката  $\hat{a}_j$  се нарича неизместена.

Неизместените оценки в някои случаи се оказват твърде сложни функции от резултатите на измерванията. В такива ситуации за опростяване на изчисленията се използват оценки, при които абсолютната величина на изместването при  $m \rightarrow \infty$  се стреми към 0. Такива оценки се наричат асимптотически неизместени.

2. **Ефективност.** Ако основната част на плътността на разпределението на  $\hat{a}_j$  е съсредоточена в малка околност на точка  $a$ , то с голяма вероятност може да се счита, че оценката се отличава от истинското значение само с малка величина. В този смисъл оценката е толкова по-точна, колкото е по-малко разсейването ѝ от истинското значение. Крамер е показал [5], че при някои общи условия средноквадратичното отклонение  $M[\hat{a}_j - a]^2$  е ограничено отдолу от едно положително число  $c$ , зависещо само от функцията на разпределение на  $\hat{a}_j$ , обема на извадката  $m$  и изместването  $b(a)$ , което се дава с равенството:

$$M[\hat{a}_j] = a + b(a) \quad (2)$$

Отношението:

$$e[\hat{a}_j] = \frac{c}{D[\hat{a}_j]} \quad (3)$$

където  $D[\hat{a}_j]$  е дисперсията на случайната величина  $\hat{a}_j$ , се нарича ефективност на оценката  $\hat{a}_j$ . Очевидно е, че:

$$0 \leq e(\hat{a}_j) \leq 1. \quad (4)$$

Ако в (4) се достига равенство отдясно, то това означава, че  $D[\hat{a}_j]$  е получила своето най-малко възможно значение и  $e(\hat{a}_j) = 1$ . Ако се оценява само един параметър и оценката с неизместена, "с" се дава с известното неравенство на Рао-Крамер [2, 3, 4, 5, ]. В [7] е показано, че по-горните разсъждения са в сила и когато оценяваните параметри са повече от един, но не безкрайно много. При това обаче се използва обобщената дисперсия, която е детерминантата на ковариационната матрица на многомерна случайна величина  $\hat{a}_j$ .

Понятието ефективна оценка се въвежда от Фишер и както беше отбелязано изразява строго математически нашата интуитивна представа за най-точна оценка. Крамер е показал [7], че ефективната оценка на един параметър е единствена.

Ако е в сила:

$$\lim_{m \rightarrow \infty} e(\hat{a}_j) = 1 \quad (5)$$

то оценката  $\hat{a}_j$  се нарича асимптотически ефективна.

3. Състоятелност. Оценката  $\hat{a}_j$  се нарича състоятелна, ако при неограничено увеличаване на обема  $m$  на извадката  $V$ , тя се стреми по вероятност към "а", т.е.:

$$\lim_{m \rightarrow \infty} P(\{\hat{a}_j - a\} < E) = 1, \quad (6)$$

където  $P$  е вероятността на събитието  $\{\hat{a}_j - a\} < E$ , а  $\{x\}$  е норма на вектора  $x$ , която се дефинира с условията:

- 1)  $\{x_1\} = 0$ , ако  $x_1 = 0$ , и  $\{0\} = 0$ ;
- 2)  $\{cx_1\} = |c|\{x_1\}$ , при произволен числов множител "с";
- 3)  $\{x_1 + x_2\} \leq \{x_1\} + \{x_2\}$ .

Изборът на една или друга норма се определя от условията на статистическата задача, която трябва да се реши.



4. Достатъчност. Нека приемем, че семейството  $F$  на допустимите значения на извадката  $V$  е зададено. Статистиката  $s$  е функция на наблюдения  $s = S(V)$  и в общия случай  $S$  е вектор.

Статистиката  $s$  [2] се нарича достатъчна за семейството  $F$ , ако условната плътност на разпределение на  $V$  спрямо  $s$  остава една и съща за всички разпределения от  $F$ .

Понятието достатъчна статистика е въведено от Фишер за означаване на тези статистики, които съдържат всичката информация за оценяваните параметри, която може да се извлече от наличната извадка.

5. Минимална достатъчност. Статистиката  $s$  се нарича минимално достатъчна [2, 5], ако при съхраняване на свойството достатъчност е невъзможно по нататъшно съкращаване на данните в сравнение със  $s$ .

Доколкото  $\hat{a}_j$  е случайна величина, то не е възможно точно да се определи степента на близост на  $\hat{a}_j$  до  $a$ , но ако са известни законите на разпределение на интересуващите ни параметри можем да намерим каква е вероятността тези параметри да се окажат в определени граници при серията измервания. Такъв подход при оценката на интересуващите ни параметри се нарича оценяване с помощта на доверителни интервали. Тук под доверителен интервал се разбира интервал със случайни краища, който с достатъчно висока вероятност (доверителна вероятност) покрива неизвестното истинско значение на параметрите.

От направените до тук разглеждания се вижда, че при избора на метод за статистическа обработка на резултатите от изследванията за да се постигне висока точност е необходимо да се използват:

- Минимално достатъчни статистики, което позволява по минимален статистически материал да се намират търсените оценки;

- Неизменни, ефективни и състоятелни оценки.

### **Статистически методи за оценяване параметри по резултатите от наблюденията**

За изследване на връзки и зависимости се използват различни методи. Изборът на даден метод зависи от целта на

изследването и от наличната информация. Съществуват различни възможности за комбинации на признаците, чрез които се представя дадената зависимост от действителността. Според тези комбинации се използват и различни методи за изследване на интересуващите ни връзки, чиито предимства и недостатъци ще бъдат разгледани в настоящия параграф.

Първият най-общ метод, за статистическо оценяване на параметри е *методът на моментите*, въведен от К. Пирсон и интензивно е използван от неговата школа. Този метод обаче позволява да се намерят асимптотически ефективни оценки само в някои частни случаи. Ето защо Р. Фишер е предложил *метода на максималното правдоподобие*, чиито най-важни свойства са следните [2, 3, 4, 5]:

1) Ако съществува ефективна оценка, то методът на максималното правдоподобие дава тази оценка;

2) Ако съществува достатъчна статистика, то методът на максималното правдоподобие дава ефективна оценка, която е функция от тази статистика;

3) Оценките, получени по метода на максималното правдоподобие, са инварианти по отношение на преобразувания на параметъра, т.е. ако  $q = q(a)$  е произволна функция от " $a$ ", установяваща еднозначно обратимо съответствие (това означава, че на всяко  $a \in A$  на  $q$  съответства едно и само едно значение  $q(a) \in Q$  и обратно, на всяко  $q \in Q$  съответства само едно значение  $a \in A$ ) между  $A$  и  $Q$ , където  $Q$  е множество от стойности на функцията  $q$ , то  $\hat{q} = q(\hat{a})$ , като  $\hat{q}$  и  $\hat{a}$  означават оценки, получени по метода на максималното правдоподобие.

Освен това при доста общи условия [2, 3, 5] функцията на правдоподобие позволява разместване на реда на операциите диференциране и интегриране. Също така ако за всяко  $m \geq 1$  и  $v \in V$  има един локален максимум по  $a \in A$  и при това е достижим, то са в сила и свойствата:

4) Оценките по метода на максималното правдоподобие са състоятелни;

5) При известни съотношения, оценките, получени по метода на максималното правдоподобие, са асимптотически нормални;

6) Оценките, получени по метода на максималното правдоподобие са асимптотически ефективни.

Методът на максималното правдоподобие, въпреки всички положителни качества не е универсален метод. В някои случаи практическото му използване е много затруднено от сложността на изчисленията, които трябва да се извършват и от необходимостта да се познава вида на разпределението на резултатите от изследванията.

Друг метод използван за статистическа оценка е *методът на най-малките квадрати*.

Оптималните свойства на този метод се основават на теоремата на Гаус-Марков [2, 3, 5].

Теоремата всъщност гарантира получаване на неизместени оценки с минимална дисперсия по метода на най-малките квадрати при така наречения линеен модел на наблюденията. Този линеен модел означава, че е в сила:

$$V = X \cdot a + \varepsilon, \quad (7)$$

където:

- $V$  е вектор-стълб на измерванията с размерност  $m$ ;
- $X$  е матрица на променливите с размерност  $m \times k$ , но стойностите на всички  $k$  променливи и всичките  $m$  измервания са известни (в случая  $X$  играе роля на матрица на коефициентите);
- $a$  е вектор стълб на търсените параметри с размерност  $k$ ;
- $\varepsilon$  е вектор стълб на случайните грешки на измерванията с размерност  $k$ .

Под линейна оценка се разбира оценка за която е изпълнено:

$$\hat{a} = U \cdot V, \quad (8)$$

където  $U$  е някаква матрица, а  $V$  е векторът на измерванията.

Ако грешката на измерванията  $\varepsilon$  е разпределена нормално, тогава оценките получени по метода на най-малките квадрати са с минимална дисперсия и когато оценките са нелинейна функция на измерванията  $V$ . Освен това при нормален закон на грешката на измерванията, оценките, получени по метода на най-малките квадрати, са [2, 3, 4, 5, 7]:

- Неизместени, състоятелни и ефективни т.е. най-добрите сред линейните оценки;

- Еквивалентни на оценките, получени по метода на максималното правдоподобие (т.е. методът на най-малките квадрати е частен случай на метода на максималното правдоподобие, когато измерванията са нормални случайни величини, а оценяваните параметри са дадени с известни функционални зависимости).

Система от различни методи за построяване на оценки [2] може да се получи като се конструира по различни методи мярата  $k$  на отклонението на емпирическата функция на разпределение  $Fm(v)$  от теоретическата функция на разпределение  $F(v, a)$ , където  $m$  е обемът на извадката. Най-общо такава мяра е функция от извадката  $V = \{v_1, v_2, \dots, v_m\}$  и от параметъра:  $k = k(v, a)$ . Ако има такава мяра, то в качеството на оценка на параметъра  $a$  следва да се вземе значението, минимизиращо мярката  $k$ . Една от най-известните и употребявани мери е *мярата хи-квадрат*, предложена от К. Пирсон [5].

Оценките получени по метода на минимума на хи-квадрат и по метода на максималното правдоподобие имат редица общи свойства. По-специално те са частни случаи от общия клас на най-добрите асимптотически нормални оценки [7]. Този клас е характерен с асимптотическия характер на състоятелността, нормалността и неизместеността на получаваните оценки.

Доколкото методите на максималното правдоподобие, на минимума на хи-квадрат и на видоизменения метод на минимума на хи-квадрат имат еднакви асимптотични свойства, то при избора на някой от тях трябва да се изхожда във всеки конкретен случай или от изчислителните удобства, или от свойствата им при малки извадки, или и от едното и от другото.

Никой от методите не предлага изчислителна процедура, която винаги да е по-проста от тази на другите методи-т.е. понякога използването на метода на максималното правдоподобие е свързано с по-големи трудности, а в други-използването на минимума на хи-квадрат и неговата модификация. Все пак, когато се работи с непрекъснати разпределения, то за използването на метода на минимума на хи-квадрат и неговата модификация е необходимо наблюденията да се групират. Тази групировка е нужна обаче само за оценяването и в други отношения в напълно

безполезна. Ето защо по мнението на много автори [7] оценяването по метода на максималното правдоподобие в достатъчно широк клас случаи има определени предимства от изчислителна гледна точка.

До тук се спряхме на такива оценки на  $a$ , които представляват само една точка от цялото възможно множество  $A$  на оценявания параметър. Такива процедури се наричат точково оценяване [3,5]. Когато като оценка се търси не една точка  $a \in A$ , а цяло подмножество на  $A$  тогава оценяването се нарича оценяване с помощта на доверителни области (или зони) [6].

Ако използваме незместени, приблизително нормални оценки, тогава доверителните интервали са толкова по-къси (по-селективни), колкото е по-малка дисперсията на оценката. Доколкото при доста общи условия оценките на максималното правдоподобие са асимптотически ефективни и асимптотически нормални, дотолкова на базата на този метод могат да бъдат получени асимптотически по-къси (по-селективни) интервали.

### **Избор на метод за статистическа обработка при изследване честотата на природните бедствия.**

От направения анализ до тук беше установено, че за да се постигне висока точност на обработените резултати от изследванията [3,5], при избора на метод за статистическа обработка е необходимо да се използват: минимално достатъчни статистики, което ще позволи по минимален статистически материал да се намират търсените неизменни, ефективни и състоятелни оценки. В тази връзка възниква проблемът за избор на метод за статистическа обработка на оценката на бедствените ситуации.

От [7] е известно, че основен статистически метод за изследване на зависимости, при който факторните и резултативните променливи са количествени признаци, е 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. Това допускане се обосновава от факта, че съгласно известната от висшата математика Теорема на Болцано-Вайерщрас, всяка гладка функция може да се представи с произволно висока точност чрез полином. Теоремата се изразява по следния начин:

За всяка функция  $f(t)$ , непрекъсната за всяко  $t \in [t_1, t_n]$  и произволно действително число  $\alpha > 0$ , може да се посочи такъв полином  $P(t)$ , че да е в сила неравенството:

$$|P(t) - f(t)| < \alpha \quad (9)$$

Тъй като процесът на изменение на природните бедствия е темпорално непрекъснат, то за него са изпълнени условията на теоремата. Следователно честотите на природните бедствия могат да се описват с произволно висока точност с полиномиални функции. Многобройните наблюдения показват, че честотите на природните бедствия обикновено се изменят като монотонни функции на времето. По тези причини при изследването им е препоръчително да се използват алгебрични полиноми и комбинация от ортогонални полиноми със степен  $s \geq 2$  [7] от вида:

$$L_L(t) = \sum_{n=0}^s \frac{b_n}{n!} \quad (10)$$

Тук  $L_L(t)$  е истинската стойност на броят дни с даден тип природно бедствие за една година, т.е. годишната честота на изследваното природно бедствие, а коефициентите  $b_n$ , имат смисъл на скорост на изменение на честотата на природното бедствие, на ускорение на изменението на честотата на природното бедствие и т.н., а  $2 \leq s \leq 8$  [7]. Функцията (10), за която се счита, че описва еволюцията на честотата на природното бедствие се нарича изглаждаща (респективно изглаждащ полином в случая (10)).

Предвид на изложеното, броят дни  $L_L(t)$  с природно бедствие за  $t$ -тата година следва да се представи със следния полином:

$$L_L(t) = b_0 + b_1 \cdot t + b_2 \cdot \frac{t^2}{2!} + \dots + b_s \cdot \frac{t^s}{s!}, \quad (11)$$

като степента  $s$  на полинома зависи от физическата природа на изследваното природно бедствие. Коефициентите на полинома

$b = \{b_0, b_1, b_2, \dots, b_s\}$  имат смисъл на начална стойност на броя на дните с природни бедствия за една година, скорост на увеличаване (намаление) на броя на дните с природни бедствия, ускорение на нарастване (намаление) на броя на дните с природни бедствия и т.н. Както беше отбелязано, те подлежат на статистическа оценка.

Оценката на коефициентите на полинома  $b = \{b_0, b_1, b_2, \dots, b_s\}$  се извършва по метода на максимума на функцията на правдоподобие, като грешки могат да възникнат при неправилно изброяване на дните с природни бедствия за една година, които най-често са разпределени нормално с нулево средно значение.

След логаритмуване на  $L(b)$  и определяне на частните производни по всяка от оценяваните величини  $b_0, b_1, b_2, \dots, b_s$ , се съставя система от уравнения на правдоподобие:

$$\begin{cases} \frac{\partial L(\vec{b})}{\partial b_0} = 0 \\ \dots\dots\dots \\ \frac{\partial L(\vec{b})}{\partial b_s} = 0 \end{cases} \quad (12)$$

Решавайки (12) алгоритмите за оценяване се получават във вида:

$$\hat{b}_i = f(b_0, b_1, \dots, b_s). \quad (13)$$

Ако степента на полинома (11) е поне  $s=2$ , тогава анализираната математическа зависимост на броя на дните с даден тип природно бедствие за една година е нелинейна.

Така например ако е известно, че  $s=2$ , от (11) за  $L_L(t)$  се получава следният полином от втора степен:

$$L_L(t) = b_0 + b_1 \cdot t + b_2 \cdot \frac{t^2}{2!} \quad (14)$$

При това коефициентите на полинома (14) имат следния физически смисъл:

1)  $b_0$  е начален брой на дните с природно бедствие от разглеждания тип за една година;

2)  $b_1$  е скоростта на нарастване на дните с природното бедствие;

2)  $b_2$  е ускорението, с което се изменя броя на дните с природното бедствие.

При Гаусов закон на разпределение на грешките при отчитане на броя на дните с природното бедствие за една година, системата (12) се получава по така наречения метод на най-малките квадрати (МНК). При този метод оценките на величините  $b_0, b_1, b_2, \dots, b_s$  се получават като се намери минимумът на сумарното притеглено квадратично отклонение на измерените стойности на изглажданата величина (т.е. броят на дните с екстремното явление за една година) спрямо нейния модел (11). В конкретно разглеждания случай трябва да се намери минимумът на функцията:

$$L(b_0, b_1, b_2) = \sum_{i=0}^{n-1} w_i \left( b_0 + b_1 \cdot t_i + b_2 \cdot \frac{t_i^2}{2!} - r_i \right)^2 \quad (15)$$

Тук са използвани следните означения:

1)  $L(b_0, b_1, b_2)$  е претегленото квадратично отклонение на броя на дните с екстремното явление за една година спрямо модела (6);

2)  $t_0 = t_0 - t_0, t_1 = t_1 - t_0, \dots, t_i = t_i - t_{i-1}, \dots$  са дискретните моменти от време (годините), през които са направени измерванията (т.е. изброени са дните с екстремното явление);

3)  $r_i$  е броят на дните с природното бедствие за  $i$ -тата година;

4)  $w_i = \frac{1}{\sigma_{r_i}}$  е „тежестта”, с която е отчетен броят на дните с

природни бедствия през  $i$ -тата година;

5)  $\sigma_{r_i}$  е средно – квадратичната грешка, допусната при определяне на броя на дните с природното бедствие в  $i$ -тата година;



6)  $n$  е общият брой години, в които са отчетени дните с природни бедствия.

Минимумът на (15) се определя след като се приравнят на 0 частните производни на  $L(b_0, b_1, b_2)$  в съответствие с (12):

$$\begin{cases} \frac{\partial L(b_0, b_1, b_2)}{\partial b_0} = \sum_{i=0}^{n-1} w_i \cdot 2 \cdot \left( b_0 + b_1 \cdot t_i + b_2 \cdot \frac{t_i^2}{2!} - r_i \right) = 0 \\ \frac{\partial L(b_0, b_1, b_2)}{\partial b_1} = \sum_{i=0}^{n-1} w_i \cdot 2 \cdot \left( b_0 + b_1 \cdot t_i + b_2 \cdot \frac{t_i^2}{2!} - r_i \right) \cdot t_i = 0 \\ \frac{\partial L(b_0, b_1, b_2)}{\partial b_2} = \sum_{i=0}^{n-1} w_i \cdot 2 \cdot \left( b_0 + b_1 \cdot t_i + b_2 \cdot \frac{t_i^2}{2!} - r_i \right) \cdot \frac{t_i^2}{2!} = 0 \end{cases} \quad (16)$$

След разкриване на скобите и съкращаване на 2 в (16), резултатът е:

$$\begin{cases} b_0 \sum_{i=0}^{n-1} w_i + b_1 \sum_{i=0}^{n-1} w_i \cdot t_i + b_2 \cdot \frac{1}{2!} \sum_{i=0}^{n-1} w_i \cdot t_i^2 = \sum_{i=0}^{n-1} w_i \cdot r_i \\ b_0 \sum_{i=0}^{n-1} w_i \cdot t_i + b_1 \sum_{i=0}^{n-1} w_i \cdot t_i^2 + b_2 \cdot \frac{1}{2!} \sum_{i=0}^{n-1} w_i \cdot t_i^3 = \sum_{i=0}^{n-1} w_i \cdot r_i \cdot t_i \\ b_0 \sum_{i=0}^{n-1} w_i \cdot t_i^2 + b_1 \sum_{i=0}^{n-1} w_i \cdot t_i^3 + b_2 \cdot \frac{1}{2!} \sum_{i=0}^{n-1} w_i \cdot t_i^4 = \sum_{i=0}^{n-1} w_i \cdot r_i \cdot t_i^2 \end{cases} \quad (17)$$

Системата уравнения (17) се опростява след като се отчетат следните обстоятелства:

1) Очевидно прецизността на измерванията в различните години е една и съща, т.е.  $\sigma_{r_i} = \sigma_0 = const$ ; това позволява в (17)

да се съкратят константите  $w_i = \frac{1}{\sigma_{r_i}} = \frac{1}{\sigma_0}$ ;

2) Моментите на измерванията могат да се представят с цели числа  $t_0 = 0, t_1 = 1, \dots, t_i = i, \dots$ ;

След отчитане на тези обстоятелства от (17) могат да се изследват модели с конкретни данни.

**Всичко това ще бъде пояснено със следния пример.**

**Модел 1:** Прави се изследване на интензивните валежи на територията на област Шумен за период от 23 години (1990г.-2012г.) и прогноза за следващите пет години при  $s=2$ . В таблица 1 и фигура 3 е показан броят на дните с интензивни валежи (над 8мм/24ч. отчетени с натрупвания).

Таблица 1: *Брой дни за една година с интензивни валежи, отчетени с натрупвания*

| Година/<br>мм/24ч | 8-10<br>мм | 8 - 20<br>мм | 8 - 30<br>мм | 8 - 40<br>мм | 8 - 50<br>мм | 8 - 70<br>мм | 8 -100<br>мм |
|-------------------|------------|--------------|--------------|--------------|--------------|--------------|--------------|
| 1990              | 6          | 14           | 15           | 15           | 15           | 16           | 17           |
| 1991              | 8          | 15           | 21           | 21           | 21           | 21           | 27           |
| 1992              | 5          | 10           | 19           | 20           | 20           | 20           | 21           |
| 1993              | 6          | 13           | 16           | 17           | 18           | 19           | 21           |
| 1994              | 8          | 21           | 26           | 29           | 30           | 30           | 30           |
| 1995              | 12         | 24           | 28           | 29           | 29           | 29           | 29           |
| 1996              | 6          | 12           | 13           | 13           | 13           | 13           | 13           |
| 1997              | 7          | 18           | 21           | 26           | 26           | 26           | 26           |
| 1998              | 5          | 8            | 13           | 13           | 13           | 13           | 13           |
| 1999              | 6          | 17           | 21           | 23           | 23           | 23           | 24           |
| 2000              | 11         | 17           | 18           | 18           | 18           | 19           | 19           |
| 2001              | 12         | 22           | 25           | 25           | 25           | 25           | 25           |
| 2002              | 15         | 25           | 30           | 31           | 32           | 33           | 34           |
| 2003              | 10         | 24           | 26           | 27           | 28           | 28           | 30           |
| 2004              | 8          | 10           | 16           | 17           | 18           | 19           | 19           |
| 2005              | 7          | 19           | 28           | 31           | 34           | 34           | 34           |
| 2006              | 6          | 20           | 28           | 28           | 28           | 28           | 28           |
| 2007              | 10         | 26           | 27           | 31           | 32           | 32           | 32           |
| 2008              | 3          | 14           | 17           | 18           | 19           | 19           | 19           |
| 2009              | 13         | 28           | 36           | 38           | 39           | 39           | 39           |
| 2010              | 8          | 32           | 42           | 44           | 46           | 47           | 47           |

| Година/<br>мм/24ч | 8-10<br>мм | 8- 20<br>мм | 8- 30<br>мм | 8- 40<br>мм | 8- 50<br>мм | 8- 70<br>мм | 8-100<br>мм |
|-------------------|------------|-------------|-------------|-------------|-------------|-------------|-------------|
| 2011              | 8          | 22          | 24          | 26          | 27          | 27          | 27          |
| 2012              | 0          | 26          | 30          | 31          | 33          | 33          | 33          |
| 2013              | 8          | 28          | 31          | 31          | 31          | 32          | 33          |



Фиг. 3 Разпределение на дните с интензивни валежи за района на Шумен по години

След заместване в (17) на данните от таблица 1 за периода 1990г.-2012г. се получава следната система уравнения:

$$\begin{cases} 23.b_0 + 253.b_1 + \frac{1}{2} 3795.b_2 = 607 \\ 253.b_0 + 3795.b_1 + \frac{1}{2} 64009.b_2 = 7324 \\ 3795.b_0 + 64009.b_1 + \frac{1}{2} 1151406.b_2 = 115618 \end{cases} \quad (18)$$

От (18) за коефициентите на полинома (14) се получава:

$$b_0 = 22,0304 ; \quad b_1 = -0,1240 ; \quad b_2 = 0,0694 . \quad (19)$$

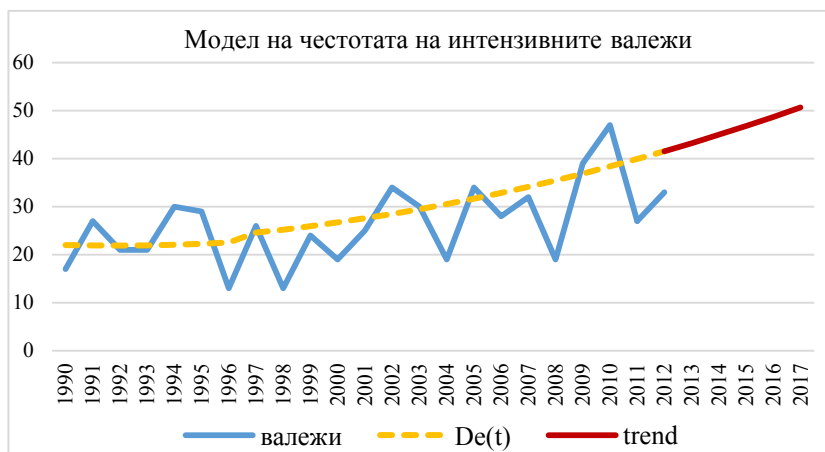
Следователно, моделът на изменение на дните с интензивни валежи за една година като функция от времето има следния вид:

$$De(t) = 22.03 - 0.1240t + 0.0694 \frac{t^2}{2!} \quad (20)$$

Изчислените стойности на  $De(t)$  за всяка от изследваните години и тенденцията на развитие за следващите пет години с Модел 1 са показани в таблица 2 и фигура 4.

Таблица 2: Резултати от изчислени и екстраполирани стойности на валежите с Модел 1

| години (t)         | 1990  | 1991  | 1992  | 1993  | 1994  | 1995  | 1996  | 1997  | 1998  | 1999  | 2000  | 2001  | 2002  | 2003  |
|--------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| бр. валежи 8-100мм | 17    | 27    | 21    | 21    | 30    | 29    | 13    | 26    | 13    | 24    | 19    | 25    | 34    | 30    |
| De(t)              | 22.03 | 21.94 | 21.92 | 21.97 | 22.09 | 22.28 | 22.54 | 24.60 | 25.24 | 25.96 | 26.74 | 27.59 | 28.52 | 29.51 |
| години (t)         | 2004  | 2005  | 2006  | 2007  | 2008  | 2009  | 2010  | 2011  | 2012  | 2013  | 2014  | 2015  | 2016  | 2017  |
| бр. валежи 8-100мм | 19    | 34    | 28    | 32    | 19    | 39    | 47    | 27    | 33    |       |       |       |       |       |
| De(t)              | 30.57 | 31.70 | 32.90 | 34.17 | 35.51 | 36.91 | 38.39 | 39.94 | 41.55 | 43.24 | 44.99 | 46.82 | 48.71 | 50.67 |



Фиг. 4 Модел на честотата на интензивните валежи в периода 1990 г.-2012 г. на територията на област Шумен и прогноза за следващите пет години

Ако се окаже, че  $s=2$  не е истинската степен на полинома, се правят подобни изчисления, но вече за  $s=3$ . Това се пояснява със следния пример.

**Модел 2:** Прави се изследване на интензивни валежи на територията на област Шумен за периода 1990г.-2012г. и прогноза за следващите пет години при  $s=3$ .

От (11) за  $L_L(t)$  се получава следният полином от трета степен:

$$L_L(t) = b_0 + b_1 \cdot t + b_2 \cdot \frac{t^2}{2!} + b_3 \cdot \frac{t^3}{3!} \quad (21)$$

Тогава системата уравнения (9) придобива вида:

$$\begin{cases} b_0 \sum_{i=0}^{n-1} w_i + b_1 \sum_{i=0}^{n-1} w_i t_i + b_2 \frac{1}{2!} \sum_{i=0}^{n-1} w_i t_i^2 + \frac{1}{3!} \sum_{i=0}^{n-1} w_i t_i^3 = \sum_{i=0}^{n-1} w_i r_i \\ b_0 \sum_{i=0}^{n-1} w_i t_i + b_1 \sum_{i=0}^{n-1} w_i t_i^2 + b_2 \frac{1}{2!} \sum_{i=0}^{n-1} w_i t_i^3 + \frac{1}{3!} \sum_{i=0}^{n-1} w_i t_i^4 = \sum_{i=0}^{n-1} w_i r_i t_i \\ b_0 \sum_{i=0}^{n-1} w_i t_i^2 + b_1 \sum_{i=0}^{n-1} w_i t_i^3 + b_2 \frac{1}{2!} \sum_{i=0}^{n-1} w_i t_i^4 + \frac{1}{3!} \sum_{i=0}^{n-1} w_i t_i^5 = \sum_{i=0}^{n-1} w_i r_i t_i^2 \\ b_0 \sum_{i=0}^{n-1} w_i t_i^3 + b_1 \sum_{i=0}^{n-1} w_i t_i^4 + b_2 \frac{1}{2!} \sum_{i=0}^{n-1} w_i t_i^5 + \frac{1}{3!} \sum_{i=0}^{n-1} w_i t_i^6 = \sum_{i=0}^{n-1} w_i r_i t_i^3 \end{cases} \quad (22)$$

След като се замести в (17) с данните от таблица 1 се получава следната система:

$$\begin{cases} 23 \cdot b_0 + 253 \cdot b_1 + \frac{1}{2} 3795 \cdot b_2 + \frac{1}{6} 64009 \cdot b_3 = 607 \\ 253 \cdot b_0 + 3795 \cdot b_1 + \frac{1}{2} 64009 \cdot b_2 + \frac{1}{6} 1151403 \cdot b_3 = 7324 \\ 3795 \cdot b_0 + 64009 \cdot b_1 + \frac{1}{2} 1151403 \cdot b_2 + \frac{1}{6} 21571033 \cdot b_3 = 115618 \\ 64009 \cdot b_0 + 1151403 \cdot b_1 + \frac{1}{2} 21571033 \cdot b_2 + \frac{1}{6} 415601835 \cdot b_3 = 2013652 \end{cases} \quad (23)$$

От (23) за коефициентите на полинома (21) се получава:

$$b_0 = 16.47; \quad b_1 = 3.25; \quad b_2 = -0.7111; \quad b_3 = 0.0707. \quad (24)$$

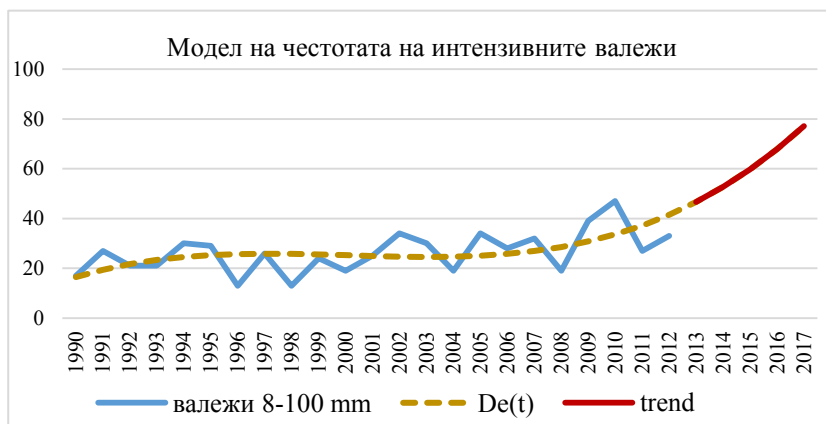
Следователно моделът на изменение на дните с интензивни валежи за една година като функция от времето има следния вид:

$$De(t) = 16.47 + 3.25 \cdot t - 0.711 \cdot \frac{t^2}{2!} + 0.0707 \cdot \frac{t^3}{3!} \quad (25)$$

Изчислените стойности на  $De(t)$  за всяка от изследваните години и тенденцията на развитие за следващите пет години с Модел 2 са показани в таблица 3 и фигура 5.

Таблица 3: Резултати от изчислени и екстраполирани стойности на броят на дните с интензивни валежи с Модел 2

| години (t)         | 1990  | 1991  | 1992  | 1993  | 1994  | 1995  | 1996  | 1997  | 1998  | 1999  | 2000  | 2001  | 2002  | 2003  |
|--------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| бр. валежи 8-100мм | 17    | 27    | 21    | 21    | 30    | 29    | 13    | 26    | 13    | 24    | 19    | 25    | 34    | 30    |
| $De(t)$            | 16.47 | 19.38 | 1.65  | 3.35  | 24.55 | 25.33 | 25.74 | 25.87 | 25.78 | 25.55 | 5.24  | 24.93 | 24.68 | 24.57 |
| години (t)         | 2004  | 2005  | 2006  | 2007  | 2008  | 2009  | 2010  | 2011  | 2012  | 2013  | 2014  | 2015  | 2016  | 2017  |
| бр. валежи 8-100мм | 19    | 34    | 28    | 32    | 19    | 39    | 47    | 27    | 33    |       |       |       |       |       |
| $De(t)$            | 24.67 | 25.05 | 25.78 | 26.93 | 28.57 | 30.77 | 33.60 | 37.14 | 41.45 | 46.60 | 52.67 | 59.72 | 67.83 | 77.07 |



Фиг.5 Модел на честотата на интензивните валежи в периода 1990г.-2012г. на територията на област Шумен и прогноза за следващите пет години

От изложеното ясно се вижда, че голям недостатък на горния метод за анализ е, че 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. Както се вижда (от представените модели 1 и 2) в разгледания пример има драстична разлика между

стойностите на коефициентите  $b$  при изчисления с полином от втора степен (19)  $-b_0 = 22.03$ ,  $b_1 = -0.1240$ ,  $b_2 = 0.0694$  и при изчисления с полином от трета степен (24)  $-b_0 = 16.47$ ,  $b_1 = 3.25$ ,  $b_2 = -0.7111$ ,  $b_3 = 0.0707$ . Ако вместо обикновен полином (10) се използва ортогонален полином на Чебишев, процедурата по съгласуване на степента на полинома с емпиричните данни се осъществява много по-лесно. Това е причината да се разглежда и анализира честотата на природните бедствия чрез ортогонални полиноми на Чебишев.

В този случай полиномът (11)

$$L_L(t) = b_0 + b_1 \cdot t + b_2 \cdot \frac{t^2}{2!} + \dots + b_s \cdot \frac{t^s}{s!},$$

се представя във формата на сума от ортогонални полиноми на Чебишев [3]:

$$L(t) = \sum_{n=0}^s \hat{C}_n \cdot Z_n(t) \quad (26)$$

Тук  $\hat{C}_n, n = 0, 1, \dots, s$  са статистически оценки на коефициентите,  $Z_n(t)$  е полином на Чебишев от  $n$ -ти ред, дефиниран върху множеството  $\{t_1, t_2, \dots, t_N\}$ , който се определя по следната рекурентната формула:

$$Z_0(t) = 1$$

$$Z_n(t) = t^n - \sum_{j=0}^{n-1} \frac{\sum_{i=1}^m t_i^n Z_n(t_i)}{\sum_{i=1}^m Z_j^2(t_i)} Z_j(t), \quad n = 1, 2, \dots, s; j = 0, 1, \dots, n-1, \quad (27)$$

Или стойностите на ортогоналните полиноми на Чебишев  $Z_0(t), Z_1(t), Z_2(t), \dots, Z_n(t)$  с първи коефициент равен на единица, по-удобно се изчисляват по следния начин:

$$\begin{aligned} Z_0(t) &= 1, \\ Z_1(t) &= t \end{aligned} \quad (28)$$

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

където регресионните коефициенти  $\hat{C}_j$  и променливите  $H_j$  се изчисляват по формулите:

$$\hat{C}_j = \frac{1}{H_j} \sum_{i=1}^N v_i Z_j(t_i) \quad (j = 0, 1, \dots, n; n < N) \quad (29)$$

при съответната стойност на  $N$

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

$v_i$  – брой на дните с анализираното природно бедствие в  $i$ -та година,

$N$  – броя на разглежданите години,

а  $t_i = \frac{tk - \bar{t}}{h}$  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  $\bar{t} = \frac{1+2+\dots+N}{N}$ .

Както е известно [3], оценката, която е прието да се нарича "изгладена функция", има вида (21):

$$\hat{L}(t_j) = \sum_{n=0}^s \hat{C}_n \hat{Y}_n(t_i). \quad (30)$$

$$\hat{C}_n = \frac{\sum_{i=1}^m v_i \cdot Y_n(t_i) \cdot w_i}{\sum_{i=1}^m Y_n^2(t_i)}, \quad n = 0, 1, \dots, \quad (31)$$

$$Y_n(t_i) = \frac{Z_n(t_i)}{\sqrt{w_i}}, \quad n = 0, 1, \dots, s \quad \text{и} \quad w_i = \frac{\sigma_0^2}{\sigma_i^2} \quad (32)$$

$\hat{L}(t_j)$  е обобщение на полиномите (26).  $Y_n(t_i)$  се наричат полиноми на Чебишев с тежест, тъй като се отчита относителното значение (тежестта)  $w_i$  на  $i$  – то измерване.

Въвеждането на тежестите на измерванията позволява да се извършва изглаждане на явленията, както по данни за една метеорологична станция, така и по данни на различни метеорологични станции.

Използването на сумата (26) в сравнение с класическия метод има следните *предимства*:

1) Статистическите оценки на коефициентите  $\hat{C}_n$  в (26) се получават направо от резултатите на измерванията;

2) Тъй като грешките на последователните измервания на честотата на анализираното природно бедствие с интервал на отчитане 24 часа са независими, то следва и оценките на коефициентите  $\hat{C}_n$  в (26) да са независими в съвкупност;

3) Ако се окаже, че при използването на сума от полиноми от ред  $s$  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 изключително много разработването на модели на природните бедствия.

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 (10) и (26) 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 модели за честотата на екстремни природни явления. Ето защо следва да се представи алгоритъм за модел на честотата на природните бедствия със сума от вида (28) и е доказана неговата ефективност.

### **Алгоритъм за синтез на модел за честотата на природно бедствие**

От направения анализ произтича следният алгоритъм за модел за честотата на конкретен вид природно бедствие.

*Стъпка 1:* Намиране на оптимална степен на полинома  $L(t)$  по (26):

$$L(t) = \sum_{n=0}^s \hat{C}_n \cdot Z_n(t),$$

На практика степента  $s$  на полинома описващ еволюцията на честотата на анализираното природно бедствие е неизвестна. От нея съществено зависи точността на модела и грешките на прогнозите. По тази причина възниква проблемът за оптимален избор на  $s$  [4].

За определяне оптималната степен  $n_0$  на полинома, описващ тенденцията в честотата на изследваното природно бедствие, е необходимо:

1.1. Да се изчислят оценките на коефициентите  $\hat{C}_0, \hat{C}_1, \hat{C}_2, \dots$ , както и коефициентите  $H_j$  по (29) за разглеждания брой години  $N$ .

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

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

1.2. Да се намерят стойностите на полиномите  $Z_0(t), Z_1(t), Z_2(t), \dots, Z_n(t)$ , по (28).

$$Z_0(t) = 1,$$

$$Z_1(t) = t$$

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

1.3. Да се изчисли сумата от квадратите на отклоненията  $S_n$  по:

$$S_n = \sum_{k=1}^N w_k v_k^2 - (\hat{C}_0^2 H_0 + \hat{C}_1^2 H_1 + \dots + \hat{C}_n^2 H_n) \quad (33)$$

представляваща обективна оценка на дисперсията  $\sigma^2$  относно изгладената крива на изменението на честотата на природното бедствие.

Добавянето на всеки нов член  $\hat{C}_{n+1} Z_{n+1}(t)$  в сумата (33) на ортогоналните полиноми  $Z_j(t)$  намалява отклонението  $S_n$  с величината  $\hat{C}_{n+1}^2 H_{n+1}$ .

Отношението

$$\sigma_n^2 = \frac{S_n}{N-n-1} = \frac{1}{N-n-1} \sum_{k=1}^N w_k [v_k - \sum_{j=0}^n (\hat{C}_j)_e Z(t_k)]^2 \quad (34)$$

служи за обективна оценка на дисперсията  $\sigma^2$ , при произволно  $n \geq n_0$ .

Всяко значение на  $S_n$ , изчислено по (33) трябва да се раздели на числото  $N - n_0 - 1$  и полученото отношение (34) да се сравни с предходното значение на това отношение. Трябва да се повишава степента на полинома до тогава, докато разликата между две съседни значения на дисперсията (35) е минимална т.е.

$$\sigma_{n_0}^2 = \frac{S_{n_0}}{N-n_0-1} \approx \frac{S_{n_0+1}}{N-n_0-2} = \sigma_{n_0+1}^2. \quad (35)$$

Това значение  $n = n_0$ , при което разликата между две съседни значения на дисперсията  $\Delta\sigma^2$  е минимална, дава оптималната степен на полинома.

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

Така търсения полином, изразяващ математически честотата на природното бедствие, се записва във вида:

$$L(t) = \sum_{j=0}^{n_0} \hat{C}_j Z_j(t) = \hat{C}_0 Z_0(t) + \hat{C}_1 Z_1(t) + \dots + \hat{C}_n Z_n(t) \quad (36)$$

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  $\eta_k$  в измерените значения на функциите  $\nu_k$  предизвикват грешки  $\beta_j$  при определяне на коефициентите  $\hat{C}_j$ . Грешките  $\beta_j$  ще са независими и ще бъдат разпределени нормално с център 0 и дисперсии  $\frac{\sigma^2}{H_j}$  ( $j = 0, 1, \dots, n$ ).

В конкретния случай дисперсията  $\sigma^2$  на резултатите от измерванията се оценява с величината  $\frac{\sigma^2}{H_j}$ . 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:  $\sigma(\hat{C}_j) = \sqrt{\frac{\sigma_0^2}{H_j}}$ , при  $j = 0, 1, 2, \dots, n_0$ . Намерените по-горе значения на коефициентите  $\hat{C}_j$  се закръглят, като се съобразява броят цифри след десетичната запетая.

*Стъпка 2:* Изчисляване на изгладените и екстраполираните стойности.

След заместване в (26) се изчислят изгладените стойности на честотата на изследваното природно бедствие. Аналогично, прогнозираното значение на честотата на природното бедствие в годината  $t_e$  се намира по формула (37):

$$\hat{L}(t_e) = \sum_{n=0}^r \hat{C}_n \frac{Z_n(t_e)}{\sqrt{w_e}} \quad (37)$$

*Стъпка 3:* Извеждане на статистическия модел на честотата на природното бедствие.

Като се заместят получените значения във формула (26) 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.

### **Модел за честотата на възникване на интензивни валежи за района на Шумен**

За подобряване работата на държавните органи, ангажирани с предотвратяването или ликвидирането на вредните последиствия при природни бедствия, вследствие интензивни валежи, е необходимо да се направят научно обосновани прогнози за честотата на интензивните валежи през следващите няколко години. Решаването на тази важна практическа задача е възможно чрез разработване на статистически модел на честотата на валежите.

#### ***Модел 1 на честотата на интензивни валежи***

Прави се изследване на дните с интензивни валежи на територията на област Шумен за периода 1990г.-2012г. и прогноза за следващите пет години. Следвайки представения алгоритъм и методиката на приложението му, изчисленията за интензивните валежи са обобщени в таблици 4, 5 и 6.

Таблица 4: *Резултати от изчисленията на изгладените регресионни коефициенти и отношенията  $H_j/H_{j-1}$  за Модел 1*

| <b><i>n</i></b>                                | 0       | 1      | 2      | 3                      | 4                      | 5                   | 6                    | 7                  |
|------------------------------------------------|---------|--------|--------|------------------------|------------------------|---------------------|----------------------|--------------------|
| <b><i><math>\hat{C}_j</math></i></b>           | 26.3913 | 0.6393 | 0.0347 | $-1.824 \cdot 10^{-2}$ | $-1.114 \cdot 10^{-3}$ | $9.4 \cdot 10^{-5}$ | $-3.8 \cdot 10^{-5}$ | $-6 \cdot 10^{-6}$ |
| <b><i><math>\frac{H_j}{H_{j-1}}</math></i></b> | 44      | 35     | 33.43  | 32.57                  | 31.82                  | 31.03               | 30.15                | 29.18              |

**Таблица 5: Резултати**  
**от изчисленията за интензивни валежи с Модел 1**

| <b>t</b>             | <b>v</b>   | <b>(v - <math>\bar{c}_0</math>)<sup>2</sup></b> | <b>Z<sub>1</sub></b> | <b>v * Z<sub>1</sub></b> | <b>Z<sub>2</sub></b> | <b>v * Z<sub>2</sub></b> | <b>Z<sub>3</sub></b> | <b>Z<sub>4</sub></b> | <b>Z<sub>5</sub></b> | <b>Z<sub>6</sub></b> | <b>Z<sub>7</sub></b> |
|----------------------|------------|-------------------------------------------------|----------------------|--------------------------|----------------------|--------------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| 1                    | 17         | 88.20                                           | -11                  | -187                     | 77                   | 1309                     | -462                 | 2508.00              | -12540               | 58140.00             | -250449.23           |
| 2                    | 27         | 0.37                                            | -10                  | -270                     | 56                   | 1512                     | -210                 | 228.00               | 4560                 | -52854.55            | 387057.90            |
| 3                    | 21         | 29.07                                           | -9                   | -189                     | 37                   | 777                      | -18                  | -1074.86             | 10260                | -58140.00            | 204913.01            |
| 4                    | 21         | 29.07                                           | -8                   | -168                     | 20                   | 420                      | 120                  | -1628.57             | 9120                 | -21141.82            | -113840.56           |
| 5                    | 30         | 13.02                                           | -7                   | -210                     | 5                    | 150                      | 210                  | -1637.14             | 4620                 | 19750.91             | -281605.59           |
| 6                    | 29         | 6.81                                            | -6                   | -174                     | -8                   | -232                     | 258                  | -1280.57             | -720                 | 45065.45             | -248052.59           |
| 7                    | 13         | 179.33                                          | -5                   | -65                      | -19                  | -247                     | 270                  | -714.86              | -5220                | 48845.45             | -82261.26            |
| 8                    | 26         | 0.15                                            | -4                   | -104                     | -28                  | -728                     | 252                  | -72.00               | -7920                | 33970.91             | 109857.90            |
| 9                    | 13         | 179.33                                          | -3                   | -39                      | -35                  | -455                     | 210                  | 540.00               | -8460                | 8198.18              | 237902.10            |
| 10                   | 24         | 5.72                                            | -2                   | -48                      | -40                  | -960                     | 150                  | 1037.14              | -6960                | -19080.00            | 254114.69            |
| 11                   | 19         | 54.63                                           | -1                   | -19                      | -43                  | -817                     | 78                   | 1359.43              | -3900                | -39354.55            | 160363.64            |
| 12                   | 25         | 1.94                                            | 0                    | 0                        | -44                  | -1100                    | 0                    | 1470.86              | 0                    | -46800.00            | 0.00                 |
| 13                   | 34         | 57.89                                           | 1                    | 34                       | -43                  | -1462                    | -78                  | 1359.43              | 3900                 | -39354.55            | -160363.64           |
| 14                   | 30         | 13.02                                           | 2                    | 60                       | -40                  | -1200                    | -150                 | 1037.14              | 6960                 | -19080.00            | -254114.69           |
| 15                   | 19         | 54.63                                           | 3                    | 57                       | -35                  | -665                     | -210                 | 540.00               | 8460                 | 8198.18              | -237902.10           |
| 16                   | 34         | 57.89                                           | 4                    | 136                      | -28                  | -952                     | -252                 | -72.00               | 7920                 | 33970.91             | -109857.90           |
| 17                   | 28         | 2.59                                            | 5                    | 140                      | -19                  | -532                     | -270                 | -714.86              | 5220                 | 48845.45             | 82261.26             |
| 18                   | 32         | 31.46                                           | 6                    | 192                      | -8                   | -256                     | -258                 | -1280.57             | 720                  | 45065.45             | 248052.59            |
| 19                   | 19         | 54.63                                           | 7                    | 133                      | 5                    | 95                       | -210                 | -1637.14             | -4620                | 19750.91             | 281605.59            |
| 20                   | 39         | 158.98                                          | 8                    | 312                      | 20                   | 780                      | -120                 | -1628.57             | -9120                | -21141.82            | 113840.56            |
| 21                   | 47         | 424.72                                          | 9                    | 423                      | 37                   | 1739                     | 18                   | -1074.86             | -10260               | -58140.00            | -204913.01           |
| 22                   | 27         | 0.37                                            | 10                   | 270                      | 56                   | 1512                     | 210                  | 228.00               | -4560                | -52854.55            | -387057.90           |
| 23                   | 33         | 43.67                                           | 11                   | 363                      | 77                   | 2541                     | 462                  | 2508.00              | 12540                | 58140.00             | 250449.23            |
| <b>S<sub>n</sub></b> | <b>607</b> | <b>1487.48</b>                                  | <b>-</b>             | <b>647</b>               | <b>-</b>             | <b>1229</b>              | <b>-</b>             | <b>-</b>             | <b>-</b>             | <b>-</b>             | <b>-</b>             |

| $t$   | $v$ | $(v - \hat{c}_0)^2$ | $Z_1$ | $v * Z_1$ | $Z_2$ | $v * Z_2$ | $Z_3$   | $Z_4$       | $Z_5$      | $Z_6$              | $Z_7$              |
|-------|-----|---------------------|-------|-----------|-------|-----------|---------|-------------|------------|--------------------|--------------------|
| $H_j$ | -   | -                   | 1020  | -         | 35420 | -         | 1184040 | 11018821.14 | 1227096000 | $3.4001 * 10^{16}$ | $1.2433 * 10^{20}$ |

Таблица 6: Резултати от изчисленията на дисперсията при различните степени на полинома

| $n$                                       | 0     | 1      | 2     | 3     | 4     | 5     | 6     | 7     |
|-------------------------------------------|-------|--------|-------|-------|-------|-------|-------|-------|
| $\sigma^2$                                | 67.59 | 44.694 | 41.83 | 40.66 | 37.58 | 36.11 | 32.76 | 30.10 |
| $\Delta\sigma_n^2 - \Delta\sigma_{n+1}^2$ |       | 2.29   | 2.86  | 1.17  | 3.08  | 1.47  | 3.35  | 2.68  |

От таблица 6 се вижда, че разликата между две съседни значения на дисперсията  $\sigma^2$  е минимална при  $n_0 = 2$

$$2.86 = \frac{S_2}{N-2-1} \approx \frac{S_3}{N-3-1} = 1.17$$

и  $n_0 = 2$  може да се приеме за оптимална степен на полинома (26).

След като са направени всички преобразувания по стъпка 2 и стъпка 3 от алгоритъма, статистическият модел за честотата на интензивни валежи, представен като сума от полиноми на Чебишев за период от 23 години има вида:

$$\hat{L}(t_j) = \hat{C}_0 Z_0(t_1) + \hat{C}_1 Z_1(t_2) + \hat{C}_2 Z_2(t_2) = \hat{C}_0 + \hat{C}_1 t + \hat{C}_2 (t^2 - 44) = 24.86 + 0.6393 * t + 0.0347 * t^2 \quad (38)$$

Изчислените стойности на  $\hat{L}(t_j)$  за всяка от изследваните години и екстраполираните стойности за следващите пет години са показани в таблица 7.

Таблица 7: Резултати от изчислени и екстраполирани стойности на интензивни валежи с Модел 1

| Години (t)           | 1990  | 1991  | 1992  | 1993  | 1994  | 1995  | 1996  | 1997  | 1998  | 1999  | 2000  | 2001  | 2002  | 2003  |
|----------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| бр. валежи 8-100 mm  | 17    | 27    | 21    | 21    | 30    | 29    | 13    | 26    | 13    | 24    | 19    | 25    | 34    | 30    |
| $\hat{L}(t_j)_{s=2}$ | 22.03 | 21.94 | 21.92 | 21.97 | 22.09 | 22.28 | 22.54 | 22.86 | 23.26 | 23.72 | 24.26 | 24.86 | 25.54 | 26.28 |
| Години (t)           | 2004  | 2005  | 2006  | 2007  | 2008  | 2009  | 2010  | 2011  | 2012  | 2013  | 2014  | 2015  | 2016  | 2017  |
| бр. дни              | 19    | 34    | 28    | 32    | 19    | 39    | 47    | 27    | 33    |       |       |       |       |       |
| $\hat{L}(t_j)_{s=3}$ | 27.09 | 27.98 | 28.93 | 29.95 | 31.04 | 32.20 | 33.43 | 34.73 | 36.10 |       |       |       |       |       |

|       |  |  |  |  |  |  |  |  |  |       |       |       |       |       |
|-------|--|--|--|--|--|--|--|--|--|-------|-------|-------|-------|-------|
| trend |  |  |  |  |  |  |  |  |  | 37.53 | 39.04 | 40.62 | 42.26 | 43.98 |
|-------|--|--|--|--|--|--|--|--|--|-------|-------|-------|-------|-------|

Следователно статистическият модел на интензивни валежи на територията на област Шумен има визуализацията от фигура 6. От фигурата и изчисленията на модела в таблица 7 е видно, че тенденцията в честотата на интензивните валежи е към повишаване.



Фиг. 6 Модел на честотата на интензивни валежи в периода 1990г.-2012г. на територията на област Шумен и прогноза за следващите пет години

Предвид изложеното, изследването на честотата на природните бедствия може да се направи с висока точност като се използва полином на Чебишев от вида (26).

### Прогнози относно честотата на интензивни валежи в област Шумен

От направените изследвания за честотата на природните бедствия в област Шумен се вижда, че в краткосрочен план анализираните явления имат тенденция за повишаване. В изчисленията на моделите не са отчетени стойностите за 2013г. и 2014г., които в някои случаи са около 30% от стойностите за 2012г., а при други превишават почти два пъти отчетените данни

в предходните години. Това налага по детайлен анализ и корекция на моделите, като се отчетат данните за следващите години или се вземат с по-малка тежест тези години, имащи минимални или максимални стойности на екстремните явления.

### **Модел 2 на честотата на интензивни валежи**

Прави се изследване на дните с интензивни валежи на територията на област Шумен за периода 1990г.-2012г. и прогноза за следващите пет години. Използват се данните в таблица 1 и алгоритъмът, като степента на полинома се определя на  $n_0 = 3$ .

След като са направени всички изчисления и преобразувания по стъпка 2 и стъпка 3 от алгоритъма, статистическия модел на дните с интензивни валежи, изразен чрез сума от полиноми на Чебишев за период от 23 години има вида:

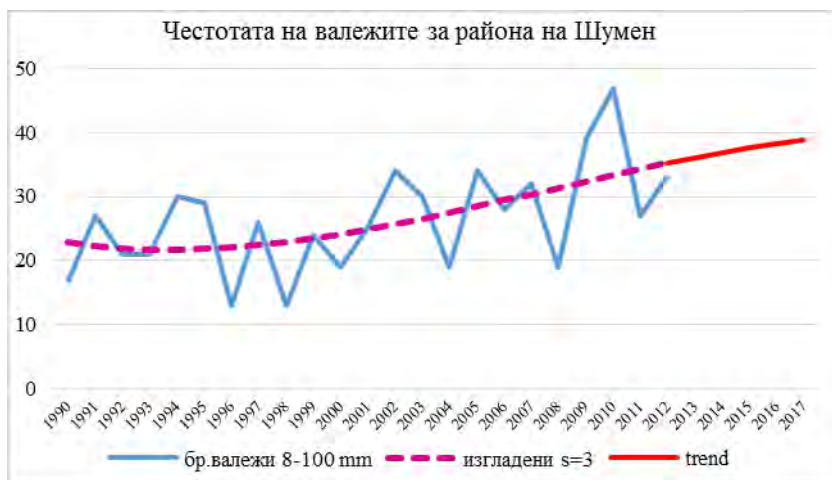
$$\hat{L}(t_j) = \sum_{j=0}^3 \hat{C}_j Z_j(t) = \hat{C}_0 + \hat{C}_1 t + \hat{C}_2 (t^2 - 44) + \hat{C}_3 (t^3 - 79 t) = 24.8645 - 0.7834t + 0.0347t^2 - 0.0018t^3 \quad (39)$$

Изчислените стойности на  $\hat{L}(t_j)$  за всяка от изследваните години и екстраполираните стойности за следващите пет години са показани в таблица 8.

Таблица 8: Резултати от изчислени и екстраполирани стойности на интензивни валежи с Модел 2

| Години (t)            | 1990  | 1991  | 1992  | 1993  | 1994  | 1995  | 1996  | 1997  | 1998  | 1999  | 2000  | 2001  | 2002  | 2003  |
|-----------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| бр. валежи 8-100мм    | 17    | 27    | 21    | 21    | 30    | 29    | 13    | 26    | 13    | 24    | 19    | 25    | 34    | 30    |
| $\hat{L}(t_j)$<br>s=3 | 22.87 | 22.32 | 21.95 | 21.75 | 21.71 | 21.81 | 22.04 | 22.40 | 22.88 | 23.45 | 24.12 | 24.86 | 25.68 | 26.56 |
| Години (t)            | 2004  | 2005  | 2006  | 2007  | 2008  | 2009  | 2010  | 2011  | 2012  | 2013  | 2014  | 2015  | 2016  | 2017  |
| бр. валежи 8-100мм    | 19    | 34    | 28    | 32    | 19    | 39    | 47    | 27    | 33    |       |       |       |       |       |
| $\hat{L}(t_j)$<br>s=3 | 27.48 | 28.44 | 29.42 | 30.42 | 31.42 | 32.42 | 33.40 | 34.34 | 35.25 |       |       |       |       |       |
| trend                 |       |       |       |       |       |       |       |       |       | 36.11 | 36.91 | 37.63 | 38.27 | 38.81 |





Фиг. 7: *Модел на честотата на интензивните валежи за периода 1990г.-2012г. на територията на област Шумен и прогноза за следващите пет години*

Следователно статистическият модел на изменение на честотата на дните с интензивни валежи за период от 23 години на територията на област Шумен е илюстриран на фигура 7. От фигурата се вижда също тенденция на увеличаване на броя на дните с интензивни валежи.

### **Модел 3 на честотата на интензивни валежи**

Прави се изследване на дните с интензивни валежи на територията на област Шумен за периода 1996г.-2013г. и прогноза за следващите пет години. Използват се данните в таблица 1 и алгоритъма, като степента на полинома се избира да е  $n_0 = 3$ .

След като се направят всички изчисления и преобразувания по стъпка 2 и стъпка 3 от алгоритъма, може да се запише в окончателен вид модела за изменение на интензивните валежи.

Следователно статистическият модел на изменение на броя на дните с интензивни валежи за област Шумен чрез полиномите на Чебишев за период от 17 години има вида:

$$\hat{L}(t_j) = \sum_{j=0}^3 \hat{C}_j Z_j(t) = \hat{C}_0 + \hat{C}_1 t + \hat{C}_2 (t^2 - 26.92) + \hat{C}_3 (t^3 - 48.25 t) = 28.9941 + 1.0736t - 0.0556t^2 - 0.0005t^3 \quad (40)$$

Изчислените стойности на  $\hat{L}(t_j)$  за всяка от изследваните години и екстраполираните стойности за следващите пет години са показани в таблица 9.

Таблица 9: Резултати от  
Изчислени стойности на интензивни валежи с Модел 3

| Години (t)           | 1996  | 1997  | 1998  | 1999  | 2000  | 2001  | 2002  | 2003  | 2004  | 2005  | 2006  | 2007  |
|----------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| бр. валежи 8-100мм   | 13    | 26    | 13    | 24    | 19    | 25    | 34    | 30    | 19    | 34    | 28    | 32    |
| $\hat{L}(t_j)_{s=3}$ | 16.16 | 18.03 | 19.81 | 21.50 | 23.09 | 24.58 | 25.97 | 27.26 | 28.44 | 29.52 | 30.48 | 31.32 |
| Години (t)           | 2008  | 2009  | 2010  | 2011  | 2012  | 2013  | 2014  | 2015  | 2016  | 2017  | 2018  |       |
| бр. валежи 8-100мм   | 19    | 39    | 47    | 27    | 33    | 33    |       |       |       |       |       |       |
| $\hat{L}(t_j)_{s=3}$ | 32.05 | 32.65 | 33.13 | 33.49 | 33.71 | 33.81 |       |       |       |       |       |       |
| trend                |       |       |       |       |       |       | 33.76 | 33.58 | 33.26 | 32.80 | 32.19 |       |



Фиг. 8 Модел на честотата на интензивни валежи в периода 1996г.-2013г. на територията на област Шумен и прогноза за следващите пет години

Моделът е визуализиран на фигура 8. От нея и изчисленията на модела в таблица 6 се вижда, че има плавно нарастване на дните

с интензивни валежи, като това нарастване се стабилизира в последните години и тенденцията е към намаляване.

### **Софтуерна система за автоматизирано синтезиране на модели за честота на природни бедствия**

За изпълнение целта на изследването е разработена универсална компютърна програма, работеща в средата на Матлаб, която реализира практически използването на Алгоритъма на модел за честотата на природните бедствия.

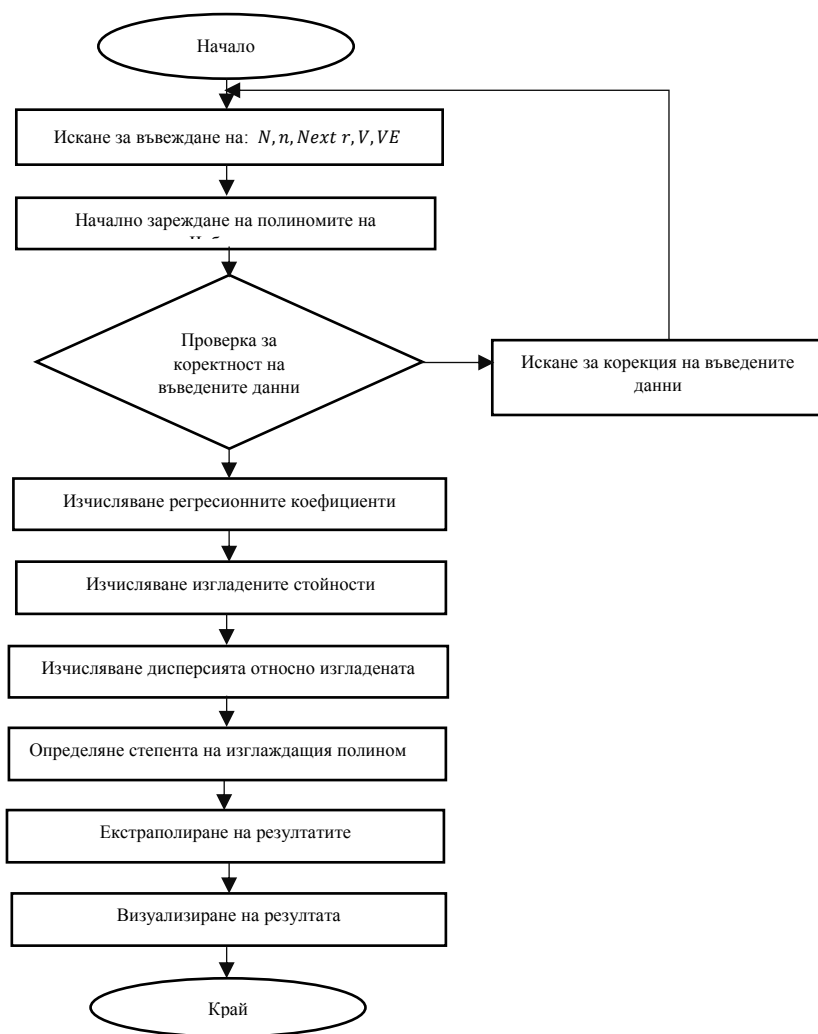
Работата на програмата се пояснява с блок-схемата от фигура 9 и може да се опише както следва.

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

- $N$  – брой на изследваните години, които при различните моделите в дисертационния труд бяха използвани стойности  $N = 17, 18, 23$ ;
- $n$  – максимална степен на полиномите на Чебишев, която трябва да бъде просто число и при моделите в дисертационния труд беше ползвана само стойността  $n = 8$ ;
- $Next\ r$  – екстраполираните стойности. При моделите в доклада се изчислява тренда само за пет години и се ползва само стойността  $Next\ r = 5$ ;
- $NE$  – общ брой на годините, като  $NE = N + Next\ r$ .

2) Следващата стъпка е въвеждане данните за изследваното явление:

- $V$  – брой природни бедствия за всяка от разглежданите години, които приемат различни стойности в зависимост от изследваното природно явление;



Фиг. 9 Блок-схема на универсална програма, реализираща алгоритъм за синтез на модел за честотата на природните бедствия

- $VE$  – брой екстраполирани природни бедствия за всяка от разглежданите години, които приемат различни стойности в зависимост от изследваното природно явление и изчисленията;

- $t_{sr}$  – средна стойност на изследвания период с природни бедствия;

- $t_{srex}$  – средна екстраполирана стойност 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:

- $Z_0(t), Z_1(t), Z_2(t), \dots, Z_n(t)$  са полиномите на Чебишев. При изчисляване моделите в доклада се използват стойностите  $n = 2, 3, 4, 5, 8$ .

- $A$  – отношения на коефициентите  $\frac{H_j}{H_{j-1}}$ , при изчисляване стойностите на полиномите.

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  $j = 1, 2, \dots, n$ ;

6) Изчисляване изгладените стойности  $Vizgl(I)$  на честотата на изследваното природно бедствие;

7) Изчисляване дисперсията относно изгладената крива –  $Dis.(\sigma^2)$ ;

8) Екстраполиране на резултатите:

- $VizglE(I)$  – екстраполирано значение на природното бедствие в годината  $t_e$ ;

9) Визуализация на резултатите:

- изчертаване развитието на честотата на изследваното природно бедствие;

- 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 и се отчитат изгладените и екстраполираните стойности на

честотата на изследваното природно бедствие. На тази база се изчислява и визуализира търсеният полином.

### **Заклучение**

В заключение можем да обобщим, че използването на математически методи за анализ и синтез на бедствени ситуации и по-конкретно ортогонални полиноми на Чебишев, многократно улеснява обработката на резултатите, чрез които са вземат обосновани управленски решения.

Въпреки своите важни положителни свойства, изглаждането с помощта на ортогонални полиноми на Чебишев 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 настоящата работа е показано, че поради еднозначно обратимо съответствие между (10) и (36) 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 оценяване честотата на природни бедствия.

### **ЛИТЕРАТУРА:**

1. Атанасов Б., Количествени методи в управлението на бизнеса, кн.1, Варна 1994
2. Гатев К., Обща теория на статистиката, София 1983
3. Димитров Б., Янев Н., Вероятности и статистика, София 1998
4. Петков П., Статистика, ВСУ "Черноризец Храбър" 2001
5. Гмурман В.Е., Теория вероятностей и математическая статистика, Москва 1977
6. Кендал М., Стюарт А., Статистические выводы и связи, Москва 1973
7. Рушимский Л.З., Математическая обработка результатов эксперимента, Москва 1971
8. Dimanova D., "Theory of modeling", Association Scientific and Applied Research, International Journal, Vol. 4, 2013

# Планиране на четвърто поколение мрежи (WLAN, All-IP, OFDM)

Драгомир И. Василев, Иван К. Цонев

## "4G Network Planning (WLAN, All-IP, OFDM)" Dragomir I. Vasilev, Ivan K. Tsonev

**ABSTRACT:** *With the expansion of third-generation networks and attempts to increase speed technology of fourth generation networks is already underway, as true forecasts of experts in the mobile industry. The deployment of fourth generation networks are now a reality and is introduced by some mobile operators and suppliers. But why is this necessary technology 4G, when 3G networks appear to meet the market enough and are still adequate to the requirements of the local high transfer speeds and quality of service?*

**KEYWORDS:** *OFDM, All-IP Networks, RNC, BSC, BTS*

С разширението на мрежите трето поколение и опитите да повишат скоростта, технологията на четвърто поколение мрежи вече е в ход, като сбъдна прогнозите на експертите в мобилната индустрия. Разгръщането на мрежите от четвърто поколение вече е реалност и е въведена от някои мобилни оператори и доставчици. Но защо е необходима тази технология 4G, когато 3G мрежите изглежда задоволяват пазара достатъчно, и са все още адекватни към изискванията на абонатите за високи скорости на трансфер и качеството на услугата?

Отговорът е, че настоящите възможности на 3G мрежите се считат за значително по-малки от прогнозните за бъдещите изисквания и приложения. Също така, бъдещите мрежи трябва да бъдат много по – евтини, което да сваля разходите на потребителите. Следователно концепциите за необходимост могат да бъдат дефинирани така:

- Мрежите от четвърто поколение ще предоставят на абонатите по-висока честотна лента и мобилна скорост на данните от 100 Mbps и повече;

- Мрежите от трето поколение, няма да могат да отговорят на нуждите от услуги, като видео конференции, видео с висока резолюция и др. по отношение качество на услугите (QoS);

- Ще има по - голяма мобилност и по-ниски разходи.

- Ще бъде възможна интеграцията на WLAN и WAN.

Първото изследване свързано с мрежите четвърто поколение е проведено в началото на 1990 г., и е било свързано с това да се разработи технология, която би могла да осигури много високи скорости на трансфер, като едновременно гарантира и качеството на услугите. Тази технология може да се види например при мобилните телефони, работещи във високоскоростни превозни средства, като например влакове, движещи се в повече от 200km/h.

Настоящите изисквания на абонатите включват изтегляне на видеоклипове, музика и други файлове, но бъдещето изглежда се движи към приложения, като онлайн игри, които изискват огромен капацитет, по-голямо качество на услугите (QoS) а също така и много ниски разходи. В обобщение може да кажем, че една 4G мрежа трябва да бъде в състояние да предоставя високо ефективни и рентабилни решения за потребителите на безжичните мрежи.

| Основни функции      | 3G                          | 4G                           |
|----------------------|-----------------------------|------------------------------|
| Скорост данни        | 384kbps - 2Mbps             | 20-100 Mbps                  |
| Честотна лента       | 1.8-2.4 GHz                 | 2-8 GHz                      |
| Bandwidth            | 5 MHz                       | About 100 MHz                |
| Ключови техники      | Верижна и пакетна комутация | Изцяло цифрова с пакети глас |
| Технология за достъп | WCDMA, CDMA, IPv4.0, IPv6.0 | OFDMA, MC-CDMA, IPv6.0       |

Таблица 1. Основни разлики между трето и четвърто поколение мрежи

### **Ключови технологии в четвъртото поколение мрежи**

Въпреки че има няколко технологии, които се смятат за основни при мрежите от четвърто поколение, OFDM (Orthogonal

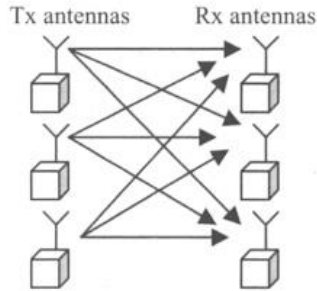


Frequency Division Multiplexing) технологията се оказва ключова на физическо ниво, както и All-IP и WLAN за по-горните слоеве.

### **OFDM (Orthogonal Frequency Division Multiplexing)**

Мултиплексиране чрез ортогонално честотно делене (OFDM) е техника, която се използва за предаване на големи пакети данни чрез радио сигнал. В основата и стои използване на честотно разделяне на сигнала, при което високоскоростния поток от данни се разбива на няколко относително нискоскоростни потоци всеки, от които се предава на отделна подносеща честота с последващото им обединяване в един сигнал. OFDM напълно изпълнява най-важните изисквания на 4G мобилни мрежи: по-голямо покритие и капацитет, с желаните QoS при минимални разходи. OFDM модулацията в този стандарт използва 84 подносещи в честотния диапазон от 4,5MHz до 21 MHz, при което отделните подносещи се модулират с помощта на фазова модулация (DQPSK, DBPSK), всяка със своята последователност от битове и след това се сумират, за да формират един информационен пакет – OFDM Symbol. В предавателя генерацията на OFDM Symbol става с Обратно преобразуване на Фурие, а при приемане се разлага на отделните съставни (хармоници), чрез Прямо преобразуване на Фурие.

Покритието в CDMA системите се ограничава, тъй като все по-голям брой потребители използват площта на една клетка. Планирането на мрежата с използване на OFMD е доста сходен с този за GSM / GPRS. Поради тази причина, функцията за управление на мощността в мрежата не е толкова важно, колкото при WDCMA мрежите, в които се налага регулиране на мощността на излъчване и разширяване на спектъра, за да се намалят смущенията. В OFDM радио мрежите, се изисква точно честотно компенсиране. Увеличаването на броя на антените може да увеличи капацитета, следователно Multiple-input/multiple-output (MIMO) антенни системи могат да бъдат използвани, както е показано на Фигура 1.

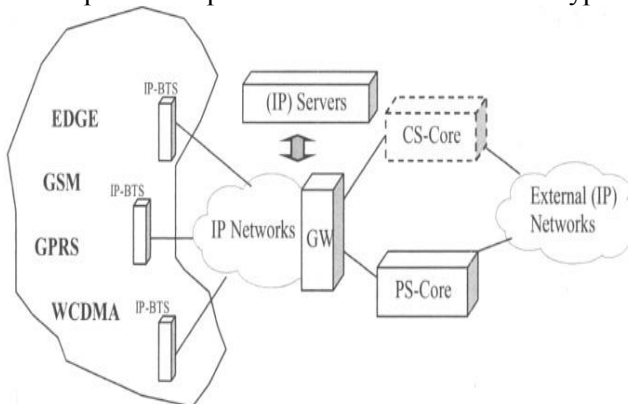


Фигура 1. Увеличаване капацитета използвайки Multiple-input/multiple - output (MIMO) антенни системи

### All-IP Networks

#### Структура

Безжична IP мрежа се състои от два компонента: безжична мрежа за достъп и фиксирана основна мрежа. Най – голямото предизвикателство пред тази технология е управлението на ресурсите, за осигуряване безпроблемно обслужване и функциониране на двете среди - фиксирана и мобилна без да се нарушава качеството на предоставяне на услугата. Освен това всяка безжична мрежа има потенциално своя собствена безжична технология и административни политики, което прави още по трудно намирането на единен механизъм за управление на ресурсите. Опростена мрежа All-IP е показан на Фигура 2.



Фигура 2. Примерна All-IP мрежа

Най - важната разлика между мрежата All-IP и съществуващите 2G и 3G мрежи е в функционалността на RNC (Radio Network Controller) и BSC (Base Station Controller), която в случая се разпространява между BTS (Base Transceiver Station), чрез набор от сървъри и шлюзове. Различни елементи в тази мрежа са:

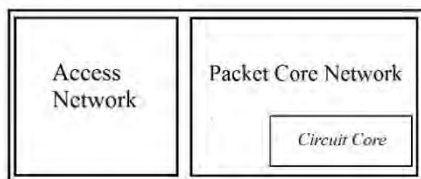
- IP-BTS - Функционалността на IP базираните базови станции е по голяма от тази на нормалните. Тези базови станции могат да бъдат също и мини RNC или BSC, способни да поддържат 1, 2 и 3 слой.

- IP сървъри – IP базираните базови станции не са в състояние да извършва всички функции на RNC / BSC на ниво мрежа. IP сървърите се справят със сигналите между мрежовите елементи, като имат способността автоматично да настройват параметрите на радиомрежата, което води до по-добро използване на радио ресурсите. Прилагането на модел с общ сървър подобрява качеството на работа и ефективността на мрежата в сравнение с модел предлагащ отделни сървъри за всеки отделен радиоинтерфейс.

- Gateways (GW) – отговарят за взаимодействието на IP-RAN (Radio Access Network) и IP-Core. Те обикновено от два вида, CS-GW и PS-GW, въз основа на вида на повикване.

## **Планиране**

Планирането на мрежата обхваща преносната мрежата, мрежата за достъп (access network) и packet core network. На Фигура 3 е показана и една малка кутийка в packet core network, дадена като подмножество, което показва, че гласовият трафик ще продължи да бъде част от мобилните комуникации, но той ще се движи по пакет от основната мрежа (за разлика от 2G и 3G мрежите).



Фигура 3. Планиране на мрежата за All-IP

### **Преглед на Процесите и протоколите.**

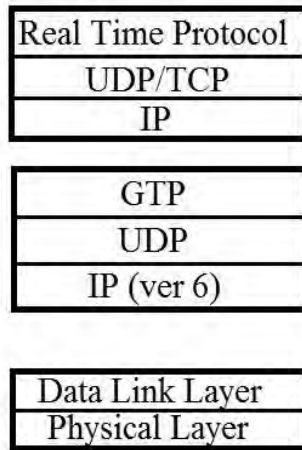
Процесът на планиране преносна мрежа е подобен на този в 3G мрежите. В този ред процесът включва:

- оразмеряване и предварително планиране
- последвано от подробно планиране и изпълнение.

Основните стъпки в предварително планиране са:

- оразмеряване на броя на елементите от мрежата, като например IP базови станции, сървъри, PS и CS, core network елементи и т.н.
- оразмеряване на капацитета на "отворени" интерфейси
- преодоляване на проблемите с оперативната съвместимост между GSM/UMTS/WLAN мрежи.

Планирането на трансмисията и core network елементите са в по - голяма взаимозависимост в сравнение с планирането при 3G мрежите следователно проучването представляват важна част от процеса на планиране.



Фигура 4. Протоколна структура в All-IP мрежите

Основната промяна в преносната мрежа, е използването на All-IP за потока на трафика. Преносните мрежи трето поколение използват слой ATM (асинхронен режим на трансфер) за потока на трафика, докато при мрежата All-IP няма такъв слой ATM. Основният ефект от тази технология е намаляване на разходите. IP (ver. 6) поема функциите на ATM слоя в тези мрежи.

Голямото предизвикателство при планирането се оказва не само прехвърлянето между различните поколения на мрежи, но и между различните технологии на едно и също поколение (All-IP, WLAN и т.н.), като същевременно се запази поддържането на стандартите QoS.

#### ЛИТЕРАТУРА

1. Цонев, И. Предаване на данни и компютърни комуникации – Шумен, Университетско издателство, 2012.
2. Ajay R Mishra. Fundamentals of Cellular Network Planning and Optimisation 2004
3. Цонев, И., Ст. Станев. Компютърни мрежи и комуникации. УИ, ШУ, 2008.

# Планиране и оптимизация на преноса в мрежите четвърто поколение

Драгомир И. Василев, Иван К. Цонев

## "4G Transmission Network Planning and Optimisation" Dragomir I. Vasilev, Ivan K. Tsonev

**ABSTRACT:** *With the expansion of third-generation networks and attempts to increase speed technology of fourth generation networks is already underway, as true forecasts of experts in the mobile industry. The deployment of fourth generation networks are now a reality and is introduced by some mobile operators and suppliers. But why is this necessary technology 4G, when 3G networks appear to meet the market enough and are still adequate to the requirements of the local high transfer speeds and quality of service?*

**KEYWORDS:** *OFDM, All-IP Networks, RNC, BSC, BTS*

Планирането на микровълнова връзка е подобна на тази за планиране GSM трансмисиите. Въпреки това в 4G мрежите предаването на данни чрез микровълнови връзки буди загриженост относно качеството им.

### Битрейт грешка

В GSM трансмисията, BER (bit error rate) от  $10^{-3}$  се счита за достатъчно приемлива, за да се постигне високо качество на услугите, но GSM преноса носи повече гласов трафик от данни. В 4G мрежите са необходими нови стандарти и системи за предаване. Основната разлика в планирането на микровълновата трансмисия между GSM и 4G е понижаването на BER. Като изискване за качество на предаване на данните се счита BER от  $10^{-6}$ . Препоръчва се използването на стандарти ITU-T G.828, ITU-T 1.356 и ITU-T 1.357 за постигане на високо качество при преноса. Препоръчителните стойности за минимум са  $10^{-3}$  и  $10^{-6}$  съответно за PDH (Plesiochronous Digital Hierarchy) и SDH (Synchronous Digital Hierarchy). Друг аспект е производителността да се измерва с

помощта на параметри като "коефициент на загуба в клетките" (CLR). За да се сведе тази стойност до минимум, обикновено се поставя висок таргет по-голям от 99.99%, имайки предвид, че основно това зависи от изискванията на оператора.

### **Топология**

Може да се видят много разновидности на преносните мрежи за GSM стандарта, като например: звезда, верига, кръг и т.н. За разлика, в 4G мрежите това няма да е случи или поне в началото. Има две основни причини за това: изискванията за капацитет и забавяне. Трафика в 4G мрежи се състои от глас, CS данни, PS данни и общи канали, като RACH, FACH и т.н. Ако има около седем потребители генериращи гласов трафик и три потребители, генериращи CS-64 и PS-64 (и двете 64 Kbps), тогава общият трафик, генериран от базовата станция (конфигурация 1 + 1 + 1) ще бъде повече от 50 Erl, от които само общи канали представляват повече от 30 Erl. Това увеличава изискуемия капацитет на почти 4 Els, докато в GSM мрежа за трансмисия на конфигурация от 1 + 1 + 1 ще трябва по-малко от една El от капацитета. По този начин, по-дълги линии за пренос (верига, кръг) не са предпочитани в 4G мрежите.

Забавянето причината за предпочитане на звездната топология в 4G мрежите за пренос. За трафика в реално време, особено данни, не забавянето е за сметка на качеството. Дългите вериги водят до повече врем за пренос на сигнала и действие на RNC / SGSN, което ще влоши качеството на повикването. Звездната топология се използва за намаляване на закъсненията.

### **Детайлно планиране**

Детайлното планиране има четири основни аспекта: 2 Мб-ово планиране, планиране на параметрите, синхронизация и планиране на система за управление на мрежата.

### **Планиране на параметрите**

Планиране на параметрите се превърнало в основна част от планирането на преносната мрежа. Поради това, планирането на преноса в 4G мрежите е по-сложна и трудна задача в сравнение с

планиране на преноса в една GSM мрежа. За да се извърши едно точно и успешно планиране е необходимо да се фокусираме върху така нареченото управление на трафика.

Отделно от виртуалните канали и виртуалните пътеки съществуват и PVC (permanent virtual connection) и SVC (switched virtual connections). PVC е създаден на постоянна основа. PVC връзките са създадени от NMS или елемент мениджърите, а SVC изисква сигнален протокол (UNI / NNI), за да осъществи връзка. Сигнални протокол се използва за създаване на виртуални връзки, което позволява превключване в крайните станции, за да осъществи обмен и пренос на данни. Принципът на действие е следният: когато едно устройство иска да създаде връзка с друго, то изпраща заявка, чрез протокол за сигнализиране, директно към свързан ATM switch, пакетите съдържат точния адрес на крайния дестинация и всички желани QoS параметри за виртуална връзка. Сигнализиращия пакет се сглобява отново, чрез превключвателите и се проверява за това дали съдържа желаните параметри QoS за създаване на виртуална връзка. След това се създава VC входяща връзка и впоследствие се изпраща искане от интерфейса, като е посочено превключване към следващия ATM switch за по-нататъшен анализ, докато се достигне дестинацията. Виртуалните връзки се създават по целия път към крайната дестинация, както всеки switch по маршрута изследва сигналния пакет и го препраща към следващия switch. Ако превключвател не е в състояние да осигури желаните QoS, искането се отхвърля, а след това съобщение се изпраща обратно към точката на изпращане. Ако крайната точка може да поддържа желаните QoS, той отговаря с „да“, приема съобщенията, както и стойностите на VCI / VPI. При приемане на връзките, функциите за управление на трафика гарантират, че всяка една от връзките се придържа към договорения трафик. Функции определящи управлението на трафика:

- параметри на трафика;
- контрол на допустимостта на връзката;
- мониторинг и контрол на съответствие;
- опашки.



## Параметри на трафика

Съществуват различни видове и класове на услуги (CBR, UBR, etc.). Всеки един от тези класове на услуги се определя от набор параметри на трафика, който описва характеристиките на източника. Тези параметри са настроени да осигурят правилното разпределение на ресурсите, за да се постигне гарантирана скорост и да се получат желаните QoS в цялата мрежа. Най-често срещаните параметри на трафика, са както следва:

- Peak cell rate (PCR) - определя се като максималната моментна скорост на предаване на потребител. Тя може да се изчисли като обратна стойност на минималния интервал от време на реакция между клетките. Ако интервалът от време между две клетки е  $1 \mu s$ , следователно PCR е  $1/(1 \times 10^{-6} s) = 10^6$  cells per second (CPS).
- Sustainable cell rate (SCR) – средно аритметичната, дългосрочна скорост на трансфер между клетките на една връзка.
- Maximum burst size (MBS) - максималният брой клетки, които могат да предават при пикова скорост на клетката.
- Minimum cell rate (MCR) – определя се въз основа на минималната ставка, която се изисква от потребителя. Скоростта на пренос никога не пада под минимума, определен с тази стойност.
- Cell-delay variation tolerance (CDVT) - това е допустима грешка, която дефинира приемливо отклонение в интервала от време за предаването; т.е. тя определя горната граница на отклонение в забавянето.

Изброените по горе параметри определят вида на трафика, като за целта се наричат *описателни*. ATM форумът е определил шест параметри за определяне качеството на трафика:

- Cell loss ratio (CLR) - Това е съотношението на броя на клетките със загуби (при предаване) към общия брой на предаващите клетки. Загубите могат да бъдат поради грешка, претовареност или значителни закъснения;
- Cell transfer delay (CTD) - когато клетка предава от източника до местоназначението, забавяне може да се дължи на размножаване на сигнала, опашки и т.н. Може да

се дефинира като средно време за разпространение от клетката до местоназначението, включително със закъсненията;

- Cell delay variance (CDV) – вариации на закъснение на клетъчния трансфер. Измерва се чрез параметъра CDV, може да се дефинира като разликата между мярката за забавяне на трансфера и средно аритметичното закъснение на същата връзка;
- Cell error ratio (CER) - съотношението на клетката(-ите) предаващи с грешка към общия брой клетки;
- Severely errored cell block ratio (SECBR) - съотношението на SES блокове (от клетки) получен от общия брой предадени блокове;
- Cell mis-insertion ratio (CMR) – наличието на грешки в някои хедъри, клетките може да трансферират в грешното дестинация. CMR е общият брой на погрешно предадени клетки наблюдавани през определен интервал от време, разделен на времеви интервал продължителност.

### **Connection Admission Control (CAC)**

CAC алгоритми определят дали една нова връзка да се приеме или отхвърли. Заявка за връзка се приема само ако са налични достатъчно ресурси и ако връзката няма да се отрази на съществуващите QoS. Фактори, определящи нова заявка за връзка са:

- параметри на трафика на нови връзки и изисквания QoS;
- съществуващи traffic contracts и връзки
- разпределена и неразпределена честотна лента.

За поддържане на оптимална производителност на мрежата се изпълняват редица механизми за работа на клетките; опашки, буфериране, клетъчно обслужване и контрол на претоварването. Изчакването ще се случи, когато трафикът от две клетки пристигне в едно и също време и отива на едно и също място. Когато клетките с по-висока скорост на предаване преминават през виртуална връзка с по-нисък трафик, се получава задръстване. Буфериране на клетките се случва, когато две или повече съответстващи клетки са предназначени за една и съща мощност по едно и също време.

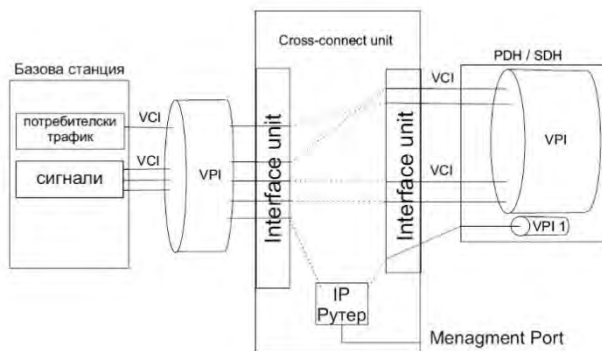
Конфигуриране на мрежовите елементи изисква уточняване на много параметри, които са свързани с интерфейсите, ATM, IP и т.н. Тъй като ATM се използват като комутация и мултиплексиране, всяка базова станция изисква устройство, което може да се справи с тези връзки. Това устройство може да се интегрира с базовата станция или може да бъде самостоятелен елемент.

### **Interface Unit**

Параметрите на интерфейс устройствата са свързани с хардуера и интерфейсни блокове PDH / SDH, които се използват за предаване на ATM върху PDH или SDH. Параметрите на хардуера са свързани с вида на системата, която се използва, т.е. дали е ETSI базирани (E1) или ANSI-базирани (T1) и др. PDH / SDH интерфейс параметри са свързани с конфигурацията на PDH или SDH терминали, които се използват. Те включват също някои параметри за изпитване с изключение на тези, необходими за да се изберат тези терминали.

### **Параметри на кръстосана връзка**

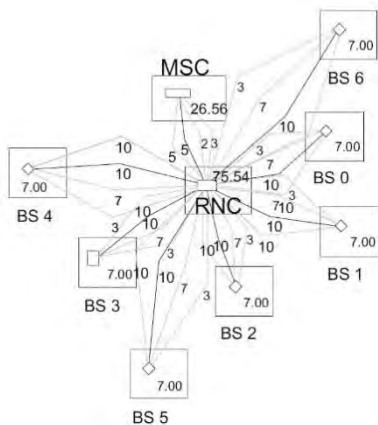
Тя включва параметри, които са необходими за идентифициране и прекратяване на виртуални канали, виртуални пътеки и техните кръстосани връзки. Също така включва параметри описващи вида на трафика който се генерира от тези виртуални канали и пътища. Кръстосаната връзка може да се осъществи на физическо ниво, ниво VP и ниво VC (В GSM мрежите за пренос, напречните връзки се осъществяват само на физическо ниво).



Фигура 1. Пример за кръстосана връзка

При планирането на преноса трябва да обърнем внимание на:

- видовете трафик
- VP и VC връзки
- броят на VP и VC (т.е. VPI и VCI)
- VP и VC кръстосани връзки
- параметри на физическите, VP и VC връзки.



Фигура 2. Планиране на линия за пренос

Със сиво са отбелязани връзките на физическо ниво, с черните линии е дадено свързването VPI и VCI

Всички тези аспекти на планирането на преноса са сложни, особено за по-голяма мрежа. През фазата на развитието на мрежата, този процес става още по-сложен. Поради тази причина се използват добри инструменти за планиране.

### Оптимизиране на преносната мрежа

В процеса на оптимизация преносната мрежа е в основата си същата като за GSM пренос, но има две допълнителни условия: настройка на параметрите и качество на обслужване. Процесът започва с определянето на ключовите показатели за изпълнение и процеса на събиране на данни, последвано от анализ им, качеството, и параметрите на настройките. След това окончателните планове за оптимизация се изработват да отговарят на желаното качество на услугата.



Фигура 3. Схема на процеса на оптимизация

Оптимизирането на мрежата е насочена основно към увеличаването на капацитета и качеството, на фона на QoS изисквания от приложенията, използвани от абонатите. В GSM мрежите има много малко ключови показатели за изпълнение, най-

вече свързани с качеството на микровълнова мрежа. Въпреки това, броят им при 4G мрежите се увеличава значително с увеличаването на ключовите показатели за изпълнение. Събирането на данни включва основно съществуващи данни за мрежата, като конфигурацията на сайт, мрежова топология, бюджетните изчисления, въвеждане на данни, наблюдаване на данни (т.е. нива на мощност наблюдавани по време на експлоатация), както и на изпълнението на ключовите показатели. Анализът на данните се състои от анализ на капацитета и анализ на качеството.

### **Анализ на капацитета**

За преноса на GSM мрежа, изчисляването на капацитета и оценката е относително проста. Ако конфигурацията на сайта на TRXs е известно, то необходимия капацитет за връзката може да се изчисли лесно. Въпреки това, анализът на капацитета на 4G мрежа не е толкова пряка. Видяхме, че изчисленият капацитет зависи от вида на трафика и така не може да се изчисли пряко от броя на TRXs или броя на заявките. Обикновено, когато капацитетът на линията е оразмерена във фазата на предварителното планиране, бъдещите нужди са взети под внимание. В GSM оптимизацията преносната мрежа повишаването на трафика ще доведе до увеличаване на броя на TRXs или броя на сайтовете. Обратно в 4G мрежите увеличение на трафика може да доведе до увеличаване на броя на сигнални процесори / мениджърите за заявки и / или TRXs в базовите станции, както и разширяването им, което ще доведе до увеличаване на капацитета на връзката. Базова станция с малък брой потребители генерира значителен трафик. Увеличаването на капацитета на връзката ще означава, че RNC капацитет трябва да бъде преразгледан.

По този начин, на капацитета на преносната мрежа може да бъде увеличаван чрез:

- увеличаване на броя на сигнални процесори /мениджърите за кандидатстване и/или TRXs;
- увеличаване на броя на базовите станции;
- увеличаване на броя / капацитета на RNC.

Оразмеряването играе много важна роля в целия процес. Мрежата е оразмерена първоначално на базата на фактори, като съществуващите ограничения, знания и оборудване по времето, когато се стартира реалното мрежата. В последствие много фактори и параметри се променят, така че се налага да се направи преоценка на оразмеряването. Общите данни се състоят от реално постигнатите и събрани данни, като топология, бюджетни изчисления за линията, анализ на смущения, капацитети на връзките и т.н. Наличните данни за работата също могат да се записват за по-дълъг период от време. Параметрите на радио мрежата отново се разделят на оразмерени и оптимизирани. Всички ефекти на оптимизиране на параметрите могат да се приложат и към преносните мрежи. По този начин в последствие връзката между някои параметри и характеристики на преносната мрежа може да се изследват, което ще позволи определянето на такива параметри, че изпълнението на оптимизацията да даде най-добрите QoS за мрежата. След като това е направено, оптимизираните параметри се прехвърлят обратно за анализ на мрежата, така че да се направи кръстосана проверка дали те дават желанния резултат за функционирането на мрежата

## **ЛИТЕРАТУРА**

1. Цонев, И. Предаване на данни и компютърни комуникации – Шумен., Университетско издателство, 2012.
2. Ajay R Mishra. Fundamentals of Cellular Network Planning and Optimisation 2004
3. Цонев, И., Ст. Станев. Компютърни мрежи и комуникации. УИ, ШУ, 2008.

# АНАЛИЗ НА СЪВРЕМЕННИТЕ ВИДОВЕ УЯЗВИМОСТИ И ЕКСПЛОЙТИ В КОМПЮТЪРНИТЕ МРЕЖИ И СИСТЕМИ

Огнян М. Фетфов, Петър Кр. Боянов, Жанета Н.  
Ташева, Тихомир Сп. Трифонов

## ANALYSIS OF MODERN VULNERABILITIES AND EXPLOITS IN THE COMPUTER NETWORKS AND SYSTEMS

Ognyan M. Fetfov, Petar Kr. Boyanov, Zhaneta N. Tasheva,  
Tihomir Sp. Trifonov

**ABSTRACT:** *In this paper analysis of modern vulnerabilities and exploits in the computer networks and systems is made. Thanks to the obtained results some weaknesses in the computer networks and systems are found.*

**KEYWORDS:** *Exploit, HP Zero Day, Java, ReversingLabs, Vulnerability.*

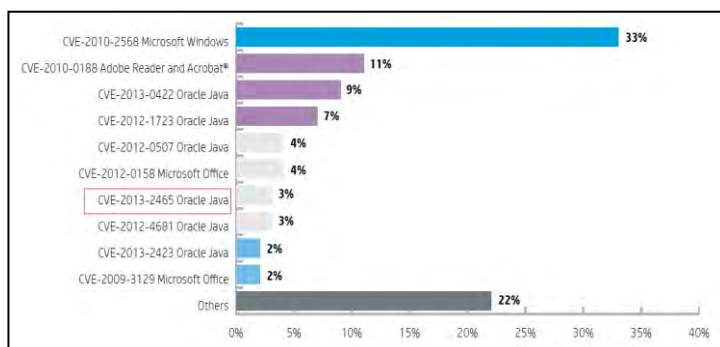
### 1. Въведение

Повечето извършени кибер престъпления са базирани на слаби места и уязвимости в компютърните системи и мрежи. Благодарение на своите задълбочени познания в компютърните технологии повечето киберпрестъпници намират начин да приложат и експлоатират опасни злонамерени компютърни и мрежови атаки [1], [4], [9], [12], [7], [16] които могат да причинят непоправими щети на ресурсите на компютърните мрежи.

През последните няколко години инжектирането на експлойти се превърна в най-зловредната кибератака. HP Security Research, HP Zero Day и ReversingLabs анализират и събират детайлна информация за най-зловредните експлойти, които масово се използват от киберпрестъпници за получаване на несанкциониран достъп до ресурсите на компютърните мрежи и системи. На фиг. 1 е показана графика с най-разпространените

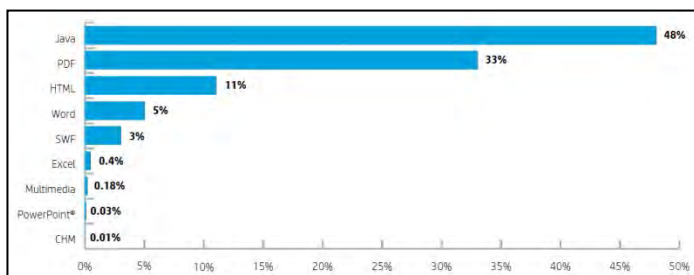


видове експлойти за периода 2009-2013 г. [3], [7], [11], [13], [16], [17]. От направения анализ на данните от фигурата, може да се направи изводът, че най-използвани са експлойтите на корпорацията Oracle Java. Както е известно, в нашето съвремие над 3 билиона устройства използват Java приложения, което крие изключително сериозен риск от кибератаки. Поради тази причина е направен избор на експлойта CVE-2013-2465 Oracle Java за осъществяване на реална кибератака за получаване на отдалечен достъп до машината на жертвата и разкриване на конфиденциална информация за нея [1], [2], [3], [5], [17].



**Фиг. 1.** Най-използваните експлойти за периода 2009-2013 г.

Един от начините за защита от тези видове злонамерени експлойти е прилагането на модифицирани и паралелни псевдослучайни генератори на битове [13], както и използването на паралелни клъстерни системи, осигуряващи стеганографска защита на информацията в компютърните мрежи и системи [16]. На фиг. 2 са илюстрирани различните видове файлове, които се използват при експлоатиране на уязвимост. Тези файлове доставят експлойта през уеб браузера (Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera и др.) или прикачвания на файлове в електронната поща [5], [6], [10], [14].



**Фиг. 2.** Най-използваните типове файлове, доставящи експлойти

## **2. Експеримент**

### **Мрежово сканиране за активни хостове**

За процеса на сканиране на безжичната локалната мрежа с цел установяване, кои хостовете са в активно състояние, е използван уеб-базирания потребителски интерфейс Access Metasploit Web UI [3], [5], [6], [7]. На фиг. 3 е показан резултатът от извършеното сканиране на локалната компютърна мрежа. От получените резултати се разбира, че осем са откритите активни хостове от проведеното мрежовия скениране с програмата Nmap. Хостът с IP адрес 1.1.1.2 има инсталирана операционна система Microsoft Windows XP SP3, а пък хостовете с IP адреси 1.1.1.12, 1.1.1.5, 1.1.1.8, 1.1.1.7, 1.1.1.4 и 1.1.1.3 имат инсталирани операционни системи Microsoft Windows 7 SP1. На хост с IP адрес 1.1.1.14 има инсталирана операционна система Microsoft Windows 8 SP0 [1], [3], [5], [8], [9], [12], [13].

### **Процес на инжектиране на злонамерен код в операционните системи Microsoft Windows 7 Enterprise и Windows 8 на хостовете-жертви**

Името на използвания експлойт е “Java storeImageArray () Invalid Array Indexing Vulnerability”. Този експлойт използва уязвимост в работното пространство на JAVA средата - Java Runtime Environment (JRE). Компонентите, които са засегнати, са Oracle SE 7 Update 7, 11, 21, 25 и SE 6 Update 45 [3], [4], [5].



**Фиг. 3.** Активни хостове в компютърната мрежа 1.1.1.0/24

Този експлойт може да причини критични щети на избраните компютърни и мрежови системи. Детайлна информация за уязвимостите са публикувани като:

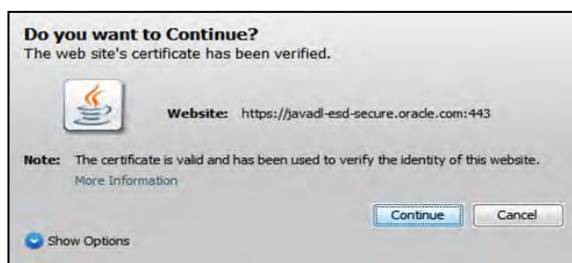
- CVE-2013-2465.
- OSVDB-96269.
- EDB-27526 и др.

Следващата стъпка е свързана с конфигурацията на експлойта в програмната среда на Metasploit Framework. Следните важни стъпки са направени:

- За източник на атаката (SRVHOST) е избран хост с логически мрежови IP адрес 1.1.1.9.
- За порт на атаката (SRVPORT) е избран порт 8080, защото този експлойт ще бъде изпълнен при HTTP протокола.
- Слушащата услуга отново е избрана да бъде на атакувания хост с IP адрес 1.1.1.9.

- Целият път за изпълнение на уеб адреса на експлойта към някой от хостовете в мрежата е : [http://1.1.1.9:8080/university\\_project.html](http://1.1.1.9:8080/university_project.html).

Целта на този уеб адрес е да бъде изпратен към някой от намерените хостове с програмата Nmap. След като е избрана жертвата, този линк пристига при нея с протокола HTTP [7], [8] и единственото нещо, което трябва да направи жертвата е да приеме Java сертификата, който от своя страна показва, че е успешно верифициран. Това е показано на фиг. 4.



**Фиг. 4.** Приемане на сертификата

След потвърждаване на Java сертификата, маркираната жертва бива успешно експлоатирана чрез тази уязвимост и злонамереният извършител получава права на достъп към конфиденциалната информация на своята жертва [6], [7], [8], [9], [16].

На фиг. 5 е показан процесът на успешно експлоатираната уязвимост в хост с IP адрес 1.1.1.8.

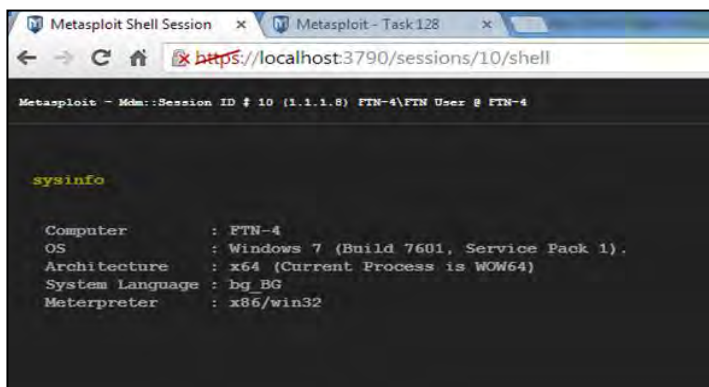
```

[!] 1.1.1.8      java_storeimagearray - Requesting: /pp/
[*] [2014.04.4-19:39:06] 1.1.1.8      java_storeimagearray - Sending
redirect...
[!] 1.1.1.8      java_storeimagearray - Requesting: /pp/
[*] [2014.04.4-19:39:06] 1.1.1.8      java_storeimagearray - Sending
HTML...
[!] 1.1.1.8      java_storeimagearray - Requesting: /pp/
[*] [2014.04.4-19:39:18] 1.1.1.8      java_storeimagearray - Sending
HTML...
[!] 1.1.1.8      java_storeimagearray - Requesting: /pp/rkJCqi.jar
[*] [2014.04.4-19:39:23] 1.1.1.8      java_storeimagearray - Sending
.jar file...
[!] 1.1.1.8      java_storeimagearray - Requesting: /pp/rkJCqi.jar
[*] [2014.04.4-19:39:23] 1.1.1.8      java_storeimagearray - Sending
.jar file...
[*] [2014.04.4-19:39:24] 1.1.1.8:50397 Request received for /DcLi...
[*] [2014.04.4-19:39:24] 1.1.1.8:50397 Staging connection for target /DcLi
received...
[*] [2014.04.4-19:39:24] Patched user-agent at offset 640488...
[*] [2014.04.4-19:39:24] Patched transport at offset 640148...
[*] [2014.04.4-19:39:24] Patched URL at offset 640216...
[*] [2014.04.4-19:39:24] Patched Expiration Timeout at offset 640748...
[*] [2014.04.4-19:39:24] Patched Communication Timeout at offset 640752...
[!] 1.1.1.12     java_storeimagearray - Requesting: /pp/
[*] [2014.04.4-19:47:03] 1.1.1.12     java_storeimagearray - Sending
HTML...
[!] 1.1.1.12     java_storeimagearray - Requesting: /pp/JfVqXCK.jar
[*] [2014.04.4-19:47:03] 1.1.1.12     java_storeimagearray - Sending
.jar file...

```

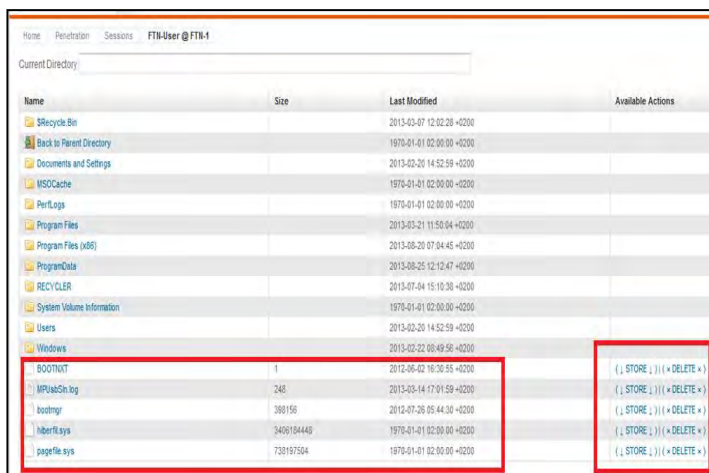
**Фиг. 5.** Успешно изпълненият експлоит на хост с IP адрес 1.1.1.8 и инсталирана операционна система Microsoft Windows 7 (Build 7601) Enterprise SP1

От фиг. 6 се разбира, че името на компютъра е “FTN-4”, типа на операционната система - “Windows 7 (Build 7601, Service Pack 1), архитектурата е “x64” битова, системният език е български - “bg\_BG” и типа на полезния товар е “x86/win32”.



**Фиг. 6.** Успешно изпълнена команда “sysinfo”, показваща основна информация за системата

На фиг. 7 са показани всички файлове и директории от системния дял в хост с логически IP адрес 1.1.1.8.

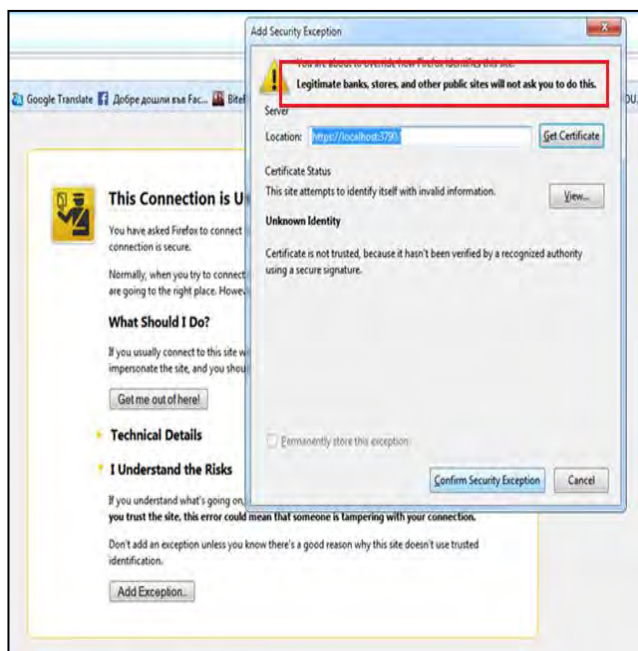


**Фиг. 7.** Пълен достъп до файловете и директориите в хост с IP адрес 1.1.1.8

От фиг. 7 се разбира още, че злонамереният извършител може да изтрие много критични системни файлове като bootmgr, hiberfil.sys, pagefile.sys, BOOTNXT и др. След тяхното изтриване и

на следващото рестартиране операционната система няма да бъде в състояние да се зареди и ще създаде сериозни проблеми на обикновения потребител. Трябва да се знае, че извършителят може да инсталира скрит софтуерен инструмент, с който да установява отдалечена връзка със своята жертва винаги, когато тя получи свързаност към интернет [16].

Същият този експлойт е успешно изпълнен и на хост с IP адрес 1.1.1.14. В случая инсталираната операционна система на хоста е Microsoft Windows 8 (Build 9200). За да бъде инсталиран върху Windows 8, жертвата трябва потвърди за въвеждането на следния уеб адрес като изключение. В случая този адрес е адресът на атакуващия хост - “https://localhost:3790/”. Важно е да се отбележи, че никога уеб адреси на легитимни банки, онлайн магазини и други важни публични сайтове не биха поискали от обикновения потребител да слага изключения за тях. Ако някой сайт поиска такова изключение, означава, че срещу потребителя се осъществява кибератака [16]. Това е показано на фиг. 8.



**Фиг. 8.** Потвърждение на дадения уеб сайт в списъка с изключения

На фиг. 9 са показани успешно изпълнените команди “sysinfo” и “ps” в операционната система Microsoft Windows 8 (Build 9200).

```

Metasploit - Mm::Session ID # 20 (1.1.1.14) FTN-User # FTN-1

sysinfo

Computer      : FTN-1
OS            : Windows 8 6.2 (x86)
Meterpreter   : java/java

ps

Process List

  PID  Name                      Arch  User                      Path
  ---  ---                      ---  ---                      ---
0      System Idle Process      NT AUTHORITY\SYSTEM  System Idle Process
4      System                   N/A                      System
36     tasklist.exe              FTN-1\FTN-User       tasklist.exe
44     cmdlogt.exe              FTN-1\FTN-User       cmdlogt.exe
392    smss.exe                 N/A                      smss.exe
360    zuFAcbbT.exe             FTN-1\FTN-User       zuFAcbbT.exe
404    svchost.exe              N/A                      svchost.exe
444    svchost.exe              N/A                      svchost.exe
448    csrss.exe                N/A                      csrss.exe
520    wininit.exe              N/A                      wininit.exe
520    csrss.exe                N/A                      csrss.exe
580    winlogon.exe             N/A                      winlogon.exe
668    services.exe             N/A                      services.exe

Meterpreter > |

```

**Фиг. 9.** Успешно изпълнените команди “sysinfo” и “ps” в машината на жертвата

Първата команда “sysinfo” показва, че името на компютъра е “FTN-1”, използваната операционна система е “Windows 8 6.2 (x86)” и типът на полезния товар е “Meterpreter - Java”.

### 3. Заключение

Дори и най-новите обновления на Java Oracle SE 7 Update 7, 11, 21, 25 и SE 6 Update 45 операционни системи на хостовете в безжичната локална мрежа бяха успешно компрометирани и този начин атакуваният хост успя с платформата Metasploit Pro да проникне в съседните хостове. Главната причина за успеха на киберизвършителя е свързана с ниското ниво на осведоменост за най-съвременните видове кибератаки, които използват Oracle Java експлойти.



Всички фирми, компании и държавни учреждения и институции трябва да организират редовни курсове за повишаване квалификацията и уменията на служителите като по този начин ще може да се подобри превенцията и противодействието на киберпрестъпленията. За момента в Република България има изградени Международната академия за обучение по киберразследвания (МАОКР) със седалище гр. София и Сектор "Компютърни престъпления, интелектуална собственост и хазарт", ГДБОП - [cybercrime.bg](http://cybercrime.bg).

## ЛИТЕРАТУРА

1. Engebretson P., The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series), Syngress, 2011, ISBN-13: 978-1597496551, pp. 180
2. Igiure V., Williams R., Taxonomies of attacks and vulnerabilities in computer systems, IEEE Communications Surveys & Tutorials, 2008, vol.10, №. 1 pp. 6-19
3. 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
4. Scambray J., Liu V., Sima C., Hacking Exposed Web Applications, Third Edition, McGraw-Hill Education, 2010, ISBN: 978-0-07-174042-5, pp. 482
5. Sharma A., Kalbarczyk Z., Iyer R., Barlow J., Analysis of credential stealing attacks in an open networked environment, In Proc. of the Fourth International Conference on Network and System Security. Washington, 2010, DC, USA: IEEE Computer Society, pp. 144-151
6. Shipley Todd G., Bowker A., Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace, Syngress, 2014, ISBN 978-0-12-407817-8, pp. 497
7. Sikorski M., Honig A., Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, San Francisco, USA, 2012, ISBN: 978-1-59327-290-6, pp. 800
8. Singh A., Agarwal M., Metasploit Penetration Testing Cookbook - Second Edition, Packt Publishing, Birmingham, UK, October 2013, ISBN 978-1-78216-678-8, pp. 320
9. Singh A., Metasploit Penetration Testing Cookbook, Packt Publishing, Birmingham, UK, June 2012, ISBN 978-1-84951-742-3, pp. 268
10. 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
11. Stallings W., Brown L., Computer Security: Principles and Practice, Pearson Education, ISBN-13: 978-0-13-277506-9, pp. 817
12. Stewart J. M., Chapple M., Gibson D., CISSP: Certified Information Systems Security Professional Study Guide, Sixth Edition, John Wiley & Sons, 2012, ISBN: 978-1-118-31417-3, pp. 936
13. Stoyanov, B. P., Kordov, K. M., Pseudorandom Bit Generator with Parallel Implementation (2014), Large Scale Scientific Computing 2013, Lecture Notes in Computer Science 8353, 557-564, SJR(2013)=0.310
14. Timm C., Perez R., Seven deadliest social network attacks, Syngress Elsevier, ISBN: 978-1-59749-545-5, 2010, pp. 1-143

15. Willie Pr., Smet D., BackTrack 5 Cookbook, Packt Publishing, Birmingham, UK, December 2012, ISBN 978-1-84951-738-6, pp.296
16. Zhelezov, S., H. Paraskevov, Possibilities for steganographic parallel processing with a cluster system, Contemporary Engineering Sciences, Volume 8, Issue 20, ISSN:1313-6569, 2015, SJR (2014) : 0.187
17. <http://www8.hp.com/bg/bg/software-solutions/cyber-risk-report-security-vulnerability/index.html> (HP cyber risk report 2015)

# СРАВНИТЕЛЕН АНАЛИЗ НА СЪВРЕМЕННИТЕ ВИДОВЕ АНТИВИРУСНИ ПРОГРАМИ

Огнян М. Фетфов, Петър Кр. Боянов, Жанета Н.  
Ташева, Тихомир Сп. Трифонов

## COMPARATIVE ANALYSIS OF MODERN TYPES OF ANTIVIRUS PROGRAMS

Ognyan M. Fetfov, Petar Kr. Boyanov, Zhaneta N. Tasheva,  
Tihomir Sp. Trifonov

**ABSTRACT:** *In this paper comparative analysis of modern types of antivirus programs in the computer networks and systems is made. Nowadays it is very obligated that each cyber security administrator has to analyze different vulnerabilities and flaws in their computer and network systems. The using of antivirus software program is necessary for stable and secure maintaining off all computer resources and processes in the selected computer system.*

**KEYWORDS:** *Antivirus program, Cyber security, Vulnerability.*

### 1. Въведение

Една от важните и задължителни задачи за всеки системен администратор и анализатор на компютърните престъпления е осигури защита на потребителската идентичност и данни. Онлайн банкирането и осъществяването на покупки са от изключителна важност за онлайн операциите. Повечето от уеб хибер връзки могат да крият в себе си скрити XSS (Cross-site scripting) кибератаки, които да причинят само с едно кликуване върху линка огромни щети на компютърните и мрежови ресурси [1], [3], [5], [7], [9], [10]. Един от начините за решаване на този проблем е изборът на подходяща антивирусна програма, която да се характеризира с голям набор от защитни механизми и инструменти. Един от начините за защита от тези видове злонамерени вируси и експлойти е прилагането на модифицирани и паралелни псевдослучайни генератори на битове [19], както и използването

на паралелни клъстерни системи, осигуряващи стеганографска защита на информацията в компютърните мрежи и системи [23].

## **2. Избор на антивирусна програма**

Изследванията и анализите в тази статия са реализирани с помощта на антивирусни програми, показващи добри резултати при откриване на злонамерени заплахи и уязвимости. Един от най-добрите институти за тестване на антивирусни програми е институтът AV-TEST. Щаб-квартирата на този институт се намира в град Магдебург, Германия [2], [4], [6], [8]. Този институт сравнява и тества всяка една антивирусна програма със следните показатели:

- Протекция.
- Производителност.
- Използваемост.

Протекцията се характеризира с това, че открива злонамерени инфекции като вируси, червеи и троянски коне. Протекцията включва още защита срещу кибератаките от “нулев ден”. Тези кибератаки най-често се проявяват като уеб или e-mail заплаха [9].

Производителността се характеризира със средното влияние на антивирусната програма върху скоростта на компютърната система при делничните дни. Докато сканира антивирусната програма, компютърната система се натоварва с теглене на софтуер, инсталиране и изпълнение на програми, копиране на данни, както и посещение на уеб страници [11], [12], [13], [14].

Използваемостта се характеризира с:

- Грешни предупреждения или блокировки при посещения на уеб страници.
- Разпознаване на легитимния софтуер като фалшива злонамерена програма.

Поради тази причина всички налични в момента на пазара платени и безплатни антивирусни програми са тестване от този независим институт [15], [16], [17], [18]. Тестваните програми са:

- AhnLab V3 Internet Security 9.0
- Avast Free AntiVirus 2015

- AVG Internet Security 2015
- Avira Antivirus Pro 2015
- Avira Antivirus Pro 2015
- BullGuard Internet Security 15.0 & 15.1
- Check Point ZoneAlarm Extreme Security 13.4
- Comodo Internet Security Premium 8.2
- ESET Smart Security 8.0
- F-Secure Internet Security 2015
- G Data InternetSecurity 2015
- K7 Computing Total Security 14.2
- Kaspersky Lab Internet Security 2015
- McAfee Internet Security 2015 MicroWorld eScan Internet Security Suite 14.0
- Norman Security Suite Pro 11.0
- Norton Security 2015
- Panda Security Free Antivirus 15.1
- Quick Heal Total Security 16.0
- ThreatTrack VIPRE Internet Security 2015
- Trend Micro Internet Security 2015
- Microsoft Windows Defender 4.7

След сравняване и тестване на всички по-горе изброени антивирусни програми се установи, че програмите Avast Free AntiVirus 2015, Bitdefender antivirus free edition, AVG Zen free antivirus и Norton Security 2015 се справиха успешно с трите важни показатели. На фиг. 1 е показана стартираната онлайн версия на Bitdefender antivirus free edition.



Фиг. 1. Графичен потребителски интерфейс на Bitdefender

Антивирусната програма Bitdefender предлага на пазара трите версии Antivirus Plus, Internet Security и Total Security.

Версията Antivirus Plus предлага:

- Съвместимост с Windows 10.
- Автоматична протекция за вируси и заплахи.
- Използване на злонамерени шаблони за откриване на нови заплахи.
- Поддържане на стабилна производителност.
- Споделена защита при парични преводи.
- Защита при уеб сърфирането.
- Защита от програми, криптиращи всички файлове и искащи след това откуп от жертвата за тяхното декриптиране (ransomware).
- Защита на потребителските пароли чрез специално приложение.
- Предотвратяване на други приложения да намалят скоростта на качване на сваляне.
- Блокиране на злонамерени линкове в социалните мрежи Facebook, Twitter и др.

Версията Internet Security предлага:

- Всички по-горе изброени функции на версията Antivirus Plus.
- Прилагане на защитна стена със система за откриване на извършители.
- Стриктна родителска защита за уеб сърфиране и осигуряване на отдалечен достъп до компютрите на децата.
- Блокиране на нежелани и злонамерени съобщения до електронната поща, благодарение на съвременна облачна технология.

Антивирусната програма Avira предлага на пазара четирите версии Free Antivirus, Antivirus Pro, Internet Security Suite и Ultimate Protection Suite. Графичният потребителски интерфейс на Avira е показан на фиг. 2.

Версията Antivirus Pro предлага:

- Техническа поддръжка.
- Защитено онлайн търгуване.
- Безопасно теглене на файлове.
- Пълна уеб протекция.
- Защита от вируси, червеи, троянски коне и др.

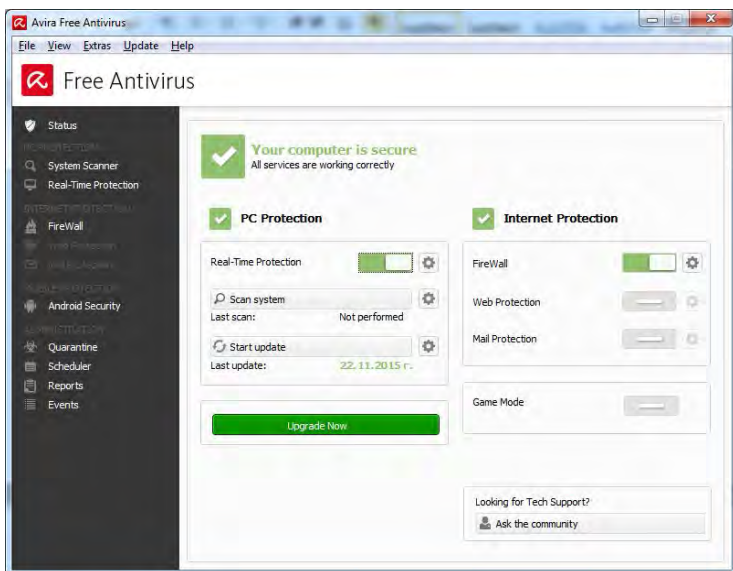
Версията Internet Security Suite предлага:

- Всички по-горе изброени функции на версията Antivirus Pro.
- По-бързо стартиране.
- Криптиране на файловете.
- Премахване на излишните файлове.
- Възможност за повече свободно облачно пространство.

Версията Ultimate Protection Suite предлага:

- Всички по-горе изброени функции на версията Internet Security.
- По-добра производителност при игрите.

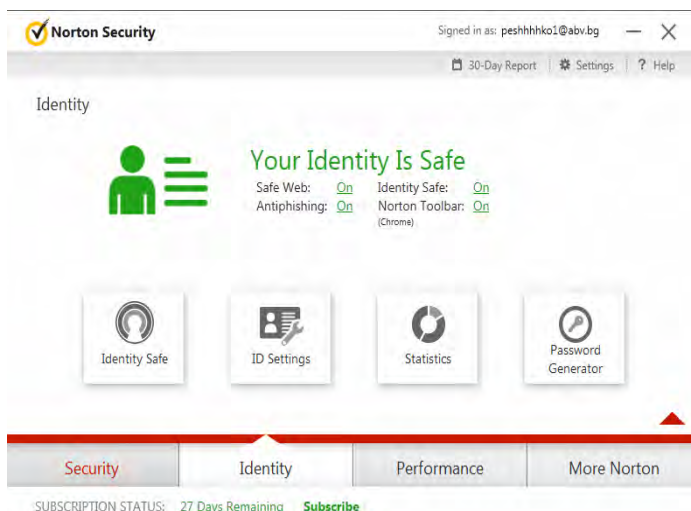
- Замяна на счупени и остарели драйвери с нови.
- Осигуряване на по-голяма производителност независимо от процеса на сканиране.



Фиг. 2. Графичен потребителски интерфейс на Avira Free Antivirus

Антивирусната програма Norton предлага на пазара трите версии Standard, Deluxe и Premium. Графичният потребителски интерфейс на Norton е показан на фиг. 3.





Фиг. 3. Графичен потребителски интерфейс на Norton

Стандартната защита се характеризира с:

- Защита срещу вируси, шпионски и вредни програми, червеи и онлайн заплахи.
- Защита на потребителската идентичност и онлайн електронни парични трансакции.
- По-добра защита от всички други на пазара антивирусни програми.
- Предлагане на 100% гаранция, че ако потребителското устройство не бъде изчистено от вируси, следва връщане на парите.

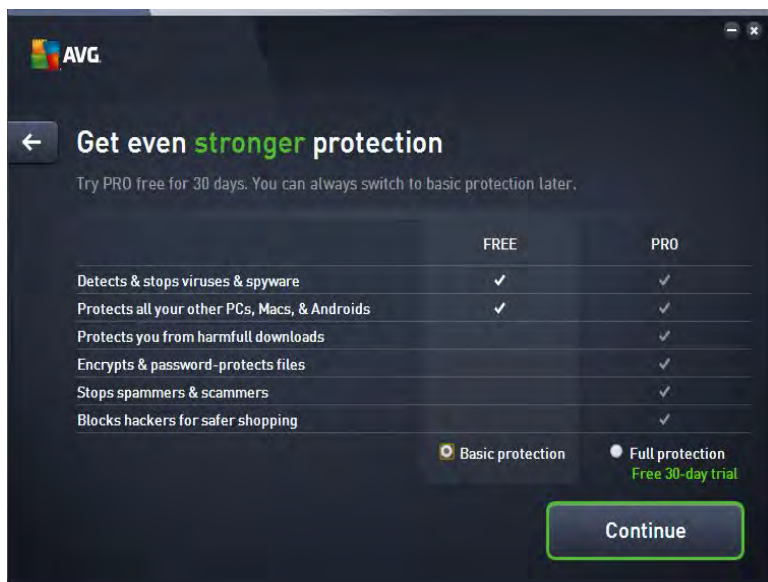
Версията Deluxe се характеризира с:

- Всички по-горе изброени функции на версията стандарт.
- Осигуряване на защита до 5 хоста. Това могат да бъдат персонални компютри, смарт телефони и таблети.
- Използване на уеб портал за лесно настройване на всички устройства.

Версията Premium се характеризира с:

- Всички по-горе изброени функции на версията Deluxe.
- Родителска защита за децата при онлайн сърфиране в INTERNET.
- Автоматично създаване на резервно копие на конфиденциалната потребителска информация.
- Предоставяне на 25 GB облачно пространство за съхранение на информация.

Антивирусната програма AVG предлага на пазара четирите версии Antivirus Free, Antivirus и Internet Security. На фиг. 4 е илюстриран графичният потребителски интерфейс на AVG.



Фиг. 4. Графичен потребителски интерфейс на AVG

Версията Antivirus Free предлага:

- Блокиране на вируси, шпионски програми и друг видове злонамерени програми.

- Защита от злонамерени уеб линкове в социалните мрежи Facebook, Twitter, както и от всички останали уеб страници.
- Защита за злонамерени прикачени файлове в електронната поща.

Версията Antivirus предлага:

- Всички по-горе изброени функции на версията на Antivirus Free.
- Онлайн протекция от теглене на злонамерени файлове.
- Криптиране и защитаване с парола на конфиденциални файлове.
- Получаване на автоматични сигурни обновления на всеки 2 часа.

Версията Internet Security предлага:

- Всички по-горе изброени функции на версията на Antivirus.
- Антиспам защита за електронната поща
- Защита с разширена защитна стена за онлайн покупки и парични преводи.

Всички по-горе изброени антивирусни програми са анализирани и сравнени на потребителски, а не бизнес критерий.

### **3. Заключение**

Всеки професионалист по сигурността, системен администратор и дори обикновен потребител трябва постоянно да разпознават и откриват новите уязвимости, дупки, слабости, експлойти и специфичен софтуер, които причиняват пълно компрометиране на целостта на избраната операционна система и изтриване на всички компютърни ресурси. По този начин е необходимо да се направи правилна конфигурация на антивирусната програма, при което производителността на компютърната система не трябва да намалява в драстични граници. Всички фирми, компании и държавни учреждения и институции трябва да организират редовни курсови за повишаване

квалификацията и уменията на служителите по избор и конфигуриране на определена антивирусна програма.

## ЛИТЕРАТУРА

18. Alofer, Yaser, and Omer Rana. "Honeyware: a web-based low interaction client honeypot." In Software Testing, Verification, and Validation Workshops (ICSTW), 2010 Third International Conference on, pp. 410-417. IEEE, 2010.
19. Beblavý, Miroslav, and Lucia Mýtna Kureková. "Into the First League: The Competitive Advantage of the Antivirus Industry in the Czech Republic and Slovakia." *Competition & Change* 18, no. 5 (2014): 421-437.
20. David, R. "Top 5 Free Antivirus for Mac: Reviews." (2013).
21. Filiol, Eric, Grégoire Jacob, and Mickaël Le Liard. "Evaluation methodology and theoretical model for antiviral behavioural detection strategies." *Journal in Computer Virology* 3, no. 1 (2007): 23-37.
22. Griffith, Eric. "The Best Free Software of 2010." (2008).
23. Hamlen, Kevin W., Vishwath Mohan, Mohammad M. Masud, Latifur Khan, and Bhavani Thuraisingham. "Exploiting an antivirus interface." *Computer Standards & Interfaces* 31, no. 6 (2009): 1182-1189.
24. Hessman, Kristy. "Pitfalls of Free Antivirus Software." (2011).
25. Heu, Kimberly. "Security of Client PCs." (2009).
26. 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
27. James, K. L. The Internet: A user's guide. PHI Learning Pvt. Ltd., 2010.
28. Kryvenko, P. "COMPUTER VIRUSES AND ANTI-VIRUS PROGRAMS." (2013).
29. Marx, Andreas. "Antivirus outbreak response testing and impact." *Virus Bulletin* (2004).
30. Morgenstern, Maik, and Andreas Marx. "Runtime packer testing experiences." In 2nd International CARO Workshop. 2008.
31. Oberheide, Jon, Evan Cooke, and Farnam Jahanian. "CloudAV: N-Version Antivirus in the Network Cloud." In *USENIX Security Symposium*, pp. 91-106. 2008.
32. Omer, Yishak Ibrahim. "A WHITELIST BASED IMPLEMENTATION OF ANTIVIRUS-DEFINITION FILE TO DETECT UNKNOWN MALICIOUS ACTIVITY." PhD diss., Addis Ababa University, 2009.
33. Rasool, Muhammad Ahsan, and Abdul Jamal. "Master Thesis "Quality of Freeware Antivirus Software".
34. Shakya, Neema. "Privacy Issues of Antivirus Apps for Smartphones." In *The 12th Winona Computer Science Undergraduate Research Symposium*, p. 17. 2012.
35. Sonawane, Y. E., K. G. Deokate, B. B. Daundkar, and M. V. Garad. "BEHAVIOUR OF EMAIL WORM AND TROJAN SPY USED FOR INFORMATION THEFT—A Case STUDY." *THE PHENOMENON OF RAPE*: 93.
36. Stoyanov, B. P., Kordov, K. M., Pseudorandom Bit Generator with Parallel Implementation (2014), Large Scale Scientific Computing 2013, Lecture Notes in Computer Science 8353, 557-564, SJR(2013)=0.310
37. Sukwong, Orathai, Hyong S. Kim, and James C. Hoe. "Commercial antivirus software effectiveness: an empirical study." *Computer* 44, no. 3 (2011): 0063-70.
38. Virus, Bootsector. "What is computer virus?" (1995).
39. Xue, Feng. "Attacking antivirus." In *Black Hat Europe Conference*. 2008.

40. Zhelezov, S., H. Paraskevov, Possibilities for steganographic parallel processing with a cluster system, Contemporary Engineering Sciences, Volume 8, Issue 20, ISSN:1313-6569, 2015, SJR (2014) : 0.187

# **СРАВНИТЕЛЕН АНАЛИЗ НА СЪВРЕМЕННИТЕ ВИДОВЕ БЕЗЖИЧНИ IP ВИДЕОКАМЕРИ В КОМПЮТЪРНИТЕ МРЕЖИ ЗА НАБЛЮДЕНИЕ И КОНТРОЛ**

**Огнян М. Фетфов, Петър Кр. Боянов, Иван О. Николов,  
Жанета Н. Ташева, Тихомир Сп. Трифонов**

## **COMPARATIVE ANALYSIS OF MODERN TYPES OF WIRELESS IP VIDEO CAMERAS FOR MONITORING AND CONTROL IN THE COMPUTER NETWORKS**

**Ognyan M. Fetfov, Petar Kr. Boyanov, Ivan O. Nikolov,  
Zhaneta N. Tasheva, Tihomir Sp. Trifonov**

**ABSTRACT:** *In this paper comparative analysis of modern types of wireless ip video cameras for monitoring and control in the computer networks is made. Nowadays it is very obligated that each company or state institution must possess built security system for monitoring and control of the whole building. Thereby, each security administrator has to maintain and control correct the security system against various internal and external malicious events.*

**KEYWORDS:** *Analysis, Computer network, IP camera, Video.*

### **1. Въведение**

Една от важните и задължителни задачи за всеки системен администратор в дадена компания или държавно учреждение е да осигури защита на сградата и хората чрез изграждане на система за видеонаблюдение с жични и безжични IP (Internet Protocol) камери. Благодарение на мрежовия протокол лицето, поддържащо системата за наблюдение, ще може и с отдалечена връзка да наблюдава всички IP инсталирани камери на служебния компютър. За осигуряване на по-добра връзка между компютъра и IP камерата повечето специалисти свързват двете устройства с мрежов кабел от категория Cat5e (1000 Mbps) и отделно

конфигурират безжична връзка между камерата и маршрутизатор. Това се извършва в случай, че ако безжичната комуникационна връзки бъде прекъсната, тогава жичната връзка да продължи да предава информацията между устройствата [1], [2], [3], [4]. [5], [6], [7].

## **2. Избор на IP камера**

В статията са изследвани и анализирани IP камерите НIK DS-2CD3132-I, Dahua DH-IPC-HFW4300SP, Hailan AP005, YUNCHI RIS-Hik881W, IMPORX IMP-HC7286-K20X-W2, IMPORX IMP-HD6200RPLAW и Apexis APM-J012-WS. Камерата НIK DS-2CD3132-I притежава следните технически характеристики:

- Само мрежов интерфейс RJ-45 10/100Mb.
- Форматът на видеокомпресия е MJPEG,H.264.
- Паричната стойност на тази камера е 100 долара.
- Сензорът е тип CMOS.
- Резолюцията е 1080P (Full-HD). 1920×1080
- Нощно виждане до 30 метра.

Камерата Dahua DH-IPC-HFW4300SP притежава следните технически характеристики:

- Само мрежов интерфейс RJ-45 (10/100Base-T).
- Форматът на видеокомпресия е MJPEG/H.264.
- Паричната стойност на тази камера е 82 долара.
- Сензорът е тип CMOS.
- Резолюцията е 1080P (Full-HD). 1920×1080
- Нощно виждане до 35 метра.

Камерата Hailan AP005 притежава следните технически характеристики:

- Само мрежов интерфейс RJ-45 (10/100Base-T) и IEEE 802.11b/g/n.
- Форматът на видеокомпресия е H.264.
- Паричната стойност на тази камера е 170 долара.

- Сензорът е тип CMOS.
- Резолюцията е 720P (HD Ready) 1280\*720
- Нощно виждане до 40 метра.

Камерата YUNCHI RIS-Hik881W притежава следните технически характеристики:

- Само мрежов интерфейс 10Base-T/100Base-TX, RJ45 connector.
- Форматът на видеокомпресия е H.264.
- Паричната стойност на тази камера е 820 долара.
- Сензорът е тип CMOS.
- Резолюцията е 1080P (Full-HD) 1920×1080.
- Нощно виждане до 100-150 метра.

Камерата IMPORX IMP-HC7286-K20X-W2 притежава следните технически характеристики:

- Само мрежов интерфейс RJ-45 10/100Mb Ethernet Slot
- Форматът на видеокомпресия е H.264.
- Паричната стойност на тази камера е 800 долара.
- Сензорът е тип CMOS.
- Резолюцията е 1080P (Full-HD). 1920×1080
- Нощно виждане до 140 метра.

Камерата IMPORX IMP-HD6200RPLAW притежава следните технически характеристики:

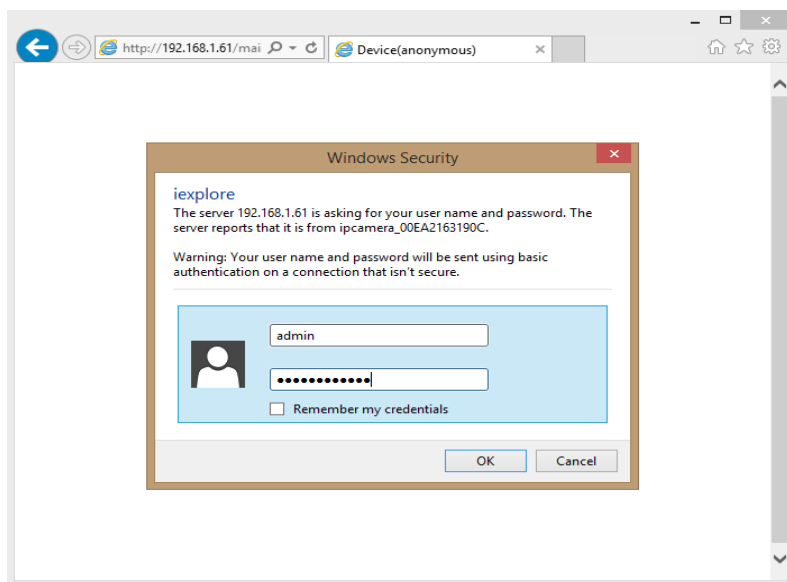
- Само мрежов интерфейс RJ-45 10/100Mb Ethernet и Wi-Fi/802.11/b/g.
- Форматът на видеокомпресия е H.264.
- Паричната стойност на тази камера е 797 долара.
- Сензорът е тип CCD.
- Резолюцията е 1080P (Full-HD) 1920×1080.
- Нощно виждане до 140 метра.

Камерата Apexis APM-J012-WS притежава следните технически характеристики:



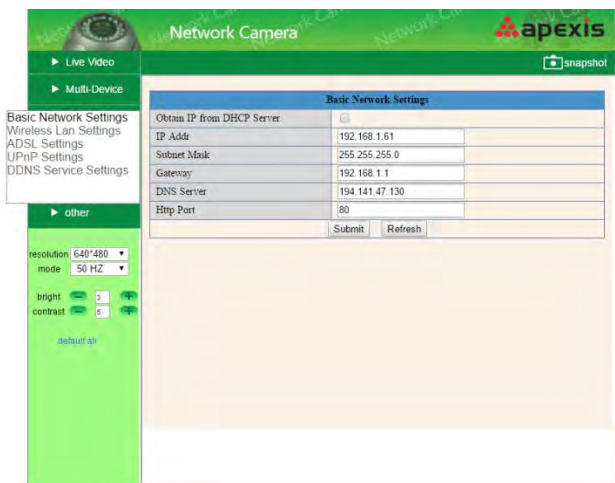
- Мрежови интерфейс RJ-45 10/100Mb Ethernet и Wi-Fi IEEE 802.11/b/g.
- Форматът на видеокомпресия е H.264.
- Паричната стойност на тази камера е 86 долара.
- Сензорът е тип CMOS.
- Резолюцията е 640×480.
- Нощно виждане до 15 метра.

Във факултета по технически науки при Шуменски университет „Епископ Константин Преславски“ се използва IP камерата Araxis APM-J012-WS с експериментална цел за наблюдение и контрол на хората. Достъпът до графичния потребителски интерфейс се осъществява чрез въвеждане на логически IP адрес 192.168.1.61 в заглавната лента на браузера Internet Explorer. Това е показано на фиг. 1.



Фиг. 1. Достъп до IP камерата





Фиг. 4. Основни мрежови настройки на IP камерата

На фиг. 4 са показани основните мрежови настройки на IP камерата. Тя е конфигурирана със следните настройки:

- За логически IP адрес е избран 192.168.1.61.
- Мрежовата маска е с 24 бита - 255.255.255.255.
- Шлюзът на мрежата е 192.168.1.1.
- DNS сървърът е с публичен адрес 194.141.47.130
- HTTP портът е 80.

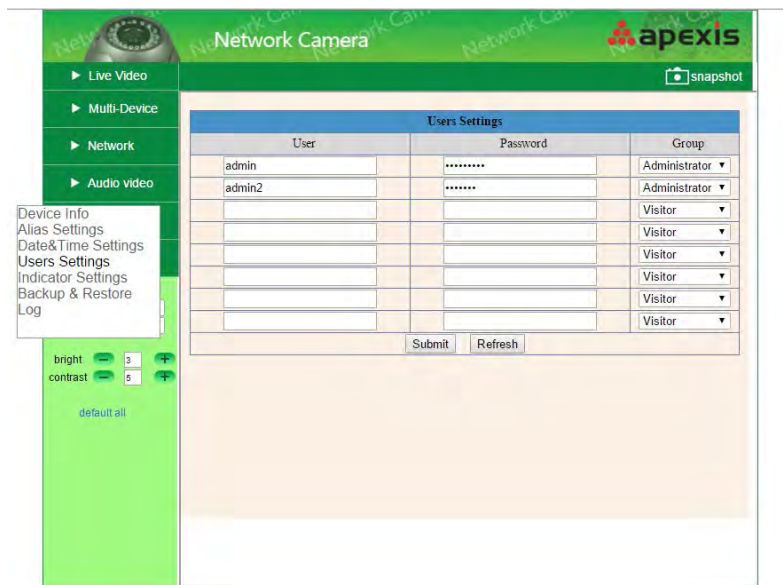
На фиг. 5 са показани безжичните настройки. Камерата е конфигурирана със следните настройки:

- Уникалното име на конфигурирана безжична мрежа е TP-LINK\_401
- Типът на мрежата е инфраструктура.
- Начинът на криптиране е WPA2 Personal (AES).



Фиг. 5. Безжични мрежови настройки на IP камерата

На фиг. 6 са илюстрирани имената на потребителите заедно с техните пароли. Групите с права на достъп са администратор, посетител и оператор. За да може да се използват всички функции на графичния потребителски интерфейс е необходимо потребителят да е част от администраторската група.



Фиг. 6. Списък с потребителските имена и пароли

### 3. Заключение

Всеки професионалист по сигурността или системен администратор, работещ в компания, фирма и държавна институция трябва много точно да направи план за разположението на IP камерите. Съвременните IP камери трябва да притежават два мрежови интерфейса за жична и безжична връзка, разделителна способност Full-HD с  $1920 \times 1080$  пиксела и нощно виждане до 100 или 150 метра. При правилно изградена система за наблюдение с IP камери се гарантира сигурност на работния процес в съответната организация.

### ЛИТЕРАТУРА

41. Kandhalu A., Rowe, A., & Rajkumar R. R., DSPcam: A camera sensor system for surveillance networks, In Third ACM/IEEE International Conference Distributed Smart Cameras ICDSC, August 2009, pp. 1-7
42. Ku C. W., Cheng C. C., Yu G. S., Tsai M. C., & Chang T. S., A high-definition H. 264/AVC intra-frame codec IP for digital video and still camera applications, Circuits and Systems for Video Technology, IEEE Transactions on, 16(8), 2006, 917-928

43. Mao J. C., & Lin, L. H., Design and implementation of wireless IP camera based on WIFI environment [J], *Microcomputer & Its Applications*, 21, 019, 2010
44. Varcheie P. D. Z., & Bilodeau G. A., Active people tracking by a PTZ camera in IP surveillance system, In *IEEE International Workshop on Robotic and Sensors Environments ROSE*, November 2009, pp. 98-103
45. Yang M. J., Tham J. Y., Wu D., & Goh, K. H., Cost effective ip camera for video surveillance, In *Industrial Electronics and Applications*, May 2009, 4th IEEE Conference on ICIEA, pp. 2432-2435
46. Yang C. S., Chen R. H., Lee C. Y., & Lin S. J., PTZ camera based position tracking in IP-surveillance system, In *3rd IEEE Sensing International Conference on Technology ICST*, November 2008, pp. 142-146
47. Wong C. J., MatJafri M. Z., Abdullah K., Lim H. S., & Low K. L., Temporal air quality monitoring using surveillance camera, In *IEEE International Symposium Geoscience and Remote Sensing IGARSS*, July 2007, pp. 2864-2868

# ИЗСЛЕДВАНЕ НА СИГУРНОСТТА НА БЕЗЖИЧНА ЛОКАЛНА КОМПЮТЪРНА МРЕЖА

Петър Кр. Боянов, Иван О. Николов, Жанета Н. Ташева,  
Тихомир Сп. Трифонов

## RESEARCH THE SECURITY OF WIRELESS LOCAL AREA COMPUTER NETWORK

Petar Kr. Boyanov, Ivan O. Nikolov, Zhaneta N. Tasheva,  
Tihomir Sp. Trifonov

**ABSTRACT:** *In this paper research the security of wireless local area computer network is made. Nowadays, it is very obligated that each security and system administrator has to research and maintain the stable security level in the particular wireless local area network against various malicious cyber-attacks. Thereby, most of the plain computer users must monitor their input and output traffic network chain in order to analyze the present of unauthorized established network connection.*

**KEYWORDS:** *IP, LTE, Port, Research, Security, Scan, WLAN, Zenmap.*

### 1. Въведение

Понастоящем индустрията на мобилните комуникации е съвкупност от развиващи се стандарти и решения, необходими за следващите стъпки в еволюцията на мобилните мрежи. На съвременния етап от развитието на обществото съществува остра нужда от високи скорости за предаване на данни [5]. Тя доведе до появата на 3GPP LTE - нов високопроизводителен радиоинтерфейс за клетъчни мобилни комуникационни системи. LTE (Long Term Evolution) представлява най-последната стъпка на 4-тото поколение радиотехнологии [5]. Този интерфейс е проектиран да увеличи капацитета и скоростта на мобилните клетъчни мрежи [1], [3], [13]. В практиката все още се използва маршрутизатор, който да осигури безжична свързаност на хостовете в компютърната мрежа. Една от най-важните задачи на

всеки системен администратор е осигуряването на защита на безжичната връзка [4], [6].

## 2. Експеримент

Експериментът е направен в безжична локална мрежа WLAN (Wireless Local Area Network) от 2 хоста в компютърна лаборатория във Факултета по технически науки при Шуменски университет „Епископ Константин Преславски”. Всеки хост използва безжичен USB адаптер 150Mbps Wireless N USB Adapter TL-WN721N. В компютърната лаборатория е използван безжичен DSL рутер с логически IP адрес 192.168.1.1 и 24-битова мрежова маска 255.255.255.0. В този маршрутизатор е активиран протоколът DHCP (Dynamic Host Configuration Protocol) с цел автоматично раздаване на IP (Internet Protocol) логически адреси на всеки хост, който се опита да се свърже с рутера. Атакуващият хост се е свързал към безжичната мрежа и използва операционна система Microsoft Windows 7 Enterprise SP1 и мрежовите скенери Advanced Port Scanner v1.3 и Zenmap Version 6.49BETA4 [8].

Адресното пространство за автоматично раздаване на IP адреси започва от 192.168.1.3 и завършва на 192.168.24.5 с 24-битова мрежова маска. Основните настройки на безжичния интерфейс на рутера са:

- Активирана опция за безжично разпръскване.
- Скриване на SSID от другите хостове.
- Максималният брой на клиентите е три.

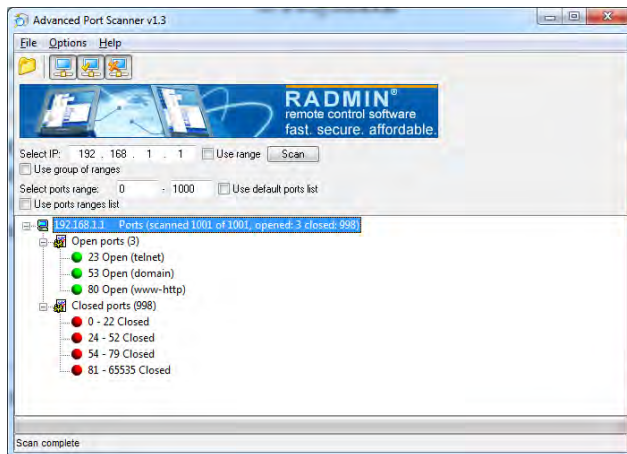
Името на SSID е избрано да бъде “pesho”. Методът на мрежова автентификация е WPA2-PSK, а криптирането на данните се осъществява със стандарта AES. Криптирането със стандарта WEP е строго забранено в рутера. Честотната лента, в която оперира маршрутизаторът е 2.4 GHz с избран тридесети номер на канала.

На атакуващия хост е раздаден логически IP адрес 192.168.1.4. Първата задача е свързана със сканиране на безжичната маршрутизатор с цел установяване кои портове са в отворени или затворени [7], [8], [9].



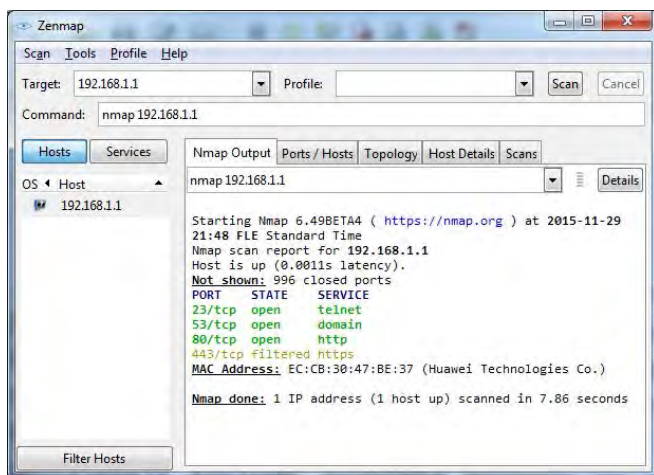
На фиг. 1 е показан резултатът от сканирането на първите хиляда порта от рутера. Портовете, които са открити след сканирането са:

- порт с №23, на който е активирана услугата Telnet;
- порт с №53, на който е активирана услугата DNS;
- порт с №80, на който е активирана услугата www-http.



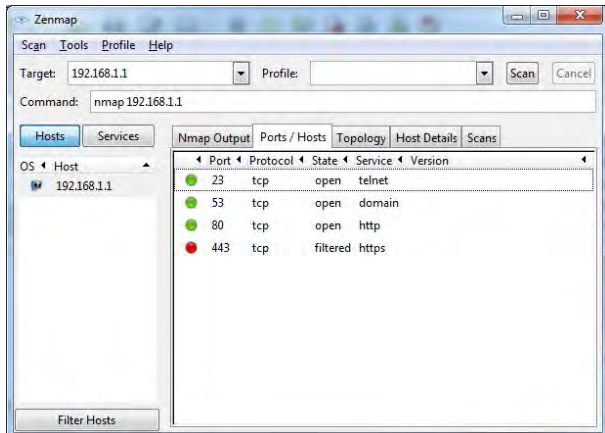
**Фиг. 1.** Получени резултати след сканирането с програмата Advanced Port Scanner v1.3

Другата сканираща мрежова програма, която е използвана по време на изследванията е Zenmap Version 6.49BETA4. За разлика от горната програма Zenmap разкрива дали сканираният порт е в филтрирано състояние [10], [11], [12]. На фиг. 2 е илюстриран показаният резултат след проведеното сканиране.



**Фиг. 2.** Получени резултати след сканирането с програмата Zenmap Version 6.49BETA4

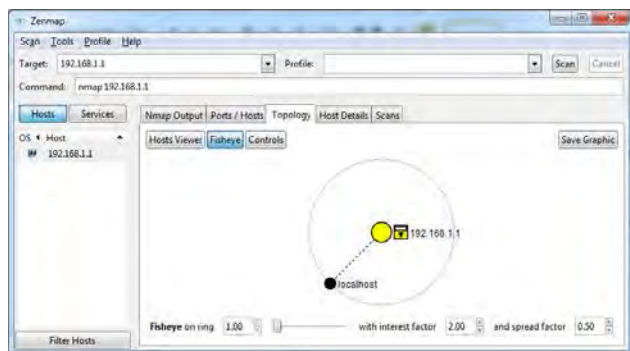
С този програма са открити три отворени и един филтриран порт. Номерът на филтрирания порт е 443 с активирана услуга https.



**Фиг. 3.** Детайлна информация за сканираните портове

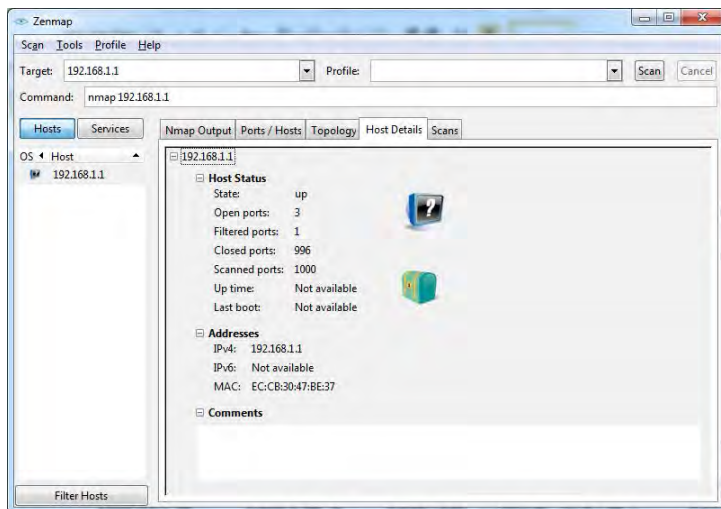
Фиг. 3 показва детайлна информация за всеки един порт. Една от най-голямата заплата е свързана с порт №23, защото

предаваната през него информация между два хоста е в обикновен вид и ако определен злонамерен извършител слуша мрежовия трафик между тях, може след това много лесно да разбере какво точно се предава по мрежата. Затова е строго препоръчително да се бъде изключената услугата telnet. Вместо нея може да се използва услугата SSH (Secure Shell) версия 2 с порт №22, при която предаваната информация между двата хоста е криптирана. На фиг. 4 е показана топологията на компютърната мрежа.



**Фиг. 4.** Топология на компютърната мрежа

Хостът е оцветен в жълто кръгче, защото броят на намерените отворени портове е три. На фиг. 5 е показана обобщена детайлна информация на хост с логически IP адрес 192.168.1.1.



**Фиг. 5.** Обобщена детайлна информация на хост с логически IP адрес 192.168.1.1.

От фиг. 5 се установи, че са сканирани общо 1000 порта. Разкрит е физическият MAC адрес на хоста - EC:CB:30:47:BE:37. Благодарение на получения физически адрес, киберпрестъпникът може за осъществи кибератака с изпращане на мрежови пакети с фалшифициране на MAC адреса на източника и по този начин да придобие отдалечен достъп до компютърните ресурси на хоста.

### 3. Заключение

Всеки професионалист по сигурността или системен администратор, работещ в компания, фирма и държавна институция трябва да прави периодични тестове за състоянието на портовете в маршрутизатора. Препоръчително е използването на хибридна защитна стена, която да е съставена от защитна стена с филтриране на пакети, динамична защитна стена с цялостно инспектиране, защитната стена с приложен шлюз, защитна стена с преобразуване на мрежови адреси, персонална защитна стена и хост-базирана защитна стена. Поради тази причина повечето от производителите на защитни стени започнаха да въвеждат хибридни защитни стени, за да могат да намалят всички възможни

слаби места и недостатъци на другите защитни стени с цел намаляване на риска от заобикаляне им и осъществяване на кибератаки

## ЛИТЕРАТУРА

48. 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.
49. Asrodia P., & Patel H., Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis, International Journal of Electrical, Electronics and Computer Engineering 1(1): 55-58(2012)
50. Caulkins, Bruce D. Proactive Self Defense in Cyberspace. ARMY WAR COLL CARLISLE BARRACKS PA, 2009.
51. CERF, Vinton G.; ICAHN, Robert E. A protocol for packet network intercommunication. ACM SIGCOMM Computer Communication Review, 2005, 35.2: 71-82.
52. Fetfov O. M., Nikolov L. G., Kulev N. Zh., "Cellular Radio Channel Carrier Aggregation Motivation and Benefits Overview" - „Machines, Technologies, Materials”, ISSN 1313-0226, YEAR VIII, ISSUE 5/2014.
53. Helmer, Guy G., et al. "Intelligent agents for intrusion detection." Information Technology Conference, 1998. IEEE. 1998.
54. Hixon, Rena, and Don M. Gruenbacher. "Markov chains in network intrusion detection." Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC. IEEE, 2004.
55. 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
56. Kahya-Özyirmidokuz E., Gezer A., & Ciflikli C., Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application, In DATA ANALYTICS 2012, The First International Conference on Data Analytics, 2012, September, pp. 18-23
57. Kocher, Joshua E., and David P. Gilliam. "Self port scanning tool: providing a more secure computing environment through the use of proactive port scanning." Enabling Technologies: Infrastructure for Collaborative Enterprise, 2005. 14th IEEE International Workshops on. IEEE, 2005.
58. KOZIEROK, Charles M. The TCP/IP guide: a comprehensive, illustrated Internet protocols reference. No Starch Press, 2005.
59. 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
60. Zhang, Bofeng, et al. "Remote Operation System Detection Base on Machine Learning." Frontier of Computer Science and Technology, 2009. FCST'09. Fourth International Conference on. IEEE, 2009.

# СИТУАЦИОНЕН ЦЕНТЪР ЗА УПРАВЛЕНИЕ НА СИСТЕМАТА ЗА СИГУРНОСТ НА ОРГАНИЗАЦИЯТА

ДИМИТЪР С. ДИМИТРОВ

## SITUATIONAL CENTRE FOR MANAGING THE SECURITY SYSTEM OF THE ORGANISATION

Dimitryr S. Dimitrov

**ABSTRACT:** *The report examines the issues related to security of special objects of government, administrative buildings and industrial objects. Proceeding from its intended purpose, the situational centre will create conditions for conducting practical exercises with the students in realization of specific management options for integrated systems with objects with different functions and configuration.*

**KEYWORDS:** *situational centre, management, security system of the organization, control of the access, security, protection of personal and corporate interests, control of the working time, restricting the access, protection of information*

Системата за контрол на достъпа чрез използване на специализирани технически средства се явява своеобразна интегрирана система за мониторинг и наблюдение в реално време и защита на специализирани обекти, която:

- осъществява наблюдение, откриване и проследяване на хора и превозни средства, незаконно навлезли в зоната на стратегическия обект или извършващи други закононарушения; открива признаци за подготвящо се нарушение;
- включва надеждна комуникационна система за обмен на информация, предаване на команди, пренос на визуална

информация в реално време;

- предприема съвременни и адекватни мерки за противодействие;
- управлява натрупаната база данни.

Сградите и помещенията за нуждите на експлоатацията на техническите системи за сигурност на даден строеж се проектират при спазване на изискванията на Приложение № 2 от Наредба № 7 за системите за физическа защита на строежите. Видът, броят и площите на сградите и помещенията се определят при отчитане на числеността на персонала за физическа защита, възложените му функционални задължения, броя и вида на монтираните технически съоръжения и системи, използваните служебни животни и използваните транспортни средства. Допуска се сградите и помещенията на звената за охрана да се проектират или устройват в общи сгради със звената на противопожарната охрана. Помещенията за транспортните средства се проектират при спазване на условията и техническите изисквания за съхранение, експлоатация и ремонт на моторните превозни средства.

Физическите и юридическите лица, които оборудват с технически системи за сигурност, декларират писмено при получаване на разрешението за извършване на охранителна дейност, че няма да разгласяват трасетата на охранителните инсталации и параметрите на техническите системи за сигурност и ще задължават писмено подчинените им длъжностни лица за същото.

При тази охрана икономическите разходи са еднократни, а сигурността е постоянна. Това е специализиран вид охрана, която включва:

- проектирането, монтажа, използването и поддържането в обекти на юридическите и физическите лица на съответна техника за тяхното опазване, защита и сигнализиране;
- проверка на получените алармени сигнали, когато сигнално-известителната техника е свързана с дежурен център.

Икономическата обосновка е съобразно функциите, които се изпълняват от принциपालа на частното охранително търговско

дружество относно техническите системи за сигурност. Функциите, които изпълняват техническите системи за сигурност, определят изискванията, които са заложиени в основата на проектирането, монтажа и експлоатацията.

Функциите, които са заложиени, могат да бъдат:

- блокировка на помещения и райони, които се контролират от централен пост на охраната;
- гарантиране задържането на лица, нямащи право да влизат безпрепятствено в охраняеми помещения;
- идентифициране на личността на сътрудниците и посетителите, които имат право да влизат в охраняемите помещения;
- контрол за цялата комуникация и работоспособността на апаратурата от системата за техническа защита;
- събиране и обработка в нагледна форма на информацията, постъпваща от охраняемата територия в централния пункт за охрана;
- неутрализиране на каналите за изтичане на информация от обекта с използването на технически средства;
- контрол за правилното носене на службата от персонала на охраната и регистрация на факти за отклонения от предписания начин за поведение по време на охрана;
- събиране на оперативна информация за всички събития, свързани с гарантиране на сигурността на обекта.

Проектирането, монтажът и експлоатацията на техническите системи за сигурност в обекти включват съответна техника за тяхното опазване, защита и сигнализиране, както и проверка на получените алармени сигнали, когато техниката е свързана с дежурен център. Въз основа на това можем да дадем работно определение за техническите системи за сигурност. При анализиране на подзаконовите нормативни актове, се установи, че техническата система за сигурност е съвкупност от централни и местни пултове, контролни панели, датчици, средства за сигнализация и устройства за предаване на сигнали от разстояние



при наблюдение и контрол, които подават алармен сигнал при опити за проникване в територията на охранявания обект.

Контрол на достъпа: осъществява се чрез система за контрол на достъпа с магнитни карти, оптични карти, цифрови ключалки, електронни ключалки и др.

Пожароизвестителни системи: те трябва да покриват всички охраняеми помещения, но без да излъчват вредни емисии за персонала. При пожар освен звукова и светлинна сигнализация трябва да изключват ел. захранването, да спират асансьорите на ниво етажи, да блокират въздуховодите и климатичните инсталации и др.

Системи за телевизионно наблюдение: позволяват визуално да се контролират всички важни помещения, трезори, каси, движение на парични средства.

Качествената техника е много надеждна, работи в непрекъснат режим и не влошава параметрите си. Желателно е цялата информация да бъде записвана непрекъснато на видеорекордер. Камерите, с които се извършва телевизионното наблюдение, са изключително важен елемент от системата. Възможно е наблюдение и на свършено неосветени обекти. За целта трябва да се използват видеокамери с инфрачервена светлина.

Съвременните датчици трябва да бъдат изградени на основата на модерна технология, да имат микропроцесорна обработка на сигнала, да са защитени от бяла светлина и радиоизлъчвания, да имат температурна компенсация и броячи, повишаващи защитата на фалшиви сработвания. Според физическия принцип на регистрация на движението датчиците, които са най-разпространени, биват няколко разновидности:

- пасивни инфрачервени;
- микровълнови; ултразвукови;
- активни акустични и др.

При изграждането на сигнално-охранителната известителна система на обектите по принцип трябва да се прилагат няколко рубежа за защита, като е задължително използването на датчици с различен физически принцип. По този начин се осигурява много надеждна работа в непрекъснат режим.

Колкото по-голяма е защитата на материалните активи и колкото по-сигурен се чувства персоналят, толкова по-успешен ще бъде бизнесът. Необходим е непрекъснат стремеж към намаляване на риска и редуциране на разходите за застраховки, без това да излага на опасност всичко, което фирмата притежава.

Някои от най-ефективните решения за сигурност на пазара следват принципа на всички останали автоматизирани системи за контрол - отворени са, може да се разширяват постепенно в зависимост от нуждите и бюджета, и са с максимална икономическа ефективност. Изгражда се система, която позволява да се управляват всички врати, камери, сензори за проникване в сградата, противопожарни устройства. Част от интелигентните системи, които може да се монтират в специалните обекти на държавната власт, административните сгради и производствените обекти се отличават именно с интегрирания си подход. Те комбинират всичко:

- видео наблюдение;
- контрол на достъпа;
- откриване и известяване за проникване;
- пожарна безопасност;
- течове;
- аварийно осветление.

Така може по-бързо да:

- се създават отчети за всяко събитие;
- бързо и ефективно справяне с пробиви в сигурността;
- да разпознаване и коригиране на повредено оборудване;
- да свързване на лична информация и видео записи, така

че да се знае къде, на територията на обекта, се намира всеки един служител.

Какви са ползите от употребата на интегрирани системи за сигурност:

- ◆ Интегрираните системи използват компоненти, които в последствие изпълняват повече от една функция. Сензорът за движение, който регистрира влизане в складовите, производствените помещения или офисите в извънработно време, може да спести и енергия чрез контролиране на осветлението и температурата.

- ◆ Осигуряват криптиране и автентификация, което предотвратява фалшифициране на комуникацията.

- ◆ Лесни са за употреба. Времето, необходимо за обучение е много кратко. Персоналът по сигурността може бързо да се научи да работи, с която и да е от предлаганите системи. Това намалява разходите.

- ◆ Разходите за монтаж, разширяване и осигуряване на платформа за интегриране, не само на системата за сигурност, но и на всички останали системи за сградна автоматизация, са минимални.

- ◆ Екипът, който работи с интегрираната система за сигурност, има видео записи и подробни отчети за всичко, което се случва на територията на административните сгради и производствените обекти и в случай на нужда, може ефикасно и бързо да съдейства на полицията.

Различните компоненти на интегрираните системи за сигурност най-често включват:

### ***Видеонаблюдение***

Съществуват няколко различни варианта за управление и анализ на видеонаблюдението. Основното им предимство е, че с тях може да се действа проактивно. Специалните им функции за наблюдение и анализ на видеоматериала, който се гледа в реално време или на запис, позволява да се предотвратят множество инциденти.

### ***Детектор за проникване в помещенията***

В интегрираната система за сигурност влизат и няколко вида детектори и аларми за неразрешено проникване в помещенията. Те взаимодействат перфектно със системата за наблюдение. В момента, в който детекторите засекат опити за непозволено влизане, освен че се включва аларма, камерите автоматично дават предварително увеличение на образа и променят наклона си така, че да заснемат максимално добре обекта.

### ***Противопожарна система***

При пожар тя ще активира не само алармата, но и цяла серия от събития - включване на аварийно осветление, изключване на газоподаване, записване на всички събития, за да може след това да се изгледа видеоматериала и да се анализира откъде е дошъл проблемът.

### ***Аварийно осветление***

Освен стандартните си функции аварийното осветление изпълнява още няколко. Автоматично се идентифицират всички неработещи осветителни тела, подава автоматични напомняния за необходимостта от рутинни тестове на системата. Така се осигурява увереност, че цялата система за сигурност е в изправност.

Уникалността на интегрираната система за сигурност е в това, че всеки един от компонентите ѝ изпълнява, освен основните си, още няколко важни функции. Това я прави по-икономична и ефективна.

Системата осигурява централизирано управление и контрол на достъпа до помещения, сгради, асансьори и др.

Идентификация на лицата се извършва посредством контактни биометрични четци. При прочитане на пръстовия отпечатък в контролно-пропускателното устройство се извършва проверка за правата на достъп и ако достъпа е разрешен се подава сигнал за отключване към електромагнитен механизъм.

Контролно-пропускателните устройства са свързани с управляващ компютър от който се зарежда списъка на служителите с карти и правата им на достъп. При всяко преминаване в управляващия компютър се записва дата, час на влизане или излизане, кода на лицето и номера на контролно-пропускателното устройство.

Системата може да се използва както за контрол на работното време, така и само за контрол на достъпа.

Системата позволява извършването на справки за извършените преминавания, за изработено време по дни и за месец, за извършени нарушения на работното време, за наличен и отсъстващ персонал и др. Всяка контролно-пропускателна точка има възможност да следи състоянието на вратата, позволява отваряне от разговорна уредба или бутон, запазва нормалната си работа при отпадане на електрическото захранване и връзката с управляващия компютър.

### ***Софтуер***

Софтуера на системата се състои от два модула за контрол на достъпа и работното време - сървър и клиент. Програмата сървър следи за преминаванията през обектите в реално време и ги записва в база данни MySQL на компютъра. Чрез нея могат да се добавят или редактират личните данни на служителите като име, презиме, фамилия, ЕГН, адрес, телефон, дата на назначаване, отдел, подотдел, длъжност, снимка и да се укаже за кои обекти и по кое време в денонощието да има достъп. Програмата клиент може да се инсталира на други компютри, които се свързват към сървъра през локална мрежа и се осъществява отдалечен контрол на работното време. С клиентската програма има възможност да се правят различни видове справки, като справка за преминаванията през обектите за определен период от време на служителите, справка за налични служители в сградата, справка за отсъстващи служители, справка за освободени служители (командировка, отпуск и т.н.) за даден период от време, справка за напуснали служители за определен период от време, справка за назначени служители за определен период от време. Главната справка за контрола на работното време е генериране на присъствена форма

76. С нея се добива пълна представа за присъствията и отсъствията на всеки един служител за всеки ден от месеца.

Докладът е на основа на разработен проект в областта на обновяване на оборудването на специализираните кабинети и усъвършенстване на процеса на обучение на студентите от специалност „Системи за сигурност” в катедрата. Поставената цел е разработване и практическо реализиране на ситуационен център за управление на системата за сигурност на организацията.

Изграждането на ситуационен работен център за управление на системата за сигурност на организацията чрез интегриране на системите за управление на контрола на достъпа, видеонаблюдението, пожароизвестяването, енергийната ефективност и екологичност на помещенията в сградата на е процес свързан с детайлното изучаване на структурата, задачите, производствените (технологичните) и другите особености на организацията (фирмата, обекта) за който е предназначена. Новоразработената система ще позволи многовариантност на настройка на техническите средства от състава ѝ в съответствие със зададените конкретни параметри на обекта. Изхождайки от предназначението му (проектиране и разработване на ситуационен работен център за управление на системата за сигурност на организацията чрез интегриране на системите за управление на контрола на достъпа, видеонаблюдението, пожароизвестяването, енергийната ефективност и екологичност на обекта), ситуационния център ще създаде условия за провеждане на практически занятия със студентите по реализация на конкретни варианти за управление на интегрирани системи на обекти с различно предназначение и конфигурация.

С разработването на проекта са постигнати и следните изследователски и методически цели:

- ◆ Проектиране, разработка и практическа реализация на ситуационен работен център за управление на системата за сигурност на организацията;

- ◆ Повишаване квалификацията на студентите от

специалност „Системи за сигурност” в усвояване на актуални методи за научноизследователска работа

- ◆ Ускоряване на интегрирането на учебния процес с последните постижения в областта на видеонаблюдението и системите за контрол на достъпа, реализираща сложни изчислителни методи за изследване на анализирания физически процеси;

- ◆ Изграждане в обучаемите знания и умения и компетенции по изграждането и управлението на системи за физическа сигурност, настройката на техническите средства от състава на системите, както и анализиране на резултатите от работата на системата;

- ◆ Мотивиране и развиване на творческите и научно-изследователските способности на студентите.

Получени са и следните резултати:

- ◆ Резултатите от проучването и анализа на проблемите позволяват създаването на реална учебна среда за проектиране, реализация и настройка на ситуационен център за управление на системата за сигурност на организации и обекти с различно предназначение и различна големина.

- ◆ Практическата реализация на проекта представлява физически модел на система за управление на сигурността, енергийната ефективност и екологичност, имаща приложение в учебния процес на студентите от специалност „Системи за сигурност”.

- ◆ Чрез създадения ситуационен център на реална учебна система, студентите ще могат да проектират, създават и настройват реален център за управление на системата за сигурност на организацията чрез интегриране на системите за управление на контрола на достъпа, видеонаблюдението, пожароизвестяването, енергийната ефективност и екологичност на помещенията в сградата на е процес свързан с детайлното изучаване на структурата, задачите, производствените (технологичните) и другите особености на организацията (фирмата, обекта) за който е предназначена.

- ◆ Повишаване квалификацията на студентите от

специалност „Системи за сигурност” в усвояване на актуални методи за научноизследователска работа.

Всичко това ще спомогне на студентите да изградят умения и компетенции за пълноценна професионална подготовка във връзка с изискванията на квалификационната им характеристика.

При разработването на проекта стремежът беше да се удовлетворят необходимостта от осигуряване на сигурност на организацията която може да бъде: специални обекти на държавната власт, административни сгради и производствени обекти, т.е. постига се резултат при който автоматизираната система за наблюдение и анализ на оперативните процеси в производството може да се комбинира с интегрирана система за сигурност. Така се контролират по-лесно нивата на достъп до различните помещения за което се получава известие автоматично.

## ЛИТЕРАТУРА

1. Лалев, Хр., Системи за видеонаблюдение, Тр., 2008г.
2. Салтиров Д., “Човешките ресурси като риск за дестабилизацията на организацията”, НК, ШУ „Ей. К. Преславски”, 2008г.
3. Салтиров Д., „Изграждане на система за контрол на достъпа чрез използване на специализирани технически средства”, НК МАТТЕХ 2012, ШУ "Епископ Константин Преславски", 2012г.
4. Христов Х., „Активна и пасивна стратегии за управление на противодействието на посегателства срещу бизнес организацията – предимства и недостатъци”, Международна научна конференция, УНИБИТ, София, 2013 г.
5. [www.andy.bg](http://www.andy.bg)
6. [www.antipodes.bg](http://www.antipodes.bg)
7. [www.optixco.com](http://www.optixco.com)
8. [www.lirex.bg](http://www.lirex.bg)
9. [www.teamiss.com](http://www.teamiss.com)
10. [www.tycois.com](http://www.tycois.com)
11. [www.rittal.bg](http://www.rittal.bg)



# Граждански контрол на сектора за сигурност

Христо А. Христов

## Civic control under security sector

Hristo A. Hristov

**ABSTRACT:** *Citizens' right to control the administration the sector of security is extremely important personal right and such it is attached to constitution and the laws in the country.*

*The control of citizens on security sector comply with special conditions and procedures provided for inseparate legislative acts as a necessary guarantee for lawful, correct, efficient and quality performance of control activities.*

*In this connection, the subject of this study are the possibilities of Bulgarian citizens to control the institutions of these security sector.*

**KEYWORDS:** *Security sector, civilian control, the Ombudsman, disputing, an appeal, an administrative act.*

*Гражданите имат правото да участват в избори, да се сдружават в граждански организации, разполагат със свобода на словото, с право на информираност за обществените и държавните дела, правото на изразяване на мнения, правото на митинги и манифестации, правото на жалби и предложения до държавните органи и органите на местно самоуправление. Това са все средства за упражняване на пряк или косвен контрол върху властта, чрез които гражданите участват в управлението.*

От практиката могат да се изведат общо пет условия, поради които гражданите биха се занимавали активно с обществени дела: Личната мотивация; Наличието на алтернативи; Влиянието върху резултатите; Приложимостта на знанията и уменията; Когато не са необходими много време и усилия. [1],[4].

Чрез участието на гражданите в решаването на въпроси от национално или местно значение се реализират политически функции като:

- На практика, участието на гражданите в политическия процес ги поставя в друг тип взаимоотношения с участниците в

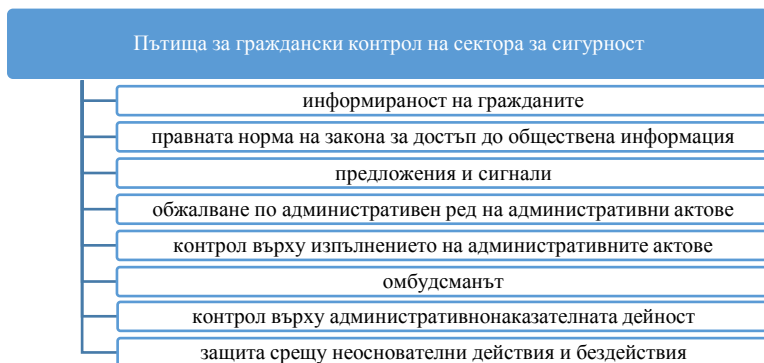
политическата система, обезпечаваша възможности да формират политики и да вземат решения и формира политическата им култура.

- Самата възможност за участие изисква от гражданите опознаване на структурата, функциите и механизмите, чрез които работи политическата система и по този начин спомага за приобщаването им към нея.

- Гражданското участие увеличава възможността за предлагането на алтернативни решения по конкретен проблем, което е в основата на демократичното управление и създава нагласи за възприемането на нов тип обществени и политически ценности. Чрез различните форми на гражданско участие се реализира принципа на обществения плурализъм.

- Участието на гражданите във формирането и реализирането на национални или местни политики дава възможност за контрол и оценка на ефективността на управлението и управляващите, което от своя страна подпомага приемането на по-добри решения, подкрепяни от обществото или тяхното своевременно коригиране. От тази гледна точка, степента на участие на гражданите в обществените процеси и предпочитаните форми за участие могат да бъдат критерии за ефективността на управлението и удовлетвореността на гражданите от функционирането на политическата система.[6]

**Ключовите пътища за граждански контрол на сектора за сигурност са:** *Информираност на гражданите; Правната норма на закона за достъп до обществената информация; Предложения и сигнали; Обжалване по административен ред на индивидуалните и общите административни актове; Контрол върху изпълнението на административните актове; Омбудсманът; Контрол върху административно-наказателната дейност на администрацията; Защита срещу неоснователни действия и бездействия на администрацията на сектора за сигурност.* (виж фигура 1). [9],[10].



**Фиг.1.** Пътища за граждански контрол на сектора за сигурност

Съществено значение за ефективния граждански контрол над дейността на сектора за сигурност има информираността на гражданите. Това е познаването от гражданите на обективното състояние и функционирането на специализираните структури от сектора за сигурност.

Правната норма на **закона за достъп до обществената информация** позволява на гражданите да отправят своите искания за достъп до определена, касаеща ги информация.

Обществена информация по смисъла на този закон е всяка информация, свързана с обществения живот в Република България и даваща възможност на гражданите да си съставят собствено мнение относно дейността на задължените по закона субекти. [11],[3].

Законът се прилага за достъп до обществената информация, която се създава или се съхранява от:

- Държавните органи, техните териториални звена и органите на местното самоуправление в Република България.
- Публичноправни субекти, различни от тези посочени по-горе, включително публичноправните организации.
- Физически и юридически лица само относно извършвана от тях дейност, финансирана със средства от консолидирания

държавен бюджет и средства от фондове на Европейския съюз или предоставени от Европейския съюз по проекти и програми.

- Организациите от общественния сектор са длъжни да предоставят информация от общественния сектор за повторно използване, с изключение на предвидените в закона случаи.

Организация от общественния сектор е държавен орган, орган на местно самоуправление и публичноправна организация, както и техните обединения.

Достъп до обществена информация се предоставя въз основа на писмено заявление или устно запитване. Заявлението се счита за писмено и в случаите, когато е направено по електронен път при условия, определени от съответния орган. Когато заявителят не е получил достъп до искана обществена информация въз основа на устно запитване или счита предоставената му информация за недостатъчна, той може да подаде писмено заявление.[7].

Основание за отказ от предоставяне на достъп до обществена информация е налице, когато:

- исканата информация е класифицирана информация или друга защитена тайна в случаите, предвидени със закон;

- достъпът засяга интересите на трето лице и няма негово изрично писмено съгласие за предоставяне на исканата обществена информация, освен в случаите на надделяващ обществен интерес;

- исканата обществена информация е предоставена на заявителя през предходните 6 месеца.

Сведенията от автоматизираните и други информационни фондове на структурите от сектора за сигурност, които съставляват държавна, служебна или следствена тайна, са закрити за достъп и въз основа на това гражданите не могат да упражняват контрол над тях. [12].

***Предложенията и сигналите са основна форма за контрол върху администрацията на сектора за сигурност.*** Понастоящем тяхната подробна уредба се съдържа в административнопроцесуалния кодекс. [8].

Предложенията и сигналите се подават до административните органи на сектора за сигурност и до други органи, които осъществяват публично правни функции. Те могат

да бъдат писмени или устни, да бъдат подадени лично или чрез упълномощен представител, по телефон, телеграф, телекс, факс или електронна поща. Не се образуват производства по анонимни предложения и сигнали. Всеки гражданин може да подава предложение или сигнал. Не се изисква лицето, което ги подава, да има личен правен интерес.

Предложения могат да се правят за усъвършенстване на организацията и дейността на административните и други органи от сектора за сигурност с публично правни функции или за решаване на други въпроси в рамките на компетентността на тези органи. Сигнали могат да се подават за злоупотреби с власт и корупция, лошо управление на държавно или общинско имущество или за други незаконосъобразни или нецелесъобразни действия или бездействия на административни органи или длъжностни лица в съответните администрации от сектора за сигурност, с които те засягат държавни или обществени интереси, права или законни интереси на други лица.

Предложенията и сигналите, които са писмени, се внасят и регистрират в деловодствата на МВР, МО и в специализираните структури.

***Гражданите могат да обжалват по административен ред индивидуалните и общите административни актове.*** Това се извършва съобразно Административнопроцесуалния кодекс.[13].

Административните актове могат да се обжалват по административен ред пред по-горестоящия административен орган по отношение на органа, който е издал акта. Жалби могат да подават само заинтересуваните граждани, т.е. тези, които имат правен интерес от издадения акт или решаването на жалбата. Обжалването става в 14-дневен срок след издаването на акта. Жалбата се подава в писмена форма чрез административния орган, чийто акт се обжалва.

В седемдневен срок, а когато органът е колективен – в 14-дневен срок от получаването на жалбата, административният орган на сектора за сигурност може да преразгледа въпроса и сам да оттегли обжалвания акт или да го измени, или да издаде съответен акт или документ, ако е отказал издаването му. В тези

случаи той е длъжен да уведоми заинтересуваните. Новият акт подлежи на обжалване по административен ред на общо основание. Ако административният орган, автор на акта, не намери основание за пререшаване на въпроса, той изпраща незабавно жалбата заедно с цялата преписка на компетентния по-горестоящ административен орган. По-горестоящият орган е длъжен да се произнесе по жалбата с мотивирано решение. Той може да отхвърли жалбата като неоснователна или ако я намери за основателна, да отмени изцяло или отчасти административния акт като незаконосъобразен или неправилен.

Когато административният орган противозаконно е отказал да издаде административен акт или документ, по-горестоящият орган го задължава да извърши това, като определя и срока. Когато издаденият административен акт е незаконосъобразен или неправилен и вместо него трябва да се издаде друг акт, по-горестоящият административен орган връща преписката на органа, издал акта, със съответни задължителни указания. Ако въпросът е изяснен от фактическа страна, по-горестоящият орган може сам да издаде акта, ако за това няма законни пречки.

Жалбата на гражданина по административен ред задвижва производства, които привеждат в действия административния контрол вътре в администрацията на сектора за сигурност. Всички производства, процедури, действия, правомощия на административните органи и процесуалните права и задължения на гражданите са стриктно регламентирани от закона. Подаването на жалбата чрез административния орган, който е издал акта, има за цел да информира органа за евентуалните нарушения, които той е допуснал при издаването на акта, и да му даде възможност да ги коригира сам. По-горестоящият орган, когато разглежда жалбата и преценява нейната допустимост и основателност, осъществява административен контрол върху акта на долустоящ, подчинен нему административен орган.

***Гражданите могат да оспорват административните актове и пред съда*** по отношение на тяхната законосъобразност с изключение на актове, за които в закон е предвидено нещо друго. В тези случаи съдът упражнява съдебен контрол върху администрацията. Контролът на гражданите върху

администрацията на сектора за сигурност в тези случаи се реализира чрез задействане на механизма на съдебния контрол заложен в Административнопроцесуален кодекс.

Предмет на оспорване:

а) първоначалният индивидуален административен акт, включително отказът да се издаде такъв акт;

б) решението на по-горестоящия административен орган, с който е изменен актът по точка „а” или е отменен и въпросът е решен по същество;

в) решенията по искания за издаване на документи от значение за признаване, упражняване или погасяване на права или задължения.

Административните актове могат да бъдат оспорени изцяло или в отделни техни части.

Основанията за оспорване на административните актове са:

- липса на компетентност;
- неспазване на установената форма;
- съществено нарушение на административно-производствени правила;
- противоречие с материалноправни разпоредби;
- несъответствие с целта на закона.

Прокурорът следи за спазване на законността в административния процес, като:

- предприема действия за отмяна на незаконосъобразни административни и съдебни актове;
- в предвидените в този кодекс или в друг закон случаи участва в административни дела;
- започва или встъпва във вече образувани по този кодекс производства и когато прецени, че това се налага от важен държавен или обществен интерес.

При участието си в административни дела прокурорът дава заключение.

Контролът на гражданите върху индивидуалните административни актове може да бъде осъществен и въз основа на други контролни производства, предвидени от специални закони.

***Контролът на гражданите може да се простира не само върху административните актове, но и върху тяхното изпълнение.***

Административнопроцесуалният кодекс предвижда възможност за обжалване от страна на гражданите на незаконосъобразни действия по изпълнение на административните актове и решения пред по-горестоящия административен орган. Гражданите могат да обжалват и наложените им административни принудителни мерки.

Гражданите имат възможност да осъществяват ***контрол и върху административнонаказателната дейност на администрацията***, съобразно със закона за административните нарушения и наказания.

Гражданите могат да обжалват наказателните постановления, с които административният наказващ орган е наложил административно наказание за извършено административно нарушение. Наказателното постановление може да се обжалва както от нарушителя, така и от пострадалия от нарушението, който е поискал обезщетение.

Законът за административните нарушения и наказания предвижда реда за обжалване пред съд на наказателните постановления, както и извънредните способи за съдебен контрол върху влезли в сила наказателни постановления.

***Защита срещу неоснователни действия и бездействия на администрацията на сектора за сигурност.*** Защитата е регламентирана в административнопроцесуалния кодекс.

#### ***А. Защита срещу неоснователни действия.***

**Право на искане.** Всеки, който има правен интерес, може да иска прекратяване на действия, извършвани от административен орган или длъжностно лице, които не се основават на административен акт или на закона. Искането се предявява писмено пред административния съд по местоизвършване на действията. Искането се разглежда незабавно от съдия.

Съдът задължава административния орган или длъжностното лице, което извършва неоснователните действия, незабавно да предостави данни за основанието на извършените действия.



Съдът може да провери чрез органите на полицията, както и по всички други начини, които не са забранени от закона, извършват ли се действията, от чие име и на какво основание.

За извършената проверка проверяващите органи съставят протокол.

**Произнасяне по искането.** Веднага след приключване на проверката въз основа на данните, събрани от нея, и представените от страните доказателства, съдът се произнася с разпореждане. С разпореждането се нарежда да бъдат прекратени безусловно действията, които не се извършват в изпълнение на представен при проверката административен акт или на закона, или се отхвърля искането. Разпореждането се изпълнява незабавно от органите на полицията.

### ***Б. Защита срещу неоснователни бездействия.***

**Предмет на оспорване.** Неизвършването на фактически действия, които административният орган е длъжен да извърши по силата на закона, подлежи на оспорване в 14-дневен срок от подаването на искане до органа за извършването му.

**Ред за оспорване.** Бездействието на административния орган по задължение, произтичащо пряко от нормативен акт, може да се оспори безсрочно, като се прилагат съответно разпоредбите за оспорване на индивидуалните административни актове.

С решението си съдът осъжда административния орган да извърши действието, като определя срок за това или отхвърля искането.

Специфична форма на контрол на гражданите върху администрацията на сектора за сигурност е предвидената в **конституцията** и в **закона за отговорност на държавата и общините за вреди**.

Държавата (общината) отговаря за вредите, причинени от незаконни актове, действия или бездействия на нейни органи и длъжностни лица при или по повод изпълнение на административна дейност.

За да възникне тази отговорност е необходимо, кумулативното наличие на следните предпоставки, при липсата на която и да е от тях води до невъзможност да се ангажира отговорността на държавата и общините:

- да е причинена вреда;
- вредата да е настъпила в следствие на противозаконен акт, действие или бездействие на административен орган или негово длъжностно лице;
- да съществува причинна връзка между вредата и противозаконния акт;
- вредата да е причинена при или по повод изпълнение дейността на съответния орган или длъжностно лице. Т.е. вредата да е причинена в процеса на изпълнение в пряка и непосредствена връзка с него.

Обезщетение за вреди от незаконни актове на администрацията може да се иска след тяхното отменяне по съответния ред. Гражданинът има право да предяви иск за обезщетение пред съда.

Държавата (общината) дължи обезщетение за всички имуществени и неимуществени вреди, които са пряка и непосредствена последица от увреждането, независимо от това, дали са причинени виновно или не от съответното длъжностно лице.

***Омбудсманът е особена форма на опосредствен контрол на гражданите върху сектора за сигурност.*** Омбудсманът в много страни се нарича народен адвокат, адвокат на гражданите или граждански защитник. Основното предназначение на институцията омбудсман е да създаде нов вид ефективна гаранция за защита правата и свободите на частните лица при тяхното накарняване в една или друга степен от администрацията или други публични власти. В съвременния свят все повече нараства влиянието и сферата на действие на администрацията на всички равнища на държавната власт. Съществуващите механизми не винаги са в състояние да осигурят бърза, навременна и леснодостъпна защита на засегнатите от администрацията лица. това предопределя необходимостта от контролен механизъм, който не дублира функциите на съществуващите контролни институции, а може да действа паралелно с тях, да инициира пряко или косвено тяхната намеса или да действа самостоятелно. [2],[11].

Омбудсманът е личностна институция. Той е едно лице, което отговаря на определени задължителни изисквания,

разполага с доверието на широки обществени кръгове и има качества, които му позволяват да разширява това доверие – висок граждански морал, ангажираност с идеите на хуманизма, демокрацията и справедливостта. В своята дейност омбудсманът е независим и се подчинява само на Конституцията и законите, като се ръководи от личната си съвест и морал. Омбудсманът в държавата се избира от парламента, а местните омбудсмани – от общинските съвети.

Правомощия на омбудсмана:

- Разглежда молби, отправени до него в каквато и да е форма от частни лица – граждани и юридически лица.

- Прави проверки, когато е сезиран с конкретен случай.

- Отправя предложения и препоръки до наблюдаваните администрации или други институции, осъществяващи публична власт или функция, за зачитане на правата и свободите на гражданите; за отстраняване на последиците от накръняване на определени права и свободи, както и на причините, довели до това.

- Може да иска и да получава навременна, пълна и точна информация от наблюдаваните институции.

- Изразява мнения и ги прави публично достояние по случаите, с които е сезиран.

- Посредничи между институциите и засегнатите лица за преодоляване на допуснатите посегателства, опитва се да примирява техните позиции.

- Уведомява органите на прокуратурата, когато в резултат на своите наблюдения и проверки установи, че има данни за извършено престъпление.

Всички граждани могат да се обръщат към омбудсмана с оплаквания и сигнали. При приемането на оплакването или сигнала в рамките на правомощията си, омбудсманът, подпомаган от своята служба, предприема необходимите действия за събиране на информация, включително проверки на документи, пряко наблюдение на дейността на съответната администрация на сектора за сигурност, анкети и други. В случай, че констатира извършването на действия или бездействия, с които се накръняват права и законни интереси на подателя или се възпрепятства тяхното осъществяване, омбудсманът отправя своите препоръки и

предложения до съответните институции. Той уведомява подателите на оплакванията и сигналите за резултатите от взетите мерки.

*С навлизането на новите технологии повечето от извършените киберпрестъпления са базирани на слаби места и уязвимости в компютърните мрежи и системи. Съвременните кибератаки причиняват огромни и непоправими щети и вреди като изтриване на конфиденциални електронни данни и файлове, несанкциониран електронен трансфер на парични средства, следене на цялата кореспонденция в социалните мрежи на потребителите [14].*

**Въз основа на изложеното могат да се направят следните изводи и заключения:**

Контролът на гражданите върху сектора за сигурност е абсолютно необходим елемент на демократичната държава. Той е важна действена форма за тяхното участие в управлението на държавата и по-конкретно в дейността на държавните административни органи. Способите и процедурите, предвидени в контрола на гражданите върху администрацията на сектора за сигурност, са изключително важна гаранция за отстояване на законните интереси на гражданите и за защита на техните права в сферата на административната дейност за реализиране сигурност на държавата.

Посредством предвидените от закона възможности за контрол върху администрацията на сектора за сигурност отделният гражданин е защитен от доминиращия авторитет на държавната администрация, който би могъл да доведе до своеволия, незаконни и неправилни действия, засягащи интересите и правата на гражданина. Като се има предвид, че в модерното развитие на държавата гражданинът се разглежда като потребител на услугите, които държавната администрация е длъжна да му предостави, контролът се явява най-ефективното оръжие на гражданина потребител в отстояването на неговата нова позиция.

Контролът на гражданите има своето ползотворно въздействие и върху администрацията, защото допринася за

усъвършенстването на организацията и дейността на административните органи на сектора за сигурност.

### ЛИТЕРАТУРА:

1. Бакалов, Й., Теоретичен модел на политика за сигурност и граждански контрол на Република България, С., 2011 г.
2. Гандова, Т., Омбудсманът – посредник между местната власт и гражданите.
3. Гарнизов, В., Третият сектор в България: статистика, тенденции, събития. В: „Инициатива за подкрепа на гражданското общество в България”, Асоциация АКЕС, С., 2003 г
4. Гражданският контрол в Република България. Принципи, параметри, практики. Асоциация АКЕС и издателство „Отворено общество”, С., 1999 г.
5. Граждански контрол над полицията, Авторски колектив, С., 1996 г.
6. Диманова Д., "Рискови фактори и заплахи за сигурността в България". Трета международна научна конференция "Наука, образование, иновации", 21 – 23 май 2014 г. Шумен.
7. Досев, Н., „Нормативна база на понятието национална сигурност в Република България” – Сборник. „Научни трудове” на конференция „40 години Шуменски университет 1971-2011”, Шумен 2011 г.
8. Иванов, Х., Гражданското общество и концепции за граждански контрол, С., 2002 г
9. Йончев, Д., Демократичното общество и гражданският контрол върху системата за национална сигурност, С., 1996 г.
10. Йончев Д., Слатински, Н., Трифонов, Т. и др. Демократичното общество и гражданския контрол върху системата на национална сигурност. Сравнителен анализ и културни особености, С., 1997 г.
11. Международни стандарти, основополагащи принципи и добри практики за институцията на омбудсмана. Европейски център по малцинствени въпроси – България и Омбудсман на република България, С., 2005 г., с. 37.
12. Кузманова, Е., Кузманов, З. Административноправен режим на достъпа до обществена информация. Сборник научни трудове от Научна конференция 2015 „Новите предизвикателства пред системите за информационна сигурност“, НБУ „В. Левски”, факултет „Артилерия, ПВО и КИС”, Ш., 2015, ISBN 978-954-9681-65-9.
13. Фотев, Г., Гражданското общество, С., 2002 г.
14. Boyanov P. K., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, Vol.3, 2013, pp. 114-124.

# Обществен контрол над сектора за сигурност

Христо А. Христов

## Public control under security sector

Hristo A. Hristov

**ABSTRACT:** *The importance of public control of the security sector of society is expressed especially in its ability to capture the inconsistencies of the acts and actions of the institutions of the security sector with the interests of the society and citizens and to express these interests by the fastest way and not always formal which define the actuality of the issues studied in this report.*

**KEYWORDS:** *Sector of security, formal and informal public control, NGOs-non-governmental organizations, political parties, trade unions, collective contract, arbitration.*

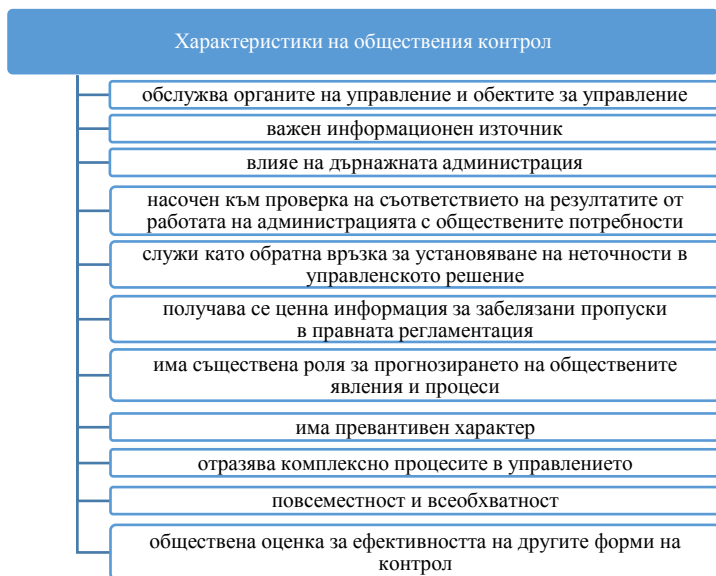
Основна задача на обществения контрол е да съдейства в позитивния процес на държавното управление – да създава обстановка, която да не позволява или да предотвратява настъпването на отрицателни явления (вреди) и на причините за тях.

**Основните характеристики на обществения контрол са изложени на фигура 1.**

Общественият контрол обслужва пълноценно двете страни в процеса на функциониране на различните сектори на държавата – органите на управление и обектите за управление (гражданите и техните организации).

Общественият контрол е важен информационен източник с особена ценност за управлението. Органът на управление (централен или местен, държавен или обществен) не може да функционира, ако не разполага със съответната информация за обекта на управление. Невинаги формално установените начини за доставяне на информация са достатъчни. Те се допълват с информацията от обществения контрол, който е в състояние да фиксира степента и качеството на изпълнението на управленските

решения, изхождайки от конкретните жизнени факти. Той не е ограничен само от преценка за законосъобразност или целесъобразност. [3],[7].



**Фиг. 1.** Характеристики на обществения контрол

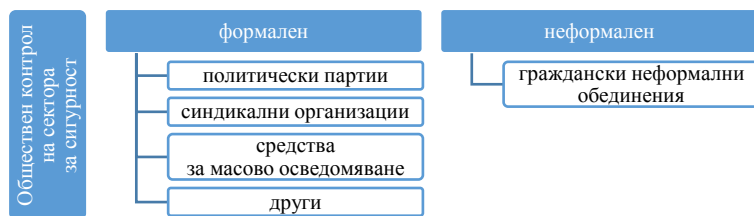
Безспорно е влиянието на обществения контрол върху държавната администрация при активното търсене на проблеми и откриването на нуждите и потребностите, чието неудовлетворяване може да породи противоречия или напрежение в обществото. Информацията, съдържаща се в обществения контрол, създава своеобразен филтър на органа на държавно управление за наблюдение, изучаване и обяснение на фактите. Тя изостря чувствителността на органа към ситуацията. Колкото по-голяма ценност има проблемът за обществения контрол, т.е. колкото е по-важен за обществеността или за обществената организация, която го осъществява, толкова по-настойчиво общественият контрол ще сигнализира органа на управление и

толкова по-бързо последният ще забележи възникналата проблемна ситуация, налагаща вземането на решение. [10]

Общественият контрол е насочен и към проверка на съответствието на резултатите от работата на администрацията с обществените потребности и интереси. С формите и средствата на обществения контрол се въздейства за непрекъснатото изучаване на обществените потребности и очаквания и за създаване на условия за правилното им насочване и удовлетворяване.[1],[8].

Общественият контрол може да предаде сведения и обществена оценка за резултатите и ефективността на другите форми на контрол, например за прокурорската намеса при регистрирани случаи на корупция в администрацията, за ефективността на съдебните органи при решаване на административни дела и др.

Общественият контрол над дейността на сектора за сигурност може да бъде *формален* и *неформален* (виж фигура 2).[5],[6].



**Фиг. 2.** Видове обществен контрол над дейността на сектора за сигурност

Неформален (нерегламентиран) обществен контрол се осъществява от граждански обединения въз основа на групи по интереси. Основава се на общите правила за поведение в обществото.

В гражданското общество *неформалните обединения от хора*, или неформалните групи, са не само допустими и тяхното съществуване се смята за естествено, но без тях то е немислимо. Те се образуват и съществуват без предварително договаряне, но



при споделяне на общоприети за членовете на отделната група рационални правила на взаимоотношения, действия и взаимодействия.

Неформалните групи обикновено са сдружения на граждани, свързани на основата на близки интереси и взаимна симпатия. Въсъщност това може да бъде допадане по характер, споделяни ценности или сходен начин на мислене по определени въпроси. Неформални групи с краткотрайно съществуване възникват навсякъде в гражданското общество и при най-различни поводи. Общественият контрол, който те осъществяват над дейността на сектора за сигурност е на емоционално равнище, при което се откриват, предотвратяват и отстраняват определени нежелани отклонения.

Формален (регламентиран) обществен контрол се осъществява чрез политическите партии, синдикалните организации, неправителствените организации, средствата за масово осведомяване и други обединения.

*Формалните групи участват в нормативното уреждане на всички основни групи обществени отношения.* Общественият контрол, който те осъществяват над дейността на сектора за сигурност, дава възможност за оказване на въздействие върху противичащите в тези специализирани структури процеси.

#### **Контрол от политическите партии или движения.**

**Партия** – свободно сдружение на граждани, създадено с цел да съдействат за формиране и изразяване на политическата воля на народа чрез избори или по друг демократичен начин. [2],[8].

За образуване на политическа партия или движение е необходимо да се спазват предписанията в нормативните актове, определящи тяхното действие. Регламентирано е, че те, както и други граждански образувания, имат свой устав.

**Партиите имат важен принос във функционирането на демокрацията в три направления:**

**Първо**, те улесняват и спомагат за ефикасния обществен контрол върху властимащите и по този начин влияят върху решенията на правителството и другите политически сили.

**Второ**, те помагат на съвкупността от гласоподавателите да направят по-рационален и ефективен политически избор.

**Трето,** те спомагат за мирното регулиране на политическите конфликти в обществото с помощта на легални демократични средства.

В съвременната епоха политическите партии са едни от най-активните субекти, упражняващи обществен контрол над дейността на сектора за сигурност.

Контрол над дейността на сектора за сигурност могат да упражняват както управляващите партии, така и партиите в опозиция.

**Направления за осъществяване на контрол и въздействие от партиите върху сектора за сигурност:**

**А.** Изработване (актуализиране) на елементи от нормативната база на сектора за сигурност.

**Б.** Парламентарен контрол на сектора за сигурност (за партиите в парламента).

**В.** Контрол на типичния бюджетен цикъл с цел реализиране на ново качество:

- подготовка на бюджета – чрез различни формални и неформални процедури;

- одобрение на бюджета – чрез проучване и определяне на обществен интерес и подходящото за целта разпределение на средствата;

- разходване (изпълнение); увеличаване прозрачността и отчетността; съблюдаване и детайлно проучване както на потребностите, така и на необходимите средства за тяхното задоволяване, за да се предотвратят ненужни преразходи на финансови средства;

- финансов преглед и отчетност – дали има неправилно изразходване на средства от правителството и от структурите на сектора за сигурност; периодична оценка на целия бюджет и самия механизъм на одитния процес с цел постигане на отчетност, точност и ефективност.

**Г.** Предлагање на стратегия за реформа на сектора за сигурност. Формиране на направления за трансформация на структурите и способностите в сектора за сигурност.

**Д.** Контрол на специфичните политики, използвани в сектора за сигурност и на текущите решения.

**Е.** Осигуряване на информация, гласност и адекватни послания относно резултатите, постигнати при функционирането на сектора за сигурност.

**Ж.** Участие със специалисти в прогнозирането на средата и факторите, които могат да въздействат върху държавата, обществото и гражданите.

**З.** Мониторинг и принос в изграждането на интегрирани модели за адекватно реагиране при различни опасности и заплахи.

**И.** Наблюдаване за законосъобразност и спазването на правата на гражданите при различни операции на структурите от сектора за сигурност.

**К.** Реализиране на обществен контрол чрез структуриране и предаване на сигнали и предложения на гражданите относно лошо управление, корупция, злоупотреби и др. в сектора за сигурност.

**Л.** Инициране и провеждане на различни форуми, на които да се дискутират ключови проблеми на сектора за сигурност.

#### **Контрол от неправителствените организации.**

**Неправителствена организация (НПО)** е всяка частна, независима от държавното управление организация, която развива някакъв вид обществена дейност без стопанска цел и се финансира от източници, несвързани с правителството.[5].

Неправителствените организации са основен партньор на държавните институции при формирането, изпълнението и контрола на отделните политики и изразходването на заделените в рамките на същите политики публични ресурси.

Активните неправителствени организации с интерес в сектора за сигурност са: Център за изследване на демокрацията, Атлантически клуб, Сдружение „Джордж Маршал” – България, Център за югоизточноевропейски изследвания, Фондация „Демокрация и сигурност”, Институт за изследване на сигурността и международните отношения, Сдружение „Българска отбранителна индустрия”, Център за либерални стратегии, Институт за регионални и международни изследвания, Европейски институт, Съюз на офицерите от резерва „Атлантик” и др.

Сред неправителствените организации се откроява и групата на сдруженията на бивши военнослужещи, в т.ч. военни,

разузнавачи и полицаи. В нея влизат Съюз на възпитаниците на военните на Негово величество училища, Съюз на офицерите и сержантите от запаса и резерва, Асоциация на разузнавачите, „НАС” – Асоциация на контраразузнавачите и др.

Ролята на университетите и изследователските организации в сектора за сигурност се изразява най-вече в притежаването от тяхна страна на експертен потенциал, който да е в състояние да предлага алтернативи на решения на най-разнообразни по характер и сложност проблеми. Включени в процеса на изготвяне на дадено решение, засягащо националната сигурност, представителите на научната общност допринасят за повишаване на ефективността на управлението на сектора в условията на непрекъсната конкуренция за оскъдни ресурси с останалите публични сфери.

В страната съществуват и няколко образователни и научни звена, които от години се ангажират с изследването на проблеми на сектора за сигурност и подготовката на специалисти в тази област. Това са **УНСС** – катедра „Национална и регионална сигурност”, Центърът за стратегически изследвания в отбраната и сигурността, катедра „Международни отношения” и др; **НБУ** – Центърът за изследване на рисковете и сигурността; **СУ** „Св. Климент Охридски” – катедра „Политология”, катедра „Международно право и международни отношения” и др.; **ШУ** „Еп. К. Преславски” – катедра „Управление на системите за сигурност”; **ВСУ** „Черноризец Храбър”.

Важна роля на НПО е да осигурят по-ефективна чуждестранна експертиза и финансиране за осъществяване на научните и образователните проекти в областта на националната сигурност. Благодарение на гъвкавостта си и на липсата на бюрократични процедури за координиране и взимане на решения НПО установяват по-лесно международни контакти и сътрудничество в сравнение с държавни институции от същия ранг, бюджет и състав.

**Дейностите, осъществявани от НПО спрямо сектора за сигурност, включват [3],[6],[7]:**

- Мониторинг на сектора за сигурност и укрепване на респекта към законността и човешките права.

- Провеждане на „стратегически” преглед на законовата уредба на сектора за сигурност и участие в актуализирането на нормативните документи.

- Предоставяне на алтернативна експертна гледна точка върху правителствената политика за сигурност. Принос към обществения дебат и формулиране на алтернативи на политиката.

- Разпространение на независими анализи и информация относно сектора за сигурност към парламента, медиите и обществото.

- Предоставяне на обратна връзка за решения в сектора за сигурност и изготвяне на независими предложения за решения под формата на доклади и други документи.

- Сътрудничество при подготовката и реализирането на съвместни проекти, планове и програми в областта на превенцията на различни опасности за държавата, обществото и гражданите.

- Утвърждаване на стандарти на прозрачност и отчетност в управлението на ресурсите за сектора за сигурност с ясни и контролируеми процедури за вземане на ресурсни решения, с редовни отчети и одит на ефективността.

- Обучение на политици, журналисти, млади изследователи и други с цел създаване на компетентност и повишаване на капацитета за решаване на проблемите на доброто управление на сектора за сигурност.

- Участие с експерти в дискусии по съществени въпроси, засягащи сектора за сигурност.

**Контрол от профсъюзите в системата на МО и МВР. [3]**

**Професионален съюз** – дълготрайно сдружение на наемни работници с цел запазване и подобряване условията на техния трудов живот.

### **Функции на професионалните съюзи:**

- **Колективно трудово договаряне.** По определение на Международната организация по труда това са „всички преговори, които се водят между работодател, група от работодатели или една или повече организации на работодатели, от една страна, една или повече организации на трудещите се, от друга страна, за

определяне на условията на труд, на заетост и/или за уреждане на отношенията между тях”.

- **Защита на работните места.** Тази функция има изключително значение по време на структурни промени в икономиката, при технологическо и техническо обновяване на производството и опасността от съкращаване на работни места. За организациите на квалифицираните работници тя е една от най-важните и профсъюзите се стремят да защитят техните работни места като регулират преквалификацията и ограниченията за заемане на определени работни места, включително чрез изискванията за съвместно разработване на длъжностните характеристики.

- **Сътрудничество с работодателя.** В много от професионалните съюзи и по много от техните функции се постига сътрудничество с работодателя. Според някои, това означава компрометиране на синдиката като движеща сила, докато други гледат на него по-прагматично, като подкрепят сътрудничеството с работодателя и смятат, че то допринася за по-ефективно постигане на неговите цели.

- **Политическа активност.** Тази функция на профсъюзите е свързана с тяхната дейност като групи за социален натиск и има дълга история. Основното предназначение на функцията е възможността за законодателна инициатива и за участие в законотворчеството на държавата.

- **Социално осигуряване и социални грижи.** Исторически функцията е възникнала първа и е свързана със системата за социалното осигуряване. На съвременния етап социалното осигуряване е под държавен контрол, а социалното подпомагане се финансира от бюджета и в тяхното управление някои от професионалните съюзи са запазили своето участие. Тази функция намира проявление и в изплащане от синдикатите на помощи при продължително боледуване, безработица, пенсиониране, стачки и др.

- **Организиране на услуги.** Тук се включват различни видове услуги, които професионалните съюзи създават за своите членове като клубове, спортни условия и други за пълноценно и рационално използване на свободното време.

### **Социален диалог и контрол.**

**Социален диалог**-процес на обмяна на информация между работодателя (държавата) и синдикалните организации по теми, свързани с функционирането на структурите от сектора за сигурност. [3]

В този смисъл форми на социален диалог са: колективното трудово договаряне, консултациите, преговорите, арбитражът; сътрудничеството чрез различни процедури и др.

### **Практики за социален диалог в сектор „Сигурност“.**

Безспорно е, че една практика може да се определи като добра, когато тя е ефективна, т.е. осигурява постигането на целения резултат с минимални усилия и ресурси. Диалогът обаче е противопоставяне на позиции с цел постигане на съгласие между участниците по въпрос от общ интерес. Това означава, че ефективността на една практика в областта на социалния диалог не се определя на първо място от изразходвания ресурс, а от възможността на всяка страна да изрази и защити позицията си.

### **Колективен трудов договор (КТД).**

В сектор „Сигурност“ в широк смисъл КТД съществува за служителите на Министерство на отбраната (МО), където функционира Отраслов съвет за социално сътрудничество. Такива има със служителите на МВР и ДАНС, които работят по трудово правоотношение. Що се касае до държавните служители в полицията, се прилагат правилата на Закона за държавния служител (ЗДСл) и Закона за МВР (ЗМВР), които определят трудовото им правоотношение като служебно. Това означава, че правомощията на държавните служители се определят със законови норми и не подлежат на преговаряне.

### **Арбитраж.**

Най-общо арбитражът може да се определи като извънсъдебен способ за уреждане на колективен трудов спор от арбитражен орган (едноличен арбитър или арбитражна комисия) с участието на страните. Основанията за сезиране на арбитър са две. Първо, когато страните не са постигнали съгласие за уреждане на колективния трудов спор чрез преговори и взаимно поискат въпроса да се разгледа от арбитър. В този случай, с оглед начина

на сезиране, е налице доброволен арбитраж. Второ, когато страните не постигнат съгласие относно минималните дейности по време на стачка. В този случай е достатъчно сезиране само от една от страните. Производството при задължителния арбитраж приключва с арбитражно решение, което определя минималните дейности или с писмено споразумение, утвърдено от арбитра.

Във връзка с това в страната функционира Национален институт за помирение и арбитраж (НИПА), който е приел правила за осъществяване на посредничество и арбитраж за уреждане на колективни трудови спорове. На него могат да се възложат и споровете в сектор „Сигурност“, но само при условие, че се осигурят арбитражи с компетентност в областта на сигурността.

Предмет на арбитража ще бъдат колективните трудови спорове (относно трудови правоотношения или осигурителни отношения) на работниците и служителите от сектор „Сигурност“ и държавата, които се представляват съответно от техните професионални организации и упълномощено от министъра лице. Така ще се ползва съществуващото производство и утвърдената практика на Националния институт за помирение и арбитраж по него, а от друга страна ще се гарантира възможността независим орган да решава спорните въпроси в сектора.

### **Право на стачка.**

Забраната за стачка на служителите от сектор „Сигурност“ не е конституционно установена. Това е направено с чл. 16, т. 4 от ЗУКТС, който гласи, че „не се допуска стачка в системата на Министерството на отбраната, Министерството на вътрешните работи, съдебните, прокурорските и следствените органи“. Следва да се отбележи, че тази забрана обхваща не само държавните служители в тези структури, но и лицата работещи по трудово правоотношение. Ако по отношение на държавните служители това ограничение за право на стачка може да се обясни с принципа на статута и принципа на непрекъсваемост, то обяснението за лицата, работещи по трудово правоотношение трябва да се търси на друга плоскост.

Може да се предположи, че във втория случай водещият мотив е свързан с прерогативите на публичната власт в сектор „Сигурност“ и „Правосъдие“. Следва да се има предвид, че



служителите в сектор „Сигурност” са длъжни да гарантират суверенитета, сигурността и независимостта на страната и да защитават нейната териториална цялост. От това конституционно предназначение на системата за сигурност може да се изведе опасността за обществото при преустановяването на цялата или част от дейността му, включително и чрез стачка на работещите в него по трудово правоотношение. Дейността в разглеждания сектор е свързана изключително със защита на националната сигурност, охраната на държавната граница, опазването на обществения ред, живота и здравето на гражданите и борбата с престъпността. Касае се за съществена, особено важна дейност, преустановяването чрез стачка на която би довело до застрашаване на сигурността, живота и здравето на гражданите.

Това разбиране е залегнало и в Международният пакт за икономически, социални и културни права (ДВ, бр. 43 от 1976 г.), който задължава държавите – страни по него, да осигурят правото на стачка на работниците и служителите. Допускат се законови ограничения при упражняването на правото на стачка във въоръжените сили, полицията и държавната администрация (чл. 8, ал. 2). Основанието за това е свързано с възможността за създаване на „опасност за живота, сигурността и здравето на хората”. Това, обаче не следва да се тълкува като забрана на правото на стачка на посочените групи лица.

**Обществени корективи на сектора за сигурност от средствата за масово осведомяване.** Потенциално най-важният компонент за формиране на масово обществено мнение и адекватна политическа нагласа по отношение на националната сигурност (сектора за сигурност) са средствата за масово осведомяване (СМО) – телевизия, печат и радио. Масовата комуникационна среда хипотетично може да играе централна роля както при подготовката на стратегически политически решения, така и към „делничните” проблеми от сферата на сектора за сигурност (организационни структури, равнище на бюджети, операции, разходване на ресурси, кадрови въпроси, правата на военнослужещите и др.).[7]

**Основни направления за контрол и въздействие на сектора за сигурност:**

А. Събиране и разпространяване на информация по проблемите на сигурността с международен и вътрешнополитически характер, която е в обществен интерес.

Б. Осигуряване на новини по стандартите за истина, точност, справедливост и безпристрастност.

В. Реализиране на прессъобщения по всички основни дебати, питания, решения, закони и др. в парламента по въпросите на сектора за сигурност.

Г. Публикации, свързани с парламентарни анкети по въпросите на сигурността.

Д. Осигуряване на трибуна за обществения дебат по най-важните за обществото въпроси на сигурността.

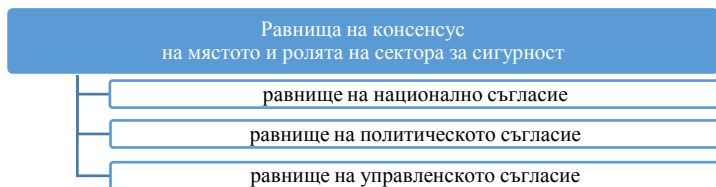
Е. Реализиране на обществени корективи по отношение на законосъобразността на действията на правителството и на сектора за сигурност.

Ж. Съдействие за развитие на гражданската страна на контрола, по-специално на неправителствените организации и сдружения на гражданите; съдействие за участието им при формиране и представяне на обществената поръчка по отношение на извършваните реформи в сектора за сигурност.

З. Формиране на обществено мнение и настроение, създаване на нагласа за обществена подкрепа (несъгласие) по отношение на националната сигурност (сектора за сигурност).

Синтезът на потенциални възможности на СМО и функционирането на „правата” и „обратната” връзка чрез свободните медии и другите елементи на гражданското общество създава **общественото мнение** по отношение на националната сигурност (сектора за сигурност). Общественото мнение от своя страна е основа на формиращото се **съгласие (консенсус) по отношение на мястото и ролята на сектора за сигурност в демократичното общество**. [5],[6].

Можем да определим три равнища на консенсус по отношение на мястото и ролята на сектора за сигурност (виж фигура 3):



**Фиг. 3.** Равнища на консенсус по отношение на мястото и ролята на сектора за сигурност

*Равнище на национално съгласие.* То обхваща постигането на съгласие за съдържанието на жизненоважните и перспективните интереси на нацията; за геостратегията и външната политика; за международните и вътрешните операции на формациите за сигурност; за системата на националната сигурност; за ключовите направления за устойчивото развитие на държавата.

*Равнище на политическото съгласие.* То обхваща направленията: място и роля на сектора за сигурност, брой и вид на специализираните структури и тяхното подчинение, нормативна уредба, бюджетни разходи и контрол, разбиране за отговорност и субординация при политическото и оперативното им ръководство и други. Това равнище очертава реалните подходи при решаването на конкретните проблеми на сектора за сигурност.

*Равнище на управленското съгласие.* На него се разполага цялата пирамида от организационно-щатни и функционално-процедурни системи и техните подразделения, чрез които секторът за сигурност се управлява от разделените власти в демократичното общество. Това е най-видимата и поради това най-уязвимата и често атакувана част от проблема. Корените на спиралата от противоречия обикновено са следствие на един обективен факт – пирамидата, наследена от предишното общество като структура, субординация, статут, кадри, традиция, манталитет и пр., не може да бъде разрушена и създадена отново. Тя трябва да бъде трансформирана стъпка по стъпка, за да не се срине общото равнище на националната сигурност. [9]

С навлизането на новите технологии повечето от извършените киберпрестъпления са базирани на слаби места и уязвимости в компютърните мрежи и системи. Съвременните кибератаки причиняват огромни и непоправими щети и вреди като изтриване на конфиденциални електронни данни и файлове, несанкциониран електронен трансфер на парични средства, следене на цялата кореспонденция в социалните мрежи на потребителите [11].

**Въз основа на изложеното могат да се направят следните изводи и заключения:**

За да изпълнява функциите си, общественият контрол над сектора за сигурност трябва да отразява комплексно процесите в управлението. Това означава контролната информация да отразява и постигнатите успехи, и положителните резултати в дейността на администрацията на всички нива. Тя трябва да дава възможност на гражданите да видят дейността на институциите от сектора за сигурност като процеси, отговарящи или неотговарящи на изискванията и очакванията на обществото.

Широката социална база на обществения контрол над сектора за сигурност създава условия за неговата повсеместност и всеобхватност. Като контрол, който отразява единството на интересите на гражданите, колектива и обществото, той е контрол за законосъобразност, за целесъобразност, за съществуващи и предстоящи нужди, за обществени очаквания и степен на удовлетвореност от функционирането на публичната администрация.

В заключение може да се определи, че общественият контрол обхваща социалната ефективност на институциите от сектора за сигурност, като изхожда от интересите на обществото, колектива, личността и тяхното оптимално съчетаване при определящия приоритет на обществените интереси.

#### **ЛИТЕРАТУРА:**

1. Арбатов, Ал., Парламентарен контрол над сектора за сигурност, С., 2003 г.
2. Бакалов, Й., Теоретичен модел на политика за сигурност и граждански контрол на Република България, С., 2011 г.
3. Граждански контрол над полицията, Авторски колектив, С., 1996 г.
4. Динев, М., Контрол в социалното управление, Изд. „Тракия М“, С., 1999 г.
5. Иванов, Х., Контрол над специализираните служби за сигурност, С., 2007 г.

6. Йончев Д., Слатински, Н., Трифонов, Т. и др. Демократичното общество и гражданския контрол върху системата на национална сигурност. Сравнителен анализ и културни особености, С., 1997 г.
7. Фотев, Г., Гражданското общество, С., 2002 г.
8. Доклад за състоянието на парламентарния контрол в 41-вото Народно събрание (2009 – 2011 г.г.), С., август 2011 г.
9. Dimanova D., " Analysis of risk factors for the occurrence of natural disasters", Association Scientific and Applied Research, International Journal, лицензиран в EBSCO, USA, Vol. 7, 2015, ISSN 1314-6289 (Анализ на рисковите фактори и заплахи за възникване на природни бедствия ).
10. Кузманова, Е., Кузманов, З. Административноправен режим на достъпа до обществена информация. Сборник научни трудове от Научна конференция 2015 „Новите предизвикателства пред системите за информационна сигурност“, НВУ „В. Левски“, факултет „Артилерия, ПВО и КИС“, Ш., 2015, ISBN 978-954-9681-65-9.
11. Boyanov P. K., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, Vol.3, 2013, pp. 114-124.

# ДЪЛГИЯТ ПЪТ НА ТУРЦИЯ КЪМ ЕВРОПА

Добромир Ж. Добрев

## Turkey's long way to Europe

Dobromir Zh. Dobrev

**ABSTRACT:** *The relations between the Republic of Turkey and the European Union are studied as well as the problems that are to be overcome in view of the country's successful accession to the structures of united Europe*

**KEYWORDS:** *Republic of Turkey, EU, history, long way, Erdogan, human rights.*

Турция се явява важен партньор на САЩ и ЕС в изграждането на глобалната система за сигурност. Като член на НАТО и кандидат за член на ЕС Турция е страна с която Западът има много близки и в същото време противоречиви отношения.

Когато Атаюрк налага модерната светска държава в Турция, Западът се оказва неин естествен съюзник. В исторически план трябва да припомним, че страната е член на НАТО от далечната 1952 г., а още по-рано през 1949 г. става член на Съвета на Европа. През 1959 г. Турция официално заявява желание да се присъедини към създадената година по-рано Европейската икономическа общност (ЕИО). В това си начинание тя получава подкрепа от САЩ.

Първоначалната динамика на отношенията с Обединена Европа не предвещава трудностите и дългият път който предстои на Турция в нейната европейска интеграция. През 1963 г. е сключено споразумение за асоцииране между ЕИО и Република Турция. Основната му цел е да доведе до създаването на митнически съюз и последващо пълноправно членство на Турция.

Тези намерения са възпрепятствани от турската интервенция в Кипър през 1974 г., а също и от военният преврат в самата Турция

през 1980 г. Двете събития се отразяват крайно неблагоприятно в отношенията с Европа и замразяват интеграционните процеси.

Възстановяването на демократичните практики в Турция затопля отношенията с ЕС и през 1987 г. тогавашният министър-председател Тургут Йозал отново поставя въпроса за пълноправното членство на страната му в Евросъюза. До преговори за присъединяване в този случай не се стига, като причините за това могат да се търсят в различни посоки.

В Европа съществуват достатъчно влиятелни лобита, които смятат, че Турция както географски така и културно не се вписва в европейския модел. Допълнителен фактор са религиозните различия.

Ако към това прибавим проблема с неспазването на човешките права в Турция, ще видим, че има солидни пречки пред нейното европейско членство.

Разпадането на тоталитарните режими в Източна Европа, допълнително забави интеграцията на Турция. Приобщаването на бившите социалистически страни се превърна в приоритет за ЕС.

„Много от страните от Централна и Източна Европа са в лоша икономическа ситуация, но са смятани политически и културно за неразделна част от Европа. Срещата на върха в Копенхаген през 1993 г. отбелязва важен вододел в отношенията между ЕС и Турция. Първо, присъединяването на страните от Централна и Източна Европа (без Турция) е приоритет за ЕС, второ Съюзът въвежда икономически и политически показатели за членство, които стават известни като критериите от Копенхаген“ [Спасов, 2012: 264].

Само ще припомним, че един от тези критерии настоява за стабилност на институциите, гарантиращи демокрацията, върховенството на закона, човешките права и закрилата на малцинствата. Все неща за които Анкара търпи критика от своите атлантически партньори. Договорът от Амстердам приет през 1997 прави копенхагенските критерии задължителни.

Като важен и много положителен факт в двустранните отношения може да се посочи създаденият между ЕС и Турция митнически съюз през 1995 г. Той води до значително нарастване на обема на търговията между тях. Не случайно в следващите

години Турция се превърна в седмия по големина търговски партньор на Съюза.

Така се стига до 1999 г. когато на Европейския съвет в Хелзинки, Турция официално е призната за страна кандидатка за членство, а няколко години по-късно през 2004 г. е решено да започват и самите преговори. Реално те са стартирани през 2006 г. и това е резултат от усилията който полага Турция да покрие критериите от Копенхаген.

Самите преговори са забавени от неизпълнението от турска страна на протокола от Анкара подписан през юли 2005 г. Той предвижда Турция в съответствие с действащия митнически съюз да отвори своите пристанища и летища за присъединилите се през 2004 г. страни в ЕС, включително и Република Кипър.

По този начин бъдещето на разделения остров е източник на проблеми за турската интеграция. Кипър настоява за официално признаване и за достъп до турските пристанища и летища. Използвайки членството си в Евросъюза, страната последователно блокира турското участие в Общата политика за сигурност и отбрана.

Като резултат само една преговорна глава „Наука и изследвания“ е затворена. Дванайсет други са отворени, като осем от тях са блокирани заради неизпълнението на споменатия протокол.

Турция от своя страна настоява, че кипърският проблем не трябва да бъде пречка за нейното членство в ЕС, както този проблем не е попречил Република Кипър да стане член на Съюза.

Друг сериозен проблем пред европейското бъдеще на Турция е недостатъчните гаранции за правата на малцинствата и конкретно за правата на кюрдите. Бавното решение на този проблем радикализира кюрдите и засилва въоръжената им съпротива срещу Анкара.

Доклада на Европейската комисия за напредъка от 14. октомври 2009 г. отчита положителен напредък по отношение правата на кюрдите.

Комисията оценява положително откриването на дебат за културните, политическите и икономическите аспекти на правата на кюрдите, но посочва, че са необходими конкретни мерки, които



да преодолеят твърде широката интерпретация на антитерористичното законодателство, ограничаващо фундаментални човешки права [Медийно досие: Отношенията на ЕС с Турция. [http://www.dnevnik.bg/evropa/razshiriavane/2010/06/07/913299\\_mediino\\_dosie\\_otnosheniata\\_na\\_es\\_s\\_turciia/](http://www.dnevnik.bg/evropa/razshiriavane/2010/06/07/913299_mediino_dosie_otnosheniata_na_es_s_turciia/)].

Кюрдският проблем си остава от първостепенно значение за Турция. Само ще напомня, че в Истанбул живеят около два милиона кюрди, което го прави най-големият „кюрдски град“ в света.

Друг проблем в отношенията с Евросъюза, е начина по-който турската държава се разправи с антиправителствените протести от 2013 г. Започнали като екологични действия срещу застрояването на парка Гези в Истанбул, те прераснаха в мащабни протести срещу про-ислямиската политика на Реджеп Тайип Ердоган и негово правителство. В продължение на няколко седмици протестите обхванаха редица турски градове и в тях се включиха над два милиона души.

Бруталният начин по-който бяха потушени протестите доведеха до смъртта на шестима, а хиляди бяха ранени.

Европейската реакция беше изразена най-ясно от Германия, която замрази преговорите за турското еврочленство.

Още от края на 80-те години в Турция започва процес на ислямизация. В една своя реч през 1990 г. Тансу Чилер, първата и единствена жена министър-председател на Турция, заяви, че Европа също носи определена вина за този процес. Липсата на интерес от страна на Брюксел към процесите в страната, прекаленият европоцентризъм и намалените квоти за турски студенти и докторанти в европейски университети дават предимство на ислямистите.

Фактът, че броят на турските студенти учещи в местни университети се увеличава за сметка на обучението в Европа се отразява крайно негативно за техният европейски избор. Като резултат от това броят на евроскептиците в администрацията и силовите структури се увеличава.

Прогнозата на Чилер, че ако този процес продължи, ислямистите ще вземат властта се сбъдна след 12 години, когато

начело на страната застава Ердоган [Ср. Чуков, Б. Ердоган срещу Ататюрк. <http://a-specto.bg/erdogan-sreshtu-atatyurk/>].

Управлението на Ердоган засили още повече страховете от ислямизация на Турция. Трябва да отбележим, обаче, че съществува и друга силна фигура проповядваща ислямската перспектива на страната. Това е религиозния проповедник и крупен бизнесмен Фетхулла Гюлен.

„Американският историк и експерт по-близкоизточните процеси Майкъл Рубин сравнява Гюлен и неговото движение с иранския аятолах Хомейни, който в периода между 1975-1978 г. успява с поредица от интервюта и възхваляващи го статии във водещи медии да убеди Запада и най-вече управляващите в САЩ, че няма никакъв интерес към властта, нито към налагане на религиозна власт. Казва им това, което искат да чуят. Това е причината американският президент да посрещне новата 1979 г. в Техеран с персийския шах само месец преди да се случи т.нар. ислямска революция. Според Рубин в случаят с Гюлен на повърхността стои един благочестив образ, но в действителност проникването на членовете на „Службата“ на всички нива на турската държава, както и заблуждаването на чужденци, вече са в огромни размери“ [Джасим, Е. Паралелната турска държава. - L'ÉUROPEO № 45, 2015, с.36-38].

Без съмнение Ердоган и неговата Партия на справедливостта и развитието, виждат в лицето на Гюлен конкурент и заплаха за статуквото. Доказателство за това са арестите на много магистрати, военни, висши полицаи и политици с обвинението, че рушат устоите на светската държава. Подобни обвинения от страна на хора като Ердоган и неговите последователи който систематично се стремят да ислямизират страната, звучат достатъчно странно.

Трябва да отбележим, че политиката на Ердоган и влиянието на Гюлен, имат немалко опоненти в самата Турция. Признат лидер на опозицията е водача на Републиканската народна партия, Кемал Калъчдароглу който защитава светските основи на държавата и наследството на Ататюрк.

Като интересно явление в турският политически живот може да се определи възходът на младият харизматичен лидер на

Демократическата партия на народите (ДПН), Селяхаттин Демирташ. Неговата основна заслуга, е че разшири подкрепата за партията която в миналото се свързваше единствено с кюрдското малцинство.

Той успя да я превърне в модерна партия, търсеща подкрепа от всички онеправдани малцинства в страната, включително и жените.

Резултатите от парламентарните избори в Турция през лятото на 2015 г. доказаха възхода на ДПН, която премина десет процентната бариера и вкара 80 депутати в парламента.

Този успех на „турският Обама“, както го наричат привържениците му провали планове на Ердоган за промяна на конституцията [Ср. Кюрдският лидер Селяхаттин Демирташ – новата звезда на турската политика. [http://www.dnevnik.bg/sviat/2015/06/09/2549619\\_kjurdskiat\\_lider\\_seliahattin\\_demirtash\\_-\\_novata/](http://www.dnevnik.bg/sviat/2015/06/09/2549619_kjurdskiat_lider_seliahattin_demirtash_-_novata/)].

Навлизането на модерни лица като Демирташ в турската политика, дава доза оптимизъм за решаването на кюрдският въпрос, а също и за светското бъдеще на страната.

Следващите години ще покажат доколко успешно Турция ще се противопостави на ислямските тенденции и ще защити европейското си бъдеще.

Освен Германия другата голяма европейска държава която е скептична към скорошното присъединяване на Турция в Евросъюза е Франция. В този случай проблемите са резултат от категоричната френска позиция относно арменският геноцид от 1915 и 1916 г. и вината на турската държава. Нещо повече, Франция в своето законодателство е инкриминирала отричането на геноцидите през XX век, включително и арменският.

Това е сериозно основание за преосмисляне на тези исторически събития от турската държава и коригиране на нейната официална позиция.

В този аспект може да се разгледат и двустранните отношения между Турция и Армения.

Положителни за турската външна политика са стъпките за нормализиране на отношенията с Армения. Пример за това са

подписаните в края на 2009 г. споразумения между двете страни за отваряне на границата помежду им. Разбира се темата за признаването на арменския геноцид от Турция остава открита в двустранните отношения.

САЩ са страната която винаги е подкрепяла Турция в нейната амбиция за членство в Евросъюза. В този смисъл не е случайно, че именно Бжежински теоретично обосновава европейското бъдеще на Турция. Той изхожда от всеобхватните реформи на Кемал Ататюрк. Империята която през XIX в. е определяна като „болният човек на Европа“ успява успешно да се трансформира и да приеме навият си постимперски статус.

„Всеобхватните реформи на Ататюрк, наложени внезапно на Турция през 1924 г. (три години след обявяването ѝ за постимперска държава), предизвикват радикални и забележително успешни промени. Страната скъсва със своята арабско-ислямска връзка, изведнъж (буквално за една нощ) приема западната азбука на мястото на арабското писмо, отстранява религиозните елементи от държавните си институции и дори и дори променя дрескода на своя народ. През следващите десетилетия тя неотклонно и решително институционализира набиращ инерция демократичен процес в рамките на ясно дефинирана светска държава“ [Бжежински, 2012 :188].

Чрез многократни сравнения с Русия, американският политолог твърди, че през XX в. Турция се е претърпяла по-успешна социална модернизация и цялостна трансформация на държавата от бившият флагман на комунизма [Ср. Цит.съч., с.186-189].

Джордж Фридман също споделя тезата за европейското бъдеще на Турция.

„За мнозина Турция не е европейска държава, а само западния издатък на Азия. Но това е голяма грешка. Без да броим геологията – тя се намира на европейската тектонична плоча, и нейният предшественик Османската империя е свързана с европейския живот векове наред. Османската империя се е простирила дълбоко в Европейския полуостров и е допринесла за облика на европейската история точно толкова, колкото всяка друга европейска сила. На някой от европейските сили е била враг,

на други – съюзник. Историята ѝ е точно толкова европейска колкото и на всички останали държави от полуострова“ [Фридман, 2015 :271].

Разбира се както показахме в предходните страници, не са малко и възраженията срещу турското еврочленство. Никой обаче не може да отрече пътя който Турция последователно извървя отстоявайки прозападната си ориентация.

Важен факт е, че през изминалите години Турция се превърна в един от близките съюзници на САЩ и ЕС. Дългогодишното и членство в НАТО и възможностите на нейната армия (втората по-численост в Алианса) я превръщат в предвидим и важен партньор.

Успешното икономическо и социално развитие на Турция, превръщането и в регионален лидер, доведоха и до изработването на нова външна политика. Неин автор е тогавашният външен министър, а в последствие и премиер Ахмет Давутоглу. Външнополитическата му доктрина наречена „Стратегическа дълбочина“ е изградена върху няколко принципа, който трябва да осмислят новата реалност в света.

„Първият методологически принцип защитава един „визионерски“ подход към регионалните въпроси, в противоположност на „кризисно-ориентирания“ подход от времената на Студената война. Вторият принцип настоява за последователност. Според този принцип „турският подход към Близкия Изток не се намира в противоречие с подхода към Централна Азия или Балканите; подходът към Африка е не по-различен от онзи към Азия“. Последният принцип подчертава важността на меката сила като новия език на дипломатията, в противоположност на сплашванията чрез военни средства. Тези принципи се опитват да характеризират Турция като приятелски настроена, но мощна държава, която цени сътрудничеството със съседите си. И понеже тези принципи са специфично адресирани към регионите, с които Турция граничи, на базисно ниво Стратегическата дълбочина се опитва да създаде нов имидж на Турция в бившите османски пространства, също както и нео-османизма на Йозал. С доктрината на Давутоглу се формира външнополитическа стратегия, свързана с активна политика в

широк периметър – на Балканите, в Близкия Изток и Средна Азия. Тя съдържа разбирането за многопосочна външна политика, която да утвърждава историческото наследство и геополитическата значимост на съвременна Турция. Широкият подход съчетава активната регионална политика със засилени отношения с ЕС и Турция активизира усилията си за присъединяване и членство. Тази линия се следва неотлъчно, обогатява се и се развива, въпреки че някои държави-членки (Франция, Германия) изразяват резерви относно бързото присъединяване на Турция, а турското политическо ръководство показва своето недоволство от това“ [Хинкова, С. Геополитическите измерения на присъединяването на Западните Балкани и Турция в ЕС. - <http://diplomacy.bg/archives/842?lang=BG>].

Когато говорим за недоволството на турските управляващи от бавният според тях напредък на преговорите с Евросъюза, трябва да отбележим, че това забавяне крие определени опасности и за двете страни.

Все по-широки слоеве от турското общество започват да губят търпение, и да се питат дали еврочленството си струва усилията. Това крие опасност от изолационизъм който би подкопал постигнатите от Турция успехи и би засилил позициите на ислямският фундаментализъм в страната. Не трябва да се пропуска и фактът, че Турция е единствената мюсюлманска държава членка на НАТО, и пример за това, че демокрацията е съвместима с ислямските традиции. На фона на сложната обстановка в ислямският свят, след ентусиазма от „арабската пролет“, една демократична (макар и с някой уговорки) Турция е изключително важен партньор за ЕС.

В противният случай една отчуждена от Европа Турция, вместо преграда за близоизточните проблеми, би се превърнала самата тя в генериращ напрежение фактор.

Въпреки вътрешните проблеми който Турция без съмнение изпитва, никой не може да отрече нейната геостратегическа роля в ключови за ЕС региони.

Тази роля се усили още повече във връзка с емигрантската вълна заляла европейските страни. Турция се показва като надежден партньор, задържайки над два милиона сирийски

бежанци в изградените от нея лагери. Нейната конструктивна позиция, доведе до затопляне на отношенията с както с Франция, така и с Германия.

На срещата на върха проведена на 15 октомври 2015 г. европейските лидери заговориха за по-ранно преразглеждане на визовия режим с Турция, както и за рестартиране на преговорния процес за членството на страната в ЕС. Фактът, че въпросът за подновяването на преговорите беше положително коментиран от френският президент Франсоа Оланд е показателен за новите реалности в Европа.

Към това можем да добавим и съвместния план на ЕС и Турция за справяне с бежанският поток, одобрен на посочената среща [ЕС одобри плана за действие за миграцията с Турция. [http://petel.bg/ES-odobri-plana-za-deystvie-za-migratsiyata-s-Turtsiya\\_130599](http://petel.bg/ES-odobri-plana-za-deystvie-za-migratsiyata-s-Turtsiya_130599)].

Показателен е и фактът, че НАТО застана зад Турция след свалянето на руският СУ-24 през ноември тази година. Генералният секретар на Алианса, Йенс Столтенберг призова към спокойствие и деескалация на ситуацията, към преговори между двете страни, но в същото време подчерта, че НАТО е солидарен с Турция [Ген. Секретар на НАТО: Съюзниците са солидарни с Турция. <http://www.vesti.bg/sviat/nato-syuznicite-sa-solidarni-s-turciiia-6046051>].

Всичко това ни дава основание да твърдим, че партньорството между Запада и Турция няма да загуби набраната историческа инерция, и въпреки ислямистките уклони на днешните управляващи в южната ни съседка ще доведе до по-високи нива на интеграция.

Политиката на изолационизъм на ЕС, и в частност към Турция е непродуктивна. В крайна сметка както САЩ така и Европа имат нужда не от изолационизъм, а от един „по-голям и по-жизнеспособен Запад“ [Бжежински, 2012: 186]. А точно това оставя Турция в голямата игра.

## ЛИТЕРАТУРА

1. Бжежински, З. (2012). Стратегическата визия. София. с. 186.
2. Спасов, С. (2012). Европейска архитектура за сигурност. София. с. 264.

3. Медийно досие: Отношенията на ЕС с Турция. [http://www.dnevnik.bg/evropa/razshiravane/2010/06/07/913299\\_mediino\\_dosie\\_otn\\_osheniiata\\_na\\_es\\_s\\_turciia/](http://www.dnevnik.bg/evropa/razshiravane/2010/06/07/913299_mediino_dosie_otn_osheniiata_na_es_s_turciia/)
4. Чуков, Б. Ердоган срещу Ататюрк. <http://a-specto.bg/erdogan-sreshtu-atatyurk/>
5. Джасим, Е. Паралелната турска държава. - L'ÉUROPEO № 45, 2015, с.36-38
6. Фридман, Дж. (2015). Взривоопасните точки на Европа. София. с. 271.
7. Хинкова, С. Геополитическите измерения на присъединяването на Западните Балкани и Турция в ЕС. - <http://diplomacy.bg/archives/842?lang=BG>
8. ЕС одобри плана за действие за миграцията с Турция. [http://petel.bg/ES-odobri-plana-za-deystvie-za-migratsiyata-s-Turtsiya\\_130599](http://petel.bg/ES-odobri-plana-za-deystvie-za-migratsiyata-s-Turtsiya_130599)
9. Ген. Секретар на НАТО: Съюзниците са солидарни с Турция. <http://www.vesti.bg/sviat/nato-syiuznicite-sa-solidarni-s-turciia-6046051>



# МУЛТИКУЛТУРНИ ПРОБЛЕМИ В ЗАПАДНИЯ СВЯТ

Доц.д-р Добромир Добрев

## Multicultural issues in the Western world

Dobromir Zh. Dobrev

**ABSTRACT:** *Liberal West and its philosophy security face a number of challenges. On the one hand, these are internal problems of the West, on the other hand, are different in cultural and civilizational modes*

**KEYWORDS:** *Mozheyko, democracy, Europa, USA, Liberal West, multiculturalism.*

Когато Париж преживя ужаса на атентатите и разстрелите в петъчната нощ на 13 ноември, мнозина обявиха мултикултурализма за мъртъв. Твърде голямо беше изкушението да се изкаже подобна теза и да се повлече общественото мнение в тази посока. На парижани им се събра много насилие и смърт през 2015 г. която започна с разстрела в редакцията на Шарли ебдо и завърши с джихадистките изстъпления в ноемврийската вечер на петък 13.

Самият факт, че повечето от радикалните ислямисти извършили атентатите бяха френски граждани, допълнително наливаше масло в огъня.

Новата 2016 г. също започна с изстъпленията на стотици имигранти през новогодишната нощ на площада в немският град Кьолн. Въпросът за спазването на законите и правилата беше приплъзнат в плоскостта на културните различия. Старият континент се задъхваше от имигрантската вълна, от липсата на координация между отделните страни и мудната брюкселска администрация. Престъпни актове като гореописаните подклаждаха недоволството и засилваха твърденията за край на мултикултурализма.

Ако трябва да бъдем точни тези твърдения не са от последните една-две години.

Концепцията за мултикултурализма в Европа стана актуална с притока на милиони имигранти от Северна Африка и Близкия изток. Те носят със себе си арабската и мюсюлманската традиции и култура и създават в центъра на Европа копия на родните си общности. Много са редки случаите, когато се наблюдава желание за интеграция и приобщаване към традициите на приемащата страна.

Редица събития през последните години обаче ни карат да преосмислим културната толерантност, към която Европа се придържаше. Ислямският фундаментализъм и радикализацията на родени в Европа мюсюлмански младежи поставят много въпросителни пред европейските мултикултурни практики. В тази връзка искам да припомня твърдението, че докато САЩ и Канада прилагат на практика мултикултурализма, европейците много често остават в рамките на академичните дискусии<sup>1</sup>. Съответно може и да се дебатира дали настоящите проблеми между общностите в Европа са продукт на мултикултурализма или на непълното му и частично прилагане.

Трудно е обаче да се поставя знак за равенство между Европа от една страна и САЩ и Канада от друга. Различният и много по-дълъг исторически път на европейските държави и все още непреодоления национализъм от миналото са фактори който предопределят мултикултурните проблеми в Стария свят.

Интересна трансформация се наблюдава в Холандия, една от най-отворените за различните култури държава. Холандия е богата страна, поради което е притегателен център за имигранти от цял свят.

Сериозният приток на чужденци в Холандия започва през 70-те години на миналия век, когато в страната са поканени работници от Мароко и Турция. Тях никой не се старае да ги интегрира, защото се смята, че след време те така или иначе ще се върнат по родните си места. Дори напротив – мароканците и

<sup>1</sup> Можейко, Е. Мултикултурализъм и постмодернизъм.

<http://www.slovo.bg/old/litforum/136/edwardm.htm> (15.02.2015г.)

турците са насърчени да запазят своята културна автономия и да се сдружават на етнически признак. От 1974 г. децата на чуждестранните работници получават възможност да изучават майчиния си език в холандските училища.

През 80-те години вече е ясно, че повечето от работниците-гости няма да се върнат в родните си страни. Макар че по това време терминът „мултикултурализъм“ все още не се използва, холандското правителство го прилага на практика. Мигрантите официално са обявени за „етнически малцинства“, чиято културна уникалност трябва да се насърчава.

В същото време започва сериозно реструктуриране на холандската икономика. Страната се деиндустриализира и към края на десетилетието една значителна част от турците и мароканците вече са безработни. Те започват да тежат на социалната система, но дори и тогава в холандското общество се смята за политически некоректно да се обръща внимание на този факт.

Междувременно поради концентрацията на имигрантите в големите градове те вече са половината от населението на Амстердам и Ротердам.

През януари 2000 г. Пол Шефер, холандски историк и политик написва статия с красноречивото заглавие „Мултикултурната трагедия“. Авторът поставя диагноза на холандското общество: слаба интеграция, нарастваща сегрегация и бързо увеличаване на мюсюлманското население.

Шефер констатира, че уважението към културните различия е надделяло над защитата на принципите на либералната демокрация и призовава холандците към „цивизационна офанзива“<sup>2</sup>.

През следващите години отношението към имигрантите става все по-резервирано. Получаването на холандско гражданство вече е много трудно, задължителните курсове по

---

<sup>2</sup> Мултикултурализмът в Европа – идва ли краят?  
<http://armymedia.bg/?p=19101> (18.02.2015г.)

холандски език вече не са безплатни. За имигрантите се въвежда тест по холандски език и култура.

През ноември 2004 г. ислямски фундаменталист убива режисьора Тео ван Гог, правнук на световноизвестния художник, и това отприщва вълна от протести и демонстрации. Регистрирани са и случаи на нападения срещу джамии и мюсюлмански училища.

Прави впечатление, че убиецът Мохамед Буйери е роден и израсъл в либерална Холандия, радикализирал се е и е станал член на младежка мюсюлманска организация.

„С убийството на Тео ван Гог общественото и медийно внимание се фокусираха върху въпроса за радикализирането на младите нидерландски мюсюлмани. Преди това трагично събитие политиките споделяха мнението, че младите последователи на тази религия ще успеят да се интегрират по-добре в светската държава и ще търсят по-умерени форми на изповядване на ислямската религия от техните родители. След престъплението срещу режисьора това схващане се промени драстично“<sup>3</sup>.

През 2011 г. позицията на холандското правителство по отношение на мултикултурализма се ожесточава още повече.

Приет е нов закон за интеграцията, представен от вътрешния министър в парламента по следния начин: „Правителството споделя социалното недоволство от модела на мултикултурното общество и планира да смени приоритета, като постави на преден план ценностите на холандския народ. В новата интеграционна система централна роля ще имат именно тези ценности“<sup>4</sup>. Примерът с Холандия е показателен и в същото време не е единствен за случващото се в Европа. Дебатът за интеграцията на имигрантите се изостри през 2010 г., след излизането на книгата на Тило Зарадин „Германия се самоунищожава“. Той е от хората, които формират общественото мнение в страната, зам.-директор на Бундесбанк. Освен категоричното заглавие, книгата защитава още по-категоричната теза, че политиката на мултикултурализма ерозира германската култура и прави държавата „по-глупава“.

<sup>3</sup> Чуков, В., П. Колева. Западноевропейският ислям. С., 2011г., с. 58

<sup>4</sup> Мултикултурализмът в Европа – идва ли краят?

<http://armymedia.bg/?p=19101> (18.02.2015г.)

След скандала Зарацин подаде оставка, но дебатът по темата не стихна.

През октомври същата година германският канцлер Ангела Меркел призна, че опитът да се изгради мултикултурно общество в Германия се е провалил.

На международната конференция за сигурност в Мюнхен през февруари 2011г. британският премиер Дейвид Камерън също обяви за провал на дългогодишната политика на страната си в тази област. Неговите констатации подчертаваха, че липсва интеграция на мюсюлманите в британското общество и това подхранва екстремизма сред тях. Идеята, която лансира британският премиер, е за „обща национална идентичност“, която да замени мултикултурализма и да намали различните форми на екстремизъм. Нещо повече, Камерън се обяви срещу пасивната толерантност и призова за по-различен либерализъм, наречен от него „либерализъм с мускули“<sup>5</sup>.

Сходна се оказа и позицията на тогавашния френски президент Никола Саркози. Той също нарече провал политиката на френската държава по отношение на имигрантите. Различията трябва да се уважават, но според него не трябва да се поощряват общности, които не се вписват в местните традиции. Тезата на Саркози е, че във Франция има национална общност и имигрантите трябва да са част от нея. Ако не желаят това, те не са добре дошли в страната.

Ако се върнем още назад във времето, ще видим, че проблемът с интеграцията на имигрантите се прояви остро във Франция през 2005г. Тогава имаше масови безредици и улично насилие, предизвикани от арабската общност, след като полицей застреля арабски младеж. В Париж и още няколко града горяха коли, грабежа се магазини, в редица райони цареше хаос. На всички беше ясно, че затавяваните с години проблеми излизат наяве и трябва да се търси решение.

---

<sup>5</sup> Либерални мускули срещу мултикултурализма.

[http://www.dnevnik.bg/sviat/2011/03/08/1055520\\_liberalni\\_muskuli\\_sresh\\_tu\\_multikulturalizma](http://www.dnevnik.bg/sviat/2011/03/08/1055520_liberalni_muskuli_sresh_tu_multikulturalizma) (21.11.2014г.)

Франция е страната, в която живеят най-много мюсюлмани по сравнение с другите европейски държави. Цифрата е около 5 милиона. Не може да се отрече, че властите се опитват да излязат от лошите практики на мултикултурализма. Последователно бяха забранени забрадките в държавните училища и носенето на бурки на обществени места. Задължителните езикови курсове за всички имигранти акцентират върху френските ценности и обичаи, правата на жените и исторически обзор на Франция. В края им участниците трябва да дадат съгласие, че ще ги спазват.

Всичко това превърна темата за запазване светския характер на обществото в една от основните теми по време на президентските избори през 2012 г. Ще припомня, че на тях лидерката на крайната десница Марин льо Пен получи трети резултат. Ако във Франция имаше избори след разстрела на журналистите от „Шарли ебдо“, то тя щеше да е победител поне на първия тур според социолозите. Трагедията, случила се на 7 януари 2015 г., тепърва ще бъде анализирана. Но е ясно, че това не е само френски и дори не само европейски проблем. Това е проблем на западното разбиране за свободата на словото и неприемането на тази свобода от ислямския фундаментализъм. Защитата на универсалността на правата е избор на либералната демокрация.

В контекста на всичко това тезата за смъртта на мултикултурализма в Европа е силно преувеличена. Ако се абстрахираме от емоциите и напъните на радикалните ислямисти да поддържат конфликта с модерността, трябва да признаем, че мултикултурното съжителство отдавна е факт в големите европейски градове. Нещо повече, аз съм напълно съгласен, че самият ЕС е мултикултурен проект.

„ЕС по дефиниция е мултикултурен проект – той не може да съществува като монокултурен национализъм. Повечето от емигрантските държави – САЩ, Австралия, Канада – също са мултикултурни, веднъж след като са изоставили расизма на „превъзходството“ на белия човек (отново през 60-70 години на миналия век). Държави с космополитни градове – Лондон, Париж,

Берлин, Амстердам и т.н. – също трудно могат да бъдат монокултурни“<sup>6</sup>.

Трябва да отбележим, че самият мултикултурализъм е натоварен с някой митологеми който трайно са се закрепили в общественото съзнание. Даниел Смилов проследява някой от най-типичните митове, но аз искам да се спра само на един от тях . Мисля, че точно той е в основата на недоверието на много хора към мултикултурните практики. Става дума за твърдението, че мултикултурализма изисква всяка общност да живее по своите си закони и правила. Кое то пък води към сепаратизъм и федерализъм.

Подобно твърдение категорично не отговаря на практиките в либерално-демократичните държави. Във всяка такава държава има върховенство на закона и този закон се отнася за всички граждани, без значение към коя културна или религиозна общност принадлежат. Принципно държавата си запазва последната дума, т.е. тя има върховната юрисдикция за да може да гарантира правата на всички.

По този начин мултикултурализма, който по дефиниция е съвместно съжителство на различни културни общности в определена държава, напълно се вписва в принципите на либерално-демократичните общности. Тези общности запазват културните различия чрез правата на отделната личност и в същото време осигуряват върховенство на закона.

Трябва ясно да кажем, че проблемът на Обединена Европа не са мултикултурните практики. Проблемите са в мудността и непоследователността с която европейските лидери прокарват общите политики. Днес ЕС има нужда от споделена миграционна политика и общ контрол по границите. Необходима е и обща европейска армия, която да легитимира Съюза като голям геополитически играч. Това е пътя по който Европа ще излезе от наложеният и образ на гигант в икономиката и джудже в политиката.

## ЛИТЕРАТУРА

---

<sup>6</sup> Смилов, Д. Мъртъв ли е мултикултурализма в Европа?  
<http://kultura.bg/web/мъртъв-ли-е-мултикултурализма-в-евро/>  
(15.02.2016г.)

1. Можейко, Е. Мултикултурализъм и постмодернизъм.  
<http://www.slovo.bg/old/litforum/136/edwardm.htm>
2. Мултикултурализмът в Европа – идва ли краят?  
<http://armymedia.bg/?p=19101>
3. Чуков, В., П. Колева. Западноевропейският ислям. С., 2011 г
4. Либерални мускули срещу мултикултурализма.  
[http://www.dnevnik.bg/sviat/2011/03/08/1055520\\_liberalni\\_muskuli\\_sreshtu\\_multi\\_kulturalizma](http://www.dnevnik.bg/sviat/2011/03/08/1055520_liberalni_muskuli_sreshtu_multi_kulturalizma)
5. Смилов, Д. Мъртъв ли е мултикултурализма в Европа?  
<http://kultura.bg/web/мъртъв-ли-е-мултикултурализма-в-евро/>



## Сборника «Вехи» и руската интелигенция

Доц. Д-р Добромир Жечев Добрев

### Corpus VEHI end the Russian intelligentsia

Dobromir Zh. Dobrev

**ABSTRACT:** *The great influence of the Russian intelligentsia of the revolutions in Russia. The spiritual roots of the revolutions. Differences between Russian and Western intellectuals.*

**KEYWORDS:** *intelligentsia, Russia, revolution, philosophy*

*Когато се разглеждат причините за руските революции от 1905 г. и 1917 г. могат да се посочат различни и достатъчно разнообразни фактори.*

Мойте усилия ще бъдат насочени само към една от основните причини за тази революция, а именно идеите на руската интелигенция. Интересно е доколко тези идеи са повлияли върху обществото и къде трябва да се търси генезиса на тяхното формиране.

В тази насока можем да се доверим на една книга, чиято поява през март 1909 г. предизвиква сензация в Русия. Това е сборника “Вехи”. В него мислители от калибъра на Николай Бердяев, Сергей Булгаков, Семьон Франк, Пьотр Струве, Михаил Гершензон и др. обръщат внимание върху спецификата на руската интелигенция и ролята и за революцията в страната. Не трябва да се подминава и факта, че критиката срещу този борник е била много по-силна от подкрепата за него. Израз на тази критика е появилият се на следващата 1910 г. сборник “Интелегенцията в Русия”, а също и много статии и рецензии. Ударите са идвали от дясно и от ляво. Достатъчно е да се споменат само имената на лидера на кадетската партия П.Н. Милюков, лидера на есерите В.М. Чернов, болшевишкият лидер В.И. Ленин и много други участвали в разгрома на “Вехи”. Такава ожесточена реакция най-

малкото засилва интереса към сборника. Ясно е че авторите, са засегнали, и са се противопоставили на редица популярни сред руската интелигенция митове.

Сборникът е издаден по предложение на известния публицист и общественик Михайл Гершензон. През 1908 г. той предлага на още шестима популярни философи, икономисти, литератори да съставят сборник, който да отрази събитията в руското общество свързани с политиката и икономиката и най-вече с последиците от революцията през 1905-1907 г. и ролята на ролята на руската интелигенция за тази революция.

Бердяев (Бердяев, 1991:24) уточнява, че става дума за типичната в руската действителност кръжочна интелигенция, която до известен период е била откъсната от общонационалния живот. Този интелигентски тип се характеризира с не особено дълбоко усвояване на духовните ценности, в това число и философията. Стига се до отричане самостоятелността на философията, до подчиняването ѝ на утилитарни и обществени цели. Разбира се, за това съществуват сериозни причини. Може да се посочи изключителното господство на утилитарно-моралните критерии на подтискащото народолюбие и пролетаролюбие. Стремeжът към висока философска култура е бил оценяван като равнодушие по отношение на народните страдания. По такъв начин, според Бердяев, проблемите на разпределението и уравниението в съзнанието на руската интелигенция винаги са доминирали над интересите на производството и творчеството. Това твърдение се отнася в еднаква степен, както за духовната

така и за материалната сфера. Интелигенцията, а по-точно преобладаващата част от нея, наречена "интелигенщина", винаги охотно и с голямо доверие се е отнасяла към идеологии, поставящи, като централни, проблемите за равенството и разпределението. Всичко това не означава никаква липса на интерес към философската проблематика. Точно обратното, руската интелигенция се е изхитрявала да придава философска украса дори и на особено банални, практически интереси. Тя винаги е имала своите кръжочни философи и своята философия, откъсната от световната. Тази философия е удовлетворявала преди всичко потребностите от цялостен мироглед, отговарящ на всички

въпроси и съединяващ теорията с обществената практика. По такъв начин авторите, удовлетворяващи изискванията за цялостен миоглед и крайните демократически тенденции на интелигенцията са били признавани за "класически". Такива "класически" за интелигенцията автори са били Чернишевски и Писарев през 60-те и Лавров и Михайловски през 70-те години на XIX век. Във философски план тяхното творчество не е дало много, но те са удовлетворявали търсенията на младежта за цялостен миоглед. През 90-те години, с навлизането на марксизма, започва процес на външно европеизиране на интелигенцията. Философското обосноваване на социалните стремежи се извършва от диалектическият материализъм, а по-късно от неокантианството. Става популярно името на Плеханов, а след него на Богданов и Луначарски. Въпреки явния превес на марксизма над народничеството не се наблюдават особени промени в природата на руската интелигенция. Бердяев настоява, че условието да бъде приета една философска концепция от интелигенцията не е нейната дълбочина и стремеж към истината. Условието е нейната постройка да благоприятства социалистическата идея. Тази интелигенция дори изучава Кант, заради обещанието на критическите марксисти, чрез него да обосноват своите идеали. Става дума за известното направление на

легалните марксисти, които чрез Кант обосновават т.н. "етически социализъм". Руската интелигенция се оказва неспособна на основното изискване към всяка философия - любов към истината. Много по-силно се е развила друга стихия, а именно уравнилната справедливост, идолопоклонничеството пред народа, което е унищожило интереса към истината. Доколкото е съществувал такъв интерес, той е бил корисен, подчинен на социалните тежнения.

В статията си "Героизъм и подвижничество" С. Булгаков (Булгаков, 1991:41) вижда революцията от 1905-1906 г. като породена от интелигенцията и под нейното духовно ръководство. Самата революция, както и всяка друга, не дава тези резултати, които са очаквани от нея. Духовният кризис, настъпил след нея,

поставя отново въпроса за самокритичната оценка на интелигенцията.

Самата интелигенция не признава своето ръководство в революцията и в зависимост от принадлежността си посочва една или друга класа, като двигател на революцията. В същото време не може да се отрече, че именно интелигенцията духовно оформя стремежите на масите. Изхождайки от това, се приема, че историята на революцията е и история на интелигенцията; присъда по отношение на интелигенцията. Определено се смята, че от интелигенцията ще зависи съдбата на руската държавност. Всъщност има два варианта, които зависят най-вече от възможността на интелигенцията да се издигне до висотата на стоящите пред нея задачи. В единия случай Русия ще получи образована класа, а в другия случай, интелигенцията в съюз с татарщината или азиатщината ще погуби страната. По такъв начин, обновяването на страната пряко се свързва с обновяването на интелигенцията. Два са факторите, влияещи върху формирането на руската интелигенция: външен и вътрешен. Външният фактор е самодържавието в Русия и насилствените методи, използвани от него. То изолира интелигенцията от живота, затруднява нейното нормално духовно развитие. Така се формира политическия монотеизъм на интелигенцията, нейната фанатична насоченост срещу държавността, символизирана от самодържавието. Вътрешният фактор, определящ характера на интелигенцията, се явява нейния светоглед и свързаната с него духовна насоченост. Именно на този светоглед основно се спира Булгаков в своята статия. В руската интелигенция, в нейния духовен облик често се изтъкват религиозни черти. Това може да се свърже с правителствените преследвания, създаващи мъченическо самочувствие у интелигенцията. Също така, се посочва нейната откъснатост от живота, водеща до мечтателност и утопизъм. Тези качества правят руската интелигенция невъзприемчива към установения, в известен смисъл еснафски, начин на живот в Западна Европа. Живот, характеризиращ се със спазване на всекидневните добродетели, интензивно трудово стопанство, духовна ограниченост. Изследвани са причините за тази антибуржоазност на руските интелигенти. От една страна,

това е проявление на господарското съзнание, на освобождения от много поколения от грижите за насъщния хляб и еснафската страна на живота. Също така това се дължи и на некултурност, на липса на трудови навици. Има и съответната доза безсъзнателно-религиозно отвращение от духовната еснафщина, от земното царство. Въобще, есхатологическите стремежи, стремежите към спасение на човечеството от страданието, са неизменна характеристика на руската интелигенция. Именно чрез духовните навици, възпитавани от Църквата, се обясняват много положителни качества на интелигенцията. Става дума за една строгост в личния живот, за своеобразен аскетизъм. Но в същото време, тези християнски добродетели, които често са придобити несъзнателно от възпитанието, семейството и други, започват да отслабват.

Отслабването на християнските навици, резултат от отдръпването на интелигенцията от Църквата, се проявява ярко в революцията. Особената религиозност на интелигенцията се усилва и от нейното чувство за вина пред народа и готовност да се жертва за този народ. Въпреки това руската интелигенция в огромното си болшинство е атеистична. Атеизмът е признак на добър вкус за тази интелигенция. Религиозното отрицание е синоним на образованост и просветеност. Руският атеизъм има своя специфика; той не е продукт на някакво научно изследване, на продължителна работа на ума и волята. Той е приет на вяра. Вяра, която има в основата си редица непотвърдени и неправилни постановки. Вяра, че науката разрешава окончателно всички въпроси; и въпросите на религията в това число. В исторически план, произходът на руския атеизъм трябва да се търси на Запад. Руската западническа интелигенция го възприема като най-висше постижение на европейската цивилизация. Но Булгаков отбелязва, че от пищното дърво на западната цивилизация, руските интелигенти са си харесали само една клонка. На такъв фундамент едва ли може да се изгради руската култура. Забравя се също така, че западната култура, по своята същност, е религиозна, т.е. - има религиозни корени. Те трябва да се търсят, както в Средновековието, така и в Реформацията. Именно реформизмът предизвиква религиозен подем в Европа и има значителна роля

при формирането на новоевропейския човек. Политическите свободи и идеите на либерализма също са непосредствено свързани с Реформацията. Също така в протестантизма се наблюдава развитие на науките и особено на философията. Може да се каже, че това развитие в Европа протича в рамките на една историческа приемственост, без големи сътресения. По такъв начин културната история на западноевропейския свят представлява едно органично цяло, в което има място, както за Средните векове и Реформацията, така и за теченията от Новото време.

Според Гершензон руският интелигент е човек живеещ вън от себе си. Той признава за достойно само това, което лежи извън личността му - народ, общество, държава. По тази логика съзнанието не се обръща към себе си, а само към външния свят.

За тези години, интелигенцията според Гершензон, не е живяла а е изпълнявала, или си е давала вид че изпълнява обществените дела. Той достатъчно образно разказва, как революционерите изкарват всички на площада - защото е срамно да се стои в къщи. Много години всички са на улицата и спасяват народа; докато в къщата (в тях) цари хаос, мръсотия и безпорядък. Разбира се на стопанина не му е до това - той спасява народа. (Гершензон, 1991:93)

Веднага уточнявам, че великите руски художници - Достоевски, Толстой, Тютчев и др. са герои на съвсем друг разказ. Тяхната самовглъбеност и техните търсения, остават неразбрани или неприети от тези както Бердяев нарича "интелигенщина". Това са същите хора, обявили прозренията на Достоевски за реакционни. Може би наистина е виновен формализма на съзнанието. Идеята на Гершензон е че формализма на съзнанието е най-доброто нивелиращо средство.

На тази основа, е извода че интелигентската маса по същество е безлична, съчетавайки в себе си радикализъм и фанатична нетърпимост. Въпросът, който се задава - дали тези хора с осакатени души могат да се приближат към народа, предлага инвариантност при отговора. Може категорично да се заяви, че това е невъзможно, и в такъв отговор ще има формална

истина. За руският народ, интелегента си остава човек без Бог в душата

т.е. остава си неразбран. Съответно усилията на интелигенцията, да изправи народа, засипвайки го с популярна литература остават напразни. Такава е позицията на Гершензон, но за съжаление в нея има един слаб момент. Става дума за последващото развитие на събитията в Русия, което опровергава идеята, че управителните и нихилистични тенденции сред интелигенцията не могат да стигнат до народа. Победата на болшевиките и подкрепата, която те получават, подсказва обратното. Народът възприема много от идеите на интелигенцията, и за съжаление това са най-вече идеи - атеистични, нихилистични и анархистични.

Достоевски в романа си “Братя Карамазови”, загатва чрез Иван Карамазов и Смердяков, какви могат да бъдат отношенията между интелигенция и народ (Достоевский, 1958:161).

“Взаимоотношенията между Смердяков и Иван символизируют някакви отношения между “народа” и “интелигенцията” в революцията (Бердяев, 1992:129).

Ходът на руската революция показва, че в нея, побеждава именно смердяковското начало - т.е. низшата страна на Иван Карамазов. Иван формулира принципа си “всичко е позволено” след дълги философски размисли върху бунта. Смердяков просто чува тази фраза и започва да живее според нея. Поради това има много истина в думите на Бердяев, че Иван Карамазов е възвишеното проявление на нахилистичният бунт, докато Смердяков и неговото ниско лакейско проявление. Именно лакеят ще осъществява на дело това което интелегента Иван само е говорил. Във всяка революция и във Руската революция в частност напред излизат масите; а там смердяковците са болшинство.

И ако по отношение влиянието на интелигенцията върху народа Гершензон не отива докрай; то в един друг пункт той е особено убедителен. Става дума за нуждата не от сливане, а от предпазване между народ и интелигенция. “Такива каквито сме ние не само не трябва да мечтаем за сливане с народа - ние трябва да се боим от него повече от всички наказания на властта, и да

благославяме тази власт, която със своите щикове и затвори още ни предпазва от народната ярост.” (Гершензон, 1991:101).

Иронията (за което казват че се корени в хитростта на разума) решава нещата по-съвсем друг начин.

Връзката между руският народ и руската интелигенция се осъществява и резултатът от тази връзка е болшевишката революция от 1917 г.

П.Струве разглежда интелигенцията като онзи революционен фактор, който е заменил казачеството в руската история. Колкото и тези два слоя да се различават в битов и социален план, интелигенцията се явява политически приемник на казачеството. Струве не разглежда интелигенцията като “образована класа”. Според него историческото значение на интелигенцията е в нейното отношение към държавата; по конкретно в отчуждението и враждебността към държавата. Разбира се тук има нюанси в някои случаи то е обсолютно, както е при анархистите, в други е относително, както при различните форми на руският социализъм. И в двата случая, обаче се наблюдава характерната за руската интелигенция безрелигиозност. В тази връзка ни е напомнено, че основната философема на социализма е пълната зависимост на човека от външните условия. Средата определя поведението на хората, и по този начин сваля от тях личната отговорност. Струве противопоставя това на религиозния мироглед “За религиозното миросъзерцание не може да съществува нищо по-скъпо и по важно от личното човешко самоусъвършенстване, на което социализмът принципино не обръща внимание”. (Струве, 1991:141).

Духовното раждане на руската интелигенция - така както е разбрана тук - се свързва с възприемането на западноевропейския атеистичен социализъм. По тази логика Бакунин се определя за първият руски интелигент. Не трябва да се пропуска , обаче че руската литература си остава област в която идеите на интелигенцията нямат влияние. За съжаление верно е и това, че самите писатели - Пушкин, Лермантов, Толстой, Достоевски и др. не са приети от типичната руска интелигенция. Тя продължава да гледа с подозрение, всичко което не е свързано с революцията, бунта и преразпределението.



Революцията от 1905 г. има тази особеност, че води до съприкосновение интелигентската и народната мисъл. Но тук проличава една от големите слабости на интелигентската доктрина за служенето на народа. Тази доктрина не предвижда никакви ангажименти, от страна на народа, и не поставя пред него никакви възпитателни задачи.

В тази връзка Струве отбелязва, че след като народа в голямата си част се състои от хора движени от интереси и инстинкти, то интелигентската идеология, при тях едва ли ще даде идеалистически плод.

В революцията се осъществява синтез между политическият радикализъм на интелигенцията и социалният радикализъм на народните инстинкти. В тези действия на Руската интелигенция

Струве, вижда огромна грешка, и то не политическа или тактическа, а морална. Корена на такава грешка е в представата, че развитието на обществото е резултат не от усъвършенстването на човека, а от използването на историческата ситуация. В тази насока се изтъква необходимостта интелигенцията да преразгледа своя мироглед. Става дума за основният пункт на този мироглед, а именно социалистическото отрицание на личната отговорност и прехвърлянето на вината върху социалната среда.

“Възпитанието може да се разбира също във външен смисъл. Него така го разбира този социален оптимизъм, които предполага че човек винаги е готов, винаги е достатъчно зрял за по-добър живот, и че само неразумното обществено упорство му пречи да прояви възможностите си”. (Струве, 1991:150).

Всъщност Струве намира основание за оптимизъм в кризата на социализма на Запад. Логиката на мисълта му е че след като руската интелигенция е родена от западноевропейският социализъм, а този социализъм в настоящият момент (началото на XX в.) е в криза, то тази тенденция неминуемо ще стигне и до Русия.

При тези разсъждения, обаче Струве не отделя достатъчно внимание на различията между западния и руският социализъм. Не случайно Бердяев, твърди че руският комунизъм е труден за разбиране, поради двойствения си характер.

“От една страна той е световно и интернационално явление, а от друга - руско и национално”. (Бердяев, 1994:5). Специално трябва да се отбележи, че познаването на марксистката доктрина не е достатъчно в този случай. Трябва да се познава и развитието на Русия, за да се разбере руският комунизъм.

Руската интелигенция също има двоинствен характер. Тя не е това което е интелигенцията на Запад, тя е пречупена през руската действителност и придобива различни черти (Атанасова, 2012:146-147).

До XIX в. тежест в Русия имат два елемента - монархията и народът. Културната прослойка е твърде слаба - притисната между тях. Постоянното чувство на вина която се изпитва пред народа, също не спомага за нейното развитие. Тук отново стигаме до спецификата на руската интелигенция. Бердеев е категорично против нейното отъждествяване със западното разбиране на интелектуалец. Основното различие е в идеологическата нетърпимост на руската интелигенция, към която принадлежат хора, които не се занимават с интелектуален труд и по думите на Бердяев “....не са особено интелигентни.” (Бердяев, 1994:19). Тук влизат различни социални класи - хора от дворянството, по късно синове на свещенници, дребни чиновници, занаятчийи, селяни. Така се стига до втората половина на XIX в. когато културната прослойка се промени и започва да се нарича интелигенция.

Тази интелигенция, живее изключително чрез идеи. Това са предимно западни идеи и учение, усвоени догматично. Идеи превърнати в религиозно откровение. Това е характерна особеност на руснака въобще, да възприема всичко тотално без критицизма на западния човек.

Може би с това е свързан стремежа към цялостност и руският максимализъм.

“Именно за руската душа е присъщо да превключвна религиозната си енергия върху нерелигиозни обекти върху относителна и отделна сфера в науката или в социалния живот”. (Бердяев, 1994:22).

Връзката между такова превключване и опасността от революция е непосредствена.

## ЛИТЕРАТУРА

1. Бердяев, Н. (1991) Философская истина и интеллигентская правда. – В: „Вехи“, Москва.
2. Бердяев, Н. (1994) Извори и смисъл на руския комунизъм. София.
3. Булгаков, С. (1991) Героизм и подвижничество. – В: „Вехи“, Москва.
4. Гершензон, М. (1991) Творческое самосознание. – В: „Вехи“, Москва.
5. Достоевский, Ф. (1958) Братья Карамазовы. Собрание сочинений, Т. 9, Москва.
6. Струве, П. (1991) Интеллигенция и революция. – В: „Вехи“, Москва.
7. Атанасова, А. (2012) Интеллигенция и „интеллигентщина“ в сборника „Вехи“. – В: Русия, Европа и светът. София.

# **Конструктивни изменения на основния заряд на 82 mm учебно-практическа мина, предназначена за тренажор за обучение на минохвъргачните разчети**

**Христо А. Христов, Цоню Г. Цонев**

## **Constructive modifications in the basic charge for 82 mm practical mine, designed for training mortar troops simulator**

**Hristo A. Hristov, Conyu G. Conev**

**ABSTRACT:** *It is presented in the report an experimental research, related to the investigation of a basic charge of 82 mm practical mine, which is designed for simulator training mortar troops.*

**KEYWORDS:** *main charge, constructive modifications*

През последните две десетилетия налице е тенденция за рязко намаляване бюджетите за отбрана, включително и в Република България. Това от своя страна води до влошаване на подготовката на личния състав, поради невъзможността да се осигури необходимата натренираност на разчетите, получавана при извършването на определен брой учебно-бойни стрелби. С цел недопускане на понижаване на бойната подготовка, в редица армии, са внедрени различни видове симулатори. Основните изисквания към тях са свързани с възможността симулаторът да позволява пълно отработване на всички видове дейности, свързани с бойната работа на разчета, с цел постигане на добра синхронизация при работа и пълнота в подготовката му.

Анализите на военните конфликти през последните години показват една нарастваща актуалност при използването на минохвъргачките в бойни операции. Възможността на същите да поразяват жива сила и техника на противника, разположена както на открито така и когато е зад сгради, на обратната страна на

височини, в дълбоки оврази, окопи, траншеи или други укрития ги прави едно от най-ефективните оръжия. Освен това, те могат (поради характера на траекторията на мината) да поразяват бронирани средства от към горната страна, която е най-слабо защитена, което позволява унищожаване на скъпоструваща техника от минохвъргачки с малък калибър.

Всичко това наред с факта, че минохвъргачките имат максимално опростено устройство, което ги прави лесни за изработка, доведе до значително повишаване на броя на този вид оръжие в армиите.

Значителното повишаване на количеството на тези системи, от своя страна доведе до увеличаване на личния състав, който ги експлоатира. Това наред с изложеното по-горе налага да се обърне сериозно внимание на обучението на минохвъргачните разчети.

В българската армия понастоящем няма приети на въоръжение тренажори за обучение на минохвъргачните разчети.

Изхождайки от всичко изложено до тук, с цел постигане на необходимата добра подготовка в условията на намалени финансови бюджети, в доклада е предложено да се изследва възможността да се разработи тренажор за обучение на минохвъргачните разчети на базата на щатна 82 mm минохвъргачка, използваща учебно-практически мини за многократна употреба и стрелба на скъсени дистанции.

Тренажорът се базира на метода на намаляване на основния метателен заряд при еднаква маса на мината.

Изчисляването на необходимото количество метателен заряд за максимално разстояние на полета на мината 100 m е извършено по методика, предложена в [5].

Целта на настоящото изследване е да се разработи основен заряд за учебно-практическата мина за стрелба на максимални дистанции до 100 m за тренажор за обучение на минохвъргачните разчети.

Основни задачи:

- да се разработи конструкция на основен заряд за учебно-практическата мина за стрелба на максимални дистанции до 100 m;

- да се проведат експериментално изследване за определяне на ефективността на предложената конструкция;

- да се обработят резултатите от експерименталното изследване, да се направят изводи и набележат насоки за оптимизиране на конструкцията на основния заряд.

В изпълнение на първата задача от експерименталното изследване бяха изработени два типа основни заряди.

Първият тип съдържа следните елементи в конструкцията си:

- гилза с метална основа и пластмасово тяло;
- капсул-възпламенител тип „Уинчестър“;
- димен барут за усиление на огненият импулс от капсул-възпламенителя;
- основен метателен заряд;
- дървена подложка с отвор;
- пластмасова запушалка;
- хартиена запушалка.

Основните данни за гилзата с метална основа и пластмасово тяло са представени в таблица 1.

Таблица 1

*Основните данни за използваната гилза*

| Калибър | Размери                                       |                                                           |                                       | Дължина на гилзата -L [mm] |
|---------|-----------------------------------------------|-----------------------------------------------------------|---------------------------------------|----------------------------|
|         | Външен диаметър на тялото на гилзата - d [mm] | Външен диаметър на металната основа - d <sub>1</sub> [mm] | Вътрешен диаметър на гилзата – D [mm] |                            |
| 2       | 20,20                                         | 22,45                                                     | 18,50                                 | 69,8                       |

Дървената подложка с отвор конструктивно е разположена между капсул-възпламенителя и основния метателен заряд, като по този начин мястото на основния заряд се премества с 20 mm по-нагоре отколкото без наличието на подложка. Поставянето на този елемент цели да се приближи намаленото количество основен заряд до направените в стабилизатора на мината отвори за изтичане на барутните газове и да се запази стандартната

дължината на гилзата. В отворът на подложката се разполага димния барут за усиление на огнения импулс.

Пластмасовата и хартиена запушалки имат за задача да уплътнят оставащото пространство в гилзата, да не допуснат разместване на основните елементи и осигурят херметичност.

Подреждането на елементи на основния заряд на учебно-практическата мина е представен на фиг. 1.

Вторият тип основни заряди включва в конструкцията си следните елементи:

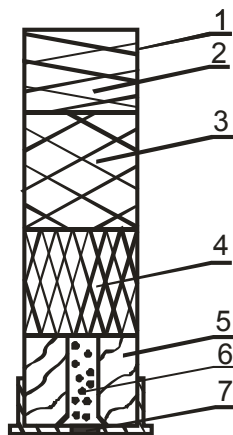
- гилза с метална основа и пластмасово тяло;
- капсул-възпламенител тип „Уинчестър“;
- димен барут за усиление на огнения импулс от капсул-възпламенителя;
- основен метателен заряд;
- пластмасова запушалка;
- 2 бр. хартиени запушалки.

За изпълнение на втората основна задача - провеждане на експериментално изследване за определяне на ефективността на предложената конструкция бяха проведени опитни стрелби на АСП „Марково“.

Същите протекоха при следния ред:

1. Подготовка на тренажора за обучение на минохвъргачните разчети за стрелба:

- привеждане на 82 mm минохвъргачка от походно в бойно положение;



Фиг. 1. Конструкция на първия тип основен заряд на учебно-практическата мина.

1- гилза с метална основа и пластмасово тяло; 2- хартиена запушалка; 3- пластмасова запушалка; 4- основен метателен заряд; 5- дървена подложка с отвор; 6- димен барут за усиление на огнения импулс от капсул-възпламенителя; 7- капсул-възпламенител.

- преглед и почистване на канала на тялото на минохвъргачката;
- проверка на механизмите за насочване на минохвъргачката;
- проверка на мерните прибори на минохвъргачката;
- проверка на учебно-практическата мина.

2. Провеждане на експериментална стрелба:

- произвеждане на 10 броя изстрели с първия тип основни заряди;
- измерване на дистанцията до всяко попадение;
- произвеждане на 10 броя изстрели с втория тип основни заряди;
- измерване на дистанцията до всяко попадение.

Забележка: измервана е само дистанцията в разстояние, като меренето започва от дулния срез на тялото на минохвъргачката и завършва в мястото на падане на мината. Не е измервано разсейването на попаденията встрани.

Резултатите от експерименталното изследване са представени в таблица 2.

Таблица 2

*Резултатите от експерименталното изследване*

| №                                            | Ъгъл<br>на<br>стрелбата<br>[grad] | Разстояние<br>до попадението<br>[ m ] | Очаквано<br>разстояние на<br>попаденията [ m ] |
|----------------------------------------------|-----------------------------------|---------------------------------------|------------------------------------------------|
| <b>Първи тип основни заряди</b>              |                                   |                                       |                                                |
| 1.                                           | 45°                               | 68,7                                  | 100                                            |
| 2.                                           | 45°                               | 74,3                                  | 100                                            |
| 3.                                           | 45°                               | 82,3                                  | 100                                            |
| 4.                                           | 45°                               | 88,3                                  | 100                                            |
| 5.                                           | 45°                               | 75,3                                  | 100                                            |
| 6.                                           | 45°                               | 80,3                                  | 100                                            |
| 7.                                           | 45°                               | 83,15                                 | 100                                            |
| 8.                                           | 45°                               | 69,7                                  | 100                                            |
| 9.                                           | 45°                               | осечка                                | 100                                            |
| 10.                                          | 45°                               | 57,4                                  | 100                                            |
| <b>Средна стойност на дистанцията - 75,5</b> |                                   |                                       |                                                |



| <i>№</i>                                            | <i>Ъгъл<br/>на<br/>стрелбата<br/>[grad]</i> | <i>Разстояние<br/>до попадението<br/>[ m ]</i> | <i>Очаквано<br/>разстояние на<br/>попаденията [ m ]</i> |
|-----------------------------------------------------|---------------------------------------------|------------------------------------------------|---------------------------------------------------------|
| <b><i>Втори тип основни заряди</i></b>              |                                             |                                                |                                                         |
| 1.                                                  | 45°                                         | 59,2                                           | 100                                                     |
| 2.                                                  | 45°                                         | осечка                                         | 100                                                     |
| 3.                                                  | 45°                                         | 45,9                                           | 100                                                     |
| 4.                                                  | 45°                                         | 27,1                                           | 100                                                     |
| 5.                                                  | 45°                                         | 47,6                                           | 100                                                     |
| 6.                                                  | 45°                                         | 57,7                                           | 100                                                     |
| 7.                                                  | 45°                                         | 20,8                                           | 100                                                     |
| 8.                                                  | 45°                                         | 79,9                                           | 100                                                     |
| 9.                                                  | 45°                                         | осечка                                         | 100                                                     |
| 10.                                                 | 45°                                         | 55,1                                           | 100                                                     |
| <b><i>Средна стойност на дистанцията - 49,2</i></b> |                                             |                                                |                                                         |

От получените резултати може да се види, че средната дистанция на попаденията при първия тип основни заряди се различава от очакваната с 24,5 %, а при втория тип основни заряди с 50,8%. Основните причини за това са следните:

1. Пластмасовата гилза се пробива при по-ниско от предвиденото налягане, което води до по-бавно горене на барута на метателния заряд.

2. Пластмасовата запушалка силно се деформира, при което се увеличава пространството в гилзата и намалява скоростта на горене на барута на метателния заряд.

3. Отсъствието на дървена подложка води до допълнително увеличаване на обема на гилзата в процеса на горене на метателния заряд, получаващо се от изместването на хартиените запушалки и смачкването на пластмасовата.

Всички тези причини водят до нееднакви процеси на горене на барутния състав и ниски стойности на импулса поради което мината не успява да получи изчислената начална скорост и да достигне предвидената дистанция на полета.

Изводи:

1. Необходимо е да се вземат мерки за постигането на приблизително еднакви условия за горене, като не се допусне изменение на първоначалния обем в който изгаря на барутния състав. Конструктивно това налага да се замени деформиращата се пластмасова запушалка с такава от недеформиращ се материал.

2. Необходимо е да се вземат мерки за повишаване на стойността на първоначалния импулс. Конструктивно това може да се постигне като се усили стената на използваната пластмасова гилза, при което тя ще се пробие при по-висока стойността на налягането.

### **ЛИТЕРАТУРА:**

1. Гулицкий Э.Г., Чистюхин В.Н. и др. Обеспечение стабильной работы основного заряда в условиях удлиненной камеры стабилизатора мины для 82-мм выстрела. Сп. Вестник Казанского Технологического Университета, №8 / 2010 год.

2. ГОСТ 7839—78, с изменения № 2 от 01.01.1984 г.

3. ГОСТ 23569 – 79.

4. Христов Хр. Експериментално изследване възможността за стрелба с 82 мм минохвъргачка на дистанции 100 м. Годишник на ФТН, ШУ „Епископ Константин Преславски“, ISSN1311-834X, стр.47 – 55, 2015 год.

5. Христов Хр. Определяне на количеството барут на основния заряд при свръхкъси дистанции на стрелба с 82 мм батальонен миномет. Научна сесия 2009, НВУ "В.Левски", стр. 35, ISSN 1314-1953, 2010 год.

**Определяне аномалните изстрели при  
експериментални стрелби с 82 mm учебно-практическа  
мина, предназначена за тренажор за обучение на  
минохвъргачните разчети**

**Христо А. Христов, Цоню Г. Цонев**

**Determination abnormal shots in experimental firings with  
82mm practical mine, designed for simulator training  
mortar troops**

**Hristo. A. Hristov, Conyu. G. Conev**

**ABSTRACT:** *There is presented an experimental research which goal is to define the abnormal shots with 82 mm mine in the report. Moreover, it is definitely variation in distance  $B_0$ , which determines shooting at short distances.*

**KEYWORDS:** *experimental shootings, analysis of experimental ballistic data*

## **1. Увод**

През последните две десетилетия налице е тенденция за рязко намаляване бюджетите за отбрана, включително и в Република България. С цел недопускане на понижаване на бойната подготовка, в редица армии, са внедрени различни видове симулатори. Основните изисквания към тях са свързани с възможността симулаторът да позволява пълно отработване на всички видове дейности, свързани с бойната работа на разчета, с цел постигане на добра синхронизация при работа и пълнота в подготовката му. В българската армия понастоящем няма приети на въоръжение тренажори за обучение на артилерийските и минохвъргачни разчети.

В доклада са представени част от проучванията, свързани с разработването на тренажор за обучение на минохвъргачните разчети на базата на щатна 82 mm минохвъргачка, използваща

учебно-практически мини за многократна употреба и стрелба на скъсени дистанции.

Целта на настоящото проучване е да се изследват балистичните данни при стрелба с 82 mm мина на дистанции до 100 m и да се определи основната характеристика - отклонението в разстояние  $B_0$ , като се отхвърлят аномалните изстрели, получени в хода експерименталните стрелби.

## 2. Основни обозначения и определения

$B_0$  - отклонението в разстояние [m];

$$D_1 = \sqrt{\frac{\left(\bar{x}_u - \bar{x}\right)^2}{\kappa - 1}}$$

$E_t$  – срединно отклонение;

$$E_\rho = \rho \sqrt{2} \cdot \sqrt{\frac{\left(\bar{x}_u - \bar{x}\right)^2}{\kappa - 1}}$$

$$E_\rho = 0.6745 \cdot \sqrt{\frac{\left(\bar{x}_u - \bar{x}\right)^2}{\kappa - 1}} \quad - \text{отклонение с изключен}$$

$$E_\rho = 0.6745 \cdot S_1$$

$$E_\rho = 0.6745 \cdot \sqrt{D_1}$$

съмнителен

резултат;

$P$  – вероятност;

$S_1 = \sqrt{D_1}$  – средно квадратично отклонение [m];

$\bar{x}$  – средно значение на измерваната величина [m];

**съмнителен резултат** - статистически (случаен) резултат, за който са възникнали съмнения за негови случаен характер, поради груби грешки, кратковременно изменение условията на опита (стрелбата) стр.200 [1].

## 1. Методи за определяне на аномалните резултати в при артилерийски стрелби

Основният проблем, който възниква при изключване на аномалните резултати, се изразява в неизвестност на причините, които предизвикват този резултат. Може обаче, да се приложи известният принцип за практическата невъзможност на малко вероятните събития [1]. Неговата същност се състои в това, че ако съмнителният резултат се е получил, то вероятността за неговото получаване е много малка. На практика фактическото отклонение на съмнителния резултат се сравнява с пределно допустимото и се прави извод за нормалност или аномалност на резултата.

Съществуват основно два метода за определяне аномалните резултати (изстрели), при условие, че експерименталните стрелби се подчиняват на хипотезата за нормалния закон на разпределение.

Когато е налице пълен набор от статистически измервания – т.е. дадени са 30 и повече изстрела.

Когато е налице непълен набор от статистически измервания – т.е. дадени са по малко от 30 изстрела. В този случай като критерий се използва  $E_t$  (срединното отклонение). Прието е да се счита, че един изстрел е аномален и неговият резултат се изключва при обработка на резултатите стр.204 [1], в случай, че:

- **Критерий 1:** отклонението му (грешката) е по голямо от  $\pm 6.E_p$ , при дадени по-малко от 10 изстрела;

- **Критерий 2:** отклонението му е по голямо от  $\pm 5.E_p$ , при дадени 10 и повече изстрела;

Определянето дали един изстрел е аномален става по следния алгоритъм, посочен на стр.204 [1].

а) Определя се значението (разстоянието на попаденията) на измерваната величина, като се изключва съмнителния резултат;

б) Изчисляват се грешките (отклоненията) на отделните резултати, включително и на съмнителния резултат;

в) Изчислява се срединната грешка, без да се включва тази на съмнителния резултат -  $E_p$ ;

г) Разделя се грешката (отклонението) на съмнителния резултат на срединната грешка;

е) Извършва се анализ на частното и се определя дали изстрелът е бил аномален или трябва да се включи при изчисления по посочените по горе критерии.

## 2. Статистическа обработка на данните

През 2013 и 2015 г. бяха проведени експериментални стрелби за да се изследват възможностите да се провеждат артилерийски стрелби с 82 mm минохвъргачка с помощта учебно-практическа мина и да се оптимизира процеса горене и конструкцията на метателния заряд. Резултатите от тях са публикувани в [3] и [4].

Прилагайки гореспоменатите методи за обработка за експерименталните стрелби проведени през 2013 г. от [3], се получават резултатите представени в таблица 1.

*Таблица 1*

*Резултати от проведените експериментални стрелби – 2013 г.*

| № на изстрела | гъл  | Разстояние до попадения | Отклонение от средно аритметич. стойност на попаденията | Отклонения по абсолютна стойност, подредени във възходящ ред | Процент от средно аритметичната стойност |
|---------------|------|-------------------------|---------------------------------------------------------|--------------------------------------------------------------|------------------------------------------|
|               | deg] | [ m ]                   | [ m ]                                                   | [ m ]                                                        | %                                        |
|               | 5°   | 43                      | -39,33                                                  | 3,33                                                         | 4,05                                     |
|               | 5°   | 69                      | -13,33                                                  | 3,67                                                         | 4,45                                     |
|               | 5°   | 79                      | -3,33                                                   | 6,67                                                         | 8,1                                      |
|               | 5°   | 86                      | +3,67                                                   | 7,67                                                         | 9,31                                     |
|               | 5°   | 90                      | +7,67                                                   | 13,33                                                        | 16,19                                    |
|               | 5°   | 97                      | +14,67                                                  | 14,67                                                        | 17,81                                    |

| № на изстрела | гъл  | Разстояние до попадения | Отклонение от средно аритметич. стойност на попаденията | Отклонения по абсолютна стойност, подредени във възходящ ред | Процент от средно аритметичната стойност |
|---------------|------|-------------------------|---------------------------------------------------------|--------------------------------------------------------------|------------------------------------------|
|               | deg] | [ m ]                   | [ m ]                                                   | [ m ]                                                        | %                                        |
|               | 5°   | 106                     | +23,67                                                  | 23,67                                                        | 28,74                                    |
|               | 5°   | 111                     | +28,67                                                  | 24,33                                                        | 29,55                                    |
|               | 5°   | 115                     | +32,67                                                  | 28,67                                                        | 34,82                                    |
| 0             | 5°   | 89                      | +6,67                                                   | 32,67                                                        | 39,68                                    |
| 1             | 5°   | 45                      | -37,33                                                  | 37,33                                                        | 45,34                                    |
| 2             | 5°   | 58                      | -24,33                                                  | 39,33                                                        | 47,77                                    |

Средното аритметично разстояние на попаденията е 82,33 m.

При провеждане на стрелбата е било установено, че изстрели с № 1, 11, 12, са получени в резултатна странични причини – неправилен горивен процес на метателния заряд [3] и затова ще бъдат изключени от разглеждане.

Резултатите тогава приемат вида представен в таблица 2. Както е видно от нея, първия резултат – 69 m, има отклонение от 24,56 m или 26,25 %. Това го прави *съмнителен резултат*.

Таблица 2

Коригирани резултати от експериментални стрелби –  
2013 г.

| № на | гъл  | Разстояние до<br>попадения | Отклонение<br>от<br>средно<br>аритметичната<br>стойност на<br>попаденията | Отклонения по<br>абсолютна<br>стойност,<br>подредени<br>във възходящ<br>ред | Процент от<br>средно<br>аритметичната<br>стойност |
|------|------|----------------------------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------|
|      | deg] | [ m ]                      | [ m ]                                                                     | [ m ]                                                                       | %                                                 |
|      | 5°   | 69                         | -24,56                                                                    | 3,44                                                                        | 3,68                                              |
|      | 5°   | 79                         | -14,56                                                                    | 3,56                                                                        | 3,81                                              |
|      | 5°   | 86                         | -7,56                                                                     | 4,56                                                                        | 4,87                                              |
|      | 5°   | 90                         | -3,56                                                                     | 7,56                                                                        | 8,08                                              |
|      | 5°   | 97                         | 3,44                                                                      | 12,44                                                                       | 13,30                                             |
|      | 5°   | 106                        | 12,44                                                                     | 14,56                                                                       | 15,56                                             |
|      | 5°   | 111                        | 17,44                                                                     | 17,44                                                                       | 18,64                                             |
|      | 5°   | 115                        | 21,44                                                                     | 21,44                                                                       | 22,92                                             |
|      | 5°   | 89                         | -4,56                                                                     | 24,56                                                                       | 26,25                                             |

Средното аритметично разстояние на попаденията е 83,56 m.



Таблица 3

## Проверка за съмнителен резултат

| №             | Разстояние [m] | Разстояние без съмнителния резултат [m] | Отклонения [m] | Отклонения на квадрат [m] |
|---------------|----------------|-----------------------------------------|----------------|---------------------------|
| ----1--<br>-- | -- 69--        | -----<br>---                            | 27,625         | -----                     |
| 2             | 79             | 79                                      | -17,625        | 310,64                    |
| 3             | 86             | 86                                      | -10,625        | 112,89                    |
| 4             | 90             | 90                                      | -6,625         | 43,89                     |
| 5             | 97             | 97                                      | 0,375          | 0,14                      |
| 6             | 106            | 106                                     | 9,375          | 87,89                     |
| 7             | 111            | 111                                     | 14,375         | 206,64                    |
| 8             | 115            | 115                                     | 18,375         | 337,64                    |
| 9             | 89             | 89                                      | -7,625         | 58,14                     |
| Средно        | 93,56          | 96,625                                  |                | $D_1 = 144,734$           |

Данните са подложени на проверката по методиката описана в [1] и са представени в таблица 3.

$$S_1 = \sqrt{D_1} \Rightarrow S_1 = 12,031 \text{ [m]};$$

$$E_p = 0,6745 \cdot S_1 \Rightarrow E_p = 8,114 \text{ [m]}.$$

Отклонението на съмнителния резултат  $\bar{x} - x_i = 96,625 - 69 = 27,625 \text{ [m]}$ ;

Определя се отношението:  $\frac{27,625}{8,114} = 3,39 < 6$ , което показва,

че съмнителният резултат по **Критерий 1** не е аномален от статистическа гледна точка и трябва да се включи в изчисленията.

Обработката на резултатите от експерименталните стрелби, проведени през 2015 г. [4] като се приложат описаните по-горе методи са представени в таблица 4.

Таблица 4

Проверка за съмнителен резултат - стрелби 2015 г.

| №      | Разстояние<br>[m] | Разстояние без<br>съмнителния<br>резултат [m] | Отклонения<br>[m] | Отклонения<br>на квадрат<br>[m] |
|--------|-------------------|-----------------------------------------------|-------------------|---------------------------------|
| 1      | 68,7              | 68,7                                          | -9,41             | 88,49                           |
| 2      | 74,3              | 74,3                                          | -3,81             | 14,49                           |
| 3      | 82,3              | 82,3                                          | 4,19              | 17,58                           |
| 4      | 88,3              | 88,3                                          | 10,19             | 103,89                          |
| 5      | 57,2              | -----                                         | <b>20,91</b>      | -----                           |
| 6      | 80,3              | 80,3                                          | 2,19              | 4,81                            |
| 7      | 83,15             | 83,15                                         | 5,04              | 25,43                           |
| 8      | 69,7              | 69,7                                          | -8,41             | 70,68                           |
| Средно | 75,49             | 78,11                                         |                   | $D_1 = 46,483$                  |

$$S_1 = \sqrt{D_1} \Rightarrow; S_1 = 6,28 \text{ [m]};$$

$$E_p = 0,6745 \cdot S_1 = 4,60 \text{ [m]};$$

Отклонението на съмнителен резултат на *съмнителният резултат*  $\bar{x} - x_i = 78,11 - 57,20 = 20,91 \text{ [m]}$

Определя се отношението:  $\frac{20,91}{4,60} = 4,54 < 6$ , което показва,

че съмнителният резултат **Критерий 1** не е аномален от статистическа гледна точка.

Обработката на резултатите от експерименталните стрелби, проведени през 2015 г. [4] за ъгъл  $65^\circ$  като се приложат описаните по-горе методи са представени в таблица 5.

Таблица 5

Проверка за съмнителен резултат – стрелби 2015 г.

| №      | Разстояние [m] | Разстояние без съмнителния резултат [m] | Отклонения [m] | Отклонения на квадрат [m] |
|--------|----------------|-----------------------------------------|----------------|---------------------------|
| 1      | 59,0           | 59,0                                    | 3,10           | 9,61                      |
| 2      | 24,5           | -----                                   | <b>31,40</b>   | -----                     |
| 3      | 52,8           | 52,8                                    | -3,10          | 9,61                      |
| Средно | 45,43          | 55,90                                   |                | D <sub>1</sub> = 9,61     |

$$S_1 = \sqrt{D_1} \Rightarrow; S_1 = 3,10 \text{ [m]};$$

$$E_p = 0,6745 \cdot S_1 = 2,09 \text{ [m]};$$

Отклонението на съмнителен резултат  $\bar{x} - x_i = 55,90 - 24,50 = 31,40 \text{ [m]}$ .

Определя се отношението:  $\frac{31,40}{2,09} = 15,02 > 6$ , което показ-ва,

че съмнителният резултат **Критерий 1** е анормален от статистическа гледна точка и трябва да се изключи от разглеждане при пресмятане.

### 3. Изводи

Всички получени отклонения при експериметалните стрелби се дължат на проблеми, свързани с вътрешната балистика: не добро изгаряне на метателния заряд; стареене на барута на метателния заряд; нееднородна твърдост на стената на гилзата и др.

### ЛИТЕРАТУРА:

1. Досев Н., Узунов Р. др., Теоретични основи на артилерий-ската стрелба. Книга първа., Издателство на МО „Св. Георги Победоносец“, С., 1996.
2. Равдин И.Ф., Външна балистика на неуправляемите ракети и снаряди., Държавно Военно Издателство, С., 1972.
3. Христов Хр., Експериментално изследване възможността за стрелба с 82 мм минохвъргачка на дистанции 100 м. Годишник на ФТН, ШУ „Еп. Константин Преславски“, ISSN1311-834X, 2015.
4. Христов Хр. и Ц. Цонев, Конструктивни изменения на основния заряд за стрелба до 100 м с 82 мм минохвъргачка. Годишник на ФТН, ШУ „Епископ Константин Преславски“, ISSN1311-834X, 2016.

# УСТРОЙСТВО ЗА ЗАЩИТА НА СЕИЗМИЧЕН СЕНЗОР ОТ СМУЩЕНИЯ В БЛИЗКАТА ЗОНА

Георгиев С.<sup>1</sup>, Колев Х.<sup>1,2</sup>, Георгиев Н.<sup>1</sup>, Пехливански В.<sup>1</sup>

<sup>1</sup> ИМСТЦХА „Акад. Ангел Балеvски“ – БАН, София,  
България

<sup>2</sup> Институт по катализ – БАН, София, България

## SEISMIC SENSOR SHIELD FOR NEAR AREA INTERFERENCE PROTECTION

Georgiev S.<sup>1</sup>, Kolev H.<sup>1,2</sup>, Georgiev N.<sup>1</sup>, Pehlivanski V.<sup>1</sup>

<sup>1</sup> IMSETHC “Acad. A. Balevski” – BAS, Sofia, Bulgaria

<sup>2</sup> Institute of Catalysis – BAS, Sofia, Bulgaria

**ABSTRACT:** The seismic signals from sources located in close proximity to the sensor are vertical seismic waves, and due to the high sensitivity of the seismic sensors, they considerably exceed the sensitivity of the sensor. Therefore, they cause an increase in false alarms and reduce the probability of correctly detecting sensors.

The purpose of this article is to create and explore the effectiveness of the device to protect the sensor from vertical seismic mechanical disturbances occurred in the nearby area. The device is based on the attenuation and dispersion of mechanical waves passing through a sequence of environments with different mechanical impedance.

**KEY WORDS:** seismic sensor, shield, protection, mechanical impedance

### Въведение

В сеизмологията и в системите за периметрова защита се използват сеизмични сензори, които са предназначени да откриват появяването на източници на сеизмични колебания - земетресения, движение на земни или снежни маси (свлачища, лавини и пр.), движение на различни обекти (хора, моторни превозни средства и др.). Тези колебания, в относително далечната зона от местоположението на източника на създаването им, са във вид на хоризонтални сеизмични вълни, поради което сеизмичните сензори най-често са вкопани под земята. Освен това чрез кабел

сеизмичните сензори се свързват с други системи и модули - най-често със системата за обработване на данните от тях, със средства за комуникация, със хранящи модули и пр.

Сеизмичните сигнали от източници намиращи се в непосредствена близост до сензора са във вид на вертикални сеизмични вълни, като поради високата чувствителност на сеизмичните сензори те превишават значително чувствителността на сензора. Ето защо дори слаби сеизмични вибрации причинени от явления в близката зона които не са обекти на регистриране (дъжд, градушка, падащи плодове и клони и пр.) предизвикват значително повишаване на лъжливите сработвания, генерирани от сензора. Освен това, при продължителни въздействия на част от тези явления (дъжд, градушка, вятър предизвикващ сеизмични колебания чрез механичното движение на кабела и др.), сензорите използващи системи за автоматично регулиране на усилването намаляват усилването си и дори предизвикват насищане на входните усилватели. Това от своя страна води до намаляване на вероятността за правилно откриване и дори до преустановяване на възможностите за откриване сензора.

Целта на настоящата работа е да се създаде и проучи ефективността на устройство за защита на сеизмичен сензор от вертикални механични смущения възникнали в близката зона. Устройството се базира на затихването и разсейването на механични вълни преминаващи през последователност от среди с различен механичен импеданс.

### **Теоретична обосновка:**

При разпространението на механична вълна в дадена среда, нейната сила намалява. При идеални хомогенни материали, налягането, което предизвиква вълната намалява само с нарастване на разстоянието. Естествените материали допълнително намаляват силата на механичната вълна поради тяхната нехомогенност, което е свързано с разсейване и поглъщане. Разсейването на механичната вълна е процес, при който отразената вълна се разпространява в направление различно от направлението на навлизане. Поглъщането е процес, отразяващ превръщането на механичната енергия в други форми на енергия.

Комбинираният ефект от разсейване и поглъщане се нарича затихване.

Затихването на механичната вълна е степента на намаляването на амплитудата на вълната при разпространението и в материала.

Затихването на механичната вълна в хомогенен материал в общия случай може да се определи от уравнение 1 [1]:

$$A = A_0 e^{-k \cdot x}, \quad (1)$$

където  $A_0$  е първоначалната амплитуда;  $x$  е разстоянието, което е преминала вълната от първоначалното си възбуждане,  $k$  е коефициент на затихване на вълната в направление  $x$  и зависи от квадрата на честотата на механичната вълна.

Стойностите на коефициента на затихване на даден материал силно зависят както от физико-химическите му характеристики, така и от начина на производството му. Ето защо дори да има фабрично обявени стойности на затихване на даден материал те не трябва автоматично да се приемат за достоверни, особено за широк честотен диапазон. Обикновено надеждни стойности на коефициента на затихване се определят само емпирично след тестове с конкретния използван материал.

Затихването често се дефинира и чрез т.нар. механичен импеданс, който зависи от скоростта на разпространение на механичната вълна и от плътността на материала през които тя се движи [1-4]. Механичният импеданс изразява съпротивлението, което материала оказва на вълната преминаваща през него и се определя чрез формула 2:

$$Z = \rho \cdot v, \quad (2)$$

където  $\rho$  е плътност [ $\text{kg/m}^3$ ];  $v$  е скорост на разпространение на вълната [ $\text{m/s}$ ].

Механичният импеданс е важен за определянето на преминаването и отразяването на механичната вълна на границата между два материала, имащи различни механични импеданси и се използва за оценка на поглъщането на механичната вълна в дадената среда, при създаване на шумозаглушаващи многослойни конструкции.

Механичната вълна се отразява на границата на два материала, когато те са с различни механични импеданси. Разликата в механичните импеданси между два контактуващи материала се нарича разсъгласуване на импеданси, като при нарастване на разсъгласуването нараства енергията която се отразява на границата между тях.

Когато механичните импеданси на материалите, от двете страни на границата са известни, коефициентът на отразяване [2 - 4] може да бъде пресметнат от формула 3 като:

$$C_{ref} = \left( \frac{Z_2 - Z_1}{Z_1 + Z_2} \right)^2, \quad (3)$$

където  $Z_1$  е импедансът на материалът, от който идва сеизмичната вълна;

$Z_2$  е импедансът на материалът, в който преминава сеизмичната вълна;

$C_{ref} \times 100 = Ref [\%]$  енергията на отразената вълна изразена, като процент от навлизащата.

Тъй като количеството на отразената енергия плюс количеството на преминалата енергия трябва да е равно на енергията на навлизащата вълна, преминалата енергия се изчислява чрез разликата на навлизащата енергия и отразената енергия.

Коефициентът на преминаване  $C_{trsm}$  се дефинира чрез формула 4:

$$C_{trsm} = 1 - \left( \frac{Z_1 + Z_2}{Z_1 - Z_2} \right)^2, \quad (4)$$

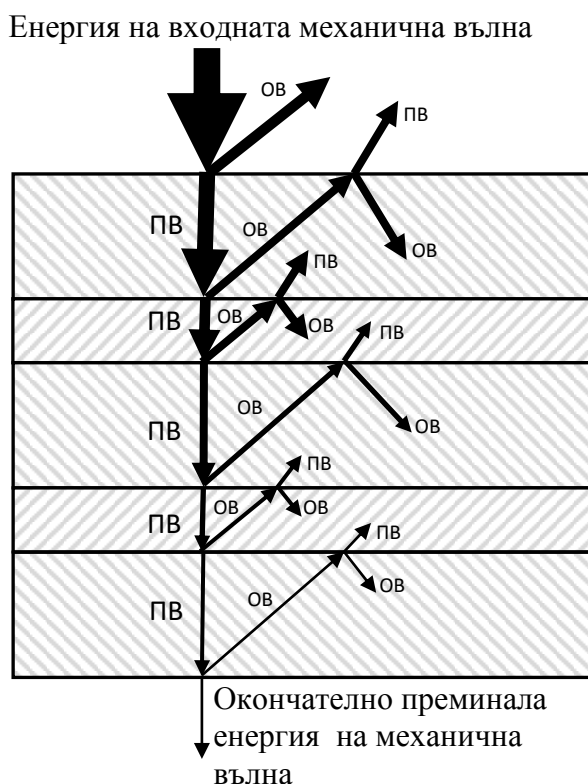
където  $Z_1$  е импедансът на материалът, от който идва механичната вълна;

$Z_2$  е импедансът на материалът, в който преминава механичната вълна;

$C_{trsm} \times 100 = Trsm [\%]$  енергията на преминалата вълна изразена, като процент от навлизащата.

Стойността на постъпилата енергия е сума от стойностите на отразената и на преминалата енергия, т.е.  $Ref [\%] + Trsm [\%] = 100 \%$ .

Когато механична вълна навлезе и премине през конструкция съставена от няколко различни материала са създава поредица от отразени и преминали вълни, както е показано на фигура 1.

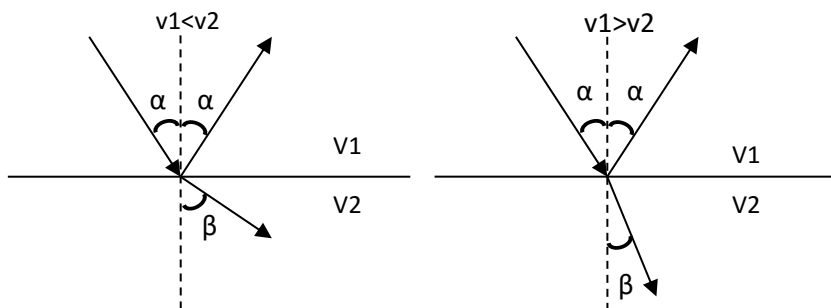


**Фиг. 1.** Принципна схема на затихване на механична вълна при преминаването и през среди с различна плътност.



Когато механичната вълна пада под ъгъл спрямо нормалата на контактната повърхност векторът на разпространение на вълната се пречупва. Пречупването се извършва на границата на двата материала поради различните скорости на разпространение на вълната в двата материала. Скоростта на вълната във всеки материал се определя от свойствата на материала - основно от неговата еластичност и плътност.

На фигура 2 е показано преминаването на механична вълна от материал с една скорост на разпространение на механична вълна в материал с друга по-висока скорост. Следователно, когато вълната срещне границата на дадените два материала, преминалата във втория материал вълна се разпространява по-бързо от вълната в първия материал. Ъгълът между преминалата вълна и нормалата към граничната повърхност е по-голям от ъгълът между нормалата и навлизащата вълна.



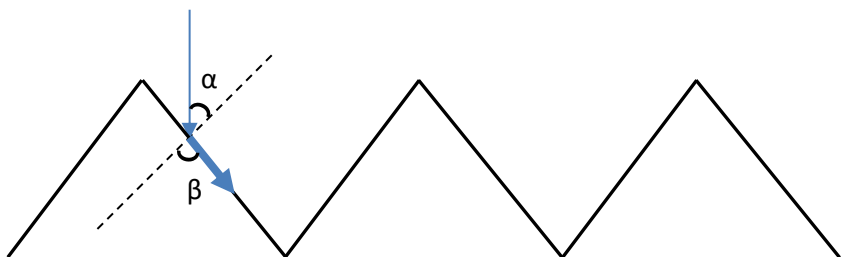
**Фиг. 2.** *Принципна схема на преминаване на механична вълна на границата на материали с различни скорости на разпространение на вълната.*

Връзката между ъгъла на падане и ъгъла на преминаване на механичната вълна и скоростите на разпространение на вълната в материала се задава от закон на Снел [5] даден чрез уравнение 5:

$$\frac{\sin(\alpha)}{v_1} = \frac{\sin(\beta)}{v_2}, \quad (5)$$

където  $v_1$  е скорост на разпространение на надлъжната вълната в среда 1, а  $v_2$  е скорост на разпространение на надлъжната вълна в среда 2.

В случаите на преминаване на механична вълна от среда с по-ниска скорост към среда с по-висока скорост на разпространение на механичната вълна съществува такъв граничен ъгъл на падане, при който практически не се наблюдава преминала вълна, а цялата енергия на преминалата вълна се предава по направление на граничния слой. По тази причина, за по-добро възпиране на механичните вълни контактите между слоевете на сеизмичния щит да бъдат назъбени, както е показано на фигура 3.



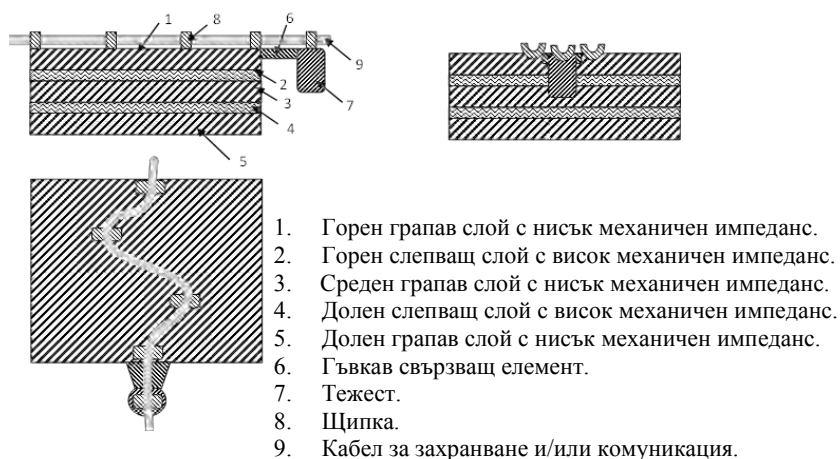
**Фиг. 3.** *Принципна схема за възпиране на механична вълна при използване на назъбен профил на границата между две среди (граничен ъгъл  $\beta \geq 90^\circ$ ).*

#### **Практическа реализация:**

Използвайки до сега описаната теория се предлага устройство за защита на сеизмичен сензор от вертикални механични смущения в близката зона, чиято принципна схема на такова устройство е представена на фигура 4.

Създаденото устройство е изградено от пет слоя материали с различен механичен импеданс и с назъбен контакт между тях. Площта на хоризонталното сечение на устройството е 15 пъти по-голяма от площта на горната част на сеизмичния сензор, т.е. около  $900 \text{ cm}^2$ . Устройството за защита на сеизмичен сензор от механични смущения в близката зона се вкопава над сеизмичния сензор, като горният му слой остава на дълбочина 5-10 см под повърхността на почвата. То има плоска форма и се състои от три

слоя с малък механичен импеданс и с дебелина три сантиметра (слоеве обозначени с 1,3,5) и два слоя с висок механичен импеданс и с дебелина един сантиметър (слоеве обозначени с 2 и 4), (фигура 4). Допълнителен източник на смущения в сеизмичния сигнал е движението на кабела (фигура 4, елемент 9) свързващ сензора с други изделия, системи и устройства. Елементите възпрепятстващи колебанията на кабела свързващ сензора с други системи и/или модули са тежест и пет щипки (фигура 4, елементи 7 и 8). Първата щипка и тежестта са интегрален елемент свързан към горния слой на компонента абсорбиращ вертикалните механични вълни чрез гъвкава връзка и намалят напречната съставна на колебанията на кабела. Надлъжният компонент на механичните вибрации на кабела се намалява чрез фиксирането му в останалите четири зигзагообразно разположени щипки.

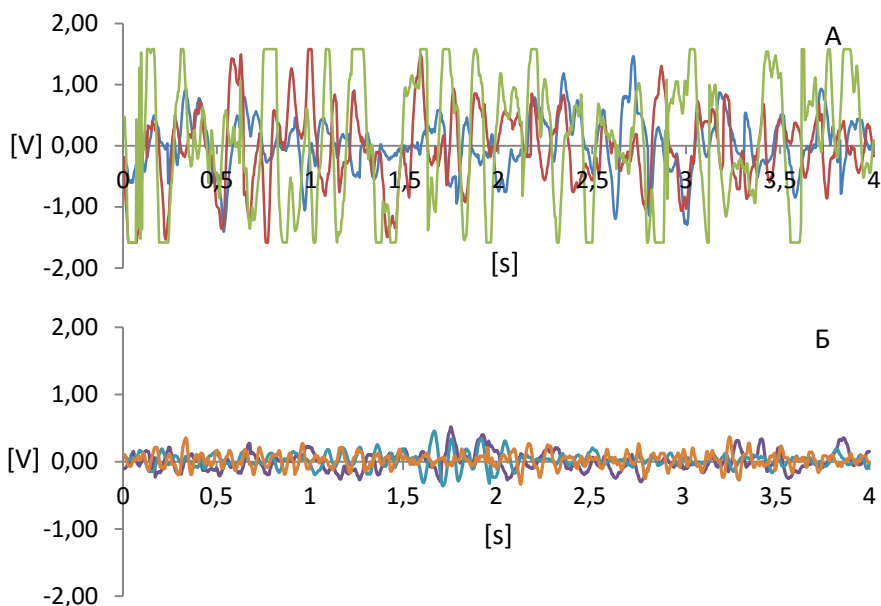


**Фиг. 4.** Принципна схема на устройство за защита на сеизмичен сензор от вертикални механични смущения в близката зона.

За среда с висок механичен импеданс е използван твърд полиуретан с дебелина над един сантиметър и зигзагообразна

форма. За среда с нисък механичен импеданс е използван полиуретан-дунапрен с дебелина три сантиметра.

За да проверим и представим ефективността на устройството (щита) за защита на сеизмичен сензор от вертикални механични смущения в близката зона се проведе експеримент по време на дъжд. Измерена е сеизмичната енергия причинена от дъждовни капки попаднали директно върху повърхността на сеизмичен сензор (Фиг. 5А) и при наличието на сеизмичен щит монтиран над сеизмичния сензор (Фиг. 5Б).



**Фиг. 5.** Аналогов сигнал на сеизмичен сензор при директни попадения на дъждовни капки върху корпуса му А и при монтиран механичен щит върху него Б.

Знаейки плътността и скоростта на разпространение на механична вълна в използваните материали – Полиуретан-

дунапен и твърд полиуретан, може да пресметнем акустичния импеданс на всяка от средите[6] - съответните стойности са представени в таблица 1.

От стойностите на акустичния импеданс и средната стойност на енергията отдадена върху сеизмичния сензор от дъждовни капки без монтиран сеизмичен щит може да пресметнем затихването при монтиран сеизмичен щит.

Измерената стойност на отдадената енергия върху сеизмичния сензор без монтиран сеизмичен щит е пропорционална на интегралната амплитуда на аналоговия сигнал на сензора – 586 mV за 4 ms.

**Таблица 1.** Стойности на механичния импеданс, плътността и скоростта на разпространение на механична вълна за полиуретан-дунапен и твърд полиуретан.

|                         | Механи<br>чен импеданс<br>- $Z$ | Плътн<br>ост –<br>$\rho$ в<br>[kg/m <sup>3</sup> ] | Скор<br>ост –<br>$v$ в<br>[m/s] |
|-------------------------|---------------------------------|----------------------------------------------------|---------------------------------|
| Полиуретан<br>н дунапен | 360                             | 6                                                  | 60                              |
| Полиуретан<br>нов твърд | 2136000                         | 1200                                               | 1780                            |

Определено е количеството преминала енергия на границата между всеки два материала от сеизмичния щит. При това е направено най-неблагоприятното допускане - че цялата енергия се е предала и се разпространява в първата среда на сеизмичния щит и няма затихване при разпространението на вълната по-дължината на материала.

Теоретично е изчислено, че преминалата енергия на границата между полиуретанов дунапен и твърд полиуретанов е:

$$E_{post} = E_{pre} \cdot C_{trsm} = E_{pre} \cdot \left(1 - \left(\frac{Z_1 + Z_2}{Z_1 - Z_2}\right)^2\right)$$

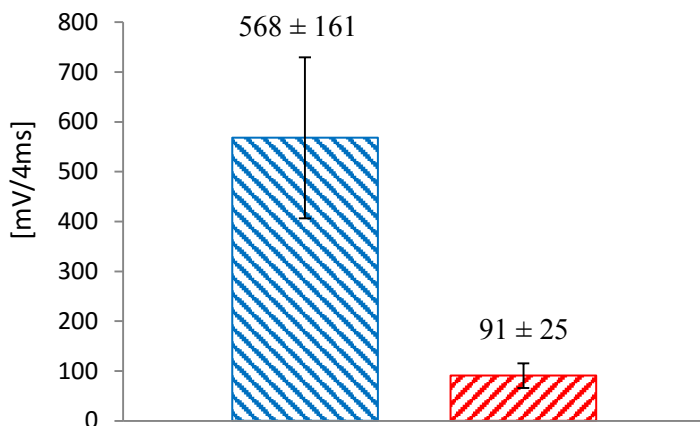
$$C_{trsm} = 1 - \left( \frac{Z_1 + Z_2}{Z_1 - Z_2} \right)^2 = 1 - \left( \frac{Z_1 + Z_2}{Z_1 - Z_2} \right)^2 = 1 - \left( \frac{360 + 2136000}{360 - 2136000} \right)^2 = 0,00067; \text{ т.е. } 00.067 \text{ \%}.$$

Така, ако в материал I се разпространява механична вълна с енергия 568 mV/4ms, то в материали IV и V следва да се е предала механична вълна с енергия практически равна на 0 mV/4ms, което представлява пълно затихване на вълната (Таб. 2).

**Таблица 2.** Пресметнат еквивалент на преминалата енергия във всеки от петте слоя на защитното устройство.

|          | E<br>I  | E <sub>I</sub><br>I<br>(E <sub>I</sub> .0.55<br>4) | E <sub>III</sub><br>(E <sub>II</sub> .0.554) | E <sub>I</sub><br>V<br>(E <sub>III</sub> .0.5<br>54) | E<br>V<br>(E <sub>IV</sub> .0.5<br>54) |
|----------|---------|----------------------------------------------------|----------------------------------------------|------------------------------------------------------|----------------------------------------|
| [m<br>V] | 5<br>68 | 0,<br>38                                           | 0,00<br>026                                  | ~<br>0                                               | ~<br>0                                 |

На фигура 6 са представени експериментално определените средни стойности и стандартни отклонения на мощността на сеизмичния сигнал при дъжд без наличието на сеизмичен щит (синьо) и средна стойност и стандартно отклонение на мощността на сеизмичния сигнал при дъжд и при монтиран сеизмичен щит (червено).



**Фиг. 6.** Еквивалент на постъпилата в сеизмичния сензор енергия

При проведените експерименти се констатира, че сеизмичната активност причинена от дъждовни капки предизвиква високоамплитуден сигнал с голяма вариация. При монтаж на сеизмичния щит, амплитудата и стандартното отклонение на смущенията намаляват значително.

Теоретично пресметнатата стойност на затихването е по-малка от емпирично измерената, защото в хода на експеримента беше констатирано влияние на механични вълни идващи от далечната зона извън монтирания щит.

### **Заклучение:**

Предложено е устройство за защита на сеизмичен сензор от смущения в близката зона, което води до намаляване на силата на смущенията над 5 пъти. По този начин се подобрява значително ефективността на сензорите при работата им в реални условия.

Устройството е апробирано в рамките на изследователски проект на Института, защитено е с патент за изобретение и е намерило добра пазарна реализация.

### **ЛИТЕРАТУРА:**

[1] T. G. Gutowski and C. L. Dym. (1976) Propagation of ground vibration: a review. Journal of Sound and Vibration. 49(2)

- [2] Michael L. Oelze, William D. O'Brien, Jr., and Robert G. (2002) Darmody. Measurement of Attenuation and Speed of Sound in Soils. Published in Soil Sci. Soc. Am. J. 66:788–796 (2002).
- [3] Julio C. Adamowski, Flfivio Buiochi, Claudio Simon, and Emilio C. N. Silva. Ultrasonic measurement of density of liquids. d. Acoust. Soc. Am. 97 (1), January 1995
- [4] B. Cox, "Acoustics for ultrasound imaging," Lecture Notes, University College London, 2012.
- [5] S.W.Rienstra & A.Hirschberg, An Introduction to Acoustics. Eindhoven University of Technology. 2015.
- [6] Britan A., Shapiro H., Ben-Dor G. Foam Engineering: Fundamentals and Applications. Chapter 19, John Wiley & Sons, 2012, ISBN 1119961092



# **ОБОБЩЕНИ ПОКАЗАТЕЛИ ЗА ЕФЕКТИВНОСТТА НА ЕДИН КЛАС СЕНЗОРИ ОТ СИСТЕМИ ЗА ЗАЩИТА**

**Николай Л. Георгиев**  
**ИМСТЦХА „Акад. Ангел Балевски“ – БАН, София,**  
**България**

## **GENERALIZED INDICATORS FOR ONE CLASS OF SENSORS OF PROTECTION SYSTEMS**

**Nikolay L. Gueorguiev**  
**IMSETHC “Acad. A. Balevski” – BAS, Sofia, Bulgaria**

**ABSTRACT** - One of the main indicators of the quality of a wide range of sensors are the time for delay in submission of the alarm and the duration of this alarm. These indicators of quality influence the probability of execution of the function of the sensor as a component of systems or devices that use the alarm to carry out certain activities. Because the sensors operate in random effects these indicators are random variables, numerical characteristics of which can be determined by the analytical method or by numerical modeling. The aim of this paper is to offer an analytical method for assessing the quality indicators of one class sensors as components of protection systems.

**KEY WORDS** – sensors, delay time, existence time, quality indicators

### **Увод:**

В системите за защита на обекти от критичната инфраструктура се използват разнообразни по характеристики и принцип на действие сензори, характеризиращи се с различни информационни възможности, чиято ефективност може да се оцени чрез съвкупност от показатели за качеството им. Те са свързани опосредствено с показателите за качеството от действията на останалите компоненти на системата за защита,

ползващи информация от сензорите. Известни са множество подходи за дефиниране на показателите за качеството на техните информационни характеристики [1,2,3,4], като в обобщен вид те се свеждат до вероятността за правилно откриване на целите на определено разстояние, точността на определяне на координатите на откриваните обекти, вероятността за правилното им разпознаване, вероятността за лъжлива тревога или за грешно разпознаване.

Стойностите на тези показатели се определят по начини, зависими от конкретните физически характеристики на въздействащите сигнали, особеностите на средата за разпространението им и конкретните алгоритми за обработване и предаване на информацията на дадения сензор.

Посочените показатели на качеството на сензорните системи са частни, отнасят се към отделни характеристики на информацията получавана от тях (пълнота, достоверност, точност и пр.) и са свързани опосредствено с функциите им като част от системите за защита на обекти от критичната инфраструктура.

Ето защо интерес представлява намирането на обобщени функционални показатели за качеството на сензорните системи от посочения клас, който да е свързан непосредствено с основното им предназначение като компоненти на системите за защита.

В повечето случаи характеристиките на сензорите осигуряващи информация за вече открити цели са такива, че точността на координатите и вероятностите за разпознаване на вече откритата цел са с показатели, които са не по-лоши от предварително зададените [1,2,3,4]. Ето защо би могло да се приеме, че обобщените функционални показатели за качеството на сензорните системи трябва да са свързани с функцията им да алармира за наличието на обект, която се характеризира с две изисквания:

- подаването на сигнала за алармено събитие да е в момента на появяване на целта или да е с някакво приемливо закъснение. Това изискване е свързано с необходимостта от своевременно реагиране срещу евентуални нарушители на охранявания

(защитавания) район, както и с ограничаване на времето през което нарушителите биха могли да въздействат върху охранявания район (обект);

- при наличие на нарушител в зоната за действие на сензора сигналът за аларменото събитие да не се преустановява за определен минимален период от време. Този период се определя от времето, което е необходимо на останалите компоненти на системата за да извършат предвидените действия (оценка на риска, взимане на решение и целеразпределение, активиране и управление на противодействащите компоненти на системата за защита и пр.) Обикновено останалите компоненти на системата за защита действат с планираната ефективност само докато има наличие на сигнал от сензорите за алармено събитие. При прекъсване на този сигнал или останалите компоненти на системата преустановяват действието си, или техните действия са със значително по-ниска ефективност[3,4,5].

Очевидно в този аспект вероятностите за правилно откриване и за лъжлива тревога са моментни събития, и те не могат да се използват непосредствено като обобщени функционални показатели за качеството на сензорните системи.

### **Изложение:**

В общия случай сензорите са предназначени да формират алармен сигнал при появяване на даден обект (цел) в зоната на действието им, като този сигнал се използва от останалите системи или устройства за осъществяване на някакво въздействие върху целта. За успешно осъществяване на това въздействие е необходимо аларменият сигнал да се появи със закъснение, чиято стойност да не по-голяма от предварително зададена ( $T_{гр}$ ) и да съществува непрекъснато за период от време, което да е не по-малко от предварително зададено ( $t_{арп}$ ). Граничните стойности  $T_{гр}$  и  $t_{арп}$  се определят в зависимост от типа и характера на конкретните системи и устройства които са потребители на информацията от сензорите и най-често зависят от тяхната инерционност.

Един широк клас сензори работят в дискретен режим, като анализират сигналите от околната среда в последователни интервали (цикли) от време  $\Delta t$  [1,2,3]. Те обикновено използват логика за формирането на алармения сигнал при наличие на откривания на цел в  $n$  последователни цикъла за вземане на решение (обозначавана като  $k/n$ ) и логика за прекратяване на алармения сигнал при наличие на  $l$  броя отсъствия на данни за цел в  $m$  броя последователни цикли (обозначена като  $l/m$ ) [1,2]. Стойността на  $n$  е дължината на паметта на логиката за инициране на аларменото събитие,  $k$  е минималното време на закъснение на неговото появяване (минималната инерционност на сензора), а  $l$  е минималната продължителност на алармения сигнал. Често, за опростяване на техническите решения, в сензорите се приемат стойности на  $k$  равни на  $n$  и стойности на  $l$  равни на  $m$ , т.е. логики за инициране и за преустановяване на алармения сигнал от типа  $k/k$  и  $l/l$  [2,4,5].

В болшинството от случаите може да се приеме, че решенията в отделните цикли са независими случайни величини, като за даден  $i$ -ти цикъл вероятността за откриване на цел можем да обозначим с  $p_i$ , вероятността за инициране на алармен сигнал за пръв път точно в този цикъл – с  $P_i$ , а вероятността за прекратяване на алармения сигнал за пръв път точно в този цикъл – с  $Q_i$ .

При условие, че логиците за инициране и за прекратяване на аларменото събитие са независими и при логика за прекратяване от типа «отсъствие на данни за цел в  $l$  броя последователни (т.нар.  $l/l$ )», то вероятностите за прекратяване на аларменото събитие точно в даден цикъл ( $Q_i$ ) може да се изчисли чрез следните формули [3]:

$$(1) \quad Q_1 = P q_1$$

където произведението е за  $i$  от 1 до  $l$ ;  $q_i = 1 - p_i$ .

$$(2) \quad Q_{l+1} = p_1 P q_1$$

където произведението е за  $i$  от 2 до  $l$

$$(3) \quad Q_f = p_1 Q_f^{-1} + q_1(p_2 Q_f^{-2} + q_2(p_3 Q_f^{-3} + q_3(p_4 Q_f^{-4} + \dots + q_{(l-2)}(p_{(l-1)} Q_f^{-(l-1)} + q_{(l-1)} p_l Q_f^{-l}))) \dots)$$

където  $f \geq (l+1)$ ;  $Q_f^z$  е функцията  $Q_f$  изчислена за  $z$  цикъла предшестващ  $f$ -тия,  $Q_f^z = 0$  при  $z < 1$ .

Ако логиката за прекратяване на алармения сигнал е  $1/m$ , то  $Q_f$  ще представлява вероятността за това във всички единични цикли, предшестващи  $f$ -тия целта да е открита, а във  $f$ -тия да не се открие, т.е.:

$$(4) \quad Q_f = Q^{-(f-m)}_f \text{Pr}_i$$

където произведението е за  $i = 1$  до  $(f-m)$ .

При логика от типа  $2/m$ , при отсъствие на единично решение за наличие на цел в цикъл предшестващ  $(f-m)$ -тия, то за да се прекрати алармения сигнал точно във  $f$ -тия цикъл е необходимо да има решения за наличие на цели за всички  $(m-1)$  цикли следващи този в който няма решение за цел, т.е.:

$$(5) \quad Q_f = p_1 Q^{-1}_f + q_1 Q^{-m}_f \text{Pr}_i$$

където произведението е за  $i = 2$  до  $m$ .

При логики от типа  $2/2$  и  $3/3$  изчисляването на  $Q_f$  може да се извърши чрез изразите:

$$(6) \quad Q_f = p_1 Q^{-1}_f + q_1 p_2 Q^{-2}_f$$

$$(7) \quad Q_f = p_1 Q^{-1}_f + q_1(p_2 Q^{-2}_f + q_2 p_3 Q^{-3}_f)$$

За случая на независими логики за прекратяване на алармения сигнал от типа  $1/1$  общият подход за изчисляване на  $Q_f$  е свързан с определяне на неговите стойности за  $f=2l$  и по-

следващо използване на рекурсивната Формула 3 или за разглежданите примери - формули от 4 до 7.

Нека приемем, че аларменият сигнал се е появил за пръв път в произволен  $f$ -ти цикъл. Тогава вероятността за това аларменото събитие да е с продължителност над  $t_{arp}$  се определя от това то да се прекрати за пръв път в произволен следващ цикъл, превишаващ определен граничен цикъл -  $j_{arp/f}$ , където:

$$(8) \quad j_{arp/f} = t_{arp}/\Delta t + f$$

Ако обозначим тази вероятност с  $F_{arp}$  то тя може да се изчисли като:

$$(9) \quad F_{arp/f} = \sum Q_f$$

където сумирането се извършва за всяко  $f \geq j_{arp/f}$ , т.е.:

$$(10) \quad F_{arp/f} = 1 - \sum Q_f$$

където сумирането се извършва за всяко  $f \leq j_{arp/f}$

При условие, че логиките за инициране и за прекратяване на алармения сигнал са независими и при логика за иницирането му от типа  $k/k$ , то вероятностите за прекратяване на аларменото събитие точно в даден цикъл ( $P_f$ ) може да се изчисли чрез следните формули[2]:

$$(11) \quad P_k = \prod P_i$$

където произведението е за  $i$  от 1 до  $k$ ;

$$(12) \quad P_{i+1} = q_i \prod P_i$$

където произведението е за  $i$  от 2 до  $k$ .

$$(13) \quad P_f = q_1 P_f^{-1} + p_1(q_2 P_f^{-2} + p_2(q_3 P_f^{-3} + p_3(q_4 P_f^{-4} + \dots + p_{(k-2)}(q_{(k-1)} P_f^{-(k-1)} + p_{(k-1)} q_k P_f^{-k})))) \dots)$$

където  $f \geq (k+1)$ ;

$P_f^z$  е функцията  $P_f$  изчислена за  $z$  цикъла предшестващи  $f$ -тия;

$P_f^z = 0$  при  $z < 1$ .

Ако логиката за поява на алармен сигнал е  $1/n$ , то  $P_f$  ще представлява вероятността за това във всички единични цикли, предшестващи  $f$ -тия целта да не е открита, а във  $f$ -тия да се открие, т.е.:

$$(14) \quad P_f = P^{-(f-n)} \prod_{i=1}^n P_{q_i}$$

където произведението е за  $i = 1$  до  $(f-n)$ .

При логика от типа  $2/n$ , отчитайки че при на единично решение за наличие на цел в цикъл предшестващ  $f$ -тия, за следващите  $(n-1)$  цикли трябва да отсъстват решения за наличие на цели, е приложима следната зависимост:

$$(15) \quad P_f = q_1 P^{-1}_f + p_1 P^{-n}_f \prod_{i=1}^n P_{q_i}$$

където произведението е за  $i = 2$  до  $n$ .

При логики от типа  $2/2$  и  $3/3$  изчисляването на  $P_f$  може да се извърши чрез изразите:

$$(16) \quad P_f = q_1 P^{-1}_f + p_1 q_2 P^{-2}_f$$

$$(17) \quad P_f = q_1 P^{-1}_f + p_1 (q_2 P^{-2}_f + p_2 q_3 P^{-3}_f)$$

Вероятността за това аларменото събитие да се появи със закъснение по-малко от  $T_{гр}$  се определя от това то да се появи за пръв път в произволен цикъл, по-малък от определен граничен цикъл -  $f_{гр}$ , където:

$$(18) \quad f_{\text{гр}} = T_{\text{гр}}/\Delta t$$

Ако обозначим тази вероятност с  $P_{\text{гр}}$  то тя може да се изчисли като:

$$(19) \quad P_{\text{гр}} = \sum P_f$$

където сумирането се извършва за всяко  $f \leq f_{\text{гр}}$ .

Отчитайки изискването за това времето за закъснение на алармения сигнал да е по-малко от  $T_{\text{гр}}$ , а продължителността му да е по-голяма от  $t_{\text{арп}}$ , то може да се приеме, че вероятността за изпълнение на функциите от сензора като компонент от системата или устройството (D) се определя от вероятностите в който и да е цикъл до  $f_{\text{гр}}$  да се инициира алармен сигнал, след което той да съществува за не по малко от  $f_{\text{арп}}$  броя цикли, т.е.:

$$(20) \quad D = \sum P_f F_{\text{арп}/f} = \sum P_f \sum Q_f$$

където първото сумиране се извършва за всяко  $f \leq f_{\text{гр}}$ , а второто – за  $f \geq j_{\text{арп}/f}$ .

В редица случаи с достатъчна за практиката точност може да се приеме, че вероятностите за откриване на цели в единичните цикли са приблизително еднакви (т.е.  $p_i \approx \text{const} = p$ ), като тогава формули 1-19 се опростяват значително. В частност те добиват вида:

$$(21) \quad j_{\text{арп}/f} = \text{const} = j_{\text{арп}} = t_{\text{арп}}/\Delta t, \text{ или}$$

$$(22) \quad F_{\text{арп}/f} = 1 - \sum Q_f = \text{const} = F_{\text{арп}}$$

където сумирането се извършва за всяко  $f \leq j_{\text{арп}/f}$ .

Отчитайки горното, Формула 20 добива вида:

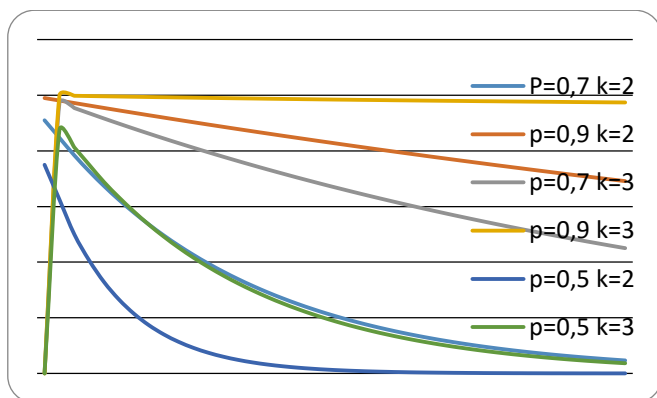
$$(23) \quad D = F_{\text{арп}} P_{\text{гр}}$$



където първото сумиране се извършва за всяко  $f \leq f_{гр}$ .

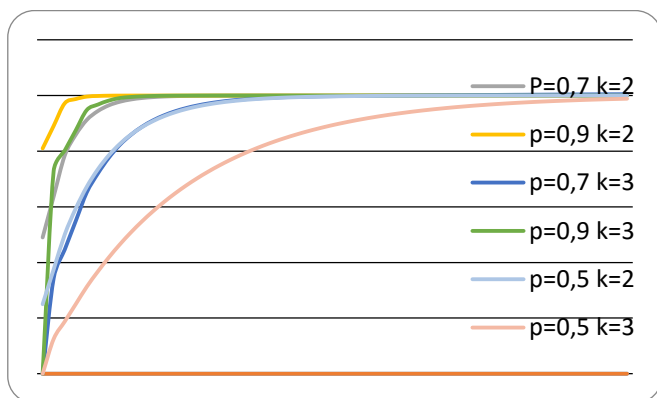
От Формула 23 следва, че при  $p_i \approx \text{const}$  е възможно при зададени  $j_{агр}$  и  $f_{гр}$  да се изчислят  $F_{агр}$  и  $P_{гр}$ , след което да се изчисли търсената вероятност  $D$ .

На Фигури 1, 2, 3, 4 и 5 са показани стойностите на вероятността  $F_{агр}$ ,  $P_{гр}$  и  $D$  при логики за инициране и за преустановяване на алармения сигнал от типа  $k/k$  и  $1/1$  за някои характерни стойности на  $p$ ,  $k$  и  $l$ . За удобство при онагледяването е приета зависимостта  $j_{агр} = w + f_{гр}$ , което позволява графично да се изобразят посочените вероятности като функция от един параметър ( $f_{гр}$ ), като стойностите на  $w$  са приети за равни на 0, 5 и 10.



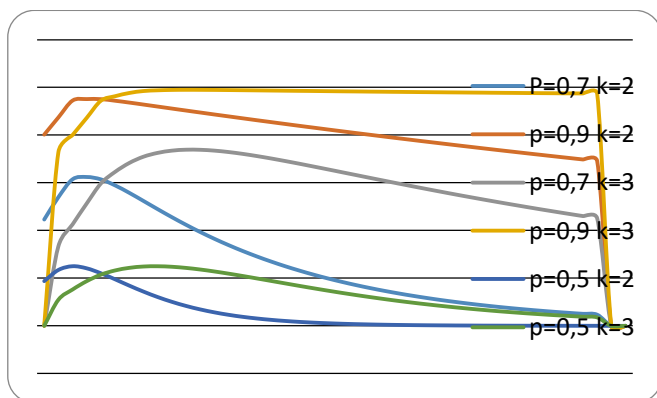
Фигура 1 Зависимост на  $F_{агр}$  от  $j_{агр}$

От Фигура 1 се вижда, че  $F_{агр}$  зависи силно от логиката за откриване и  $p$ , като при стойности на  $j_{агр}$  от порядъка на 5-10 стойността на  $F_{агр}$  се изменя два-три пъти. Вижда се също така, че стойностите на  $F_{агр}$  за логика  $2/2$  и  $p=0,7$  са близки до тези за логика  $3/3$  и  $p=0,5$ .



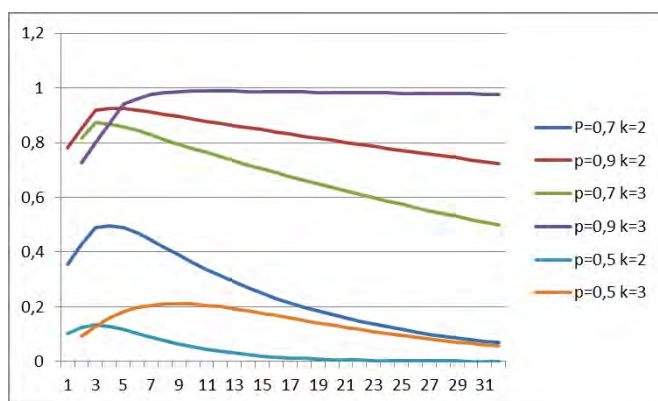
Фигура 2 Зависимост на  $P_{гр}$  от  $f_{гр}$

От Фигура 2 се вижда, че зависимостта на  $P_{гр}$  от  $f_{гр}$  при стойности на  $f_{гр}$  превишаващи 5-10 са близки за разглежданите логики, с изключение на случая за логика 3/3 и  $p=0.5$ . Забелязва се и това, че зависимостите на  $P_{гр}$  от  $f_{гр}$  за логика 3/3 и  $p=0.9$  е близка до тази за логика 2/2 и  $p=0.7$ .



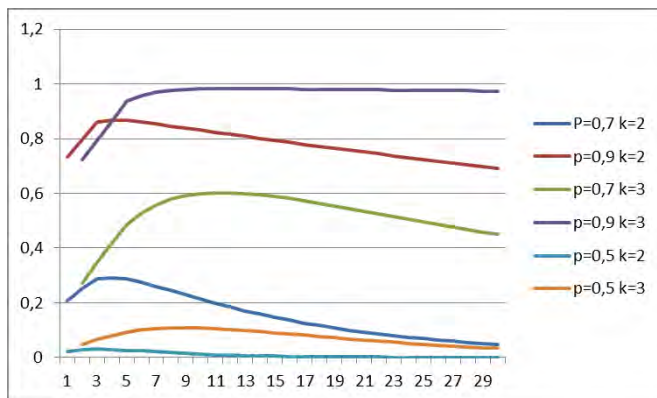
Фигура 3 Зависимост на  $D$  от  $f_{гр}$  при  $w=0$

От Фигура 3 се вижда, че ако изискването е максималното закъснение на алармения сигнал да е равно на минималното необходимо време за неговото съществуване ( $w=0$ ), вероятността за това сензорът да изпълни функциите си зависи силно както от логиките инициране и прекратяване на алармения сигнал, така и от стойностите на  $p$ . При стойности на  $p=0.9$  и за двете разглеждани логики стойностите на  $D$  са относително високи, при  $p=0.5$  те са малки. При  $p=0.7$  и стойности на  $f_{гр}$  от порядъка на 5-10 вероятността  $D$  е относително висока и е приблизително еднаква за логики 2/2 и 3/3. За по-големи стойности на  $f_{гр}$  и  $p=0.7$  се наблюдава значително нарастване на влиянието на избраните логики върху стойността на  $D$ , като логика 3/3 е по-ефективна.



Фигура 4 Зависимост на  $D$  от  $f_{гр}$  при  $w=5$

От Фигура 4 се вижда, че ако изискването е времето за неговото съществуване на алармения сигнал да е с 5 бр. цикли по-дълъг от максимално допустимото му закъснение ( $w=5$ ), се формират две области на зависимостите на  $D$  от  $f_{гр}$ . Първата, характеризираше се с относително високи стойности на  $D$ , се отнася за стойности на  $p=0.9$  и за логика 3/3 при  $p=0.7$ . За останалите случаи от разглежданите се формират зони с ниски стойности на  $D$ .



Фигура 5 Зависимост на D от  $f_{гр}$  при  $w=10$

От Фигура 5 се вижда, че ако изискването е времето за неговото съществуване на алармения сигнал да е с 10 бр. цикли по-дълъг от максимално допустимото му закъснение ( $w=10$ ), се формират две области на зависимостите на D от  $f_{гр}$ . Първата, характеризираше се с относително високи стойности на D се отнася за стойности на  $p=0.9$ . За останалите случаи от разглежданите се формират зони с ниски и средни стойности на D, като зависимостта се доближава да тази за  $w=0$ .

Разгледаните вероятностни характеристики на алармения сигнал се отнасят за случаи при които той е предизвикан от реален обект намиращ се в зоната на действие на сензора - т.е. за истински алармен сигнал. Поради стохастическия характер на решенията взимани от сензорите е възможно те да инициират и лъжлив алармен сигнал[4,5,6]. При оценка на лъжливите алармени сигнали трябва да се анализира не само вероятността за появата му за пръв път в даден цикъл (както е при определяне на времето на закъснение на истинския алармен сигнал), а и в останалия период на работа на сензора.

Нека вероятността за поява на лъжливо единично решение за откриване на цел (при липса на реална цел) за даден  $i$ -ти цикъл обозначим с  $po_i$ , вероятността за инициране на лъжлив алармен

сигнал – с  $P_{0i}$ , а вероятността за прекратяване на лъжливия алармения сигнал – с  $Q_{0i}$ .

Най-често сензорите имат системи за поддържане на постоянна лъжлива тревога[1,2,3], т.е:

$$p_{0i} \approx \text{const} = p_0$$

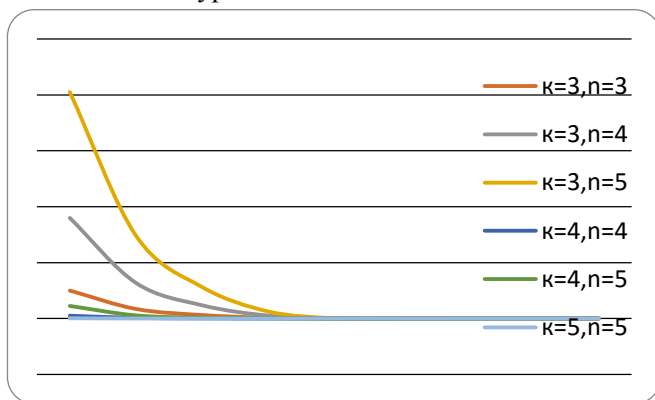
$$P_{0i} \approx \text{const} = P_0$$

При това допускане с известно приближение може да се приеме, че появата на лъжлив алармен сигнал се осъществява по схемата на Бернули, т.е.  $P_0$  може да се изчисли по известната формула за Биномния закон[4], а именно:

$$P_0 = C_{nk} p_0^k q_0^{(n-k)}$$

където  $q_0 = (1 - p_0)$ ,  $C_{nk} = n! / (k!(n-k)!) -$  биномен коефициент.

В общия случай стойности на  $n$  са от порядъка на 3-5, а  $p_0$  е под 0.1, като зависимостта на  $P_0$  от  $p_0$  за няколко типични логики  $k/n$  е показана на Фигура 6.



Фигура 6. Зависимост на  $P_0$  от  $p_0$  за някои логики  $k/n$

От Фигура 6 се вижда, че за логика на формиране на алармен сигнал  $3/4$  и  $3/5$  вероятността за появяване на лъжливо алармено събитие е значително по-висока от тази за другите разглеждани логики. Във всеки от разглежданите случаи обаче тази вероятност е по-малка от  $0.01$ , а при  $p_0$  от порядъка на  $0.03$  и по-малка вероятността за появяване на лъжлив алармен сигнал е по-малка от  $0.001$ . Ето защо определянето на логиките за инициране на алармен сигнал и на методите за поддържане на постоянната лъжлива тревога в единичните цикли на работа на сензорите трябва да са взаимосвързани.

Общият брой на циклите на работа на сензора в рамките на един период на неговото активиране ( $N$ ) би могъл да се изчисли като:

$$N = T/\Delta t,$$

където  $T$  е продължителността за активиране на сензора.

При  $T$  от порядъка на няколко часа до няколко денонощия и  $\Delta t$  - от порядъка на единици секунди до няколко микросекунди, то  $N$  е от порядъка на няколко десетки хиляди до няколко стотин милиона (в някои случаи и повече).

Ако разгледаме последователността от  $n$  последователни цикли в рамките на които се взема решение за появяване на алармен сигнал, то отношението  $Z=N/n$  е със стойност превишаваща няколко десетки хиляди. Вероятността  $P_0$  може да се разглежда като вероятност за това в даден  $Z$ -ти сегмент от времето за работа на сензора да се появи лъжлив алармен сигнал. Казано иначе би могло да се приеме, че появяването на лъжлив алармен сигнал в рамките на  $Z$  броя сегменти на реализиране на логиката  $k/n$  е с биномно разпределение и с вероятност за реализиране равна на  $P_0$ .

Поради голямата стойност на  $Z$  и малките стойности на  $P_0$  за разглежданите сензори би могло да се твърди, че появяването на

лъжлив алармен сигнал е малко вероятно събитие, което би могло да се появи в условията на много голям брой единични експерименти. Следователно може да се приеме, че вероятността за появяване на  $r$  броя лъжливи алармени сигнали ( $Pr$ ) за периода от време  $T$  е подчинена на закона на Поасон[4], т.е.:

$$Pr = (\lambda^r / r!) \exp(-\lambda)$$

$$\lambda = ZP_0, \text{ т.е.:}$$

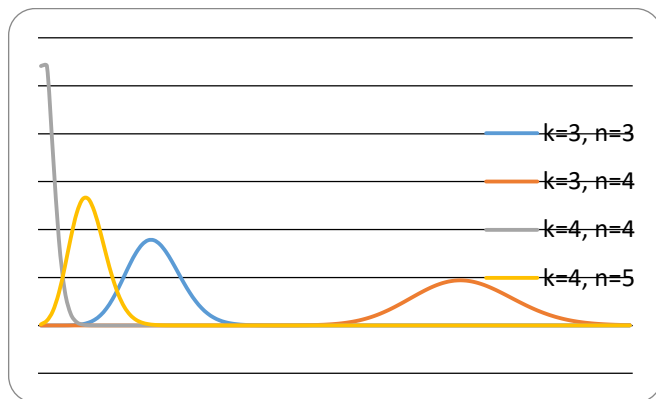
$$Pr = ((ZP_0)^r / r!) \exp(-ZP_0)$$

където  $\lambda$  е честотата на появяване на лъжлив алармен сигнал, равен на математическото очакване на биномното разпределение на лъжливите алармени сигнали за съответната логика.

На Фигура 7 е показана зависимостта на  $Pr$  от  $r$  за някои логики при  $p_0 = 0.1$  и  $Z=20000$ , което е средната му стойност за разглежданите логики (брой на  $n$ ) при  $T=24$  часа и  $\Delta t=1$  секунда

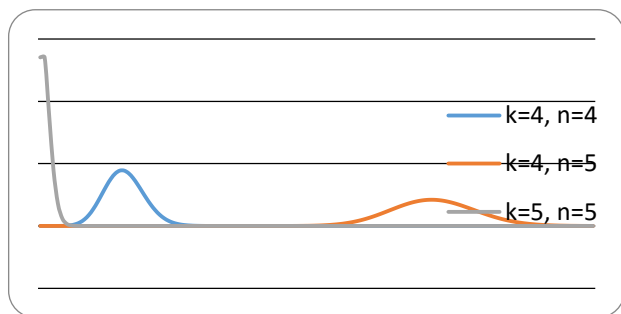
На Фигура 8 е показана зависимостта на  $Pr$  от  $r$  при същите условия за Фигура 7 и стойност на  $p_0$  и  $Z=200000$ , което е средната му стойност за разглежданите логики при  $T=24$  часа и  $\Delta t=0.1$  секунда..

На Фигура 9 е показана зависимостта на  $Pr$  от  $r$  за някои логики при  $p_0 = 0.01$  и  $Z=20000$  а на Фигура 10 - при същите условия като за Фигура 9 и  $Z=200000$ .



Фигура 7. Зависимост на  $P_\gamma$  от  $\gamma$  за някои логики,  $p_0 = 0.1$  и  $Z=20000$

На Фигура 7 се вижда, че максималните стойности на броя на лъжливите алармени събития варира от 2 (за логика 4/4) до 72 (за логика 3/4). При логика 3/5 тази стойност е 180, а при логика 5/5 тя е 0.2. Следователно за малки стойности на  $p_0$  е необходимо да се използват логики от типа  $k/k$  или логики  $k/n$ , но при  $k > 3$ .

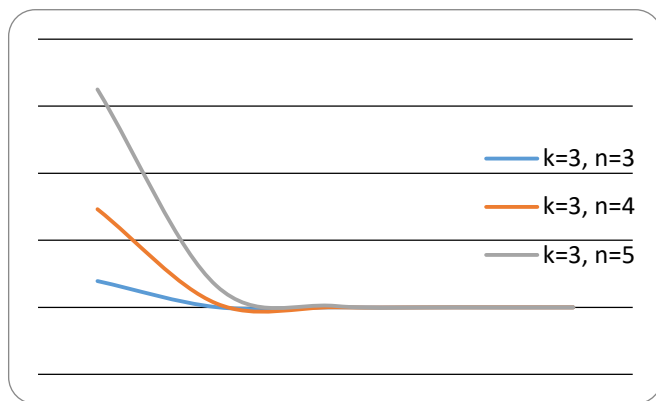


Фигура 8. Зависимост на  $P_\gamma$  от  $\gamma$  за някои логики,  $p_0 = 0.1$  и  $Z=200000$

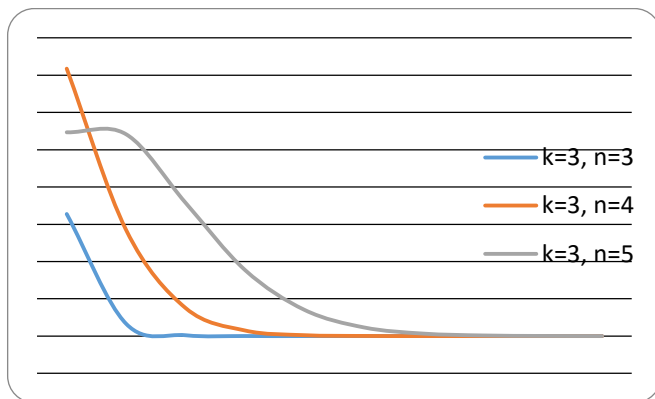


Фигура 8 показва силната зависимост на вероятността  $P_r$  от количеството на броя на условните сегменти за вземане на решения за инициране на алармен сигнал  $Z$  (т.е. от  $T$ ).

Показани са зависимостите за относително „твърди“ логики - 4/4, 4/5 и 5/5, защото при логики със стойности на  $k=3$  вероятността  $P_r$  има реално значими стойности за брой на лъжливи алармени сигнали от порядъка на десетки до хиляди, които са неприемливи за повечето сензори. Следователно при относително големи стойности на  $p_0$  (от порядъка на 0.1) и високи стойности на  $Z$  (свързани с по-дълъг период на работа на сензора или с висока честота на единичните цикли) е целесъобразно да се използват логики при които  $k > 3$ .



Фигура 9. Зависимост на  $P_r$  от  $r$  за някои логики,  $p_0 = 0.01$  и  $Z=20000$



Фигура 10. Зависимост на  $Pr$  от  $r$  за някои логики,  $p_0 = 0.01$  и  $Z=200000$

Фигура 9 показва силната зависимост на  $Pr$  от намаляването на  $p_0$ , като логики за които  $k > 3$  са свързани с пренебрежимо малки стойности на  $Pr$ .

Фигура 10 показва силната зависимост на  $Pr$  от нарастването на  $Z$ , като отново стойността на  $Pr$  за логики при които  $k > 3$  е пренебрежимо малка.

От изложеното се вижда, че изключително важно е избраната логики за откриване да гарантират появяване на лъжливи алармени сигнали под определена стойност. Най-често това изискване може да се зададе като допустима стойност на средния брой лъжливи сигнали за определен период от време (или за еквивалентната му стойност на  $Z - R_Z$ ) или на вероятността  $Pr_0$  за това броят на лъжливите алармени сигнали за даден период от време  $T$  да е по-малък от предварително зададен ( $r_0$ ).

Отчитайки, че  $Pr$  е с разпределение на Поасон, средната стойност на  $r$  (т.е.  $R_Z$ ) се определя като[4]:

$$R_Z = ZP_0 = (T P_0)/(\Delta t n)$$

Стойностите на  $R_T$  за разглежданите примери са показани в Таблица 1, от която се вижда, че при  $p_0$  от порядъка на 0.1 използването на логики от типа 3/n е нецелесъобразно, поради възможността от появяване на голям брой лъжливи алармени сигнали

Таблица 1 Стойност на  $R_Z$  за някои типични ситуации

|                | 0   | /3  | /4    | 2/5  | 1/4               | 2/5                | 4/5               | 5 |
|----------------|-----|-----|-------|------|-------------------|--------------------|-------------------|---|
| 0 <sup>4</sup> | .1  | 0   | 2     | 80   |                   |                    | .2                | 0 |
|                | .01 | .02 | .0792 | .198 | .10 <sup>-4</sup> | 9.10 <sup>-5</sup> | .10 <sup>-6</sup> | 2 |
| 0 <sup>5</sup> | .1  | 00  | 20    | 800  | 0                 | 0                  |                   | 2 |
|                | .01 | .2  | .792  | .98  | .10 <sup>-3</sup> | 9.10 <sup>-4</sup> | .10 <sup>-5</sup> | 2 |

Същевременно, отчитайки, че  $Pr$  е вероятността за поява на точно  $r$  броя лъжливи алармени сигнали, както и формули 30 и 27, за  $Pr_0$  получаваме израза:

$$P(r \leq r_0) = 1 - \sum Pr = 1 - \sum ((R_z)^r / r!) \exp(-R_z)$$

като сумирането се извършва за всички стойности на  $r$  по-големи от  $r_0$ .

По Формула 32 за разглежданите примери и за  $p_0=0.01$  стойностите за това да не се появи нито един лъжлив алармен сигнал е над 0.8 - 0.9. При стойности на  $p_0=0.1$ , за логики 4/4 и  $Z=20000$ , както и за логика 5/5 и  $Z=200000$  вероятността да не се появи нито един лъжлив алармен сигнал е едва 0.13 и чак за три лъжливи алармени сигнали тя става 0.85. В останалите от разглежданите случаи, за времето на работа на сензора, с вероятност над 0.5 ще се появяват десетки или стотици лъжливи алармени сигнали, което в повечето случаи е неприемливо.

Освен вероятностите за появяване на определен брой лъжливи алармени сигнали за периода на работа на сензорите (или за единична част от този период - напр. едно денонощие, един час и пр.) интерес представлява и продължителността на тези сигнали. Продължителността на лъжливите алармени сигнали зависи от логиките за прекратяване на алармените сигнали, което обикновено се осъществява при отсъствие на открита цел в  $l$  от  $m$  последователни цикли (т.нар. логика  $l/m$ ).

При условие, че логиките за прекратяване на аларменото събитие е от типа  $l/l$ , и при отчитане на Формула 24, то условните (т.е. при условие, че са се появили) вероятностите за прекратяване на аларменото събитие точно в даден цикъл ( $Q_{0i}$ ) може да се изчисли като [2,3]:

$$Q_{0i} = P_{q_{0i}} = q_0^l$$

където произведението е за  $i$  от 1 до  $l$ ;  $q_i = 1 - p_i$ .

$$Q_{0l+1} = p_{01} \Pi q_{0i} = p_0 q_0^l$$

където произведението е за  $i$  от 2 до 1

$$Q_{0l+1} = p_{01} \Pi q_{0i} = p_0 q_0^l$$

където произведението е за  $i$  от 2 до 2 1

$$Q_{0f} = p_{01} Q_{0f}^{-1} + q_{01}(p_{02} Q_{0f}^{-2} + q_{02}(p_{03} Q_{0f}^{-3} + q_{03}(p_{04} Q_{0f}^{-4} + \dots + q_{0(l-2)}(p_{0(l-1)} Q_{0f}^{-(l-1)} + q_{0(l-1)} p_{01} Q_0^{-1}))) \dots)$$

където  $f \geq (l+1)$ ;  $Q_{0f}^{-z}$  е функцията  $Q_{0f}$  изчислена за  $z$  цикъла предшестващ  $f$ -тия,  $Q_{0f}^z = 0$  при  $z < 1$ .

При най-често използваните логики от типа 3/3, 4/4 и 5/5 изчисляването на  $Q_f$  може да се извърши чрез изразите както следва:

$$Q_{0f} = p_{01} Q_{0f}^{-1} + q_{01}(p_{02} Q_{0f}^{-2} + q_{02} p_{03} Q_{0f}^{-3});$$

$$Q_{0f} = p_{01} Q_{0f}^{-1} + q_{01}(p_{02} Q_{0f}^{-2} + q_{02}(p_{03} Q_{0f}^{-3} + q_{03} p_{04} Q_{0f}^{-4});$$

$$Q_{0f} = p_{01} Q_{0f}^{-1} + q_{01}(p_{02} Q_{0f}^{-2} + q_{02}(p_{03} Q_{0f}^{-3} + q_{03} (p_{04} Q_{0f}^{-4} + q_{04} p_{05} Q_{0f}^{-5})))$$

На базата на горните изрази и приемайки, че е в сила Формула 24, то за изчисляване на условните продължителности на лъжливите алармени сигнали при логики на прекратяване 3/3, 4/4 и 5/5 могат да се използват формулите:

$$Q_{0f} = p_0 Q^{-1}_{0f} + q_0 p_0 Q^{-2}_{0f} + q_0^2 p_0 Q^{-3}_{0f};$$

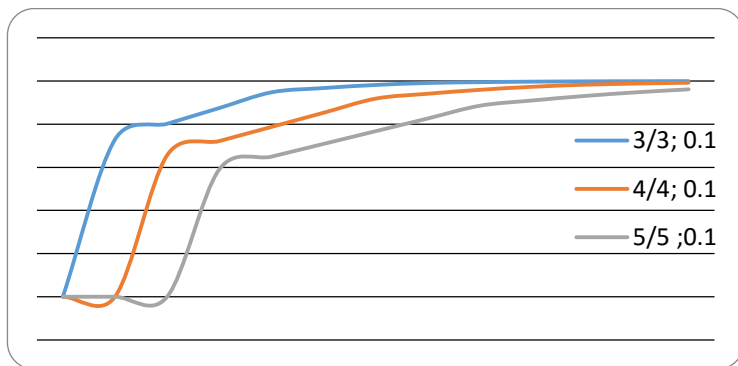
$$Q_{0f} = p_0 Q^{-1}_{0f} + q_0 p_0^2 Q^{-2}_{0f} + q_0^2 p_0 Q^{-3}_{0f} + q_0^3 p_0 Q^{-4}_{0f};$$

$$Q_{0f} = p_0 Q^{-1}_{0f} + q_0 p_0 Q^{-2}_{0f} + q_0^2 p_0 Q^{-3}_{0f} + q_0^3 p_0 Q^{-4}_{0f} + q_0^4 p_0 Q^{-5}_{0f}$$

За използването на тези формули е необходимо предварително да се изчисли  $Q_{0f}$  за  $f \leq 21$  по Формула 35, след което да се приложат рекурсивните формули 36-42.

На Фигура 11 е показан вида на  $Q_{0f}$  при  $p_0=0.1$ , от която се вижда, че условната продължителност на лъжливите алармени сигнали, дори и при малки стойности на  $p_0$ , с вероятност над 0.8 е от порядъка до 7- 8 единични цикли (от 1.72 цикъла за логика 3/3 до 2.94 цикъла за логика 5/5).

Средните продължителности на лъжливите алармени сигнали са произведението между вероятността за появяването им за съответната логика и продължителността им, т.е. за разглежданите примери те са близки до стойността от  $Q_{0f}(1+1)$  до  $Q_{0f}(1+3)$ .



Фигура 11 Условна продължителност на лъжливите алармен сигнали за някои логики при  $p_0=0.1$

### Заклучение:

Предложен е математически апарат, даващ възможност да се изчислят обобщените показатели за качеството на един клас сензори. Като такива са приети вероятността за това аларменият сигнал да се появи със закъснение, чиято стойност да не по-голяма от предварително зададена и да съществува непрекъснато за период от време, което да е не по-малко от предварително зададено. Разгледани са случаите за това подобен сигнал да е предизвикан от действителен обект (цел) или да е лъжлив, като са приети някои най-разпространени логики за работа на един клас сензори. В случай на по-сложни логики е целесъобразно процесите да се опишат с вериги на Марков, а при динамично изменение на вероятностите за откриване на целите в отделните цикли - да се приложи метода на цифровото моделиране.

Извършеният анализ за някои характерни случаи показва, че използването на логики за прекратяване на алармения сигнал от типа 3/4 и 3/5 при относително високи вероятности за лъжливо откриване в единичен цикъл (от порядъка на 0.1) е свързано с появяването на голям брой лъжливи алармени сигнали и е

нецелесъобразно. Използването на логики за прекратяване на алармения сигнал от типа 5/5 при вероятности за лъжливо откриване на обект в единичен цикъл от порядъка на 0.1 е свързано с по-голямата му продължителност. Ето защо е целесъобразно в тези случаи логиките за инициране на алармен сигнал да са от типа 4/4, а за неговото прекратяване - от типа 3/3.

### **ЛИТЕРАТУРА:**

[1] Павел П. Коцев, Николай Л. Георгиев, Павел С. Танчев, 1988 Основи на автоматизацията на управлението на противовъздушната отбрана на войските - В.А. «Г.С. Раковски».

[2] Георгиев Николай Л Време на закъснение на аларменото събитие в един клас сензори, XXIX Международна конференция “Дефектоскопия’15”, Созопол, 15-19 юни 2015г., ISSN 1310-3946

[3] Георгиев Николай Л Време на съществуване на аларменото събитие в един клас сензори, XXIX Международна конференция “Дефектоскопия’15”, Созопол, 15-19 юни 2015г., ISSN 1310-3946

[4] Gerard C.M. Meijer, 2008 Smart Sensor Systems

[5] Jerry A. Koenig and Larry Taylor, 2007 Perimeter Security Sensors Handbook for (DARPA)

[6] Jacob Fraden, 2010 Handbook of modern sensors Physics Designs, and Applications.



# ПРИЛОЖЕНИЕ НА WAVELET ФУНКЦИИТЕ ЗА СЕГМЕНТАЦИЯ НА ВИДЕОИЗОБРАЖЕНИЕ

Христо Л. Лалев, Явор И. Спасов

## APPLICATION OF WAVELET FUNCTIONS FOR VIDEO IMAGE SEGMENTATION

Hristo L. Lalev, Javor I. Spasov

**ABSTRACT:** *The segmentation of the image in the most general case is a process of image processing, with the result that the separation is carried out or breaking the image areas by taking into account the similarity of the properties of the elements of the image.*

**KEYWORDS:** *bilayer luminance segmentation with Wavelet functions*

### ВЪВЕДЕНИЕ

Изображението на физически процес или явление представлява пространствено разпределение или разпределение във времето на мощността и спектралния състав на светлинните потоци, които могат да бъдат излъчени или отразени от обекта.

Светлинният поток се описва с две функции:

-мощност –  $w(x, y, z, t)$ ;

-спектрален състав –  $\Delta(x, y, z, t)$ .

Изображението може да бъде: Полутоново (черно – бяло) неподвижно, Полутоново (черно – бяло) подвижно, Цветно неподвижно, Цветно подвижно

Полутоновото (черно – бяло) неподвижно изображение се описва само с мощността, която се оценява по яркостта  $B$ , а функцията зависи само от координатите  $(x, y)$ . [1]

$$\Delta(x, y, z, t) = \text{const}; \quad (1)$$

$$w(x, y, z, t) \rightarrow B(x, y). \quad (2)$$

Следователно при полутоновите изображения се предава само информация за яркостта.

При дискретизацията аналоговите стойности на яркостите се преобразуват в дискретни с определен брой градации, тоест това е едно аналого-цифрово преобразуване. Дискретизацията на аргументите на изображението представлява замяна на непрекъснатата функция на изображението чрез крайно множество от значения.

Едномерна дискретизация – дискретизация по време ( $t$ ) – подвижното изображение представлява поредица от неподвижни изображения (кадри) през интервал  $T_k$ .

Двумерна дискретизация – дискретизация по  $t$  (последователност от кадри) и по  $y$  (обхождане на изображението по редове).

Тримерна дискретизация – дискретизация по  $t$  (последователност от кадри), по  $y$  (обхождане на изображението по редове) и по  $x$  (всеки ред се представя чрез определен брой точки).

При дискретизацията трябва да са изпълнени следните условия:

1. Теоремата за дискретизация, където  $f_s$  е честотата на дискретизация, е максималната честота в спектъра на дискретизирания сигнал.

2. Дискретите (отчетите), които се формират при дискретизацията, представляват импулси с променлива амплитуда (амплитудата на дискретизирания сигнал в съответния момент от времето  $n\Delta t$ ). Тези импулси трябва да са с безкрайно малка продължителност.

3. При възстановяването на аналоговия от цифровия сигнал да се използва идеален нискочестотен филтър с гранична честота (НЧФ с правоъгълна характеристика).

НЧФ (—) трябва да пропуска само основния спектър.

След дискретизацията изображението се представя чрез  $N$  реда, всеки от които се състои от  $M$  точки.

1. Матрична форма – изображението се представя чрез двумерен масив от числа, отговарящи на яркостта и цветността на всяка от точките. Използва се при предаване и обработка на изображения.

2. Векторна форма – получава се от матричната чрез определен закон на подреждане на елементите от масива. Използва се при синтез, анализ и разпознаване на изображения.

3. Структурно описание – описва се структурата на изображението.

Яркостта се представя чрез  $m$  на брой нива.

$m = 2$  – бинарно (черно – бяло) изображение

$m = 256$  – полутоново изображение.

Ако изображението е цветно освен матрица за яркостта ще има и матрици за цветността – за цветовия тон и наситеността. Ако изображението е подвижно всеки кадър се описва със съответните матрици.

### ИЗЛОЖЕНИЕ

Съществуват различни методи за обработка на изображения, които се прилагат в зависимост от поставените задачи. Повечето методи могат да се прилагат както при обработка на полутонови изображения, така и при цветни изображения. Други се прилагат само върху единия от двата вида изображения (примерно цетова сегментация се прилага върху цветни изображения). Най-общо методите могат да се разделят на няколко групи, като за всяка от тях се използват различни алгоритми за обработка :

- контрастиране (подобряване на контраста);
- промяна на рязкостта на изображението (повишаване детайлностите на изображението);
- филтрация на шумовете (различни методи в зависимост от вида на шума);
- корекция на геометрични изкривявания;
- сегментиране на области с еднаква яркост или цветност;
- отделяне на контури;
- псевдоцветно преобразуване;

При някои от методите за обработка на изображение се използва хистограмата на изображението. Хистограмата показва броя на пикселите с еднаква яркост / цветност. Тя представлява интегрална характеристика за оценка на разпределението на стойностите на пикселите в изображението от статистическа гледна точка.

## АЛГОРИТЪМ ЗА ЯРКОСТНА СЕГМЕНТАЦИЯ

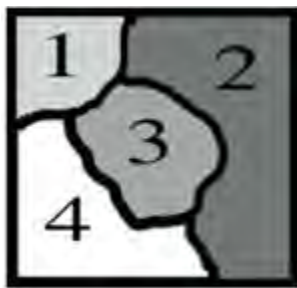
Сегментацията на изображението в най-общия случай е процес на обработка на изображението, в резултат на което се извършва разделяне или разбиване на изображението на области чрез отчитане на сходството в свойствата на елементите на изображението. Сегментацията на изображението се извършва по различни признаци. Така най-често реализираната процедура за сегментация на изображението е тази за яркостна сегментация. Сегментацията на изображението може да бъде и контурна сегментация, текстурна сегментация, сегментация по форма и други. Яркостната сегментация, приложена върху обектите в изображението, дава възможност да се извършат операции като отделяне на контура, определяне на оптическата плътност и други. [1]

Предмет на изследването е двупластова яркостна сегментация с Wavelet функции.

Изображението се разделя на области с приблизително еднакви яркости. Всеки елемент се маркира ( $\lambda_k$ ). Определят се прагове, с които се сравняват стойностите на яркост на отделните елементи на изображението

$$\theta_1 < \theta_2 < \dots < \theta_N$$

$$X(i,j) = \lambda_k, \text{ ако } \theta_k \leq B(i,j) < \theta_{k+1} \quad (k = 1 \div N) \quad (3)$$



Фиг. 1. Разделяне на области

## АЛГОРИТЪМ НА ИЗСЛЕДВАНЕ:

Първа стъпка: Отделяне на контури.

Контурът е границата между областта с различна яркост. Контурите носят основна информация за областите в изображението. Отделянето на контури се използва при анализа и разпознаването на

обекти. За да се отдели контур трябва да се вземе решение дали даден елемент принадлежи към контура или не.

Втора стъпка: Контурите се интерпретират като:

- граници на обектите;
- ръбове между отделни повърхности в сцената;
- граница между единствена осветена повърхност и сянката ѝ.

Асоциират се със скокообразно изменение или точка на прекъсване във функцията на яркостта на изображението или нейната първа производна.

За статични изображения осветеността и позицията на наблюдение са постоянни.

Трета стъпка: Въвеждане на две нива на Wavelet функция.

Основната идея при wavelet представянето се съдържа в разбиването на сигнала на две съставки - едната е груба (апроксимираща), а другата е детайлизирана и по-нататъшното им раздробяване с цел изменение на нивото на декомпозиция на сигнала. Вследствие на това непрекъснатото wavelet преобразуване използва две непрекъснати и интегрируеми по осите  $t$  (или  $x$ ) функции:

- wavelet функцията  $\psi(t)$ , за която е изпълнено

$$\int_{-\infty}^{\infty} \psi(t) dt = 0$$

и определяща детайлите в сигнала и създаваща детайлизиращите коефициенти;

- мащабиращата функция  $\varphi(t)$ , за която е изпълнено

$$\int_{-\infty}^{\infty} \varphi(t) dt = 1$$

и определяща грубото приближение на сигнала и създаваща апроксимационните коефициенти.

Ако енергията на сигнала  $s(t)$  е ограничена в пространството  $V$  на сигнала с област на ограничение  $R$ , то правото wavelet преобразуване се дефинира чрез изчислението на wavelet коефициентите от следното равенство:

$$C(a, b) = \int_R s(t) a^{-1/2} \psi\left(\frac{t-b}{a}\right) dt \quad (4)$$

Обратното wavelet преобразуване за непрекъснати сигнали се извършва чрез реконструкция във времева област по следната формула:

$$s(t) = \frac{1}{K_{\psi}} \iint C(a,b) a^{-1/2} \psi\left(\frac{t-b}{a}\right) \frac{dad b}{a^2}, \quad (5)$$

където  $K_{\psi}$  е константа, определяща функцията  $\psi$ .

В резултат на направените допускания, основна задача при wavelet преобразуването се явява реконструкцията на сигнала с достатъчна точност в зададена локална област или като цяло.

Четвърта стъпка: Дискретно wavelet преобразуване.

Поради своята сложност непрекъснатото wavelet преобразуване изисква големи изчислителни процедури, което налага при практически използвания да се извърши дискретизация на коефициентите  $a=2^j$  и  $b=k2^j$ , където  $j$  и  $k$  са цели числа, дефинирани в някакво множество  $Z$ . От своя страна wavelet функцията може да бъде представена във вида:

$$\psi_{j,k}(t) = a_0^{-j/2} \psi(a_0^{-j}t - k). \quad (6)$$

Следователно правото дискретно wavelet преобразуване (DWT) се свежда до изчислението на коефициентите  $C(a,b)$  по формула (3) с отчитане на дискретните значения на  $a$  и  $b$ :

$$C(j,k) = d_{j,k} = \int a_0^{-j/2} \psi(a_0^{-j}t - k) s(t) dt, \quad (7)$$

където  $C(j,k) = d_{j,k}$  са детайлизиращите коефициенти за wavelet -декомпозицията на сигнала за нивото  $k$ .

Обратното дискретно wavelet преобразуване (IDWT) за непрекъснататаи сигнали се задава с израза:

$$s(t) = \frac{1}{C_{\psi}} \sum_{j \in Z} \sum_{k \in Z} C(j,k) a_0^{-j/2} \psi(a_0^{-j}t - k). \quad (8)$$

В литературата се доказва, че за ортогонални wavelet-и е възможно след правото и обратното дискретно wavelet-преобразуване точно възстановяване на сигнала, наречено реставрация, с използването на допълнителната функция  $\varphi$ . В противен случай възстановяването дава сигнал близък до входния, при минална средноквадратична грешка.[2]

Кратномасштабния wavelet-анализ се базира на следните предпоставки:

- пространството на сигнала  $V$  може да бъде разбито на йерархически вложени подпространства  $V_j$ , които са непресичащи се и обединението им се извършва в границите  $L^2(R)$ ;

- за произволна функция  $s(t) \in V_j$  нейната свита версия принадлежи на  $V_{j-1}$ ;

- съществува такава функция  $\varphi(x) \in V_0$ , за която преместването  $\varphi_{0,j}(t) = \varphi(t - k)$  при  $k \in \mathbb{Z}$  образува ортонормиран базис в пространството  $V_0$ ;

От последното условие се получава, че функцията  $\varphi_{j,k}(t) = 2^{-j/2} \varphi(2^{-j}t - k)$  образува ортонормиран базис в пространството  $V_j$ . В резултат на свойствата на мащабиращата функция сигналът  $s(t)$  може да бъде представен чрез множество негови последователни приближения  $s_j(t)$  в подпространствата  $V_j$ :  

$$s(t) = \lim_{j \rightarrow \infty} s_j(t)$$
 Променливата  $j$  се нарича мащабиращ коефициент. В резултат на това апроксимацията на сигнала може да се извърши посредством следната итерационна формула:

$$s_j(t) = \sum_k C(j, k) \varphi_{j,k}(t) \quad (9)$$

където:  $\varphi_{0,0}(t) = 2 \sum_k h_k \varphi(2t - k)$ , а  $h_k$  е някаква произволна последователност.

Честотният подход дава възможност честотна област на уейвлетите да бъде разбита на две съставлящи - нискочестотна и високочестотна, които могат да се представят чрез два филтъра  $L_0$  и  $H_1$ . Това дава възможност да бъдат използвани квадратурно-огледални филтри, които се дават с основните зависимости:

$$|H(\omega)|^2 + |G(\omega)|^2 \equiv 2 \quad (10)$$

$$\overline{H(\omega)}H(\omega + \pi) + \overline{G(\omega)}G(\omega + \pi) = 0 \quad (11)$$

Анализираният кадър от изследваното видеоизображение има двумерен характер. Двумерното wavelet преобразуване може да бъде изразено като се отчете, че и по двете напавления на сигнала имаме свои собствени стойности  $a$  и  $b$ . В такъв случай вместо израза

$$a^{-1/2} \psi\left(\frac{t-b}{a}\right)$$

за едномерния уейвлет, изведен спрямо независимата променлива  $x$  получаваме следния израз за двумерния непрекъснат уейвлет:

$$\frac{1}{\sqrt{a_1 a_2}} \psi_0\left(\frac{x-b_1}{a_1}, \frac{x-b_2}{a_2}\right), \quad (12)$$

където  $V=(x,y) \in R^2$ . За двумерното дискретно wavelet преобразуване се получава:  $(j,k) \in Z^2$ ,  $a=2^j$ ,  $b=k2^j=ka$ , и  $\psi_{j,k} = 2^{-j/2} \psi(2^{-j} V - k)$ ,  $\varphi_{j,k} = 2^{-j} \varphi(2^j V - k)$ .

Използвайки квадратурно-огледалните филтри можем да получим три съставляващи уейвлета:

$$\Psi_{LH}(x, y) = \varphi(x)\psi(y) \quad (13)$$

$$\Psi_{HL}(x, y) = \psi(x)\varphi(y) \quad (14)$$

$$\Psi_{HH}(x, y) = \psi(x)\psi(y), \quad (15)$$

-където H- означава реализация на високочестотен филтър, а L- на нискочестотен филтър.

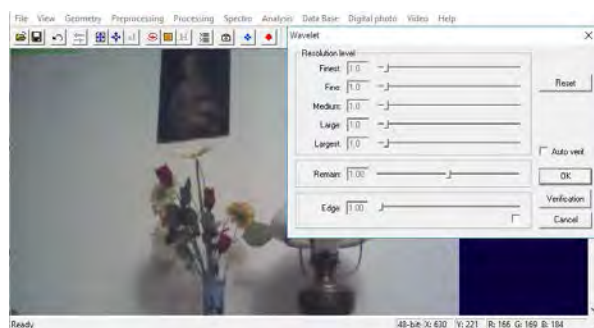
Изследването на кадрите е извършено в програмна среда Iris [3]

Въвеждане на входното (изследвано) изображение:

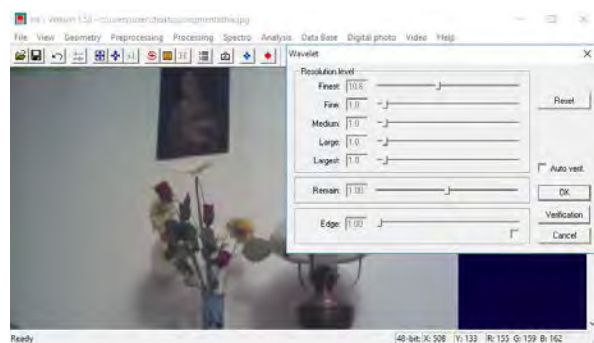




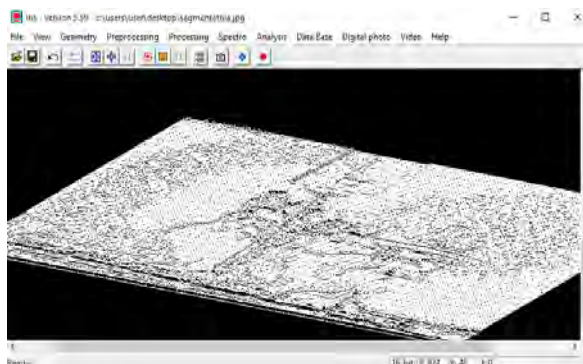
Фиг.2. Входно изображение



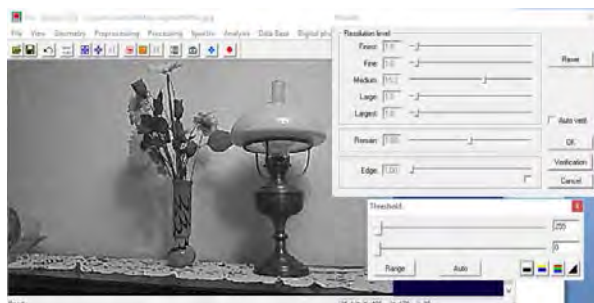
Фиг. 3 Активиране на Wavelet функция



Фиг.4. Въвеждане на fitness функция



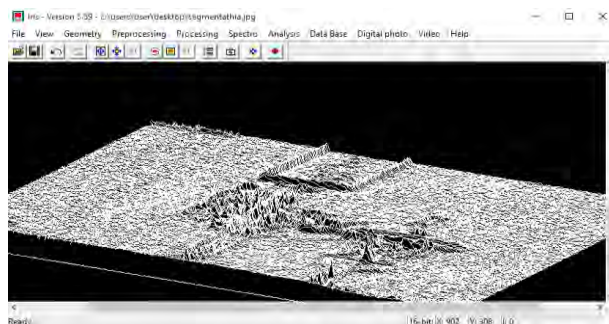
Фиг. 5. 3D изображение на сегментирания видеокадър



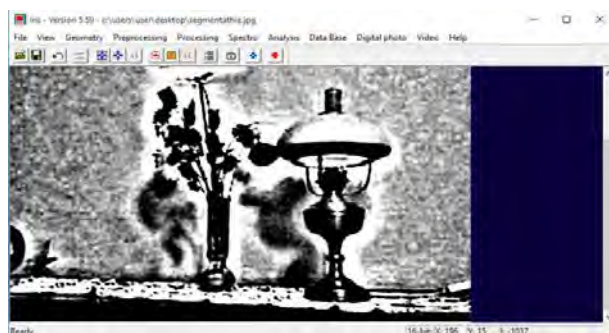
Фиг. 6. Въвеждане на 3- то ниво (medium) на Wavelet функция



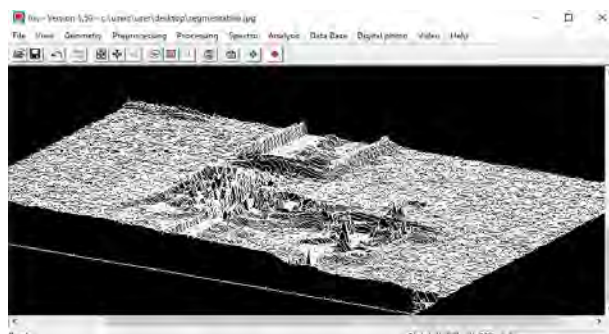
Фиг. 7. Яркостна сегментация на входното изображение



Фиг. 8. 3D изображение на сегментирания видеокадър



Фиг. 9. Яркостна двупластова сегментация на входното изображение



Фиг. 10. 3D изображение на сегментирания видеокадър

### **ИЗВОДИ:**

Приложението на двупластовото Wavelet преобразуване дава ясно очертаване на контурите на обектите на фона на сцената на заснетия видеокадър. Използването на този подход в системите за разпознаване минимизира сходимостта на алгоритмите.

### **ЛИТЕРАТУРА:**

- [1] Маринов, Б., Цифрова обработка на изображения, С., 2012 г.
- [2] Новиков Л.В. Основы вейвлет-анализа сигналов. Учеб. пособие. – СПб.: Изд. «МОДУС», 1999.
- [3] hilt: <http://www.astrosurf.com/bull>, Iris 5.9 - 2010 г.

# КОСМИЧЕСКИ ГРАВИТАЦИОННИ МИСИИ CHAMP, GRACE И GOCE- ЕДНА НОВА ЕРА НА СПЪТНИКОВА ГРАВИМЕТРИЯ

Красимира Кирилова, Андрей Андреев

## SATELLITES GRAVITY MISSIONS CHAMP, GRACE AND GOCE- A NEW ERA OF SATELLITE GRAVIMETRY

Krasimira K. Kirilova, Andrey Andreev

**ABSTRACT:** *The subject of the survey are the satellite missions in which the satellites are used like surveillance platforms and for studying different aspects of the Earth, connected with the Geodesy and Geodynamic.*

*For the first time in satellite geodesy, three gravity missions have the potential of being realized: (1) CHAMP is a low-cost mission, an intermediate step between our present knowledge and the ambitious goals that are formulated by geodesists, solid Earth geophysicists and oceanographers; (2) GRACE is planned as being a more advanced mission, especially aimed at monitoring long wavelength time variations of the gravity field; (3) GOCE will open a completely new range of spatial scales (in order of 100 km) of the geopotential spectrum to research. [5]*

*They deliver data about the fundamental force of nature and they have broad range of applications in Earth sciences.*

**KEYWORDS:** *CHAMP, GRACE, GOCE, Gravity missions, Gravity model, geoid*

Усъвършенстването на космическите технологии, не само улесниха ежедневието, но и отвориха нова глава в изследването на формата и размерите на Земята, нейната атмосфера и хидросфера. Гравитационното поле на Земята, отразявайки различията в плътността на земната кора, играе важна роля при изследването на процесите, протичащи под, на и над земната повърхност. [1] Днес, благодарение на космическите мисии, са налични високоточни гравиметрични данни за цялата земна повърхност. Започвайки от 2000г, възстановяването на погледа върху сателитното

гравитационно поле навлезе в световна „геопотенциална декада“ със стартирането на три комплементарни мисии посветени на мониторинга на гравитационното поле. Това са:

- Challenging Minisatellite Payload - **CHAMP**;
- Gravity Recovery And Climate Experiment – **GRACE**;
- Gravity field and steady state Ocean Circulation Explorer – **GOCE**;

Тези мисии имат за цел детайлното изучаване на Земята като система. Това включва изследване на гравитационното поле, на климатичните процеси, океанските течения и повърхност. Резултатите от тези мисии, се представят като модели, служещи като основа за изследване на:

- **Геосферата** - проучване на структурата на Земята и процесите, протичащи във вътрешността ѝ - от ядрото, през мантията до земната кора, както и на взаимодействието на земната кора с океаните и атмосферата;

- **Хидросферата** - за по-прецизно изследване на циркулацията на океаните, на промените в нивата на световния океан и на кратко-времените промени в глобалния воден баланс;

- **Атмосферата** - глобално проучване на вертикалните слоеве на неутралната и йонизираната газова обвивка на Земята и връзката между земния и космическия климат;

От първостепенно значение във всяка от трите мисии е определяне на статичното земно гравитационно поле и времените му вариации [2]. Мисиите реализират три основни метода за сателитна гравиметрия:

-Спътниково проследяване в режим „високо-ниско“, реализиран от мисията **CHAMP**;

-Спътниково проследяване в режим „ниско-ниско“, реализиран от мисията **GRACE**;

-Спътникова гравитационна градиометрия, реализирана от мисията **GOCE**;

### **Мисия CHAMP**

Немският сателит CHAMP (CHALLENGING Minisatellite Payload) (фиг.1) е изстрелян в орбита през лятото на 2000г. За да се осигури баланс между гравитационните и магнитните измервания спътника е изведен в почти кръгова полярна орбита (с

наклон  $87.3^\circ$ ) с първоначална височина от 454 km. Височината постепенно намалява с около 1.5 km/месец [8].



**Фиг. 1 Спътник CHAMP**

Една от главните цели на тази мисия е да подобри знанията за гравитационното поле на Земята. За тази цел спътника е оборудван с високотехнологични инструменти, двучестотен GPS приемник и триосен акселерометър. В сравнение с всички предишни спътникови мисии, използвани за статично определяне на Глобалното гравитационно поле на Земята, CHAMP има следните съществени предимства:

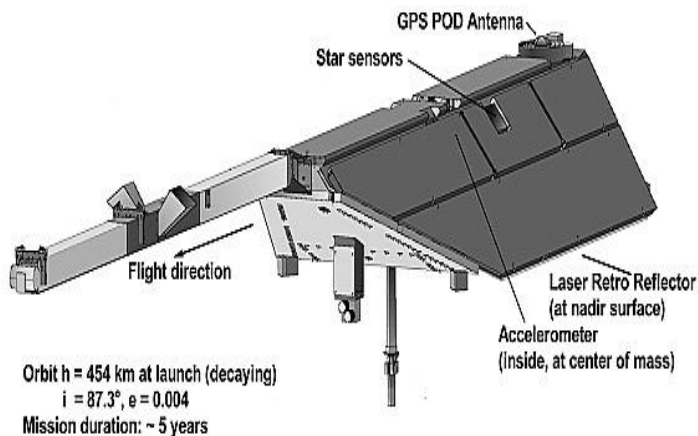
1. Сателитът непрекъснато се следи от максимум 12 GPS спътника едновременно, сравнявайки едно-дименсионално проследяване само на къси фази.

2. CHAMP изпитва усилване на гравитационния сигнал, поради ниската височина с пълно покритие на Земята, благодарение на почти кръгова орбита.

3. Директното измерване в орбита на не-гравитационни спътникови ускорения замества неудовлетворителните модели на плътността на въздуха и радиационното налягане.

Апаратурата позволява прецизно определяне на орбита дори с ниска височина на полета [Neumayer et al., 2000] и разделяне на гравитационни и не-гравитационни ускорения за изчисляване на параметрите на гравитационното поле.[4]

Схема на спътника с разположение на инструментите свързани с определяне на гравитационното поле както и характерните параметри на мисията е показана на (фиг.2).



**Фиг.2 Схема на CHAMP сателит**

Целта на CHAMP е чрез малък сателит, летящ в близка до Земята орбита, да бъдат направени измервания, които да осигурят [8]:

- високоточен модел на статичното Земно гравитационно поле и промените в него, причинени от преразпределение на масите в атмосферата, океанските течения, промените в нивото на световния океан в следствие топенето на ледовете и др. Метода, използван за гравитационните измервания, е сателитно проследяване в режим високо-ниско;

- високоточен модел на магнитното поле на Земята, определящ основното магнитно поле и това, създадено от Земната кора, както и вариациите на модела в пространство-времето;

- набавяне на информация за температурата, водните изпарения и съдържанието на електрони на база изследване на информация за рефракция на GPS сигнала при разпространението му в атмосферата и йоносферата;



На база измерванията, направени от CHAMP, са създадени няколко модела на земното гравитационно и магнитно поле, както и модел на влиянието на йоно- и тропосферата върху GPS сигнала. От съществена важност за геодезията са моделите на гравитационното поле. Те са наречени EIGEN и са развити в три поколения:

1) EIGEN-1S (European Improved Gravity model of the Earth by New techniques) - е единствения сателитен модел на гравитационно поле, който включва 88 дневно събиране на данни от CHAMP. Модела е рзвит до 100 степен и ред на сферичните хармоники:

2) EIGEN-2- второ поколение гравитационен модел, създаден единствено на база измервания от CHAMP, извършени в периода Юли-Декември 2000г. и Септември-Декември 2001г. Модела е рзвит до 120 степен и ред на сферичните хармоники. Точността на EIGEN-2 е доста под 10cm и 0.5mGal от гледна точка на геоидните височини и гравитационните аномалии.

3) EIGEN-03S-трето поколение гравитационен модел, създаден единствено на база измервания от CHAMP, извършени в периода Октомври-Юни 2000г. Модела е рзвит до 120 степен и ред на сферичните хармоники. Точността на EIGEN-2 е около 5cm и 0.5 mGal от гледна точка на геоидните височини и гравитационните аномалии.[5]

### **Мисия CRACE**

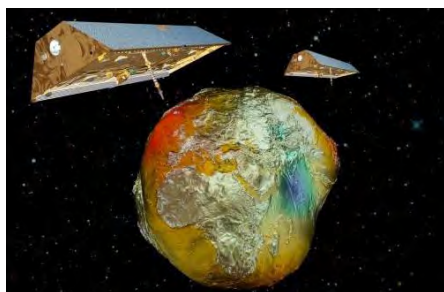
GRACE (The Gravity Recovery and Climate Experiment) е специално предназначена спътникова мисия, чиято цел е да картографира глобалното гравитационно поле с максимална точност на спектрален интервал от 500 km до 40,000 km. Високоточните измервания с високо пространствена и времева разделителна способност, позволяват да се проучат гравитационните сигнали свързани с масова обмяна между Земята и хидрологията, океана и атмосферните компоненти. Първоначалното измерване предоставено от "високоточна междуспътникова система за определяне на разстояния" (HAIRS) е в обхвата между два сателита, което позволява измерване с прецизност по-голяма от 10 микрона. GRACE осигурява

високоточни измервания на глобалното гравитационно поле веднъж на всеки тридесет дни.

Двата спътника на мисията GRACE са изстреляни в околоземна орбита на 17 Март 2002 г. от космодрума в Плесецк, Русия (фиг. 3). Първоначалната височина на орбитите е между 485 и 500 km, като е предвидено намаляването ѝ във времето, главно поради атмосферното съпротивление и слънчевата активност. Поради спецификата на метода, използван за измерване на гравитационното поле, двата спътника трябва да летят на разстояние от около 220 km един от друг. Това изисква постоянно следене на орбитите и коригирането им, когато е необходимо. Продължителността на мисията е пет години, като е възможно използването на спътниците и за по-дълъг период от време.

Основната цел на мисията е да измери гравитационното поле на Земята и вариациите му във времето с голяма точност. Поради спецификата на използвания метод за измерване на гравитацията, а именно сателитно проследяване в режим ниско-ниско, в околоземна орбита са изстреляни два спътника. Гравитационните измервания, направени от тях, са съчетани със сезонните промени в глобалния воден кръговрат (топенето на ледовете на Северния и Южния полюс и топенето на големите ледникови маси). Така GRACE предоставя и информация за промяната на формата на геоида във времето.

Второстепенна цел на мисията е да проучи Земната атмосфера, йоносфера и тропосфера.



Фиг. 3 Два спътника на мисията GRACE с изчислено Земно гравитационно поле чрез данни получени от GHAMP

Резултатите от гравиметричните измервания, направени по време на мисията са представени под формата на модели:

- Комбиниран гравиметричен модел EIGEN-5C, развит до 360 степен и ред на сферичните хармоники, съставен от измервания, направени от GRACE, LAGEOS и наземно измерени гравиметрични данни, публикуван през Септември 2008 г;

- Гравиметричен модел EIGEN-GL04S1, развит до 150 степен и ред на сферичните хармоники, съставен от измервания, направени само от сателитните мисии LAGEOS и GRACE, публикуван през Май 2006 г;

- Комбиниран гравиметричен модел EIGEN-GL04C, развит до 360 степен и ред на сферичните хармоники, съставен от измервания, направени от GRACE, LAGEOS и наземно измерени гравиметрични данни, публикуван през Май 2005 г;

- Комбиниран гравиметричен модел EIGEN-CG03C, развит до 360 степен и ред на сферичните хармоники, съставен от измервания, направени от CHAMP, GRACE и наземно измерени гравиметрични данни, публикуван през Май 2005 г;

- Комбиниран гравиметричен модел EIGEN-CG01C, развит до 360 степен и ред на сферичните хармоники, съставен от измервания, направени от CHAMP, GRACE и наземно измерени гравиметрични данни, публикуван през Октомври 2004 г;

- Втори гравиметричен модел на Земята EIGEN-GRACE02S, развит до 150 степен и ред на сферичните хармоники, отново съставен само от измервания, направени от GRACE, публикуван през Август, 2004 г;

- Първи гравиметричен модел EIGEN-GRACE01S, съставен само от измервания, направени от GRACE, публикуван през Юли 2005 г; [9]

### **Мисия GOCE**

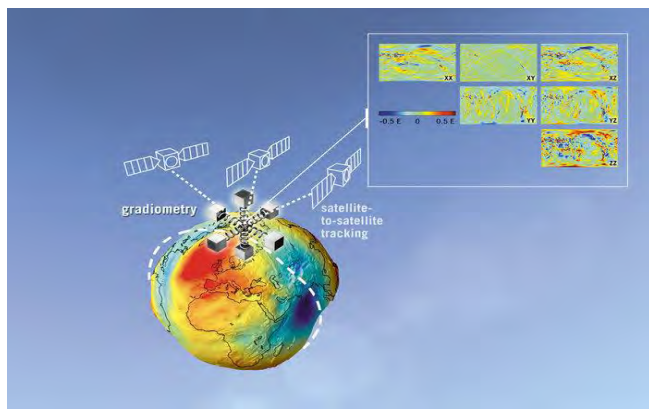
GOCE е първата сателитна мисия, която използва понятието градиометрия „gradiometry”. Сателитна градиометрия е измерената разлика в ускорението на късите базисни линии между всички маси на акселерометрите вътре в спътника. С високочувствителните си акселерометри градиометричния

инструмент е способен да предостави високо ефективни първоначални гравитационни данни. По този начин ефекта от височинно зависимото намаляване на земното гравитационно притегляне е противодействано (уравновесено). Въпреки, че градиометъра е високоточен сам по себе си, той не е способен да картографира цялото гравитационно поле по всички космически скали с необходимата точност. По този начин за да преодолее това ограничение, положението на GOCE спътника се проследява от GNSS сателити с височина от 20 000 km-концепция която е известна като "високо-ниско сателит-сателит проследяване". Анализа на движението на сателитите в орбита предоставя информация за гравитационното поле причинена от феномена на едрия мащаб. Най-общо, високо-пространствената резолюция постигната от продукта GOCE геоид е съществена за определянето на стационарната океанска динамична топография и по-точна за високорезолюционно определяне на океанската циркулация. В допълнение данните от GOCE са полезни за изравнение с GPS, навигация, проучвания на континенталната литосфера и за глобално унифициране на височинни системи, позволяващи като пример-установяването на система за мониторинг на глобалното морско ниво [7].

Спътникът GOCE (фиг. 4) е изведен в орбита през март 2009.[6] Орбитата му е синхронизирана с движението на слънцето и е с наклон  $96.7^\circ$ , а височината ѝ е около 270 км.[10]



Фиг. 4 Спътника на мисията GOCE



Фиг. 5 GOCE прави шест едновременни измервания на гравитационното поле

Синхронизацията със слънцето има две цели – да повиши точността на градиометричните измервания и да осигури енергия за спътника, защото частта му, огрявана от слънчева светлина, е покрита със соларни панели. Орбитата на сателита е на максимално ниска височина от Земята, което позволява най-качествени данни за гравитацията. GOCE разполага с:

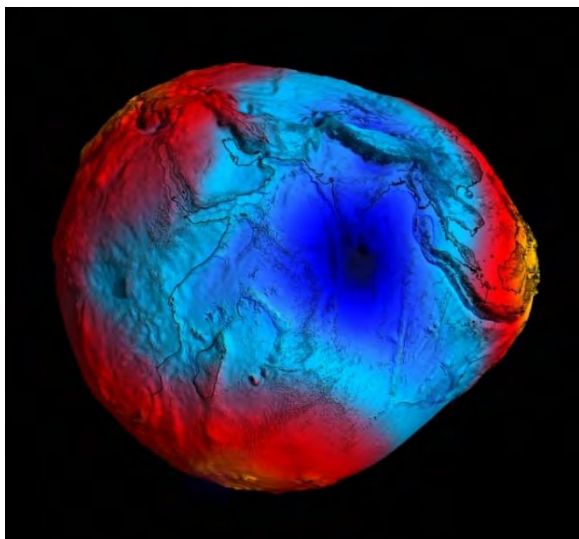
- *Триосен гравитационен градиометър*, представляващ устройство, съставено от три двойки измерители на ускорение, разположени на разстояние 50 cm един от друг в три перпендикулярни оси. Всеки измерител измерва ускорението, породено както от гравитационните, така и от негравитационните сили. При формирането на сумата и разликата на измерените ускорения между всеки два измерителя, разположени на една ос, се изчислява гравитационното ускорение и по точно вторите производни на потенциала на привличане.

- *Двучестотен GPS приемник*, следящ до 12 GPS спътника едновременно, оптимизиран за работа в ниска орбита. GPS приемника осигурява информация в реално време за положението на спътника в пространството и за скоростта му. Тя се използва както за анализиране и коригиране на орбитата, така и за извличане на гравитационни данни (фиг. 5):

- Система за контрол на височината на спътника, съставена от системата за движение на спътника „без съпротивление“, система за следене на звездите, триосен магнитометър и други сензори. От особено значение за точното определяне на гравитационното поле е системата „без съпротивление“ – специална система, осигурява постоянното „свободно падане“ на спътника около Земята, т.е. компенсираща негравитационните ускорения, действащи на спътника (основно въздушното съпротивление) и елиминирането им. Това се постига чрез измерване на не-гравитационните ускорения и компенсирането им посредством подаване на съответстваща тяга на йонната система.

Резултати от мисията са класифицирани по нива. „Ниво 0“ е „сурова“ информацията директно от сателита. „Ниво 1b“ е преработената информация от „Ниво 0“ и съдържа градиентите на полето на силата на тежестта, измерените величини при сателитното проследяване, позицията на сателита в пространството, както и данни за линейното и ъгловото ускорение на сателита и височината му. За крайния потребител е предназначена информацията от „Ниво 2“. Тя съдържа гравитационните градиенти, модели на полето на силата на тежестта и данни за прецизно определяне на орбити.

През 2011 г. благодарение на гравиметричните данни от GOCE е получен съвършен модел на "геоид" (фиг. 6). Цветовете на изображението представляват отклонения във височина (-100 m до +100 m) от идеалния геоид. Сините нюанси представляват ниските стойности, а червените / жълти представляват високите стойности. До средата на 2014 г., не по-малко от пет модела на гравитационното поле и съответно геоиди са създадени от данните на GOCE. Всяка версия е по-точна от предишната.



Фиг. 6 GOCE геоид 2011

### **Заклучение:**

За геодезията, геодинамиката и физиката на атмосферата, мисиите CHAMP (Challenging Mini-Satellite Payload for Geophysical Research and application), GRACE (Gravity Recovery and Climate Experiment), GOCE (Gravity field and Ocean Current Explorer) са от важно значение. Те допринасят за изучаване на гравитационното поле на Земята, атмосферата и океана. Всичко това показва една от основните тенденции в космическата геодезия – превръщането и в много важна съвременна интердисциплинарна наука за изследване на Земята. [3]

### **ЛИТЕРАТУРА:**

1. Андреев А. Съвременни методи за локално моделиране на геоида. ВТС. Шумен 2008 г.
2. Михайлов Г. Анализ и оценка на гравиметричните данни в България. София 2011г.
3. Минчев М., Здравчев И., Георгиев И. Основи на приложението на GPS в геодезията София УАСГ 2005

4. A high-quality global gravity field model from CHAMP GPS tracing data and accelerometry (EIGEN-1S)- R. Christoph, G. Balmino, P. Schwintzer, R. Biancale, A. Bode, J. Lemoine-за рхемата
5. CHAMP, GRACE and GOCE mission concepts and simulations - G. Balmino, F. Perosanz, R. Rummel, N. Sneeuw, H. Sunkel
6. GOCE: Obtaining a Portrait of Earth's Most Intimate Features - M. Drinkwater, R. Haagmans, M. Kern, D. Muzi & R. Floberghagen
7. GOCE's Measurements of the Gravity Field and Beyond – R. Floberghagen, M. Drinkwater, R. Haagmans, M. Kern;
8. <http://op.gfz-potsdam.de/champ/> - официална страница на мисия CHAM;
9. <http://www.csr.utexas.edu/grace/> - официална страница на мисия GRACE
10. <http://earth.esa.int/GOCE/> - официална страница на мисия **GOCE**



# РЕЗУЛТАТИ ОТ ГЕОДЕЗИЧЕСКИ ИЗМЕРВНИЯ И ИЗСЛЕДВАНИЯ С ИЗПОЛЗВАНЕТО НА ГНСС В РАЙОНА НА СТРУМСКАТА РАЗЛОМНА ЗОНА - СТРУМСКИЯ И КРУПНИШКИЯ РАЗЛОМ

Кирил Янчев, Андрей Андреев

## RESULTS FROM GEODETIK MEASURED AND STUDIES USING GNSS IN THE AREA STRUMA FAUL ZONE - STRUMA AND KRUPNIK FAULT

Kiril Yanchev, Andrey Andreev

**ABSTRACT:** *Aim of the study is the impact of geodynamic processes on the geodetic measurements and networks. The report presented research and analysis of local geodetic network designed to monitor the movement of the earth's crust in the Krupnik region and conducting geodetic measurements using Global Navigation Satellite Systems (GNSS). The results compared with the previous and subsequent measurements will help to obtain comprehensive reliable picture of the event and the nature of modern crustal movements in the area.*

**KEYWORDS:** GNSS, GPS, БГС2005.

Една от най-активните в геодинамично отношение области на Северно-Егейската сеизмична зона е Югозападната част на територията на България, Струмската разломна зона и в частност районът на пресичането на Струмския и Крупнишкия разломи. Безспорно това не може да не привлече интересът на различни специалисти от Науките за Земята в тяхното изследване, в това число и на геодезистите. Началото на геодезическите изследвания тук започва през 1970г., с ново нивелиране на част от първокласната нивелачна линия Доспат-София за установяване на съвременни активни главни и второстепенни разломи и съвременните вертикални движения по тях. След това

изследванията се разширяват и задълбочават с изграждане на цялостен геодинамичен полигон в района на пресичане на Крупнишкия и Струмския разломи, с привличане на нова съвременна електронна и спътникова техника за геодезически цели и интегрирането на резултатите в комплексните изследвания на района. Определянето може да стане разделно за хоризонталните и вертикалните или едновременно за тридименсионалните премествания и то с висока точност, особено при използване на съвременната електронна геодезическа техника за измерване и най-вече ГНСС [1].

## 1. Описание на обекта

Измерванията са проведени в участъка на пресичането на Струмския и Крупнишкия разломи на построената през 1983г., от БАН - Лаборатория по геотехника, локална прецизна тридименсионална мрежа. Мрежата обхваща площ от около 16  $km^2$  и се състои от 16 точки. Те са стабилизирани със стълбове за наблюдение, имащи устройства за принудително центриране и нивелачни болтове от страни. Средната дължина на страните е 800 - 900m. При някои от точките са налице стръмни визури поради големите превиишения. Надморската височина на която е разположена мрежата е от 250m до 800m. През 1986г. в участъци на терена, където ясно са очертани разломите са построени две малки  $M_1$  и  $M_2$  мрежи от тип геодезически четириъгълник със средна дължина на страните съответно 114 - 260m. за първата и 52 - 124m. за втората, те обхващат по отделно двата разлома. Районът е известен като епицентър на най-голямото известно земетресение за последните 200 години в Европа с магнитуд 7,8. Това е станало на 04. 04. 1904 г. и е последвано от вторичен трус с магнитуд от 7,2 [1].

След като беше направено обследване и анализ на физическото състояние на точките от локалната прецизна тридименсионална мрежа се установи, че 7 от тях са разрушени и негодни за ползване. Останалите 17 броя точки са в добро

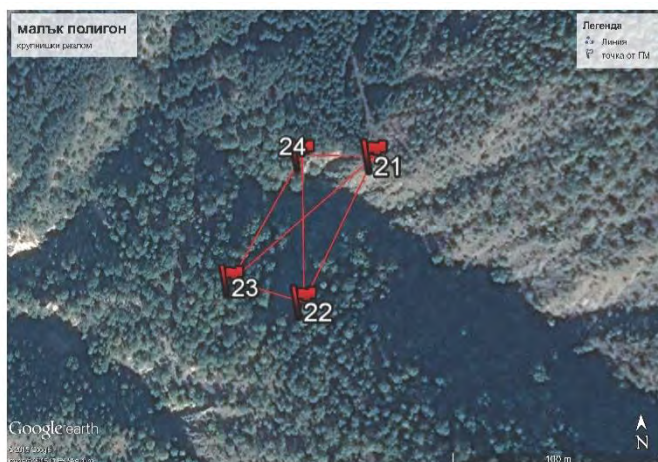
физическо състояние. Някои от точките се налага прочистване от дървесна и хростовидна растителност за осигуряване ГНСС използваемостта на станцията. Схема на геодезическата мрежа предназначена за наблюдение на движението на земната е дадена на фигура 1. Схеми на малките мрежи са дадени на фигура 2 и фигура 3.



**Фиг.1** Схема на геодезическата мрежа предназначена за наблюдение на движението на земната



**Фиг.2** Схема на полигон на Струмски разлом  $M_1$



**Фиг.3** Схема на полигон на Крупнишки разлом  $M_2$

Всички точки са разположени на здрав, защитен терен и с видимост във всички посоки над  $15^\circ$  от хоризонта, на голямо разстояние от водни басейни, стени, покриви и други местни предмети със значително отразяваща повърхност. В района няма предавателни антени, радио-магнитни, електросмущения и други излъчвания, които могат да предизвикат смущения или блокиране на сигналите на спътниците.

## 2. Провеждане на измервания с ГНСС

Всички точки от геодезическата мрежа са измерени, като са използвани 3 броя двучестотни GNSS приемници, TOPCON „HurepPRO” и 3 броя двучестотни GNSS приемници, TRIMBLE „R4” (фиг.4 и фиг.5). За определянето положението на всички точки е използван статичен метод. Наблюденията са с продължителност 6 часа и са проведени през светлата част на деня 9-17 h. Интервалът на регистрация на измерванията е 15 секунди,

минимална зададена височина над хоризонта  $10^\circ$ . Центрирането над точките е осъществено с помощта на специални конусни болтове. Височината на антената е измерена с нивелир. По време на полските измервания са водени карнети на GNSS измерванията.



**Фиг.4** Измерване с TOPCON



**Фиг.5** Измерване с TRIMBLE

## 2. Обработка на резултатите от проведените измервания

Обработката на резултатите от измерванията за определяне координатите на геодезическата мрежа е извършена с научноизследователския софтуер Bernese 5.2, в съответствие с най-съвременните концепции и стратегии в тази област, препоръчани от EUREF, а именно:

- Европейската земна координатна система ETRS89 е базирана на последната реализация на ITRF2008 (IGb08) за стабилната част на Евразийската тектонична плоча;

- обработени са всички видове наблюдения от високоточни геодезически приемници, кодови и фазови и на двете честоти;

- обработени са едновременно единичните и двойни фазови разлики с използването на йоносферни модели;

- използвани са пет линейни комбинации на честотите L1 и L2;

- в обработката са включени наблюдения от 30 перманентни европейски станции, използвани за реализацията ITRF2005 на ITRS, а именно ANKR, BUCU, GLSV, GRAZ, JOSE, ISTA, SOFI, MATE, AUT1, BACA, COST, DEVA, DRAN, DUTH, EVPA, IGEO, KTVL, KUST, LARM, MDVJ, METS, NOA1, ONSA, PAT0, PAZA, SAND, SOFA, TROY, WTZR и ZIMM;

- използвани са абсолютни модели на вариациите на антенните фазови центрове;

- за новоопределяемите точки са изведени годишни стойности на скоростите от модела NUVEL 1A, като по този начин е моделирано движението на земните станции заради тектонските движения, приливите в твърдата земна кора и океанските приливи;

- за всяка една от станциите е изведен тропосферен модел за оценка на тропосферния градиент;

- използвани са прецизни орбитни данни, както и хомогенни с орбитите координати на полюса от Центъра за извеждане на орбитите в Европа (CODE);

- при обработката са синхронизирани часовниците на всички приемници и спътници;

- използвани са различни стратегии за разрешаване и фиксиране на неопределеностите;

- моделирани са параметри, зависими от времето, чрез линейна непрекъсната функция. Приложени са при оценяване на тропосферните (и градиентни) параметри, параметрите на ориентация на Земята и извеждане на глобалните йоносферни модели;

- при разрешаване на неопределеностите са получени последователно плаващо и фиксирано решения за епохата на измерване, като в началото неопределеностите са третираны като неизвестни параметри и са оценени техните стойности като реални числа, чрез използвани по-напред статистически тестове на ковариационните им матрици.

- стратегията използвана за фиксиране на неопределеностите (Ambiguity Resolution Strategy, ARS) е т. нар. квази-йоносферна стратегия (Quasi Ionosphere Free, QIF);

- предварително координатите на станциите, участващи в решенията и полюсния модел са приведени в епохата на измерване;

- комбинирани са системите нормални уравнения от дневните решения, като получените координати на станциите са приведени към средната епоха на кампанията 28.10.2015 г. 12:00:00 часа;

- Получените средни квадратни грешки в определяне на координатите на точките са дадени в таблица 1.

Таблица 1

| № на точка | средни квадратни грешки (m) |         |         |
|------------|-----------------------------|---------|---------|
|            | U                           | N       | E       |
| 1          | 0.00153                     | 0.00037 | 0.00031 |
| 6          | 0.00094                     | 0.00026 | 0.00022 |
| 7          | 0.00108                     | 0.00028 | 0.00024 |
| 11         | 0.00100                     | 0.00027 | 0.00023 |
| 12         | 0.00094                     | 0.00026 | 0.00022 |

|    |         |         |         |
|----|---------|---------|---------|
| 13 | 0.00099 | 0.00027 | 0.00023 |
| 14 | 0.00093 | 0.00025 | 0.00022 |
| 15 | 0.00150 | 0.00034 | 0.00037 |
| 16 | 0.00105 | 0.00027 | 0.00025 |
| 17 | 0.00241 | 0.00062 | 0.00066 |
| 18 | 0.00160 | 0.00045 | 0.00035 |
| 19 | 0.00167 | 0.00035 | 0.00042 |
| 20 | 0.00191 | 0.00038 | 0.00050 |
| 21 | 0.00184 | 0.00033 | 0.00038 |
| 22 | 0.00237 | 0.00036 | 0.00050 |
| 23 | 0.00186 | 0.00038 | 0.00043 |
| 24 | 0.00136 | 0.00031 | 0.00032 |

- получените координати в епохата на реализацията са трансформирани към изходната координатна система ETRS89, на която е базирана БГС2005. Така получените координати са хомогенни с БГС2005 и са реализирани чрез ETRS89, реализация ITRF2005, eph. 2005.0; [2]

### **Заклучение:**

Измерванията за изследването чиято цел е да се определи влиянието на геодинамичните процеси върху геодезическите измервания и мрежи са проведени в един от най-невралгичните геодинамични райони в страната - пресичането на Струмския и Крупнишки разломи.

Получените резултати сравнени с предишни и следващи измервания очертават възможности и са от съществено значение за получаване на цялостна достоверна картина за проявата и характера на съвременните движения на земната кора в района. Те



са важен принос в комплексното изучаване на район с особено научно, социално и обществено значение и тяхното продължаване е безусловно необходимо.

### **ЛИТЕРАТУРА:**

1. Милев Г. "Обобщение на резултатите от геодезическите измервания и изследвания в района на Крупник"
2. Михайлов Г. "Отчет за извършени дейности по поддръжката на ДГМ 1012-1014 Г."

# **ГОДИШНИК**

**НА ШУМЕНСКИЯТ УНИВЕРСИТЕТ  
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“**

**ТЕХНИЧЕСКИ НАУКИ**

**T. V E**

**Формат 16/80/84**

**ISSN 1311-834X**

Университетско издателство  
“Епископ Константин Преславски“ 2016