ГОДИШНИК

НА ШУМЕНСКИЯТ УНИВЕРСИТЕТ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

ТЕХНИЧЕСКИ НАУКИ

Т. IV Е

ANNUAL

OF KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN

Vol. IV E

FACULTY OF TECHNICAL SCIENCES

Универистетско издателство
“Епископ Константин Преславски“ 2014

Настоящият годишник съдържа доклади изнасяни през 2013 от преподавателите във Факултета по технически науки

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

ISSN 1311-834X

Съдържание

АДМИНИСТРАТИВНО-ТЕХНИЧЕСКИ АСПЕКТИ НА НАЗЕМНОТО ЦИФРОВО ТЕЛЕВИЗИОННО РАДИОРАЗПРЪСКВАНЕ

Атанас К. Атанасов

ADMINISTRATIVE-TECHNICAL ASPECTS OF THE DISPERSAL OF GROUND DIGITAL TELEVISION.

Atanas K. Atanasov

***ABSTRACT*:** *This article is referring to the administrative and technical problems connected with introducing the digital broadcast television to Bulgaria.*

KEYWORDS: *digital, television, broadcast*

Общ преглед на състоянието, въвеждането и развитието на наземното цифрово телевизионно радиоразпръскване (DVB-T)

В световен мащаб в различните райони са разработени и се използват няколко стандарти за цифрова ефирна телевизия. В Европа са избрани стандартите DVB-T и DVB-T2; в Северна Америка и Корея стандартът е ATSC ; в Япония и Латинска Америка стандартът е ISDB-T ; в Бразилия стандартът е SBTVD/ISDB-Tb ; в Китай стандартите са DMB-T/H ефирно/мобилно, ADTB-T и DMB-T ; стандартът в Корея е T-DMB.

Като стандарт за ефирна цифрова телевизия в Европа е избран стандартът DVB-T. Този стандарт се характеризира с честота на полукадрите 50 Hz, брой на редовете 625, презредова развивка (i),

формат 16:9, и звук във формат Dolby AC-3. Използва се за предаване на аудиосигнала стандарт MUSICAM.

DVB (от английски Digital Video Broadcasting — цифрово видео предаване) — представлява семейство стандарти за цифрова телевизия, разработени от международен консорциум „DVB Project“. Стандартите разработени от този консорциум се делят на групи по област на използване, като всяка група използва съкратеното наименование DVB. Стандартите DVB са стандартизирани от Европейския институт за телекомуникационни стандарти (ETSI). Някои от тези стандарти DVB са свързани със стандартите за компресиране на видеосигнали MPEG-1, MPEG-2 и MPEG-4, които определят вида на използвания комуникационен канал и начините за компресия в цифровата телевизия.

При избора на стандарта за наземно телевизионно разпръскване в България- DVB-T са били взети в предвид следните изисквания:

- системата да използва съществуващата наземна телевизионна разпръсквателна мрежа с широчина на честотната лента на канала 8 MHz (съответно 6 и 7 MHz.);
- системата да е максимално близка до DVB-S и DVB-C, което да позволи оптималното използване на приемната техника при приемането на различните варианти цифрови програми;
- цифровото наземно разпространяване да позволява приемането на програмата както със стационарна покривна антена, така и с портативна антена в сгради и извън сгради;

- системата да позволява излъчването да се осъществи с едно честотни мрежи (Single Frequency Networks - SFN) със синхронно предаване на цифровия поток;
- да е възможно използването с йерархична модулация.

На втората заключителна сесия на Регионалната радиоконференция на Международния съюз по далекосъобщения за планиране на наземно цифрово радио- и телевизионно радиоразпръскване, състояла се през 2006 г. в Женева, е подписано „Регионалното споразумение Женева 2006 г.“ С него е утвърден „План Женева – 06“ за въвеждане на наземно цифрово радио- и телевизионно радиоразпръскване в честотните обхвати 174-230MHz и 470-862 MHz., състоящ се от цифров и аналогов план за разпределение на честотите. „План Женева – 06“ представлява основа на прехода от наземно аналогово към наземно цифрово телевизионно радиоразпръскване. Заключителните актове на Регионалната радиоконференция за планиране на службите за цифрово наземно радио- и телевизионно радио-разпръскване са утвърдени с Решение № 534 от 6август 2007 г. на Министерския съвет, в сила от 17 юни 2007 г. Разпоредбите на споразумението влизат в сила от 17 юни 2006 г., когато започва и преходният период, в който може да се излъчва както аналогова, така и цифрова телевизия. За регистрираните в аналоговия план честотни назначения за телевизионно радиоразпръскване е предвидена защита в рамките на преходния период с оглед осъществяването на плавно въвеждане на наземното цифрово телевизионно радиоразпръскване. Институциите на ЕС – Европейският парламент, Съветът на Европейския съюз и Европейската комисия, провеждат целенасочена политика за повсеместно въвеждане на наземно цифрово телевизионно

радиоразпръскване в държавите членки още от 90-те години до сега, включително чрез приемане на редица актове в тази област, както и Стратегията на ЕС „Европа 2020“ като стратегически документ. С резолюция на Европейския парламент от 16.11.2005 г. се препоръчва на държавите – членки на Европейския съюз, до началото на 2012 г. окончателното спиране на наземната аналогова телевизия. В заключения на Съвета на ЕС от декември 2005 г. относно ускоряване на прехода от наземно аналогово, към наземно цифрово телевизионно радиоразпръскване, държавите членки се приканват да приключат този процес до 31 декември 2012 г. През 2007 г. в своя резолюция от 13.11.2007г. Европейският парламент поддържа становището, че успешното преминаване в най-кратки срокове от наземно аналогово към наземно цифрово телевизионно радиоразпръскване трябва да е приоритет, и изразява безпокойството си във връзка с възможното закъснение по отношение спазването на крайния срок – 2012 г.

Държавите членки, които още не са приключили цифровия преход, се приканват да потвърдят поетия ангажимент за ефективно изключване на наземното аналогово телевизионно радиоразпръскване, като приемат предложения краен срок за Европейския съюз – 1 януари 2012 г., и предприемат необходимите подготвителни мерки. Съгласно Препоръка 2009/848/ЕО5 държавите членки следва да предприемат всички необходими технически мерки, за да се гарантира, че всички услуги за наземно телевизионно радиоразпръскване ще се предлагат чрез цифрова технология на предаване и ще прекратят използването на аналогова технология на предаване на тяхната територия до 1 януари 2012 г. Предвижда се до 1 януари 2013 г. държавите членки да предоставят радиочестотния обхват 800 MHz. (радиочестотната лента

790-862 MHz.) за електронни съобщителни услуги в съответствие с хармонизираните технически условия, установени съгласно Решение № 676/2002/ЕО7 и по-специално в съответствие с разпоредбите на Решение 2010/267/ЕС. В тези държави членки, в които изключителни национални или местни условия биха попречили на използването на тази честотна лента, Европейската комисия може да разреши специфични отстъпки до 2015 г. В съответствие с Решение 243/2012/ЕС за първата програма за политика в областта на радиочестотния спектър Република България ще продължи да използва своя радиочестотен спектър за целите на обществения ред, обществената сигурност и отбраната, докато системите, съществуващи във въпросната радиочестотна лента, излязат от експлоатация. Това се дължи на усилията, които положи българската държава при изготвянето на документа. От своя страна Европейският институт по стандартизация в далекосъобщенията (ETSI) и Европейският съюз по радиоразпръскване (EBU) са публикували голям брой документи (стандарти, спецификации, препоръки и др.) по отношение на параметрите и начините за използване на апаратните и програмните технически средства за наземно цифрово телевизионно радиоразпръскване.

Наземно цифрово телевизионно радиоразпръскване в държавите – членки на ЕС

В Европа процесът на цифровизация на наземното телевизионно радиоразпръскване стартира още през 1998 г. и следва различен ход в отделните страни. В някои държави преходът протича стъпаловидно, като например в Швеция е имало 5 фази между 2005 г. и 2007 г. или във Великобритания – 14 заключителни фази от 2008 г. до 2012 г. в различните региони. В други случаи цялата страна преминава

към наземно цифрово телевизионно радиоразпръскване наведнъж, като примери за това са Финландия през септември 2007 г. или Словения през декември 2010 г. Към края на 2011 г. в 17 държави – членки на ЕС, преходът към наземното цифрово телевизионно радиоразпръскване е приключил и всички аналогови предаватели са изключени.

От държавите – членки на ЕС, по-късни дати за преустановяване на наземното цифрово телевизионно радиоразпръскване са заложили: България (от 1 септември 2013 г.), Гърция (2013 г.),Полша (2013 г.) и Румъния (2015 г.). Съседните на България страни са планирали дати за изключване на аналоговите телевизионни радиопредаватели: Сърбия – 2012 г., Румъния – 2015 г.

Цели на прехода и въвеждането на наземното цифрово телевизионно радиоразпръскване(DVB-T). Цел на Плана за въвеждане на наземно цифрово телевизионно радиоразпръскване(DVB-T) в Република България (План 2012)

Главна цел при въвеждането на наземното цифрово телевизионно радиоразпръскване е ефективно и ефикасно използване на радиочестотния спектър, осигуряване на по-добро качество и програмно разнообразие, както и предоставяне на допълнителни услуги за потребителите. Преходът от наземна аналогова към наземна цифрова телевизия има и няколко допълнителни цели:

- да осигури свободен достъп до цифровите версии на обществените и търговските доставчици на аудио-визуални медийни услуги;
- да запази тези зрители, които и в момента приемат наземно телевизионен сигнал;

- да бъдат информирани семействата в Република България, за да имат възможност за техническа подготовка за прехода към наземно цифрово телевизионно радиоразпръскване и преустановяването на наземното аналогово телевизионно излъчване.

Приемането на наземно цифрово телевизионно радиоразпръскване, както и аналоговото наземно телевизионно радиоразпръскване, е алтернатива на приемането от спътникови и кабелни мрежи по следните показатели:

– цена – програмите, излъчвани от предаватели за наземно цифрово телевизионно радиоразпръскване, трябва да са свободни (не криптирани) и съответно безплатни за приемане от зрителите в случай че има криптирани програми, то в рамките на Първия етап техният брой да е ограничен;

– атрактивност на програмите – възможен подход е в националните програми да се предават и местни програми;

– допълнителни услуги – по този параметър наземното цифрово телевизионно радиоразпръскване трудно се конкурира с цифровите кабелни мрежи и IPTV, особено при цифровизиране на кабелните мрежи;

– мобилно приемане и портативно приемане в сгради – сферата, в която наземната телевизия е без конкуренция.

Конкретните задачи на прехода са:

- своевременно информиране на населението с ясна и ефективна кампания относно предимствата на наземното цифрово телевизионно радиоразпръскване

спрямо аналоговото наземно телевизионно радиоразпръскване и начините за приемането му;

- осигуряване на достъп на населението до програми, разпространявани чрез наземното цифрово телевизионно радиоразпръскване;
- освобождаване на заетия за нуждите на Министерството на отбраната спектър в зависимост от осигуряване на финансов ресурс в рамките на бюджета на Министерството на отбрана за съответната година;
- осигуряване на възможност за снабдяване на населението с крайни декодиращи устройства.

Основната цел на План 2012 е да осигури предвидим и плавен преход от наземно аналогово към наземно цифрово телевизионно радиоразпръскване, като от 1 септември 2013 г. България преминава изцяло към наземно цифрово телевизионно радиоразпръскване, което ще осигури постигането на целите на прехода, към момента на преустановяване на наземното аналогово телевизионно радиоразпръскване. Посочени са основните фактори, които биха осигурили прехода, включително необходимостта от осигуряване на свободен радиочестотен спектър, чрез хармонизирането му и в съответствие с Европейските документи, посочени в този план. Планът включва етапите, сроковете и условията за въвеждане на наземното цифрово телевизионно радиоразпръскване. В плана се предвиждат действия за ефективно и навременно информиране на населението относно въвеждането на наземното цифрово телевизионно радиоразпръскване, заменящо наземната аналогова телевизия.

Състояние на ограничения ресурс – радиочестотен спектър, предназначен за нуждите на наземното телевизионно радиоразпръскване

Наземно аналогово телевизионно радиоразпръскване

За нуждите на съществуващите мрежи за наземно аналогово телевизионно радиоразпръскване в настоящия момент се използват честоти в III обхват VHF (174-230 MHz, т.е. 7 телевизионни канала с широчина на лентата 8 MHz), IV обхват (470-574MHz, т.е. 13 телевизионни канала с широчина на лентата 8 MHz) и V обхват (574-862 MHz, т.е. 36 телевизионни канала с широчина на лентата 8MHz) UHF телевизионни обхвати. За изграждане на мрежата на Българската национална телевизия са направени 668 честотни назначения, от които 78 в IV и V телевизионни обхвата за БНТ 1, и 15 честотни назначения в IV и V телевизионни обхвата за регионални програми. За изграждане на мрежата на „БТВ Медиа Груп“ – ЕАД, са направени 672 честотни назначения, от които 664 в IV и V телевизионни обхвата. За изграждане на мрежата на „Нова Броуд кастинг Груп“ – АД, са направени 215 честотни назначения в IV и V телевизионни обхвата. За изграждане на мрежи за наземно аналогово телевизионно радиоразпръскване с местно покритие са направени 118 честотни назначения, от които 117 в IV и V телевизионни обхвата. От възможните общо 49 телевизионни канала в IV и V UHF телевизионни обхвата, 26 са заети от Министерството на отбраната, а именно канали 22, 23, 25, 36 – 38, 43 – 47, 53 – 56, 58 – 63, 65 – 69. Част от тези 26 телевизионни канала могат да се използват за определени населени места след съгласуване с Министерството на отбраната.

Съгласно План Женева 2006 г. за нуждите на наземното цифрово телевизионно радиоразпръскване се използват честоти в III, IV и V телевизионни обхвати. За Република България е осигурен радиочестотен ресурс с възможност за изграждане на 10 мрежи за наземно цифрово телевизионно радиоразпръскване с национално покритие, 31 мрежи с регионално покритие и 26 мрежи с регионално покритие за територията на градовете София, Пловдив и Варна. Необходимо е да се подчертае, че радиочестотният спектър за наземно аналогово и за наземно цифрово телевизионно радиоразпръскване е един и същ, поради което произтичат и трудностите при стартиране на наземното цифрово телевизионно радиоразпръскване, докато все още не е преустановено аналоговото излъчване. За условията в България този проблем е съществено изразен. Предвид проблемите с освобождаването на част от необходимия радиочестотен спектър от страна на Министерството на отбраната и с оглед разпоредбата на ЗЕС за издаване на разрешение за ползване на индивидуално определен ограничен ресурс – радиочестотен спектър за още една електронна съобщителна мрежа за наземно цифрово телевизионно радиоразпръскване с национален обхват, реализирането на мрежи за наземно цифрово телевизионно радиоразпръскване с регионален обхват към момента е необосновано от гледна точка на наличния радиочестотен спектър. В допълнение към горното, поради определянето на радиочестотната лента 790-862 MHz. (обхват 800 MHz.) за цифров дивидент и бъдещото използване на тази лента в съответствие с хармонизираните технически условия, установени с Решение 2010/267/ЕС, една част от мрежите, с национално и регионално покритие, за наземно цифрово телевизионно радиоразпръскване, за

които първоначално в План Женева – 06 са защитени радиочестотни назначения, няма да могат да се реализират.

С приемането на Закона за изменение и допълнение на Закона за радиото и телевизията (ЗИД на ЗРТ) (обн., ДВ, бр. 14 от 2009 г.) и Закона за изменение и допълнение на Закона за електронните съобщения (ЗИД на ЗЕС) (обн.,ДВ, бр. 17 от 2009 г.) се създадоха условия за реално стартиране на процеса за преминаване от наземно аналогово телевизионно радиоразпръскване към наземно цифрово телевизионно радиоразпръскване.

План/2008 е приет с решение по т. 24 от Протокол № 5 от заседанието на Министерския съвет на 31 януари 2008 г. План/2008 е изменен и допълнен с решение по т. 35 от Протокол № 11от заседанието на Министерския съвет на 19 март 2009 г. и с решение по т. 13 от Протокол№ 51 от заседанието на Министерския съвет на 30 декември 2009 г.

В План/2008 са подробно описани както политиката и документите на Европейския съюз в областта на въвеждането и развитието на цифровата телевизия, така и състоянието на прехода в отделните държави – членки на ЕС, към момента на изготвянето и приемането му. Посочени са предимствата на цифровата технология пред аналоговото телевизионно радиоразпръскване. Описано е състоянието на ограничения ресурс – радиочестотен спектър в Република България към 2008 г. В План/2008 са уредени основни принципи, въз основа на които следва да се осъществи преходът, поставени са стратегическите основи за изграждане на DVB-T мрежите, план-графикът за стартиране на цифровото излъчване на програмите на „островен“ принцип, изключването на аналоговите предаватели и

срокът за преустановяване на аналоговото излъчване – 31 декември 2012

Цели на провеждане на фаза на едновременно телевизионно радиоразпръскване (симулкаст)

Фазата на едновременното телевизионно радиоразпръскване (симулкаст) ще предостави достатъчно време на всички потребители да се запознаят с условията за достъп до наземно (ефирно) цифрово телевизионно радиоразпръскване, както и да предприемат мерки за осигуряване на приемането на цифровия сигнал. Едновременното излъчване започва след осигуряване на 95 % покритие на населението от търговската и обществената мрежа по Първия етап. Периодът на съвместна работа на предавателите за наземно аналогово и наземно цифрово телевизионно радиоразпръскване се ограничава до осем, но не по-малко от три месеца**.** След из-тичането на този срок предавателите за наземно аналогово телевизионно радиоразпръскване в обхвата на териториално покритие на „острова“ се изключват. Периодът за едновременното наземно аналогово и цифрово телевизионно радиоразпръскване започва от 1 март 2013 едновременно във всички „острови“. Графикът за спиране на аналоговите предаватели ще бъде изготвен от Органа по цифровата телевизия по предложение на Комисията за регулиране на съобщенията. Контролни измервания на покритието по население на мрежите за наземно цифрово телевизионно радиоразпръскване се извършва от Комисията за регулиране на съобщенията, с оглед оценка на съответствието на действителното покритие, с теоретично определеното със специализиран софтуер за планиране. Измерванията се извършват със сертифицирана и калибрирана измервателна апаратура и в съответствие с приложимите

стандарти и препоръки в областта на цифровата телевизия. Резултатите от измерванията се изпращат на Органа по цифровата телевизия.

Представители на заинтересованите страни от Първия етап на прехода могат да присъстват на контролните измервания. За тази цел Комисията за регулиране на съобщенията изпраща на заинтересованите страни (доставчици на аудио-визуални медийни услуги и предприятията от Първия етап) уведомление за графика (по дати и часове) и местата, където ще бъдат извършвани измерванията на покритието. Съставя се нарочен протокол за извършените контролни измервания, който се подписва от присъстващите заинтересовани страни. Отсъствието на поканена заинтересована страна или отказът на присъстваща заинтересована страна да подпише протокола по предходното изречение няма отношение към резултатите, констатирани от Комисията за регулиране на съобщенията

В периода от 1 септември 2013 г. до 1 ноември 2013 г. най-късно приключва съвместната работа на предавателите за наземно аналогово и наземно цифрово телевизионно радиоразпръскване (симулкаст). Комисията за регулиране на съобщенията продължава разрешенията на предприятията за наземно аналогово радиоразпръскване на телевизионни сигнали с местно покритие за срок до окончателното преустановяване на разпространението на телевизионни програми чрез наземно аналогово телевизионно радиоразпръскване в Република България. Окончателната дата за преустановяване на наземното аналогово телевизионно радиоразпръскване се определя от Органа по цифровата телевизия, отчитайки изпълнението на ангажиментите на държавата по от Плана. Взетото решение от членовете на Органа по цифровата телевизия,

съдържащо окончателната дата за преустановяване на наземното аналогово телевизионно радиоразпръскване и графика за спиране на аналоговите предаватели, се публикува на интернет страницата на Министерството на транспорта, информационните технологии и съобщенията, чиято администрация изпълнява функциите на секретариат на органа. Ангажираните в процеса органи ги вземат предвид при изпълняване на правомощията си съгласно настоящия План и приложимото законодателство. След окончателното преустановяване на наземното аналогово телевизионно радиоразпръскване в зависимост от наличието на заявен интерес или по инициатива на компетентния регулаторен орган ще се даде право на ползване на защитения в План Женева 2006 г. свободен радиочестотен ресурс за мобилни приложения, разширяване обхвата на паневропейски услуги, в съответствие с политиката на Европейския съюз за усвояване на т. нар. „цифров дивидент“. Конкретните срокове за освобождаване на спектъра, попадащ в рамките на „цифровия дивидент“, предстои да се уточнят във връзка с уведомяването на Европейската комисия, че в България тези честоти се използват за нуждите на националната сигурност и отбраната в изпълнение на разпоредбите на Решение 243/2012/ЕС за първа програма за политика в областта на радиочестотния спектър. Следва да се има предвид, че телевизионните канали, попадащи в рамките на т. нар. „цифров дивидент“, не са предвидени за изграждане на електронни съобщителни мрежи за наземно цифрово телевизионно радиоразпръскване съгласно приложение № 2 към настоящия план.

Радиочестотен спектър, предназначен за наземно цифрово телевизионно радиоразпръскване, ползван от Министерството на отбраната.

От възможните общо 49 телевизионни канала в IV (470-574 MHz.) и V (574-862 MHz.) UHF телевизионни обхвата, 26 са заети от Министерството на отбраната (МО), а именно канали 22, 23, 25, 36 – 38, 43 – 47, 53 – 56, 58 – 63, 65 – 69.

Част от тези 26 телевизионни канала могат да се използват за определени зони на обслужване, както и в отделни райони на страната след съгласуване с МО. От радиочестотните назначения за наземно цифрово телевизионно радиоразпръскване съобразно предвидения Първи етап няма телевизионни канали, заети от МО. Относно радиочестотните назначения съобразно предвидения Втори етап МО следва да освободи следните телевизионни канали: 45 и 46 за зона Благоевград; 25 и 44 за зона Бургас; 45 и 46 за зона Видин; 22 и 38 за зона Плевен; 43 за зона Пловдив; 45 за зона Русе; 38 за зона Смолян и 23 и 47 за зона Стара Загора. За освобождаването на телевизионните канали, заети от Министерството на отбраната, в хода на бюджетните процедури, считано от 2013 г. и съобразно развитието на икономическите процеси в страната, се планират финансови средства от държавния бюджет за финансиране на дейностите на министерството, свързани с хармонизиране на радиочестотния спектър. На базата на това Министерството на отбраната разработва прогнозен график за освобождаване на телевизионните канали.

Технически изисквания и специфика на цифровите технологии (технологични параметри на мрежите)

Изборът на системната конфигурация се прави в зависимост от конкретното приложение, като техническите параметри могат да варират съществено спрямо тези, заложени в еталонната конфигурация. По-долу са посочени параметри на избраната конфигурация от предприятията, получили разрешения, при MPEG-4 кодиран цифров поток. Параметри:

- Ширина на канала 8 MHz.
- Режим 8 k
- Защитен интервал 1/4
- Кодово отношение 2/3
- Модулация 64 QAM
- Вероятност на покритие по място 95 %
- Скорост на транспортния поток 19,91 Mbit/s

Изборът на вертикална поляризация на излъчване на телевизионните радиостанции е подходящ и за трите еталонни конфигурации, но ще създаде трудности за населението в периода на съвместна работа на аналоговите и цифровите предавателни станции поради факта, че се налага използването на две различни приемни антени. Същевременно е необходимо и подходящо вертикалната поляризация да бъде поетапно въвеждана. За целта е необходимо още през 2012 г. предприятията, получили разрешения за ползване на радиочестотен спектър за наземно цифрово телевизионно радиоразпръскване, съгласно Първия етап от прехода да започнат да внедряват вертикалната поляризация на излъчване на телевизионните радиостанции. Процесът на подмяна от хоризонтална към вертикална поляризация следва да се осъществява при подходящи метеорологични условия – от началото на май до октомври, координирано с

доставчиците на медийни услуги, които осъществяват наземно аналогово радиоразпръскване. През Първия етап с цел осигуряване на плавен преход за приемане на цифрова телевизия от населението аналоговата телевизия може да се излъчва съвместно с цифровата с вертикална поляризация, тъй като вертикалната поляризация е приложима както за наземното аналогово, така и за наземното цифрово телевизионно радиоразпръскване при достатъчно силен сигнал. Покритието по население, което е важен компонент от въвеждането на наземното цифрово телевизионно радиоразпръскване, следва да се осъществява от предприятията поетапно, по групи от зони на обслужване, при минимализиране на възможностите за евентуални смущения. Във връзка с промяната на поляризацията и очакваните прекъсвания на аналоговото излъчване Органът по цифровата телевизия ще обсъди графика за пренастройване на антените и възстановяване на аналоговото излъчване и списък на проблемните точки.

Важен елемент в прехода от аналогово към цифрово наземно телевизионно радиоразпръскване е наличието на пазара на съответни приемници. Големите търговски специализирани вериги за техника и отделни магазини, както и в интернет се предлагат разнообразни телевизионни приемници. Телевизионните приемници в голямата им част са с LCD и плазмени екрани. По отношение параметрите им, свързани с обработката на сигналите, съотношението на приемници със и без DVB-T е почти равно, като делът на приемниците с вграден DVB-T тунер с MPEG-4 (H.264/AVC) декодиране нараства съгласно данни на Международния съюз по далекосъобщения. На пазара се предлагат декодиращи устройства (STB – Set Top Box) с MPEG-2 и MPEG-4 декодиране и портативни активни антени за DVB-T. Осигуряването на

ефективна информационна кампания включва създаване и разпространение на информационни материали, включително аудио- и аудио-визуални клипове, и провеждане на социологическо проучване относно степента на информираност на населението за достъп до наземна цифрова телевизия и относно техническата готовност на населението за приемане на сигнала. Чрез предоставяне на ясна и леснодостъпна информация, както на национално ниво, така и на регионално, българските граждани трябва да бъдат запознати с това как ще могат да приемат ефирно (наземно) цифров телевизионен сигнал, какви са начините за приемане на телевизионен сигнал (ефирно, от сателит, по кабел, чрез мобилен достъп и др.) и коя е крайната дата за спиране на наземното аналогово телевизионно излъчване.

При организирането на информационната кампания и подготовката на клиповете е необходимо да се вземат под внимание редица елементи, като:

- осведоменост на гражданите към момента,
- тяхното разбиране за прехода и технологията,
- отношението им,
- нагласата и подготовката им за промяната
- и на последно място – техните очаквания.

За целта трябва да бъде организирана добра и разбираема информационна кампания.

Във връзка с информационната кампания авторът има определени резерви. Никъде не беше указано че ще се промени поляризацията на ЕМВ от хоризонтална на вертикална и съответно честотният диапазон. Това изисква използването на антени с вертикална поляризация и други размери на елементите (дипол и директори). При

запитване към указания електронен адрес на информационната кампания беше отговорено че “нашите специалисти ще направят проучване и ще Ви отговорят“. Отговор така и не се получи.

Входният сигналът най-напред се подлага на кодиране на източника, след това на кодиране на канала, и формираната цифрова поредица постъпва на модулатор, след което се подава на канала за пренос - спътников канал, кабелна разпределителна мрежа или наземен предавател. Кодирането на източника обхваща MPEG-2 кодирането съкращаването на цифровия поток на видео- и звуковите сигнали и формирането на транспортния цифров поток. Каналното кодиране обхваща външната защита от грешки, което се осъществява в Read Solomon-кодер, разместване на битовете и вътрешна защита от грешки чрез използването на нагъващ кодер, формираният след каналното кодиране цифров поток постъпва на модулатор, след което високочестотният сигнал се подава към канала за връзка. В приемната страна се осъществяват обратните процеси и съответно във функционалната схема на приемника има противоположни на предавателя блокове. На модулатора съответства демодулатор, на нагъващия кодер - нагъващ декодер, работещ по алгоритъма на Витерби, на блока за разместване на битовете - блок за връщане на изходния порядък на битовете, на Read Solomon кодера - Read Solomon декодер, след което възстановеният транспортен цифров поток постъпва на MPEG-2 декодер. От MPEG-2 декодера се получават видео- и звуковите сигнали, които се подават за възпроизвеждане.

При DVB-T модулацията е COFDM, което позволява да се работи в условие на многолъчево разпространяване на сигнала и при

едночестотни мрежи, а освен това се характеризира с добро използване на честотната лента на канала за пренос. Последното дава възможност в честотната лента на наземната телевизионна мрежа да се предава същия цифров поток, както в спътниковите, така и в кабелните разпределителни мрежи. При COFDM за модулиране на отделните подносещи сигнали се използва 64-QAM. Нагъващото кодиране се изпълнява от 6-разряден преместващ регистър със суматори по модул 2 в обратните връзки. Нагъващият кодер формира цифровите потоци със степен на кода $R_C = 2/3$.

След пунктиране цифровият поток постъпва на схема за вътрешно разместване на битовете. При DVB-T има два вида разместване - по-битово и по блоково. Побитовото разместването става в блокове с дълбочина 126 бита. На побитово разместване се подлага само полезната информация. Поблоковото разместване става по блокове с дължина 126 символа, като дълбочината на разместването е 48 блока при избрания режим 8К. Поблоковото разместване обхваща 48 x 126 = 6048 символа в режим 8К, т.е. разместването е в рамките на един цикъл на модулацията на подносещите в рамките на един OFDM символ. Подреждането на символите в реда, необходим за модулиране на отделните носещи сигнали, става в специален блок за подреждане на символите. В изхода на блока се формират двата цифрови потока на символите - синфазен (реален) и противофазен (имагинерен). След вътрешното разместване на битовете и символите цифровият поток постъпва на блок за подреждане на символите, след което се подава на блок за формиране на OFDM рамката. В този блок се въвеждат и съответните пилотни синхронизиращи сигнали. В следващ блок се осъществява OFDM модулацията чрез инверсно дискретно

преобразуване на Фурие. OFDM модулираният сигнал постъпва на блок за въвеждане на защитен интервал който в случая е избран 1/4, след което се подава на предавателя. От схемотехнични съображения блокът за инверсно дискретно- преобразуване функционира само с брой на носещите сигнали, равен на цяло число 2^n. Стандартът за DVB-T предвижда два режима на работа, условно означени като 2К и 8К, при които броят на носещите сигнали е:

- режим 2К: $(n_{нос})_{теоретично} = 2^{11} = 2048$;
- режим 8К:$(n_{нос})_{теоретично} = 2^{13} = 8192$.

На практика се използват по-малък брой на носещите сигнали. За предаване на полезната информация - полезния цифров поток на видеосигнала, звуковите сигнали и предаваните допълнителни данни плюс битовете за вътрешна и външна защита от грешки и битовете за синхронизация съответно са необходими следния брой носещи сигнали режим 8К - 6048 носещи сигнала. След добавяне на пилотните сигнали броят на носещите сигнали нараства при режим 8К - 6817 носещи сигнала.

Честотите на подносещите сигнали са разпределени равномерно, като отстоянието между тях се избира равно на F/n. Тук F е честотната лента на телевизионния канал -8 MHz, а n е избраният брой на подносещите сигнали. Това условие гарантира ортогоналност на съседните носещи сигнали, откъдето произтича названието OFDM на честотно мултиплексирания сигнал. Ортогоналността на следващите един след друг носещи сигнали е необходима, за да може да се припокриват спектрите на съседните модулирани сигнали, без да се смущават взаимно.

Благодарение на ортогоналността в момента на максимума на сигнала на всяка една от подносещите сигналът на всички останали подносещи сигнали е 0. По този начин, независимо от плътното разположение на спектрите на подносещите, не съществуват условия за взаимно смущение между тях. Общият спектър на OFDM сигнала е равен на сумата от спектрите на отделните подносещи.

Литература:

1.Решение №494 от 22 август 2013 г. актуализация на плана за въвеждане на наземното цифрово телевизионно разпръскване (DVB-T) в република България.

2.Конов. Цифрова телевизия. 2005 г. София.

3.Ерве Беноа. Цифрова телевизия, първо издание, 1998 г.Изд.“ЛИК“ София

АНАЛИЗ НА ПРОИЗВОДИТЕЛНОСТТА НА ПРЕНОСИМ КОМПЮТЪР, ОБОРУДВАН С ПОЛУПРОВОДНИКОВО УСТРОЙСТВО ЗА СЪХРАНЕНИЕ НА ДАННИ

ТИХОМИР С. ТРИФОНОВ

PERFORMANCE ANALYSIS OF A MOBILE COMPUTER EQUIPPED WITH SOLID STATE DISK

TIHOMIR S. TRIFONOV

ABSTRACT: *The Solid State Disks (SSD) are very popular today. The intention for very rapid research and development of these devices is to replace classic mechanical hard disk drives (HDD). The purpose of this paper is to describe the results of an analysis of a mobile personal computer upgraded with a SSD. An analysis of main advantages and disadvantages of SSDs over HDDs is made at the beginning of the paper. The main purposes for choosing a SSD as a data storage instead of a HDD are presented. At the end, the results from the performance analysis of a mobile computer is depicted.*

KEYWORDS: *Solid State Disk (SSD), Hard Disk Drive (HDD), SATA, NAND Flash, SLC, MLC, Form Factor, Read/Write performance, Reliability, Mean Time Between Failure, Annualized Failure Rate, Annualized Replacement Rate, Block Size, IOPS, Access Time, Average Access, Average speed, SMART .*

Полупроводниковият диск (Solid State Disk – SSD) се разработва с цел да замени твърдия диск – един доста уязвим детайл в преносимите компютри. Устройството на SSD е следното: в метален или пластмасов корпус е поместена печатна платка, върху която са разположени определен брой интегрални схеми – флаш памети и контролер, който осигурява взаимодействието с персоналния компютър по протокол ATA или SATA. SSD-дисковете към момента се произвеждат във всички популярни форм-фактори – 2,2”, 2,5”, 1,8” и рядко в 3,5”.

Основните предимства в използването на SSD вместо обичайните твърди дискове (Hard Disk Drive – HDD) са: подобрени параметри на

скоростта четене/запис и малко време за намиране на необходимата информация, което е недостижимо за обикновените HDD и има огромно значение при работата с голям брой малки по размер файлове. Също така, към предимствата на SSD се отнасят малкото тегло и ниската консумация на електроенергия, което е особено важно при използването им в мобилни устройства. Наличието на стандартни за пазара на HDD интерфейси, позволява използването дискове SSD както в нови, така и в стари модели преносими компютри, таблети и други мобилни устройства.

Според експерти, надеждността на SSD е по-висока от тази на HDD, но това твърдение все още е спорно. Единственото, което може да се твърди със сигурност е, че SSD-дисковете превъзхождат HDD по надеждност заради отсъствието на подвижни части. Следователно, при падане или удар по време на работа, информацията върху тях ще се запази, което не може да се твърди за HDD.

За SSD са характерни и редица недостатъци. На първо място – тяхната цена. Например, към момента, SSD диск 2,5” с обем 120GB е на цената на два HDD 2,5” по 500GB. Вторият проблем се изразява в сравнително малкия обем съхранявана информация. С развитието на мултимедията, пазарът изисква все по-големи капацитети на устройствата за съхранение на данни. В момента, капацитетът на обикновените IDE-дискове е над 2TB (2048 GB), а такива обеми засега са немислими за SSD. Поради гореизброените причини, основната сфера на използване на SSD дискове е в бизнес-устройства, където е важна производителността и надеждността, а не обемът, позволяващ съхранението на музика, филми и игри.

Производството на SSD има своите особености. Съществуват две технологии, които се използват за производство на NAND - флаш памети – SLC и MLC.

SLC - single-level-cell – технология за производство на чипове с еднобитова технология за запис на данните. Това означава, че една клетка се използва за съхранение на един бит данни.

MLC - multi-level-cell – технология със заряд на много нива. Това означава, че една клетка може да съхранява не един, а 4 бита данни (16 нива на заряд).

Следователно, на базата на технологията MLC могат да се създават по-големи по обем чипове памети, което се отнася и за SSD-дискове. Но това става за сметка на намаляване на скоростта четене/запис в сравнение с технологията SLC. Затова, както и в много други области, на потребителите се налага да избират между скорост и обем. Също така, цената е различна, тъй като MLC - паметите са по-евтини от SLC-паметите при един и същ обем

Надеждност и срок на експлоатация на SSD.

Производителността не е единствен показател на устройствата за съхранение на данни. Важен показател за качеството на устройствата за съхранение на данни е тяхната надеждност.

Темата е още по-актуална, във връзка с масовото преминаване към технологичен процес 25 nm, а от скоро и към 20 nm. По-тънкият процес предполага намаляване на цената на производство на NAND-памети, затова тенденцията за намаляване на дебелината на процеса се превръща в закономерност. Във връзка с това, става все по-трудно преодоляването на проблемите с паметите, произведени по технология 20 nm. Потребителите все още могат да разчитат на добра производителност и надеждност на новите твърдотелни дискове, в сравнение с предишните поколения. Преходът към по-тънък технологичен процес води до намаляване на броя на циклите на презапис на клетките памет, което трябва да се компенсира по някакъв начин. Прилагат се специални алгоритми за изравняване на износването на клетките и компресия на данните.

За предишното поколение SSD дискове, които използват NAND памет произведена по 34 - нанометрова технология гарантирания брой цикли на запис е 5000. С други думи, една NAND клетка може да се изтрива и записва 5000 пъти, преди, да започне да губи способността си за запазване на данни. Въз основа на факта, че средният потребител записва максимум 10 GB на ден, дискът ще стане неизползваем след около 31 години .

За поколението SSD с 25-nm животът на диска памет е около 18 години. И тук, нещата са силно опростени без да се вниква в

специфични проблеми на SSD като неизбежното увеличаване на обема на записваните данни заради изтриването и записването на по-големи блокове (Write Amplification), компресиране на данните, както и събиране на боклука (Garbage Collection). Всички гореизброени особености могат да окажат влияние върху реалния резултат.

Друга причина за повреда на SSD е свързана с отказ на електронни компоненти. Кондензатор или чип памет може да дефектира, което води до повреда на диска. Разбира се, подобни проблеми са по-малко очаквани, в сравнение с конвенционалните HDD, които, поради наличието на движещи се части, неизбежно ще се повредят след определен период от време.

Въпросът дали липсата на движещи се части прави SSD по-надежден вълнува все по-голям брой компютърни ентусиасти и IT - специалисти..

Когато става въпрос за измерване на надеждността на устройство, често се използва параметърът средно време между отказите (MTBF - Mean Time Between Failure), която се определя като средното време между отказите и средно време до отказ (MTTF - Mean Time To Failure), като основната разлика е предположението, че след отказа на системата тя не може да бъде възстановена .

Следва да се отбележи, че публикуваните стойности на MTBF/MTTF често се основават на резултатите от ускорени тестове - за ограничен период от време, което позволява да се разкрият предимно производствени дефекти. В този случай, заявената стойност на MTBF не съответства на надеждността и на трайността като процент на дефектни продукти. Например, MTBF на твърдия диск е приблизително 1 милион часа, което очевидно не означава 114 години непрекъсната работа - и то не само защото експеримент с такава продължителност не може да се извърши, но също така и защото производителят възлага ресурс (експлоатационен живот) под 5-10 години и период на гаранционния срок от 1 до 5 години.

Например, за механичен диск Seagate Barracuda 7200.7, производителят заявява 600 000 часа MTBF. При използване на достатъчно голяма извадка, половината от тези дискове ще се повредят в първите 600 000 часа. Тъй като статистиката на отказите на HDD в

голяма извадка е сравнително равномерно разпределена, като се очаква, например, че на всеки час ще откаже един диск. С тази стойност може да се изчисли процентът MTBF откази за година (Annualized Failure Rate, AFR), който ще бъде 1,44% .

Фактът, че броят на отказалите устройства не винаги отговаря на броя на дисковете, които трябва да бъдат заменени. Ето защо, някои изследователи не измерват надеждността с AFR, а с интензивността на подмяна на дискове (Annualized Replacement Rate - ARR) .

За съжаление, нито един от производителите на твърди дискове не публикува данни относно връщането на устройства за подмяна, като това се отнася и за производителите на SSD.

В резултат на изследвания на HDD, значителен ефект върху тяхната надеждност имат контролерът, фърмуерът и интерфейсът. За SSD дисковете сред основните фактори са контролерът и фърмуерът, като тяхната роля е още по-важна.

Може би най-неприятен е фактът, че всеки продавач продава твърди дискове и SSD, без да предоставя обективни данни относно тяхната надеждност, въпреки че те определено знаят истинското състояние на нещата, продавайки милиони единици годишно.

Безспорно е, че честотата на отказите зависи от много фактори, някои от които са извън компетентността на производителя (качество на доставката, спецификата на работата на устройството). При благоприятни обстоятелства при HDD AFR достига 3% през петата година на работа, който е сравним с цифрите за SSD. Според експерти, към настоящия момент SSD не осигуряват по-висока надеждност в сравнение с твърдите дискове.

Надеждността на твърдите дискове е добре проучена в подробни изследвания, тъй като този начин на съхранение на данни се използва от дълго време. С течение на времето ще се получи и много повече информация за надеждността на SSD .

Основни причини за избор на SSD в качеството на устройство за съхранение на данни :

– Необходимост от ускоряване на работата с програми;
– SSD е необходим като системен диск;
– SSD като замяна на твърдия диск на преносимия компютър;
– SSD е необходим за специални цели;
– SSD като надстройка на стар компютър.

При избор на SSD, трябва да се обърне внимание на главния параметър - скоростта на четене. Той е този, който представлява основен аргумент в полза на използването на SSD. Да се намери най-добрата комбинация от цена, производителност и обем е трудна задача, и може да бъде решена само с разбиране на това, което в крайна сметка трябва да се постигне.

Най-бързите SSD (произведени по технология SLC) имат малък обем, но имат най-висока скорост. Те са приложими там, където е необходимо бързо стартиране, например операционната система. В този случай използването на SSD е много изгодно: обемът на данни е малък и броят цикли на запис е малък. Ако е необходимо да се подобри производителността на дисковата подсистема при голям обем на данните се избират SSD, базирани на технологията MLC: скоростта им е по-ниска, но все още достатъчно висока, а цената е по-ниска (в сравнение с моделите със SLC) .

Основните причини за предпочитане на SSD ще бъдат разгледани поотделно.

Ускорение на работата с програми.

Дългото време на зареждане на програмата създава у потребителя дискомфорт, особено в случаите, когато са важни ефективността и бързината. Понякога, корекцията на дума или символ в документ отнема много по-малко време, отколкото времето за стартиране на текстовия редактор и отваряне на файла. Съществуват множество софтуерни продукти, които заемат значително място на диска и се състоят от огромен брой библиотеки, файлове и добавки (Photoshop, Matlab, MS Office и др.). Времето за първоначално стартиране на такива продукти

може да достигне десетки секунди. Други примери на програми, изискващи интензивен обмен на данни с диска са графичните и видео редакторите и игрите.

Използването на SSD не винаги помага за ускоряване на работата на софтуера: програми с малък обмен с диска или изискващи повече време, за да запишат своите данни в RAM, програми, за които "ограничаващ фактор " са RAM и производителност на CPU. Скоростта на браузъра, интернет комуникатори и други подобни програми (включително аудио и видео плейъри) няма да се увеличи чрез поставянето на SSD .

SSD е необходим за системен диск (инсталация на Windows).

Значително увеличение на бързодействието на компютъра при използването на SSD е възможно, ако операционната система се инсталира върху него. При това, няма нужда от голям обем - дори и Windows 7 лесно се инсталира върху диск 32 GB или 64 GB за 64 - битова версия. Използването на SSD в качеството на системен води до значително намаляване на времето на зареждане на ОС в сравнение с HDD 7200 об/мин. .

Удобството при работа се увеличава значително, тъй като се намаляват времената за реакция на ОС. Много по-бързо и по-лесно се превключва работата между няколко приложения и т.н.

SSD като алтернатива на твърдия диск на преносимия компютър.

Специфичен случай, където SSD дава предимство е използването му в мобилни устройства. Със SSD устройствата зареждат и се изключват по-бързо и не са критични към механични въздействия. Що се отнася до становищата за по-ниска консумация на твърдотелното устройство - това е един от поредните митове. Действително, SSD консумира малко по-малко енергия от HDD заради бързото изпълнение

на заявките. SSD загряват по-малко, което намалява необходимостта от охлаждане. Всичко това води до по-ефективно използване на батерията на мобилния компютър. Въпреки че точни цифри трудно могат да се посочат (според различни източници, от 3 до 14 %), работата със захранване от батерия се удължава. Повечето преносими компютри са оборудвани с твърди дискове с обем от 250 GB до 1 TB и честота на въртене 5400 об/мин. Дискове с по-висока скорост 7200 об/мин се поставят само на мобилни устройства от по-висок (бизнес) клас. В повечето случаи, преминаването към SSD е напълно оправдано, независимо, че обемът може да е по-малък. Ако преносимият компютър е голям по размери и тегло и се използва през повечето време като настолен, използването на SSD не е оправдано.

SSD е необходим за специални цели.

SSD може ефективно да се използва в екстремни ситуации, когато устройството е подложено на високи механични натоварвания: вибрации, температурни аномалии, внезапни промени в налягането, удари. Компютър, оборудван с твърд диск и подложен на подобни натоварвания е изложени на риск от загуба на ценна информация.

SSD като надстройка на стар компютър.

В повечето случаи използването на SSD дискове за ускоряване на работата на стар компютър не дава резултат. Това е свързано с редица хардуерни и софтуерни ограничения: в момента SSD се произвеждат с интерфейс SATA 6 Gb/s., а старите компютри поддържат по-ранни версии и не могат да се използват пълните възможности. Освен това, SATA - контролерът трябва да поддържа AHCI, като предпоставка за използване на функцията TRIM. Всеки твърд диск може да се използва и без функцията TRIM, но с намалена производителност. Ако се използва операционна система Windows, тя трябва да бъде Windows 7 или Windows 8. По-старите версии няма да работят добре със SSD.

Общо изискване към системата е, че за да има смисъл използването на SSD, трябва да има минимално ниво на производителността на процесора и паметта. Необходимо е системата да има съвременен двуядрен процесор и поне няколко гигабайта RAM. В противен случай, SSD няма да доведе до желания ефект и ще се окаже, че е необходимо да се актуализира самата платформа.

В резултат на направени проучвания и имайки предвид гореизложеното, беше закупен SSD с цел използването му в преносим компютър вместо механичен твърд диск. В публикацията са отразени резултатите от замяната от гледна точка на производителност и надеждност.

Използваното устройство е марка Kingston, модел SVP200S37A, с капацитет 120 GB. Същото е с форм-фактор 2,5”, интерфейс SATA 6GB/s и позволява директно монтиране в замяна на съществуващия HDD на преносимия компютър. SSD е част от т.нар. Upgrade Kit (комплект за надграждане), включващ: SSD, кутийка за външен USB твърд диск, шини за закрепване в настолен компютър на мястото на 3,5” диск, преходни кабели за захранване и диск със софтуер Acronis True Image Home за прехвърляне на информацията от съществуващия диск на новия. Заявените от производителя характеристики са следните:

Форм-фактор 2.5";

Интерфейс SATA 3.0 (6Gb/s), SATA 2.0 (3Gb/s), SATA 1.0 (1.5Gb/s);

Скорост на последователно четене: SATA 3.0 - 535MB/s, SATA 2.0 - 280MB/s;

Скорост на последователен запис: SATA 3.0 - 480MB/s, SATA 2.0 - 260MB/s;

Четене/запис на блокове 4k в случаен ред: 20,000/44,000 IOPS

Максимална скорост на четене/запис на блокове 4k в случаен ред: 85,000/55,000 IOPS;

Консумация: 0.565 W пр. ход / 1.795 W четене / 2.065 W запис;

Температура на съхранение: -40°C ~ 85°C

Работна температура: 0°C ~ 70°C

Размери: 69.9 x 100 x 7mm

Тегло: 92.3 g.;

Вибрации при работа: 2.17G;

MTBF 1,000,000 часа;

Общо количество записани байтове - Total Bytes Written (TBW): 96TB;

Гаранционен срок: 3 години;

Тестова система: ASRock P67 Motherboard, Intel Core i7 2600k 3.4GHz CPU, 8GB System Memory, NVIDIA.

Устройството е реализирано на базата на контролер Sand Force SF2281 и асинхронни 25nm MLC флаш-памети Intel. Подобна конфигурация е характерна за SSD от „потребителски" клас в ниската ценова категория.

SSD е монтиран и се експлоатира в продължение на 8 месеца в преносим компютър Dell Latitude E5520 с основни характеристики: CPU Intel Core i5 2410M 2.3-2.9 GHz, RAM 4GB DDR3/1333MHz, Intel HM65, поддържащ SATA 3.0, OS: Windows 7 64bit. В оригиналната си конфигурация компютърът беше оборудван с твърд диск Seagate ST9500420AS, с капацитет 500GB и скорост на въртене 7200 об/мин, който след замяната се използва като външен с включената в комплекта на SSD USB кутия. Някои от по-важните параметри на HDD са следните:

Интерфейс SATA 2.0 (3Gb/s);

Обем на буфера: 16MB;

Консумация: 0.69 W пр. ход / 2,1 W четене / 2,2 W запис;

Работна температура: 0°C ~ 60°C

Размери: 69.9 x 100 x 9,5mm

Тегло: 110 g.;

Вибрации при работа: 1G;

Ниво на шум: 2,7 B;

Годишна честота на отказите (AFR): 0,4%.

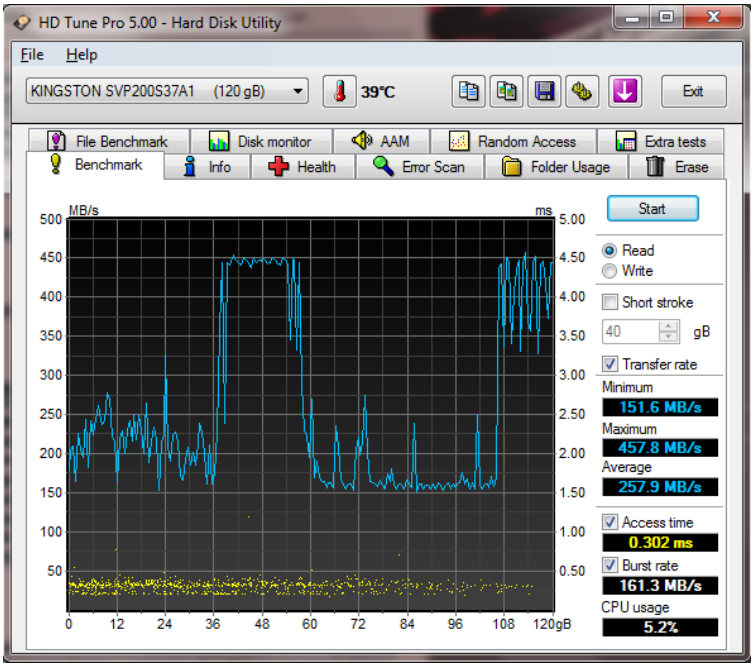
От посочените характеристики се вижда, че разликите в консумацията между двете устройства е минимална и следователно не може да се очаква увеличаване на времето на работа на компютъра на батерия. Разликите в теглото и работните температури също са минимални. Изключение правят устойчивостта на вибрации и липсата на шум при SSD.

Резултати от проведените тестове.

Методиките за тестване на производителността на устройства за съхранение на данни са многобройни и разнообразни. Основно се измерват: скоростта на непрекъснато четене и запис от началото на диска до края при различни по големина блокове от данни, случайно време за достъп при различни по големина блокове, скорост на четене/запис на файлове с различна големина и др. С цел тестване и анализ на производителността на HDD, могат да се използват редица програми: Aida64, ATTO Disk Benchmark, HD Tune и мн. др. В настоящото изследване са използвани голяма част от тях, но тъй като се получават сходни резултати, ще бъдат представени данни, получени с програмата HD Tune Pro 5.0.

Основната разлика в производителността между HDD и SSD идва от два фактора: линейната скорост на четене/запис и времето за достъп до търсения блок от данни. При механичния диск ST9500420AS линейната скорост варира между 100 MB/s в началото (външната част на плочите) и 50 MB/s в края. Средното време за достъп варира между 10 и 25 ms в зависимост от това дали информацията е в началото или в края. При SSD линейната скорост на четене зависи от характера на записаната информация и не зависи от това дали е в началото или в края

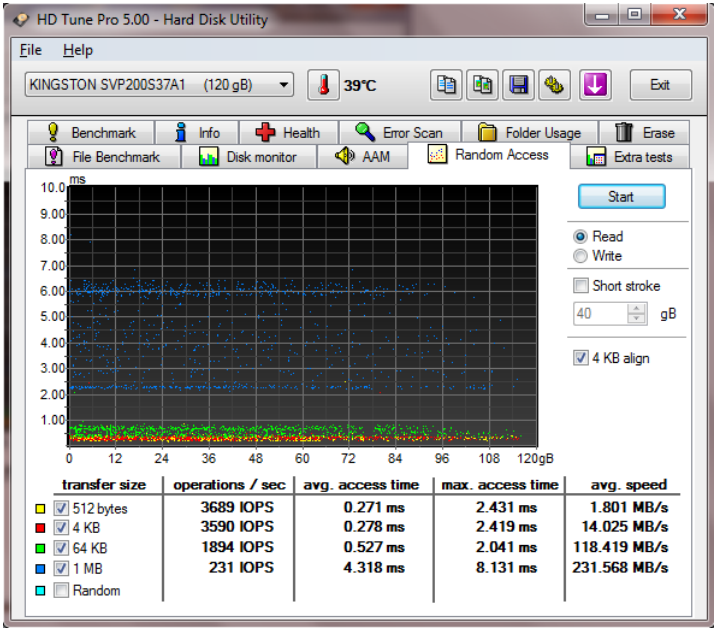
на обема. В тествания модел контролерът използва алгоритъм за запис с компресия на данните с цел намаляване на обема данни върху флаш паметите и удължаване на срока на експлоатация. Тук следва да се отбележи, че всички скорости на четене, посочени като технически данни са постигнати при нов (празен) SSD. Както ще бъде показано, на практика резултатите са доста по-ниски. Това се дължи на факта, че блокове от данни, съдържащи само „нули" се декомпресират много по-бързо, отколкото блокове, съдържащи случайни числа. Същото се отнася и за скоростите на запис, тъй като и те зависят от структурата на данните, т.е. дали се компресират с голям коефициент или не. На фигура 1 е показана графиката на скоростта на четене на SSD при размер на блоковете 512 KB:



Фигура 1 Линейна скорост на четене на SSD

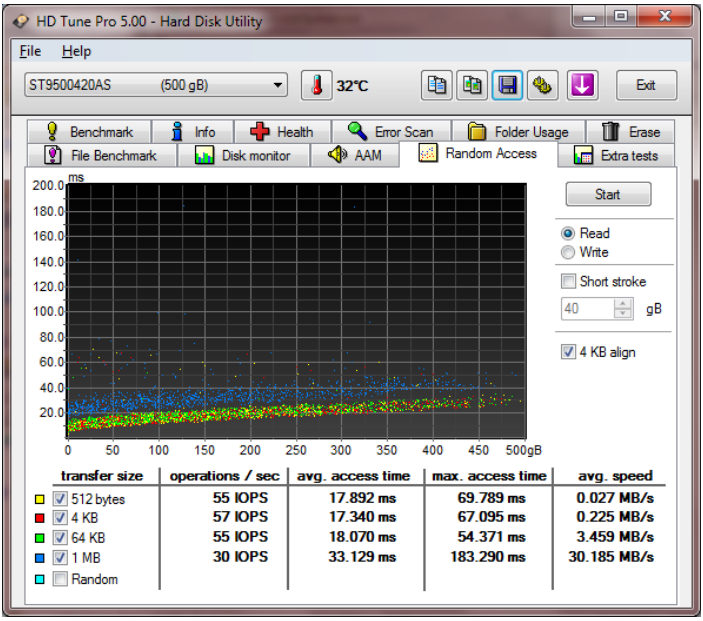
На фигурата се вижда, че скоростта се изменя в доста широки граници и зависи от данните, записани на диска. В случая, SSD е

разделен на два основни дяла, като в първия дял са операционната система и програмите, а във втория дял са инсталации, снимки, документи и др. Вижда се, че максимална скорост се постига на местата, където дискът не е записан. На местата, където има записани данни, скоростта е от 150 до 250 MB/s. Освен това, стойността 457.8 MB/s е по-ниска от заявената от производителя 525 MB/s. На практика, интерес представлява само скоростта на четене в записания участък, която е средно 1,5 до 2,5 пъти по-висока в сравнение с тази на механичния диск. Прави впечатление много по-малкото средно време за достъп от около 0.3 ms, спрямо 18 ms за HDD. Следователно, очакваната разлика в производителността между SSD и HDD би се дължала в малка степен на разликите в линейните скорости и в по-голяма – на времето за достъп. Следващите две фигури дават ясна престава за средните скорости на четене при различни размери на блоковете данни.



Фигура 2. Времена за достъп и средна скорост на четене от HDD

Вижда се, че разликите между средните скорости на четене (avg. Speed) са доста големи: за блокове от по 512 B – 67 пъти, за блокове от по 4 KB – 62 пъти, за 64 KB – 34 пъти и за 1 MB – около 8 пъти. Същото се отнася и за броя на входно-изходните операции в секунда (IOPS), които се увеличават с почти същите коефициенти.



Фигура 3. Времена за достъп и средна скорост на четене от SSD

Това се обяснява с факта, че при по-малки блокове съществена роля играе малкото време на достъп, а при по-големи блокове – линейната скорост. Следователно, основното предимство на SSD е високата средна скорост на четене на малки по размер блокове (файлове). Това предимство се проявява в реалните тестове като много по-бързо зареждане на операционната система Windows 7 – около 12 – 15 s. (от скриването на стартовия екран на BIOS до пълна готовност). За механичен диск времето за зареждане е около 50 – 60 s. При изключване на компютъра разликата не е толкова голяма: 10-12 s. при SSD и 15-20 s. при HDD. Всички приложения се стартират много по-бързо, което е

безспорно удобство. Например Matlab, които обикновено стартира за 20 – 25 секунди, със SSD стартира за около 3 s. Недостатък на SSD е малкият обем (111 GB полезно пространство, от които 17 GB са заети от Windows), но все пак за ежедневна работа е напълно достатъчен. Проведени са и тестове за продължителност на автономна работа на компютъра от батерия, но реална разлика във времето не беше установена.

Надеждността на тестваното устройство е висока. За 8 месеца експлоатация не е показало никакви дефекти. За периода, съгласно SMART параметрите на SSD са записани общо 1,6TB данни. Съгласно спецификациите на устройството, животът му се измерва в общия брой записани байтове и е 96 TB. Ако за една година се записват около 2 TB, може да се направи извода, че в близките години няма никаква опасност SSD да дефектира заради износване на клетките памет. Също така, в SMART параметрите няма данни за грешки или пренасочени сектори. В периода на експлоатация производителят публикува и нова версия на фърмуера, която беше изтеглена и инсталирана. При това, процедурата по актуализация на фърмуера е бърза и лесна, а данните се запазват непроменени.

Заключение

Полупроводниковите дискове са бързо развиваща се технология с основна цел замяната на механичните твърди дискове с памети. Основното предимство на SSD е тяхната висока скорост на четене и малкото време на достъп, което в голяма степен премахва слабото място в компютърната система – устройството за съхранение на данни. Недостатък на SSD е ограниченият брой цикли на презапис на клетките памет, който не е чак толкова важен, особено за обикновени потребители. Важно е да се отбележи, че техническите характеристики, давани от производителите най-често са завишени или са постигнати при строго специфични условия. В реални условия бързодействието не е чак толкова високо, колкото се твърди, но все пак е в пъти по-добро от това на механичните дискове. Основен недостатък на SSD е тяхната цена за един и същ обем, но използването им в съвременните преносими компютри е напълно оправдано. За потребители с основна насоченост

към колекции от музика, филми, игри, ел. книги и др. е препоръчително да използват механичен твърд диск.

ЛИТЕРАТУРА:

1. http://www.thg.ru/
2. http://www.kingston.com/en/support/technical/products?model=SVP200S3
3. http://www.seagate.com/staticfiles/support/disc/manuals/notebook/momentus/7200.4/100534376c.pdf
4. http://www.overclock.net/t/1133897/windows-7-ssd-tweaking-guide

ХАРАКТЕРИСТИКА НА ИНТЕРНЕТ ПРОТОКОЛ ВЕРСИЯ 4 В КОМУНИКАЦИОННИТЕ И КОМПЮТЪРНИТЕ МРЕЖИ

ПЕТЪР КР. БОЯНОВ

A CHARACTERISTIC OF THE INTERNET PROTOCOL VERSION 4 IN THE COMMUNICATION AND COMPUTER NETWORKS

PETAR KR. BOYANOV

ABSTRACT. *In this paper a common characteristics of the The Internet Protocol version 4 (IPv4) is made. IPv4 is used for routing the traffic mainly on the Internet public space. This protocol is characterized by connectionless, best effort and media independent.*

KEYWORDS: *Addressing, Best effort, Connectionless, IPv4, IPv6, MTU.*

1. Въведение

Мрежовият слой (Network Layer) от отворения еталонен модел (OSI - Open Systems Interconnection) осигурява необходимите услуги за обмяна на индивидуални потоци от данни през мрежата между идентифицирани крайни устройства. За да се осъществи този краен процес на транспортиране, мрежовият слой използва 4 основни процеса:

- Адресация (Addressing).
- Капсулация (Encapsulation).
- Рутиране (Routing).
- Декапсулация (Decapsulation).

2. Изложение

2.1. Адресация (Addressing).

Първоначално мрежовият слой трябва да осигури механизъм за адресация на тези крайни устройства. Ако индивидуалните потоци от данни са директно адресирани към крайното устройство, тогава това

крайно устройство трябва да притежава уникален адрес. Когато е добавен уникален адрес към крайното устройство в IPv4 мрежа, тогава това устройство приема името хост (host).

2.2. Капсулация (Encapsulation).

Мрежовият слой трябва задължително да осигури процес на капсулиране на потока от данни. Не само крайните устройства, но и отделните протоколни единици на потока от данни трябва да съдържат този уникални адреси. Докато трае процеса на капсулация, мрежовият слой (слой 3) получава протоколната единица от транспортния слой (слой 4) и след това добавя хедър (заглавна част) от слой 3 към тази протоколна единица от слой 4 с цел създаване на протоколна единица от слой 3. Когато се разглежда мрежовия слой, тогава протоколната единица се нарича пакет. След като пакетът е създаден вече, хедърът трябва да съдържа също така допълнителна друга информация, от която е и адресът на крайното устройство, към което е предназначен дадения пакет. Този адрес се нарича още адрес на получателя (Destination Address). Слой 3 съдържа също така адресът на оригиналното крайно устройство. Този адрес се нарича адрес на източника (Source Address) [1],[2],[9]. След като мрежовият слой приключи с процеса на капсулация, тогава пакетът се изпраща надолу към каналния слой (слой 2) с цел да бъде подготвен за транспортиране през дадената среда.

2.3. Рутиране (Routing).

При процеса на рутиране на потока от данни мрежовият слой трябва да осигури услуги за директното предаване на пакетите към дадения адрес на получателя. Двете крайни устройства - източникът и получателят не винаги са свързани в една и съща мрежа. В действителност пакетът трябва да премине през много различни мрежи. По време на своето пътуване всеки пакет трябва да бъде упътван през мрежата с цел достигане до крайната дестинация. Посредническите устройства, които свързват мрежите, се наричат рутери (маршрутизатори). Ролята на устройството рутер е да селектира пътищата и да изпрати напред пакетите към тяхната дестинация. Този процес е известен като рутиране на потока от данни [1],[6],[7].

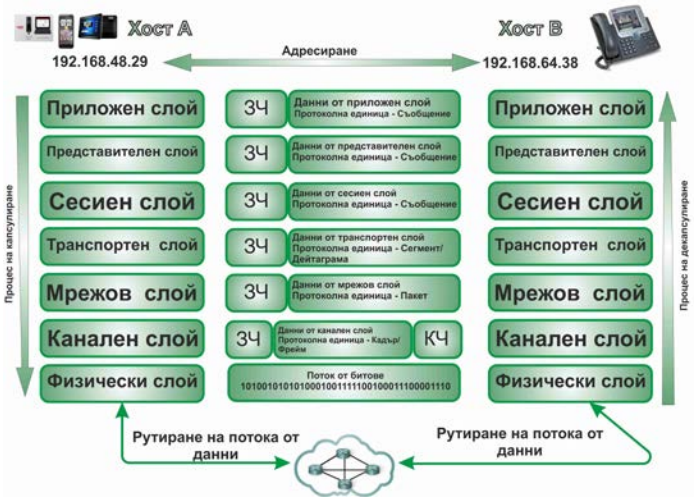
По време на процеса на рутиране през интернет мрежата, даденият пакет може да премине през много посреднически устройства. Всеки маршрут, който поема пакетът, за да стигне до следващото устройство, се нарича хоп (скок). Когато пакетът е изпратен напред, той продължава да съдържа протоколната единица от транспортния слой, докато не стигне адресът на получателя.

2.4. Декапсулация (Decapsulation).

Най-накрая пакетът пристига при своя краен получател. Крайното устройство проверява за адреса на получателя, за да се разбере дали пакета е адресиран към правилното устройство. Ако адресът е коректен, тогава пакетът се декапсулира от мрежовия слой и протоколната единица от слой 4, съдържаща се в пакета, преминава нагоре към подходящата услуга на транспортния слой.

За разлика от транспортния слой, който управлява траспортирането на потока от данни между процесите, протичащи през всеки хост, протоколите от мрежовия слой определят структурата на пакета и процесите, използвани за пренасянето на потока от данни от един хост към друг хост [1],[3],[4],[9],[10].

На фиг.2.1. са показани основните процеси на адресиране, капсулиране, рутиране и декапсулиране на потока от данни между двете крайни устройства.



Фиг. 2.1. Основните процеси на адресиране, капсулиране, рутиране и декапсулиране на потока от данни между двете крайни устройства

2.5. Протоколни стекове от мрежовия слой.

Протоколните стекове от мрежовия слой са [3-7]:

- Интернет протокол версия 4 от протоколния стек TCP/IP (TCP - Transmission Control Protocol, IPv4 - Internet Protocol version 4);

- Интернет протокол версия 6 от протоколния стек TCP/IP (TCP - Transmission Control Protocol, IPv6 - Internet Protocol version 6);
- Протоколи на фирмата Novell (IPX - Internetwork Packet Exchange);
- Протоколи на фирмата AppleTalk;
- Протоколи от протоколния стек на DECnet (Digital Equipment Corporation);
- Протоколи от мрежовата услуга на CLNS (CLNS - Connectionless Network Service).

2.6. Характеристики на интернет протокол версия 4 (Internet Protocol version 4).

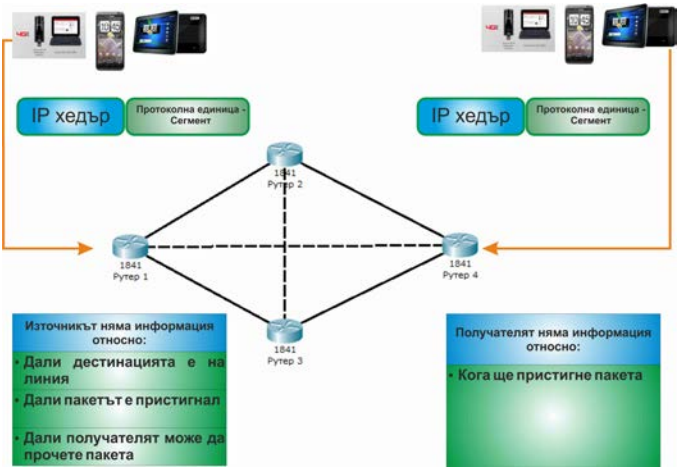
Протоколът IPv4 е проектиран като протокол с малка натовареност на връзката. Той осигурява само функции, които са необходими за доставянето на пакет от източника до дестинацията през многото свързани системи от мрежи. Този протокол не е проектиран да управлява потока от пакети [3],[5],[7],[8],[10].

Основните характеристики на протокола IPv4 са:

- Протокол, който не е ориентиран към връзката (Connectionless).
- Протокол, който се характеризира с най-добро постижение, усилие (Best Effort, unreliable).
- Протокол, който е независим от преносната среда (Media Independent).

2.6.1. Протокол, който не е ориентиран към връзката (Connectionless).

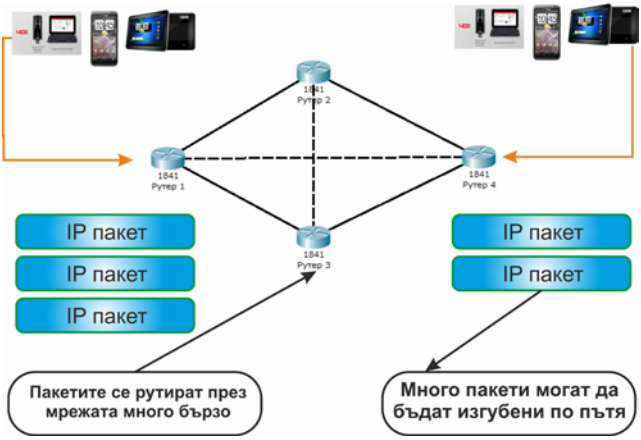
Когато се прилага протокола IPv4, тогава не се изисква предварително създаване на виртуален канал. Поради тази причина този протокол не е ориентиран към връзката и това от своя означава, че пристигащите пакети в дадената дестинация може да не са с последователен номер (out of sequence). Възможно е даже да има пакети, които изобщо да не пристигнат. Поради тази причина услугите от по-горните слоеве ще имат за задача да разрешат тези проблеми [3],[4],[5],[6]. На фиг. 2.2. е показана комуникация, която не е ориентирана към връзката.



Фиг. 2.2. Комуникация, която не е ориентирана към връзката

2.6.2. Протокол, който се характеризира с най-добро постижение, усилие (Best Effort, unreliable).

Протоколът IP не натоварва IP услугата с осигуряване на надеждност. IP хедърът (заглавната част) е много по-малък от другите протоколи, които осигуряват надеждност. Като се транспортират тези малки заглавни части се изисква много по-малко натоварване на мрежата. Малко натоварване означава, че всъщност ще има много малко закъснение при доставката на потока от данни. Мисията на мрежовия слой е да транспортира пакетите между крайните устройства. Като допълнение мрежовия слой не се интересува от типа на комуникацията, която се съдържа в пакета. Тази отговорност се пада на по-горните слоеве. По-горните слоеве могат да вземат решение ако комуникацията между услугите се нуждаят от надеждност. В практиката протоколът IP е известен още като ненадежден протокол. Това означава, че протоколът IP не разполога със способността да управлява и поправя недоставените или повредени пакети [1],[2].[3],[5],[7],[10]. На фиг. 2.3. е показано рутирането на пакетите през мрежата.

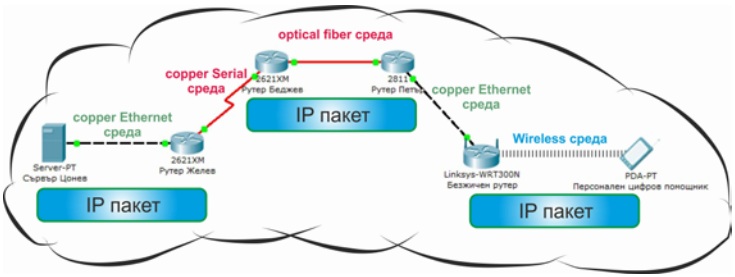


Фиг. 2.3. Рутиране на пакетите през мрежата

2.6.3. Протокол, който е независим от преносната среда (Media Independent).

Протоколите IPv4 и IPv6 оперират независимо от средата, през която се пренасят потока от данни към по-ниските слоеве на протоколния стек. На фиг. 2.4. е показано как всякакви индивидуални IP пакети се пренасят през различните среди. В зависимост от средите се различават следните три вида сигнала [3-8]:

- Copper Ethernet, Copper Serial cable - електрически сигнал;
- Optical fiber - оптически сигнал;
- Wireless - радиосигнал.



Фиг. 2.4. Пренасяне на отделните IP пакети през различните комуникационни среди

Каналният слой от отворения еталонен OSI модел е отговорен за вземането на IP пакета и подготвянето му за предаване през комуникационната среда. Поради тази причина транспортирането на IP пакетите не зависи по никакъв начин от специфичната комуникационна среда.

Въпреки това ние трябва да отбележим, че няма правило без изключение. Това изключение е свързано с максималния размер на протоколната единица (PDU - Packet Data Unit), която всяка среда може да транспортира. Тази характеристика се казва максималната предавателна единица на информация, която е най-големият физически пакет, който може да се предава по дадената мрежа (MTU - Maximum Transmission Unit). Част от контролната комуникация между каналния слой и мрежовия слой е установяването на максималния размер на пакета. Каналният слой пропуска максималната предавателна единица (MTU) нагоре към мрежовия слой. Мрежовият слой от своя страна определя колко голям пакет да бъде създаден. В практиката посредническите устройства (маршрутизаторите) ще искат да разделят пакета, когато го изпращат от една среда към среда с по-малка максимална предавателна единица (MTU). Този процес е наречен фрагментиране на пакета (фрагментация - fragmentation) [4],[6],[8],[9].

3. Изводи и предложения

Интернет протокол версия 4 (IPv4) продължава да се използва още в компютърните мрежи като актуалната тенденция е

задължителното преминаване към по-новата версия на този протокол , а именно Internet Protocol version 6 (IPv6) . Протоколът IPv4 се характеризира с 32 битово адресно пространство, докато протоколът IPv6 ще характеризира с 128 битово адресно пространство. Главната причина за преминаване към по-новия мрежови протокол е, че протокола IPv4 през 2010 г. беше напълно изчерпан от интернет потребителите. Този научен труд намира широко приложение за студентите при разглеждане на комуникационните процеси в дадена компютърна мрежа.

ЛИТЕРАТУРА:

5. **Боянов** П. К., Методи за защита на комуникационните процеси в каналния слой на малки локални мрежи, // Научна сесия с международно участие от 2 май 2012 г. на ВВМУ "Н. Й. Вапцаров" - "Курсантите и студентите на морско училище и науката", Варна, Издателски център и размножителна база на ВВМУ "Н. Й. Вапцаров", 2012, с.527-532
6. **Боянов** П. К., Технологии за обединение на фиксираните и мобилните комуникационни мрежи. // Сборник научни трудове от научна сесия 2010. Шумен, Творческо студио и Рекламна агенция „Химера" ООД - гр. Шумен, част II, 2011, с. 422-430
7. **Feit** S, "SNMP, A Guide To Network Management", McGraw-Hill, 1995
8. **Hekmat** S, "Communication Networks", "PragSoft Corporation", USA, 2005 г.
9. **Piscitello** D., Chapin L, "Open Systems Networking TCP/IP and OSI", Addison-Wesley, Reading, MA, 1993 г.
10. **Stallings** W, "Handbook of Computer Communications Standards, Volumes I and II", "Howard Sams and Company", Carmel, 1990 г.
11. **Stallings** W, „ISDN and Broadband ISDN, Second Edition", „Macmillan", NY, 1992 г.
12. **Stallings** W, „Data and Computer Communications, Fourth Edition", „Macmillan", NY, 1994
13. **Stanew** S., Tsonev I., Boyanov P., Research of Communication Processes in the Data Link Layer on Small Local Area Networks. В: Сборник доклади от International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, Bulgaria - Varna, RTU Printing House - Riga, 2012, pp. 56-59
14. **Tsonev** I., Boyanov P., Processes Modeling in the Data Link Layer on Small Local Area Networks. В: Сборник доклади от International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, Bulgaria - Varna, RTU Printing House - Riga, 2012, pp. 51-55

ИЗСЛЕДВАНЕ НА СТРУКТУРАТА НА ИНТЕРНЕТ ПРОТОКОЛ ВЕРСИЯ 4 В КОМПЮТЪРНИТЕ МРЕЖИ

ПЕТЪР КР. БОЯНОВ

A RESEARCH OF THE INTERNET PROTOCOL VERSION 4 STRUCTURE IN THE COMPUTER NETWORKS

PETAR KR. BOYANOV

ABSTRACT: *In this paper a common research of the The Internet Protocol version 4 (IPv4) structure in the computer networks is made. The IPv4 header consists of different field and each field performs a specific function in order to be sent the determined packet.*

KEYWORDS: *Destination IP Address, IPv4, IPv6, Source IP Address, TOS, TTL.*

1. Въведение

На фиг. 1.1. е илюстриран пакетния хедър (заглавна част) на протокола IPv4.

Фиг. 1.1. Пакетен хедър (заглавна част) на протокола IPv4

2. Изложение

2.1. Характеристика на полетата в пакетния хедър на протокола IPv4.

2.1.1. Версия (Version).

Това четири битово поле показва коя версия на интернет протокола (IP - Internet Protocol) се използва. Текущата версия е четвърта (IPv4). Числото 410 представено в двоична система е 01002 и по този начин това играе ролята на двоичен шаблон. Възможните стойности за полета на версията са показани на табл. 2.1.

Табл. 2.1. Възможните стойности за полета на версията

IP версия (IP Version)	Описание (Description)
0	Резервиран (Reserved)
1-3	Неопределен (Unassigned)
4	IP версия 4 (IP Version 4)
5	Поточен режим на IP дейтаграма, експериментален протокол (Stream IP Datagram mode, experimental protocol)
6	IP версия 6 (IP Version 6)
7	Експериментален протокол TP/IX(TP/IX: The Next Internet)
8	Интернет протокол P (PIP The P Internet Protocol)
9	Протокол TUBA(TUBA - TCP and UDP with bigger addresses)
10-14	Неопределен (Unassigned)
15	Резервиран (Reserved)

Протоколите (TP/IX: The Next Internet), (PIP - The P Internet Protocol) и (TUBA - TCP and UDP with bigger addresses) бяха едни от основните протоколи, които трябваше да сменят IPv4, но комуникационната индустрия взема решение и избра за наследник на протокола IPv4 протоколът IPv6 [1],[8],[9],[10].

2.1.2. Дължина на Internet хедъра (IHL - Internet Header Length).

Това четири битово поле дава дължината на хедъра на протокола IPv4 в 32-битови думи. Минималната дължина на хедъра на протокола IPv4 е пет 32-битови думи. Хедърният шаблонен бит е 01012 ,т.е. 510.

2.1.3. Тип на услугата (TOS - Type of Service).

Полето ”тип на услугата” в пакетния хедър на протокола IPv4 е 8 битова двоична стойност, която се използва за определяне на приоритета на всеки пакет. Тази стойност активира механизма качество на услугата (QoS - Quality of Service) към високо приоритетните пакети като тези, които пренасят гласови данни. Маршрутизаторът от своя страна решава кой пакет да бъде изпратен първи като се базира на стойността качество на услугата [3],[4],[5],[6],[7].

Първите три поредици от битове - 0002, 0012, 0032 показават стойност за предимство. Следващите поредици от битове представляват комбинация между различни стойности. На табл.2.2. са показани различните комбинации и съответните им стойности за всяка комбинация за настройка на услугата качество на услугата (QoS - Quality of Service).

Табл. 2.2. Различни комбинации на качество на услугата (QoS - Quality of Service)

Шаблон на битовете (Bits Pattern)	Описание (Description)
000	Шаблонен, установен (Routine)
001	Приоритет (Priority)
010	Незабавен (Immediate)
011	Светкавичен (Flash)
100	Светкавично надхвърляне (Flash Override)
101	Обработка на критично и спешно повикване (CRITIC/ECP - Critical and Emergency Call Processing)
110	Контрол на Internet мрежата (Internetwork Control)
111	Контрол на мрежата (Network Control)

Четвъртата поредица от битове показва закъснението. Ако стойността на бита е 0, тогава се разбира нормално закъснение. Ако стойността на бита е 1, тогава се разбира малко закъснение. Петата поредица от битове показва пропускателната способност. Ако стойността на бита е 0, тогава се разбира нормална пропускателната способност. Ако стойността на бита е 1, тогава се разбира голяма пропускателната способност. Шестата поредица от битове показва надеждност [3],[4]. Ако стойността на бита е 0, тогава се разбира нормална надеждност. Ако стойността на бита е 1, тогава се разбира голяма надеждност. Седмата поредица от битове показва намалена стойност. Ако стойността на бита е 0, тогава се разбира нормална стойност. Ако стойността на бита е 1, тогава се разбира намалена стойност [2].

Осмата поредица от битове е резервирана за бъдещо използване и се означава с термина (MBZ - Must be Zero).

Четирите бита, които представят стойностите на типа на услугата, са обобщени на табл.2.3.

Табл.2.3. Обобщение на четирите бита

Код на типа на услугата (ToS Code)	Значение (Meaning)
1000	Минимално закъснение (Minimum Delay)
0100	Максимална пропускателна способност (Maximum throughput)
0010	Максимална надеждност (Maximum Reliability)
0001	Минимална стойност (Minimum monetary cost)
0000	Нормална услуга (Normal Service)

2.1.4. Дължина на пакета (Packet Length).

Полето ”дължина на пакета” се състои от 16 бита и по този начин показва размера на целия пакет в байтове. Този размер включва дължината на хедъра и големината на полезните данни. Минамалната дължина на IP дейтаграмата е 20 байта. Когато дължината на пакета е 20 байта, тогава IP хедърът не носи никакви потребителски данни. Максималната дължина на пакета е 65535 байта.

2.1.5. Идентификация (Identification).

Полето ”идентификация” се състои от 16 бита и показва идентифицираща стойност, назначена от източника на пакета с цел асемблирането на фрагментите на IP пакета. Когато пакетът е фрагментиран на множество пакети, тогава протоколът IP дава на всички фрагменти същия идентификационен номер, защото после този номер се използва за идентифициране на IP фрагментите в приемащата страна.

2.1.6. Флагове (Flags).

Полето ”флагове” се състои от 3 бита и те показват възможности за фрагментиране на пакета. Първият бит не се използва и винаги трябва да има стойност 0. Следващият бит (флаг) е наречен „недей да фрагментираш” (DF - Don`t Fragment). Ако флагът DF е настроен на 0, тогава това показва, че IP пакета може да бъде фрагментиран. Ако флагът DF е настроен на 1, тогава това показва, че IP пакета не може да бъде фрагментиран. Следващият последен бит (флаг) е наречен “повече фрагменти” (MF - More Fragments). Този флаг показва, че много фрагменти пътуват по средата към своята дестинация. Флагът MF заедно с полето отместване на фрагмента (Fragment Offset) служат за фрагментиране и след това за възстановяване на пакетите. Когато флагът MF е настроен на 1, тогава това означава, че това не е последния фрагмент от пакета. Когато получаващият хост погледне пристигналия пакет с флаг MF = 1, тогава той проверява полето за отместването на фрагмента, за да разбере къде трябва да сложи този фрагмент за възстановяването на пакета. Ако дестинацията получи фрагмент с MF = 0 и нулава стойност в полето за отместване на фрагмента, тогава дестинацията поставя фрагмента на последно място във възстановения пакет. Когато MF = 0 и FO = 0, тогава това означава, че пакетът не е фрагментиран [4],[5],[6].

2.1.7. Отместване на фрагмента (Fragment Offset).

Полето за отместване на фрагмента идентифицира последователността, по която трябва да бъде поставен дадения фрагмент при възстановяването на пакета. Когато настъпи процес на фрагментиране пакетът IPv4 използва полето (Fragment Offset) и флагът MF, за да може после да се възстанови пакета, когато той пристигне при своята дестинация.

2.1.8. Време за живот (TTL - Time to Live).

Полето ”време за живот” съдържа осем бита информация, която показва оставащия живот на пакета. При всяко едно преминаване през даден рутер (всеки хоп), стойността на TTL се намалява с единица. Когато стойността стане 0, тогава рутерът отхвърля или унищожава пакета и по този начин пакетът е премахнат от мрежата. Този механизъм предотвратява да не се появи безкраен цикъл на препращане на пакети от един рутер към друг друг. Ако рутиращите цикли бяха разрешени, тогава цялата мрежа щеше да бъде много натоварена с пакети, които никога няма да достигнат до дадената дестинация.

2.1.9. Протокол (Protocol).

Полето ”протокол” съдържа 8 бита, които показват типа на полезния товар, който пакета пренася през дадената среда. Това поле позволява на мрежовия слой да пропусне потока от данни към подходящ по-горен протокол. Примерни стойности на по-горни протоколи са [1],[9],[10]:

- 01 ICMP (Internet Control Message Protocol).
- 06 TCP (Transmission Control Protocol).
- 17 UDP (User Datagram Protocol).

2.1.10. Проверовъчна сума на хедъра (Header Checksum).

Това поле съдържа 16 бита изчислена стойност, която проверява валидността само на хедъра (заглавната част) на IP пакета. Това поле се преизчислява във всеки един маршрутизатор, когато полето TTL се намали с единица.

2.10.4.1.11. Адрес на източника (Source IP Address).

Това поле представя мрежовия адрес на източника на пакета. Дължината на това поле е 32 бита.

2.1.12. Адрес на получателя, дестинацията (Destination IP Address).

Това поле представя мрежовия адрес на получателя на пакета. Дължината на това поле е 32 бита.

2.1.13. IP допълнителни опции (IP Options).

Това поле осигурява допълнителни услуги, но за съжаление се използва рядко.

2.1.14. Допълване с нули (Padding).

Полето Padding осигурява допълнителни битове от нули, за да може цялата дължина на хедъра да бъде кратна на 32 бита.

2.1.15. Полезните потребителски данни (Data).

Това поле съдържа същинските полезни потребителски данни като тяхната дължина може да се изменя.

2.2. Типичен IP пакет.

На фиг. 2.1. е показан типичен завършен IP пакет със съответните стойности на полетата.

Фиг. 2.1. Типичен IP пакет

Този типичен IP пакет се характеризира със следните стойности:

- Версията на IP протокола е 4.
- Дължината на Internet хедъра е 5, т.е. 5*4 = 20 байта. Минималният валиден размер е 20 байта. В нашия случай това условие е изпълнено.
- Дължината на пакета, която включва хедъра и полезните данни е 472 байта.
- Идентификацията е 111. Това е оригиналният пакетен идентификатор и той ще се използва после ако IP пакетът ще бъде фрагментиран.

- Флагът е 0 и това показва, че пакетът може да бъде фрагментиран ако е необходимо.
- Отместването на фрагмента е 0 и това показва, че този пакет не е фрагментиран.
- Времето за живот е 115. Това показва, че след 115 междинни устройства пакетът ще бъде унищожен ако не се намери неговата дестинация.
- Протоколът е 6. Това означава, че данните, които се пренасят от този пакет, са от тип TCP сегмент.
- Адресът на източника е 192.168.2.29, т.е. това е частен адрес.
- Адресът на получателя, дестинацията е 192.168.3.13, т.е. това е пак частен адрес.

3. Изводи и предложения

Всяко едно поле от протокола IPv4 играе изключително важна роля за правилното изпращане и доставяне на определените IP пакети. Този протокол се характеризира с бързо доставяне на протоколните единици до получателя в мрежата, но в същото време този протокол не съдържа поле за проверяване цялостта на получените данни. В този научен труд е илюстриран примерен IP пакет, който се изпраща от един частен адрес до друг такъв. Този научен труд също така намира широко приложение за студентите при разглеждане на функциите на отделните полета в даден IP пакет за дадена компютърна мрежа.

ЛИТЕРАТУРА:

1. **Боянов** П. К., Методи за защита на комуникационните процеси в каналния слой на малки локални мрежи, // Научна сесия с международно участие от 2 май 2012 г. на ВВМУ "Н. Й. Вапцаров" - "Курсантите и студентите на морско училище и науката", Варна, Издателски център и размножителна база на ВВМУ "Н. Й. Вапцаров", 2012, с.527-532

2. **Боянов** П. К., Технологии за обединение на фиксираните и мобилните комуникационни мрежи. // Сборник научни трудове от научна сесия 2010. Шумен, Творческо студио и Рекламна агенция „Химера" ООД - гр. Шумен, част II, 2011, с. 422-430

3. **Feit** S, "SNMP, A Guide To Network Management", McGraw-Hill, 1995

4. **Hekmat** S, "Communication Networks", "PragSoft Corporation", USA, 2005 г.

5. **Piscitello** D., Chapin L, "Open Systems Networking TCP/IP and OSI", Addison-Wesley, Reading, MA, 1993 г.

6. **Stallings** W, “Handbook of Computer Communications Standards, Volumes I and II”, “Howard Sams and Company”, Carmel, 1990 г.

7. **Stallings** W, „ISDN and Broadband ISDN, Second Edition”, „Macmillan”, NY, 1992 г.

8. **Stallings** W, „Data and Computer Communications, Fourth Edition”, „Macmillan”, NY, 1994

9. **Stanew** S., Tsonev I., Boyanov P., Research of Communication Processes in the Data Link Layer on Small Local Area Networks. В: Сборник доклади от International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, Bulgaria - Varna, RTU Printing House - Riga, 2012, pp. 56-59

10. **Tsonev** I., Boyanov P., Processes Modeling in the Data Link Layer on Small Local Area Networks. В: Сборник доклади от International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, Bulgaria - Varna, RTU Printing House - Riga, 2012, pp. 51-55

МОНИТОРИНГ И АНАЛИЗ НА МРЕЖОВ ТРАФИК С ИЗПОЛЗВАНЕ НА GPU

ФИЛИП И. ЛЮБОМИРОВ

MONITORING AND ANALYSIS OF NETWORK TRAFFIC USING GPU

FILIP I. LYUBOMIROV

ABSTRACT: *In laboratory Fermilab is a method that uses the capabilities of computer graphics accelerator (GPU) for monitoring network traffic . This method is referred to as G-NetMon. Many tools for monitoring and analysis are facing extreme performance and scalability of network environments such as 40GE/100GE. GPU technology began to be applied to accelerate scientific and engineering calculations. The architecture of the GPU fits well with the functions of an application for monitoring and analyzing network packets. At Fermilab, has developed a prototype of the architecture of the GPU accelerator that performs capture, monitoring and analysis of network traffic . With an Nvidia GPU M2070, can handle 11 million or more packets per second without losing one . In the lines below, we will examine the architectural approach in the development of GPU serving to capture and analyze packets.*

KEYWORDS: *Network monitoring, GPU, multicore, manycore, high-speed networks.*

1. Въведение

Мониторинг и анализ на мрежата трафик е процеса на следене и улавяне на трафик с което се цели да се получи информация каква се случва с дадената мрежа. Още от създаването на компютърни мрежи, мониторинг и анализ на трафика е незаменим инструмент в мрежовите операции и управление, планиране на капацитета и отстраняване на проблеми при реализацията им. Експоненциалния растеж на данни преминаващи през мрежите, изисква приложения които служат за обработката им и анализът им да имат по-висока производителност. В рамките на един център за данни, ръстът на работата на сървъра в съчетание с възможности за виртуализация, запълват портовете с пропускателна способност от 10GbE. Това на свой ред, доведе до развитие на тези центрове и налагането им към портове с

пропускателна способност 40GE и 100GE. При такива високи скорости на предаване на данни, приложенията наблюдаващи мрежовия трафик и анализирането му, особено на тези от тях които участват в контрола на трафика(на база за всеки пакет) изискват огромна изчислителна мощ и висока I/O (входно/изходната) пропускателна способност. Тези приложения са изправени пред екстремна производителност и мащабното предизвикателство за справяне с тези данни.

Към днешна дата разполагаме с две големи изчислителни платформи които се използват за мониторинг и анализ на мрежовия трафик . Първата от тях е специализиран хардуер базирани на NPU (мрежов процесор) и/или ASIC (приложно ориентирани интегрални схеми) технологии. Основният недостатък на този подход е, че NPU и ASIC са трудни за програмиране и трудни за използване в мащаби, разходите за развойна дейност са много високи. Другата платформата е с общо предназначение при която се използва CPU (централен процесор), който е в състояние да изпълнява много видове задачи едновременно. Възникват малко подозрения, че процесорите могат да се използват за мониторинг и анализ на мрежовия трафик . С последните постижения в многоядрените технологии , един процесор може да осигури множество ядра за обработка на мрежовия трафик в паралел. Изследователите са направени ефективно използване на многоядрени системи в мониторинга и анализ на мрежовия трафик . Въпреки това се твърди, че CPU не е оптимална - изчислителна платформа за мониторинг и анализ на мрежовия трафик, и приложение то му в мрежи с висока производителност не е подходящото, това е защото архитектурата на процесора е не подходяща.

Напоследък графичните процесори се прилагат широко за повишаване и ускоряване на изчисленията при научни и инженерни изследвания. Големият брой от GPU ядра предлага по-висока производителност и изчислителна мощ, отколкото CPU . Модел изпълнен с GPU за обработка на паралелна данни и достатъчно висока честота на паметта на GPU може ефективно да се понижи латентността при изчисления. Програмите среди CUDA и OpenCL предоставят на програмистите по лесна работа и програмиране при използване на GPU.

В Fermilab, е създаден прототип за мониторинг и анализ на мрежовия трафик на система базирана на GPU, който анализира мрежовия трафик на базата на пакети. В тази статия, ще опишем архитектурната реализация реализирана с помощта на GPU.

2. Система за мониторинг и анализ на мрежов трафик с помощта на GPU ускорител

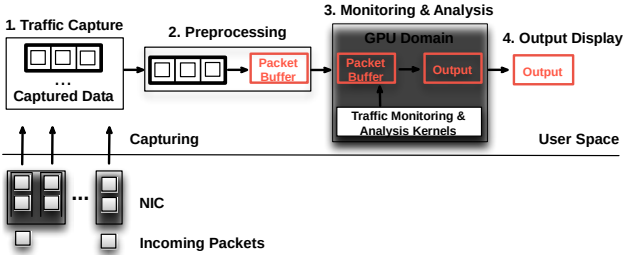
Приложението базирано на GPU за следене на мрежата за наблюдение и анализ работи в потребителски режим, за да се възползва от приятелската среда на GPU програмирането с CUDA и OpenCL. Както е показано на фигура 1, модела се състои от четири типа логически единици: прихващане на трафика, предварителна обработка, мониторинг и анализ, както и дисплей за визуализация.

- Прихващане на трафика. Прихваща се мрежовия трафик и го премества от канал към CPU. Прихващане на трафика има за цел да улови пакети без загуба, дори и при високи скорости на предаване на пакети.

- Предварителна обработка. Обработва прихванатият мрежов трафик и копия на пакетите от CPU към GPU.

- Мониторинг и анализ. Изпълнява мрежови мониторинг и анализ използващ GPU процесори. Реализиран с GPU библиотека за мониторинг на мрежовия трафик и анализ. Библиотеката се състои от различни CUDA ядра, които могат да бъдат комбинирани по различни начини за изпълнение на предвидените операции за наблюдение и анализ.

- Дисплей за визуализация. Резултатите от мониторинга и анализ на мрежата са визуализират или съхраняват.



Фигура 1 Архитектура

Когато системата е в експлоатация, тези тип логически единици работят в сътрудничество за извършване на планираните

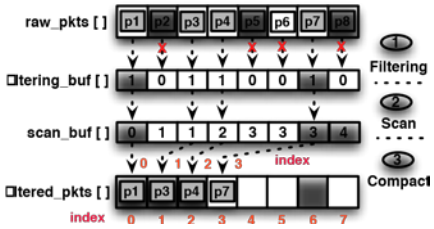
задачи. За една и съща група на мрежовия трафик, логическите единици са в режим на конвейер с последователност: " Прихващане на трафика → Предварителна обработка → Мониторинг и анализ → Дисплей за визуализация." За различните групи на мрежовия трафик, тези логически единици работят в паралел за да се максимизира общата производителност от операциите.

Експериментите показват, че със система може да се постигне изключително висока производителност. Приносът на е:

- Доказва се, че GPU може значително да ускори мониторинг на трафика и анализ на висикоскоростни мрежи. С едно Nvidia GPU M2070, система може да се справи с 11 милиона и повече пакети в секунда без да бъде загубени пакети.

- В момента се изготвя и прилага обща I/O архитектура, за да се следи мрежовия трафик от канал до GPU. I/O архитектурата позволява мрежовия трафик, да бъде прихванат и копиран към GPU без загуба на пакети.

- Приложението на GPU библиотека за следене мониторинг и анализ на мрежовия трафик. Библиотеката се състои от различни CUDA ядра, които могат да бъдат комбинирани по различни начини за изпълнение на задачи за мониторинг и анализ. Фигура 2 илюстрира механизма за филтритане на пакетите към ядрото. За мониторинг и анализ на мрежи с висока скорост, се използват разширените възможности за пакетно филтриране на скорост в канала са необходими, така че може да се следят и анализират само тези пакети, които са от интерес който ни е необходим. Пакетното филтриране включва в себе си набор от правила с които да работи. Ако даден пакет съвпадне със зададените правила, пакетът ще бъде приет, в противен случай, този пакет ще бъде отхвърлен. Тъй като Packet Filter Berkeley (BPF) [3] е най-широко използваният пакетния филтър, той е използван основен. Богатството и изразителността на синтаксиса BPF позволява да филтрирате различни типове мрежов трафик.



Фигура 2 Механизъм за филтритане на пакетите към ядрото

ЛИТЕРАТУРА

1. Han, S. et al. PacketShader: a GPU-accelerated software router, In Proc.
2. ACM SIGCOMM'10.
3. Luigi Rizzo, Netmap: a novel framework for fast packet I/O, In Proc.
4. USENIX ATC'12.
5. McCanne, S. et al. The BSD packet filter: A new architecture for userlevel packet capture. In Proc. USENIX Winter 1993.
6. Wu, W et al. G-NetMon: A GPU-accelerated network performance monitoring system for large scale scientific collaborations. In IEEE LCN'11, 2011.

СОФТУЕРНА РЕАЛИЗАЦИЯ НА КЛАСИЧЕСКИЯ СТЕГАНОГРАФСКИ СПОСОБ „CARDAN GRILL”

ДОБРОМИР К.АПОСТОЛОВ , СТАНИМИР С.СТАНЕВ

SOFTWARE IMPLEMENTATIONS OF CLASSICAL STEGANOGRAPHY TECHNIC „CARDAN GRILL”

DOBROMIR K.APOSTOLOV , STANIMIR S.STANEV

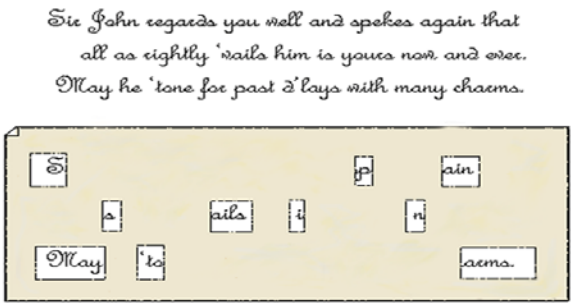
ABSTRACT: *The report examines algorithm and implementation program of the combination of two classic steganographic tecnics - Cardan grill and newspaper code. Specifically considered is the module that generates the grill. Given are promising directions for the computer implementations of other classic methods.*

KEYWORDS: *Steganology, steganography, information hiding, cardan grill.*

От древните времена, откакто са изобретени писмените знаци, до съвременните информационни технологии, защитата на важна информация от нежелано разкриване не е загубила своята актуалност. Един от аспектите на информационната сигурност е скриването на информацията. За постигане на тази цел като най-ефективни постепенно са се оформили две основни направления – скриване на съдържанието на съобщенията чрез използване на шифри, и скриване на самото съществуване на такава информация при нейното съхраняване или предаване. Второто направление включва много техники и средства за скриване на наличието на тайни съобщения, знанието и техническите умения за които се се обособили в научно-приложна област, наречена днес стеганография. Макар че думата „стеганография” се използва за пръв път през XVI век от немският абат Йоханес Тритемеус (Johanes Trithemeus) , използването на стеганографски методи започва от преди няколко хиляди години. Много от изобретени стеганографски средства,техники и методи са разгледани в редица публикации, но е невъзможно да се отразят всички [1].

Интернет и компютърните мрежи откриха нови възможности за скрита връзка. Развиха се нови високотехнологични методи за стеганография за защита на чувствителна информация. Но както и почти всяко изобретение, неговата „тъмна" страна е използването му от хора и организации за незаконни действия. Защитата от такива действия изисква специалистите по стеганографска защита да познават добре както средствата на съвременната стеганография, така и принципите на скриване на съобщения с класически средства, развивани през годините. Още повече, е според специалистите , съвременните престъпници не използват винаги за комуникация съвременни методи пради развитите средства срещу такива методи, а по-скоро използват компютърните мрежи като среда за реализиране на системи от условни знаци, пренаредени фрази и символи и други средства (някои ги наричат средства на нискотехнологична стеганография) [2].

През XVI век век италианският математик Джироламо Кардано преоткрива древния китайски метод на тайнопис – използването на шаблони с дупки, през които върху чиста хартия се пише секретното съобщение. След това се снема шаблона, и между написаните букви се написват други букви, части от думи и цели думи, образуващи заедно с предишните невинен текст. Разбира се, предварително еднакви шаблони (скари) получават и подателите, и получателите на тайните послания. На фиг. 1 е показан модел на скарата, използвана в средновековна Европа за прочитане на тайни съобщения, вложени в текста на писмо [2].



Фиг.1

Историческите извори разкриват събития за използването на стеганографски техники и в българските земи. В новата ни история това е тайнописът, използван от революционерите от периода на националното ни възраждане, в това число и от Апостола на свободата Васил Левски. Разгледаните като криптографски в [3] средства, използвани от него и комитетите - симпатични (невидими) мастила и шаблони (наричани „скари", „лозинки", „книги"), сега могат по-коректно да се класифицират като средства на класическата стеганография. Сега този метод се приписа на Кардан , а шаблонът се нарича „Скара на Кардан". Може да се счита че тези скари са ранен образец на секретен ключ (стего ключ) [4].

По-късно, по време на Викторианската епоха, любовници са изпращали тайни писма чрез дупчене с игла над определени букви във вестникарски статии. Писмата са били четени след подреждането на маркираните по този начин букви. Този метод все още се използва - нарича се вестник- код [5].

Тези два способа днес специалистите пречисляват към текстовата стеганография, компонент на лингвистичната стеганография [6,7]. Лингвистичната стеганография е също дял от класическата стеганография, но при развитието на съвременните технологии, нейните методи се реализират основно с компютърни системи и софтуерни продукти.

В днешно време високата интензивност на текстовия трафик в Интернет дава възможност за предаване на секретни съобщения чрез директното им поставяне в съществуващите текстове, оставайки ги незабелязани. Текстовата стеганография се занимава именно с това. При това за нея е важно да бъде съхранен съществуващия текст по смисъл и съдържание.

Лингвистичните стеганографски системи са един от най-сложните обекти за атаки и от нарушители, и от стеганалитици. Поради това разработването на примерни модели за класическите им форми и тяхната реализация дори и с познавателна гледна точка, биха допринесли за по- доброто разбиране на принципите на построяване , като предпоставки за разрушаването на такава система.

Целта на разработката е компютърното моделиране на класически стеганографски способ – „скара на Кардан”, и възможността за комбинирането му с метода „вестник-код”.

Редът за реализация на класическия метод „скара на Кардан”, е следният:

1. Подателят на тайните послания изработва от картон шаблон („скарата на Кардан”) – в картона се изрязват отвори, през които върху лист с хартия се изписват след това букви или срички, от които се съставя тайното съобщение.
2. Изработват се копия на шаблона и по секретни канали се доставят на всички кореспонденти.
3. От подателя с използване на шаблона се изписва върху лист хартия секретния текст.
4. Подателят съчинява произволен (но смислен) текст, съставен от думи и срички, свързващи в „невинен” текст елементите на сектерното съобщение.
5. Писма с явния текст се разпращат на получателите.
6. Всеки получател използва своятя скара, за да прочете сектерното послание.

Основният недостатък на този метод (освен сложното доставяне на „скарите”) е необходимостта от точното изработване на копията на шаблона и позиционирането им точно върху получените писма. Тези недостатъци са се проявявали и в практиката на нашите революционни комитети и понякога са пречели на коректното четене на тайните съобщения [3] .

Естествено, при компютърната реализация на електронната скарата остава само проблема с нейната секретна доставка.

Предлага се разработена софтуерна реализация на посочените класически стегометоди. Програмата се състои от следните модули:

1. Модул за генериране на еднократна скара.
2. Модул за генериране на универсална скара.
3. Семантичен модул за генериране на явен текст.
4. Модул за криптиране и предаване на скарите.

За да се комбинират двата класически метода , е променен посоченият алгоритъм по следният начин (фиг. 2).

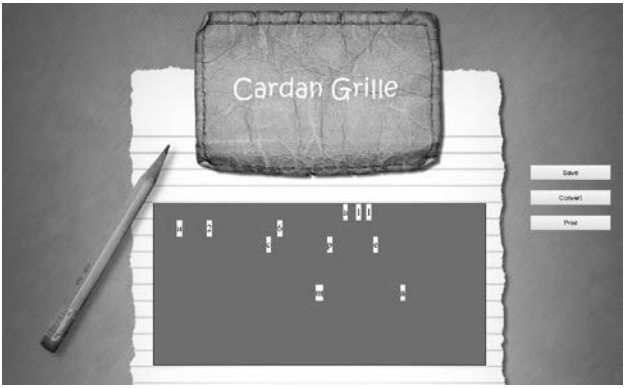
Фиг. 2

Програмата на модула за генериране на еднократна скара реализира следния алгоритъм:

-първи етап – съставя се се тайното послание;

-втори етап – изработва се контейнера (текста, в който ще бъде скрито тайното послание). В него се съдържат всички знаци ,последователно разположени, с различно отстояние между тях. По тази начин в края на този етап имаме и запълване на контейнера, чрез влагане в него на скритата информация .

-трети етап - подготовка и изработване на стегано ключа. Реализацията на този етап става чрез подготовката и изработването на „Скарата на Кардан“.



Фиг. 3

На фиг.3 е показан екрана при работа на този модул. За функционира системата, на екрана има следните полета:

- Поле за въвеждане на текста контенер, в същото поле да може да се избират буквите за скритото съобщение. Тук се създава и шаблона („скарата“), която позволява при налагане на върху текста да се прочете съобщението. „Скарата“ трябва да се появява върху самия текст, като има възможност след това да се скрива отново и да се вижда текста.

-Поле, в което да бъдат реализирани бутоните за действия:

-Съхраняване на въведения текст

-Конвертиране на текста в шаблон „Скара“

-Принтиране на получените елементи

За улесняване на работата с продукта има и кратка пояснителна информация, която да излага алгоритъма за работа с продукта. Тази пояснителна информация е поместена на удобно място, като тази информация не е постоянно видима, за да не се бърка с реализацията на метода. Поради тази причина е предвидено тя да се реализира чрез бутон, който да бъде в отделно поле така че да не се бърка с функционалните бутони. Бутонът от своя страна извиква пояснителните данни във вид, удобен за четене, в нов прозорец.

Скарата се нарича единична, защото се получава на базата на един открит текст (по аналогия с вестник-кода). Тя може да се използва в две направления- да послужи за шаблон за генериране на други скрити

съобщения и открити текстове, и директно за разшифроване на предадения в първия случай явен текст, от който е формирана.

След подготовката на стеганоконтейнера и стегано ключа, реализирания програмен модул, позволява те да бъдат отпечатани, като по този начин се позволи пълна реализация на класическия стеганографски метод.

Програмният модул за генериране на единична скара е разработен с използването на Web- тегнологиите JavaScript, HTML 5.0 и библиотеката JQuery [8]. Тя е бърза и богата на JavaScrip фукции и обекти. Библиотеката позволява чрез удобен интерфейс леко манипулиране на HTML документи, обработка на събития, анимации с Ajax, в различни браузъри. На фиг. 3 е показан диалоговия екран след маркиране със скара на тайно съобщение от предварително въведен явен текст.

Модулът за генериране на универсална скара определя първо дължината (в символи) на секретното съобщение и формира скара за създаване на скрито съобщение в рамките на явен текст , поместен на стандартен лист хартия формат А4.

Най-сложният проблем е да се синтезира явен тест- контейнер.

В разработката е представен само първият модул. Детайлното описание на другите е предмет на други публикации

В областта на лингвистичната стеганография постоянно излизат нови публикации и разработки. Със сигурност ще се създадат нови и по-сложни техники и ефекта от това ще бъде увеличеният риск те да бъдат използвани за злонамерени цели. Това повдига нови предизвикателства пред трудния въпрос за предоставяне на информационна сигурност [9].

Едно от средствата за подготовка на специалисти по стегозащита е и компютърната реализация на нискотехнологични стеганографски методи.

Съществуват и други идеи за компютърна реализация на класически стеганографски техники, но тяхното разглеждане излиза извън целите на настоящата работа.

ЛИТЕРАТУРА:

1. Judge,J. Steganography: Past, Present, Future. SANS Insitute, 2001. [онлайн].[прегледан 19 април 2012]. http://www.sans.org/ reading_room/ whitepapers/stenganography/steganography-past-present-future/552.php.
2. Conway, M. Code Wars: Steganography, Signals Intelligence, and Terrorism. Knowledge, Technology and Policy (Special issue entitled 'Technology and Terrorism') Vol. 16, No. 2 (Summer 2003): [онлайн]. [прегледан 28.05.2012]. http://doras.dcu.ie/494/1/know_tech_pol_16 _2_ 2003.pdf.
3. Илиев, И. Симпатични мастила, „скари" и цифрови шифри, използвани от Васил Левски в периода 1870–1872 г.В:Исторически преглед, 2005, № 5–6, стр. 62–63.
4. Станев, С., Стеганологична защита на информацията. Шумен: Университетско издателство „Еп. К. Преславски", 2013. ISBN: 978-954-577-825-??
5. Cox,I., Miller,M., Bloom,J., Fridrich, J. and T. Kalker. Digital Watermarking and Steganography, Second Edition. Elsewier, Morgan Kaufmann Publishers, 2008.
6. Хорошко,В. и А.Чекатков. Методы и средства защиты информации. [онлайн]. [прегледан 27.04.2013].http://www.spectrall.ru/metody-i-sredstva-zashchity-informatsii-str1.html.
7. Алексеев А. и В. Орлов. Стеганографические и криптографические методы защиты информации. Самара: ИУНЛ ПГУТИ, 2010, стр. 330. ISBN 978-5-904029-12-8.
8. Библиотека JQuery - http://jquery.com/
9. Христов, Х. Организация и управление на оперативното противодействие на нерегламентиран достъп до чувствителна информация в социалната организация. В: Сборник научни трудове на научна конференция „Защита на информацията –състояние и перспективи" на АПВОКИС, Шумен, 2012. стр.

ИЗСЛЕДВАНЕ ЕФЕКТИВНОСТТА НА ГРАВИМЕТРИЧНИТЕ ПОСТРОЕНИЯ ПО МНМК

Андрей И. Андреев

Красимира К. Кирилова

EXPLORATION OF THE EFFECTIVENESS OF GRAVIMETRIC FRAMES WHIT MNMS

Andrey I. Andreev

Krasimira K. Kirilova

***ABSTRACT**: The subject of the study is the evaluation of the effectiveness of gravimetric frames by equalization of gravimetric data in two different methods - standard method and the method including the amendment of drift, as extra unknown in pre-processing of the data.*

Proposed method of equalization may find application in the practice as creates prerequisites for significant concessions in the overall technology of measurement and processing of gravimetric measurements, provided that zero of the tool retains linear character of offset.

***KEY WORLDS:** МНМК, дрейф, гравиметър*

Гравиметричните измервания еволюират от древността до наши дни. Началото им е свързано с първите опити за определяне фигурата на Земята. Принципите и методите на гравиметричните измервания претърпяват голямо развитие в последните години, особено с навлизане на спътниковите технологии в геодезията. Гравитационното поле на Земята в геодезията служи за внасяне на корекции в геодезическите измервания и инерциалните системи в геодезията, координирането и навигацията. На практика гравитационното поле определя орбитите на

спътниците, естествените географски координати и височините в геодезията. Използването на нови математически модели и методи на анализиране на резултатите успешно решават геодинамичните проблеми.

За да се анализира ефективността на гравиметричнте построения по метода на най-малките квадрати (МНМК), е необходимо да се решат следните задачи:

- Да се анализират данните от гравиметричните измервания и резултатите от обработката им;
- Да се да се направи сравнителен анализ на получените резултати по различни методи.

1. Анализ на данните от гравиметричните измервания и резултатите от обработката им

1.1 Анализ на гравитационното поле на Земята, аномалното поле и редукциите

Гравитационното поле на Земята се задава с полето на силата на тежестта или по-точно със големината на вектора на ускорението на силата на тежестта $\vec{g}$. Същата се явява резултантна на две основни сили: силата на привличане ***b*** на Земята и центробежната сила ***c***, дължаща се на денонощното въртене на Земята около оста си, както и привличането на Луната, Слънцето, други небесни тела и масата на земната атмосфера.

Стойността на силата на тежестта на земната повърхност зависи от фигурата и вътрешното разпределение на масите на Земята. Ето защо изучаването на гравитационното поле на Земята доставя ценни данни за фигурата и вътрешният й строеж. Величината на силата на тежестта измерена на физическата земна повърхност (ФЗП), определя също и геометричните характеристики на повърхнината на Земята. Реалното гравитационно поле може да се представи като нормално и смутено гравитационно поле.

Нормалното гравитационно поле има главно две предназначения:

- да служи като добро приближение на реалното гравитационно поле, за да може в случай на липса на данни от измервания на реални характеристики (например силата на тежестта) по формули, основани на приетия модел, да бъдат изчислени техни приближения.

- да се отдели една значима част (като нормално гравитационно поле) от реалното гравитационно поле, за да се провеждат изчисленията върху една относително малка остатъчна част, наричана

аномално гравитационно поле. Тя именно представлява смутеното гравитационно поле.

Съгласно теорията на потенциала на земното гравитационно поле тези три полета се представят с реален, нормален и смущаващ потенциал. Дефинирането на тези потенциали е неизбежно свързано с непосредствени гравиметрични измервания и изчисления.

1.2 Анализиране методите за измерване на силата на тежестта

Основните методи за измерване на силата на тежестта са абсолютното и относителното определяне на силата на тежестта.[3],[6]

Абсолютното определяне на силата на тежестта е на принципа на определяне на стойностите на разстоянията и времето, чрез които се изразява стойността на силата на тежестта. Наблюдава се свободното движение на пробна маса в гравитационното поле. По настояще при метода на свободното падане се постига точност от $\pm 10^{-7} - 10^{-9} g$. С усъвършенстваните инструменти и методи могат да се предвидят систематичните грешки. Основен метод за абсолютни измервания е махалния метод. Балистичен метод също се използва за изследване на свободно падащо тяло в гравитационното поле. Средна квадратна грешка за единично измерване е ± 0.3 – 5 μms^{-2}, за серия от измервания 10 – 100 ±0.05 –0.3 μms^{-2}, за последователност от 10 – 30 серии (1- 3 денонощия) ±0.02 – 0.1 μms^{-2}.

С откритието на лазера и атомните часовници се повишава точността на абсолютните измервания. Интерференционния метод на измерване на разстояния е усъвършенстван с помощта на кохерентното и монохроматично излъчващите лазерите.

Относителните махални измервания определят разликата между силата на тежестта в дадена точка спрямо някоя друга, служеща за изходна. Относителните измервания се разделят на *динамични* и *статични.*

При относителните динамични измервания влияят различни източници на грешки. Основната е колебанието на махалото. Ако се увеличи продължителността на наблюдение до час и повече може да се пренебрегнат систематичните грешки от измерването на времената, а също и влиянието на смущаващото вертикално ускорение. Различните схеми на измерване позволяват в значителна степен да се намали влиянието от формата и деформацията на махалото. Ако амплитудното колебание, температурата и разликата във всички точки на наблюдение

е една и съща, то влиянието на периода на колебание съществено се намаля. Също влияние оказва люлеенето на статива и микросеизмичните движения. Тези грешки се отстраняват като се използват различни махални апарати и повторенията на наблюденията в контролните точки.

При относителните статичните методи действието на силата на тежестта върху пробна маса поражда противодействаща сила, която може да се измери. При този принцип на измерване на силата на тежестта с вертикална пружина се използват следните видове – свободно окачена тежест на пружина, окачена тежест на рамо свързано с пружина и уравновесяване на тежест с навита пружина.

1.3. Анализ на приборите за измерване на силата на тежестта

Приборите използвани за определяне на силата на тежестта се наричат гравиметри. В зависимост от редица фактори те се класифицират по следните по важни признака:

- по вида на тялото, което създава еластична сила Q;

- според материала, от който са направени пружините на механичните гравиметри;

- по начина на преместване на чувствителния елемент;

- по начина на отчитане.

В практиката свързана с геодезически и геоложки проучвания масово се прилагат относителни гравиметрични измервания. Поради това обект на внимание са релативните статични гравиметри. Съвременните статични гравиметри имат висока чувствителност и точност на измерванията, достигащи до няколко хилядни от милигала, малка продължителност на наблюденията до 2-3 минути на точка, висока портативност, елементарна техника на измерване и обработка. Тези качества правят гравиметрите подходящи за извършване на подробна гравиметрична снимка и за построяване на опорни гравиметрични мрежи.

Гравиметрични измервания включват следните дейности- Калибровка на гравиметри Еталониране на гравиметъра; полски измервания с гравиметри. При измерванията е необходимо да се изпълнява стриктно технологията на завода производител или разработената методика на базата на дългогодишни изследвания и опит.

Гравиметрични измервания могат да са наземни, въздушни, спътникови и морски. Те служат за създаването на: [1],[5]

- Гравиметрични мрежи.

  - Световна гравиметрична мрежа (IGSN-71).

  - Световна абсолютна гравиметрична мрежа (IAGBN).

  - Национални (държавни) гравиметрични мрежи.

  - Държавна гравиметрична мрежа на Р. България.

  - Еталонна гравиметрична мрежа.

- Гравиметрични снимки

Обработка на резултатите от гравиметричните измервания включва етапи като:

- Предварителна обработка на резултатите.

- Параметрично изравнение.

- Условно изравнение.

Източници на грешки при измерванията с гравиметрите са инструментални и външни.

Много голямо значение се отдава на намаляване на ефекта от дрейфа, което се постига чрез предварително съставени програми за измерване по определени методи. При стационарните наблюдения и работата в поле, с течение на времето се изменя отчета на гравиметрите. Този ефект се нарича смущение в нулпункта (дрейф) на гравиметъра. Характера и големината на дрейфа зависят от;

- типа и характеристиките на инструмента – чувствителната система на гравиметрите със своите термоеластически свойства. Кварцовите гравиметри имат по-голям дрейф от металните гравиметри.
- възрастта на прибора и интензивността на използване.
- разликата в окръжаващата температура при транспортирането и измерванията, а също и вибрациите и сътресенията върху чувствителната система.
- влиянието от атмосферните условия при транспортиране и измерване, а също и вибрациите и сътресения на чувствителната система.

Дрейфът може да се разложи на две съставни части :

- стационарен дрейф – стареене на пружината, дългопериодичните разлики от температурата и налягането.

- дрейф при транспортирането - сътресения при транспортирането, краткопериодични температурни разлики, появяващи се при полеви измервания.

Моделирането на дрейфа на гравиметъра е на основата на развитието на функцията на отчета z за време t в Тейлоров ред.[6]

(1)

$$z(t\} = z(t_0) + \left(\frac{\partial z}{\partial t}\right)_0 (t - t_0) + \frac{1}{2}\left(\frac{\partial^2 z}{\partial t^2}\right)_0 (t - t_0)^2 + \frac{1}{6}\left(\frac{\partial^3 z}{\partial t^2}\right)_0 (t - t_0)^3 + ...$$

t_0 - начален момент на измерването. Заместваме коефицентите на производните с означенията d_1, d_2,……..и получаваме полинома:

(2)

$$z(t\} = z(t_0) + d_1(t - t_0) + d_2(t - t_0)^2 + d_3(t - t_0)^3 + ... = z(t_0) +$$

$$+ \sum_{p=1}^{s} d_p (t - t_0)^p = z(t_0) + D(t),$$

Моделирането на дрейфа е основна закономерност преди извършването на гравиметрични измервания. Необходимо е извеждането на коефициентите d_1, d_2….., като принципа на извеждане зависи от типа на гравиметъра и от отделно всеки един прибор има своите характерни стойности за коефициентите. Където $z(t_0)$ отчет в момента, в който се задава модел на дрейфа. Коефициентите на уравнението на дрейфа се намират чрез повторни измервания, който трябва да следват равномерно във времето в зависимост от типа дрейф (линеен, нелинеен, скокообразен) и големината му, а също и от необходимата точност и типа на модела гравиметър. След определянето на дрейфа за оценка избраните модели на дрейфа може да се направи статистическа проверка. Разработени са различни схеми на полски измервания:

2. Експериментални изследвания за определяне на дрейфа с прилагане на изравнителни изчисления по МНМК

Направен е експеримент като са сравнени два метода на параметрично изравнение.. Първият метод представлява стандартен подход на изравнение на гравиметрични данни прилаган в практиката.

При него се налага предварителна обработка на данните за определяне изменението на дрейфа на нулата на инструмента, преди параметричното изравнение.

При втория метод е предложено решение, при което не се налага предварителна обработка на данните заради дрейфа на нулата, а се пристъпва към параметрично изравнение, като дрейфа на нулата се включва като допълнително неизвестно.

Обект на изследването е една от проблемните сеизмогенни зони в България - Горнотракийската низина.

- *Изходни данни за изследванията*

За изследването, любезно ни бяха предоставени данни от прецизни гравиметрични измервания на Института по геофизика, геодезия и география при БАН. Измерванията са осъществени чрез три съвместни експедиции на ЦЛВГ с Кралската обсерватория на Белгия, по съвместен международен проект за комплексно изследване на зоната на земетресенията от април 1928 год.

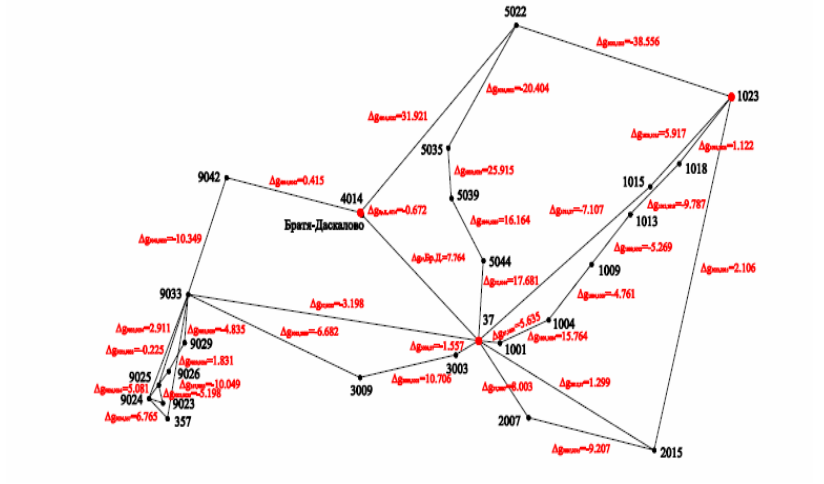
Гравиметричните измервания са направени на Чирпанския сеизмичен полигон (фиг. 1) в периода 12 – 16 май 2004 г. За целта е използван руския кварцов астезиран гравиметър ГАК-7Т №524 с константа $K = -6.8550$. Измерванията са проведени по репери от Държавната нивелация I и II клас по профилите, пресичащи главните разломи в района. Измерванията в изследвания район са привързани към гравиметрични станции от Основната гравиметрична мрежа на България в градовете Пловдив, Стара Загора, Поповица и Братя Даскалови.

- *Обработка на гравиметричните данни*

В карнетите са отбелязани инструментът, неговата константа, номерата на точките, както и датата и часът на всяко измерване. За всяка точка са направени три отчета в mGal, които биват осреднени. Средните отчети са коригирани с константата на гравиметъра, като се записва тяхното произведение.

Земната кора се влияе от привличащата сила на небесните тела. Поради тази причината са въведени приливни корекции върху измерванията, за премахване на дългопериодичния дрейф, зависещи от деня и часа на конкретното измерване. Приливните корекции се отчитат от таблици в зависимост от времето на измерването и часовата зона. Тъй като приливните корекции са сравнително малки величини,

те са записани в дименсия μGal. По този начин отчетите се записват с нанесени приливни корекции към тях.



Фиг.1 Чирпанския сеизмичен полигон

Изчислява се също така и редуцираното време, което представлява разликата между времената на извършване на две съседни по време измервания в една и съща станция. Така полученото редуцирано време е записано в дименсия минути. Отбелязва се времето от началото на рейса също в дименсия минути. То се пресмята като брой минути от началото на денонощието до часът на съответното измерване.

Изчисляват се разликите в силата на тежестта между измерените точки. Това се осъществява като се пресмятат разликите между коригираните отчети с константата на гравиметъра и с приливните корекции между две съседни точки. Разликите в силата на тежестта са записани в дименсия mGal.

Към всеки карнет се прилага схема на измерените точки от мрежата.

- *Изравнение на гравиметричната мрежа по МНМК-параметрично изравнение.*

- Стандартен подход налагащ предварителна обработка на резултатите от гравиметричните измервания.

Подобно на останалите видове геодезически измервания и при гравиметричните се прави предварителна обработка на резултатите. По този начин се добива представа за качеството на измерванията. [2],[4]

Приемат се следните означения:

ΔO_i – изменение в отчета, което се дължи на дрейфа на нулата ;

U_i – влияние на дрейфа на нулата в точка i .

При прост гравиметричен рейс:

(3) $$U_i = C\frac{O_i^{"} - O_i^{'}}{t_i^{"} - t_i^{'}}$$

където:

C – константа на уреда;

$O_i^{"}$ и $O_i^{'}$ – отчети направени с гравиметъра;

$t_i^{"}$ и $t_i^{'}$ – времената, в които са направени отчетите;

i=1,2,…,n;

n – брой гравиметрични станции.

Ако с Ū означим средна тежестна стойност на дрейфа на нулата, тогава получаваме:

(4) $$\overline{U_i} = \frac{\sum_{i=1}^{n} U_i p_i}{\sum_{i=1}^{n} p_i}$$

където:

Pi – тежест на i-тото измерване.

Тежестта се изчислява по следната формула:

(5) $$p_i = \frac{c}{m_i^2}$$

където:

m_i – средната квадратна грешка на i-тото измерване;

c – константа, която се избира за всички измервания;

(6) $$m_i^2 = m_i^{'2} + m_i^{"2}$$

Във всяка станция могат да бъдат направени няколко измервания и по този начин могат да бъдат намерени m_i т.е. m_i е функция на $o_i^{'(1)}, o_i^{'(2)}$ ....., $o_i^{'(k)}$.

(7) $$\overline{O}_i^{'(1)} = \frac{1}{k}\sum_{j=1}^{k} O_i^{'(j)},$$

където:

$\overline{O}_i^{'}$ – средна стойност на измерванията;

k – брой измервания.

Поправките се изчисляват по следната формула:

(8) $$v_i^{'(j)} = O_i^{'(j)} - \overline{O}_i^{'}$$

Тогава:

(9) $$m'_i = \pm\sqrt{\frac{[v'v']}{k-1}}$$

Като се имат предвид следните зависимости би могло да се изчисли тежестта на i-тото измерване:

(10) $$m_i^2 = m_i^{'2} + m_i^{''2}$$

$$m_i^2 = \frac{1}{p'_i} \text{ и } m''^2_i = \frac{1}{p''_i}$$

Тогава:

(11) $$\frac{1}{p_i} = \frac{1}{p'_i} + \frac{1}{p''_i}$$

Тежестта е обратно пропорционална на временния интервал между дадения начален момент (t_o) и момента на измерване на станцията:

(12) $$p'_i = \frac{1}{t_i^{'} - t_0}$$

където:

t_o – начален момент;

$t_i^{'}$ – първо измерване на i-тата станция;

За времето на първото измерване на първата станция, съвпадащо с началния момент ($t_o \equiv t_i^{'}$) тежестта е равна на единица (p'_i=1).

Аналогично:

(13) $$p''_i = \frac{1}{t_i^{''} - t_0}$$

Тогава за тежестта на i-тото измерване получаваме следния израз:

(14) $$p_i = \frac{1}{t_i^{'} - t_i^{''} - 2t_0}$$ и

$$p_i = \frac{p_i^{'} p_i^{''}}{p_i^{'} + p_i^{''}}$$

Коригираните отчети могат да се запишат по следния начин:

(15)

$$\overline{O_i} = O_i + \overline{U_{cp}}(t_i - t_0)$$

Сумират се разликите в силата на тежестта за всеки затворен полигон и се получават несъвпаденията за съответния затворен полигон.

(16) $$\sum_j^i \Delta g'_{ij} = \omega \approx 0$$

Разхвърля се несъвпадението върху разликите на силата на тежестта за всяка стойност спрямо времето на наблюдение. Намираме времето на продължителност за всеки рейс.

(17) $$\Delta t = t_1^H - t_1^{кр.}$$

Поправената стойност на силата на тежестта Δg_{ij} се получава по формулата:

(18) $$\Delta g_{ij} = \Delta g'_{ij} - \frac{\omega}{\Delta t}\Delta t_{ij},$$

където $\Delta t_{ij} = t_j - t_i$ е разликата във времето на отчитане между точките *j* и *i*.

Заключение:

Обектът на изследването е оценката на ефективността на гравиметричните построения чрез изравнение на гравиметрични данни по два различни метода – стандартен метод и метод включващ изменението на дрейфа като допълнително неизвестно в предварителната обработка на данните.

Предложения метод на изравнение може да намери приложение в практиката като създава предпоставки за значителни облекчения в цялостната технология на измерване и обработка на гравиметричните измервания, при условие, че нулата на инструмента запазва линейния си характер на изместване.

Литература:

1. **Андреев А**. „*Учебник по Физическа геодезия и гравиметрия* “ , Шумен , 2013 г.
2. **Андреев А.** „*Ръководство за упражнениия по физическа геодезия и гравиметрия* “, Шумен , 2013 г.
3. **Веселов, К.Е**. Гравиметирческая съемка, Москва, “Недра”,1986
4. **Михайлов Пл.** „*Ръководство за упражнения по геодезични мрежи* “ **,** Шумен , 2007 г.
5. **Младеновски Мл.,** Принос към работите и изследванията в България в областта на гравиметрията и свързаните с нея геодезични проблеми. Автореферат към дисертация. НИИГиФ към ГУГКК. Секция "*Висша геодезия - опорни мрежи"*
6. **Торге, В.** Гравиметрия. Пер. с английского под редакцией ктн. А.П.Юзефовича, Москве "Мир", 1999г.

ИЗСЛЕДВАНЕ НА ПРИЛОЖЕНИЕТО НА ГРАВИМЕТРИЧНИТЕ МЕТОДИ ЗА ДЕФИНИРАНЕ НА СЕИЗМОГЕННИ ЗОНИ И ФИЗИЧЕСКИ ПРОЦЕСИ

Андрей И. Андреев

Кирил Ф. Янчев

STUDY OF THE APPLICATION OF GRAVIMETRIC METHODS FOR DEFINING THE SEISMOGENIUS AREAS AND PHYSICAL PROCESSES

Andrey I. Andreev

Kiril F. Yanchev

***ABSTRACT**: Geodesies studies of the modern movements of the earth's crust caused by seismotectonics reasons are an important part of learning of seismogenius areas. Geodesies measurements allow to determine and trace the spatial position of material on the ground control points. Set in some of their moving in space and in the development of fast and slow movements, given the opportunity to be acquainted processes of accumulation, liberation and transfer of tectonic economic shifts voltages.*

KEY WORLDS:** ДНМ, ИГГГ, БАН, WGS'84**.

Изучаването на фигурата на Земята е основна задача на науката „Геодезия". Това е пряко свързано с познаването на външното гравитационно поле на Земята. Геодезическите измервания, както и човешката дейност се обуславят пряко от гравитационното поле. Изучаването му е свързано с преки измервания, тъй като неговото непосредствено моделиране е невъзможно. Познаването на плътността и структурата на Земята е от голямо значение, тъй като действителният

градиент на силата на тежестта W се променя регионално и локално под въздействието на топографските маси и промяната на плътността под земната покривка. Това дава решения на много от геодезическите задачи. [1]

Основна задача на науките за Земята е да се изучат процесите, водещи до силни земетресения и да се открият и предприемат подходящи мерки за ефективно противодействие. Това характеризира проблема с особена степен на актуалност в световен и национален мащаб и го поставя в категорията на приоритетните научни направления.

В тази връзка в доклада е представено изследване за приложението на гравиметричните методи за дефиниране на сеизмогенни зони и физически процеси чрез:

- Анализ на гравиметричните методи за дефиниране на сеизмогенни зони и физически процеси.
- Оценка на експерименталните данни от физикогеографско описание на сеизмичен район от територията на Р.България.

1. Анализ на гравиметричните методи

Гравиметрията намира приложение при изучаването на земната кора и горната мантия, както и за определянето на структурите в дълбочина. Гравиметричните измервания са подходящи за откриване на полезни изкопаеми, при търсене и проучване на самото месторождение, за решаване на геоморфоложките и инженерногеоложките задачи, за контрол при режима на експлоатация на газови находища и газохранилища и др. [12,13]

Гравиметричните методи за изследване са основани на изучаването на естественото поле на силата на тежестта. Резултатите от измерването на силата на тежестта или наречено само гравитационно поле, дават възможност да се съди за разпределението на маси с различна плътност в изследвания подземен масив, както и дават представа за неговия състав и строеж.

Гравиметричните работи при експлоатационното проучване се състоят в измерване елементите на гравитационното поле на

изследвания подземен масив, внасяне на поправки в данните от измерванията и интерпретация на получените резултати.

Права и обратна задача от теорията на потенциала

При гравиметричната интерпретация на получените аномалии се решават две задачи от теорията на потенциала: [6]

Правата задача :

Дадени са един или няколко смущаващи геоложки обекта с определена форма, намиращи се на известна дълбочина и имащи определена аномална плътност (под аномална плътност се разбира разликата в плътността на някои обекти и среди). Необходимо е да се изчисли аномалното гравитационно поле, обусловено от тези среди.

Тази задача се решава еднозначно.

Обратната задача:

Дадено е аномално гравитационно поле. Трябва да се определи смущаващото тяло или тела, тяхната форма, дълбочинно разположение и аномална плътност.

Обратната задача от теорията на потенциала представена в общ вид няма еднозначно решение. Вариантите за решенията могат да бъдат намерени чрез въвеждане на ограничаващи условия, които се определят от допълнителни геоложки и геофизически наблюдения.

Обикновено при гравиметричната интерпретация се използва метода на сравнение на наблюдаваните аномалии с теоретически изчислените аномалии за различни случаи на разположение на геоложките обекти. Освен това се използват и общи представяния.

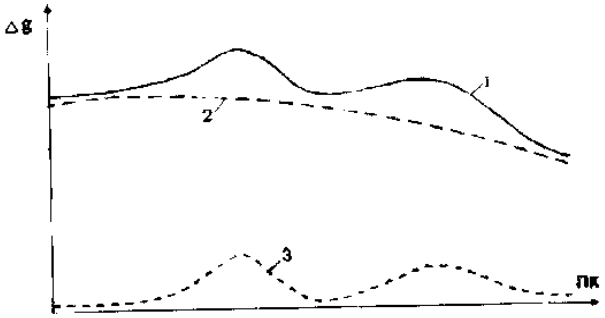
Сравнявайки наблюдаваните аномалии по профили с теоретически изчислените криви за търсените геоложки обекти може да се установи вида на смущаващия обект: право или наклонено стъпало, антиклинална гънка, наклонен слой и др.

За по-задълбочено тълкуване на наблюдаваните аномалии се извършват различни по своя характер математически обработки. Такава интерпретация се нарича „качествена”.

В практиката при оценяването на гравиметричните резултати (карти, графики и др.) се различават два етапа–количествен и качествен. При качествената интерпретация по формата на изолиниите Δg и графики на Δg може да се съди за местоположението, примерни размери и форма на геоложки обекти.

Първият етап от анализа на резултатите, получени от гравиметрични наблюдения се явява *качествената интерпретация*. Чрез нея се дава визуално описание на характера на аномалиите на силата на тежестта по карти и профили. Отбелязва се вида на аномалиите, тяхното разположение, примерни размери, амплитуди. Установява се връзка между гравитационните аномалии и геоложкия строеж. Разграничават се регионални аномалии, свързани със строежа на земната кора, регионални структури и тектонически зони, също и локални аномалии, свързани с утаечните скали, указващи местоположението на полезните изкопаеми.

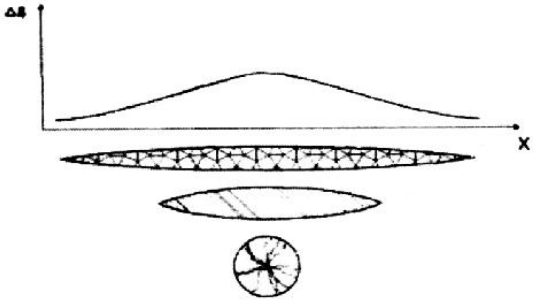
Отделянето на регионалните аномалии (плавното изменение на аномалиите $\square g$ на значително разстояние) от локалните е снемане на регионалния фон. Аномалиите на гравитационното поле представляват сума от гравитационния ефект на редица геоструктурни етажи и геоложки тела с различни закони за разпределение на плътността, форма и дълбочинно разположение. При тези условия не винаги може визуално да се установи аномалията в „чист" вид, неусложнена от съседни аномалии. По тази причина са разработени различни методи за преобразуване и трансформация на изходното (наблюдаваното) аномално поле, с помощта на които е възможно визуално да се представят, както локалната така и регионалната аномалия.



Фиг. 1. Наблюдавана „1", регионална „2" и локална „3" аномалия на силата на тежестта

На фиг.1. е представено графично изравнение на наблюдаваното поле и разделянето му на плавно изменящо се регионално поле и локални аномалии $\Delta g_{лок} = \Delta g_{набл.} - \Delta g_{рег.}$. По карти и графики за $\Delta g_{лок}$, $\Delta g_{набл.}$ и $\Delta g_{рег.}$, използвайки изводите от решението на правата задача е възможно да се направят качествени заключения за геоложките обекти, създаващи тези аномалии.

Количествената интерпретация на резултатите от гравиметричните измервания е основана на решаването на обратната задача и се свежда до определянето на местоположението, оценка на дълбочинното положение на центъра на тежестта, размера, понякога и излишната маса на аномално създаващите тела. Решението на обратната задача е неоднозначно.



Фиг. 2 Пример за нееднозначността на решението на обратна задача, в следствие на създадените еднакви аномалии на силата на тежестта от геоложки обекти с различна форма, размери и плътност.

При достатъчно обосновано предположение за формата на обекта и разделяне на отделните аномалии Δg се приема аналитичен метод за решаване на обратна задача, при които параметрите на аномално образуващите маси се определят по характерни точки от кривата Δg. Съществуват аналогични подходи и формули за изчисляване на дълбочината на тела с неправилна геометрична форма.

Количествената интерпретация може да бъде пряка, при която елементите на гравитационните маси се определят непосредствено от карти и графики Δg , *Wxz*, *Wzz* и др., и косвена, основана на сравнение между наблюдения и теоритични криви.

Методите за пряка интерпретация обезпечават получаването на информация за аномалното тяло, непосредствено от гравитационните аномалии, която в значителна степен се оказва независима от истинската форма на тялото.

2 Оценка на експерименталните данни

Анализиран е Сеизмотектонския модел на Маришкия сеизмичен район, които е създаден въз основа на идеята за съвременно развитие на разломяване и формиране на антитетични разсядания по периферията на планинските системи на Родопите и Средна гора. В

условията на регионална екстензия и некомпенсирано вертикално налягане под оградните планини, в Горнотракийската депресия се създават условия за активно разломяване, съпроводено със засилена сеизмична активност.

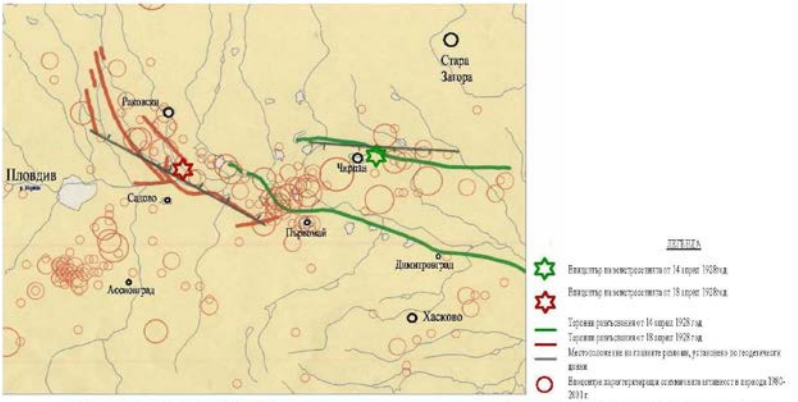
Обект на изследването е една от изявените сеизмогенни зони в България - Горнотракийската низина, известна в сеизмичен аспект най-вече със земетресенията от април 1928 г. в района на Чирпан и Пловдив. За изследванията любезно бяха предоставени данни от прецизни гравиметрични измервания на Института по Геофизика, Геодезия и География (ИГГГ) при БАН. [10]

Гравиметричните изследвания са важна част от изучаването на сеизмогенните зони, която дава информация за главните тектонски нарушения в земната кора – сеизмогенните разломи. За тази цел по-подробно са представени описанието на обекта, представяне на изходните данни за изследването, сгъстяване на мрежата от гравиметрични станции, ибработка на данните, анализ и интерпретация на получените резултати.

Физико-географско описание:

- Географско положение, граници и големина.
- Геоложки строеж.
- Развитие на релефа.
- Инженерно-геоложки строеж.

Геолого-тектонска характеристика.



Фиг. 2.1 Извадка от карта в М 1:500 000 с главните теренни разкъсвания от трусовете от 14 април 1928 год. (зелено) и 18 април 1928 год. (червено)(Бончев и Бакалов, 1928) на фона на инструменталната сеизмичност в района за периода 1980-2001 (Ботев, 2003). Със сини пълни линии са представени главните разломи на двата труса от 14 и 18 април 1928 год., определени от геодезически данни определени от ко-сеизмични премествания и моделиране (Димитров, 2009). Епицентрите на двата труса са показани със звезди в съответните цветове

Източник - Института по Геофизика, Геодезия и География (ИГГГ) при БАН.

Изходни данни за изследванията

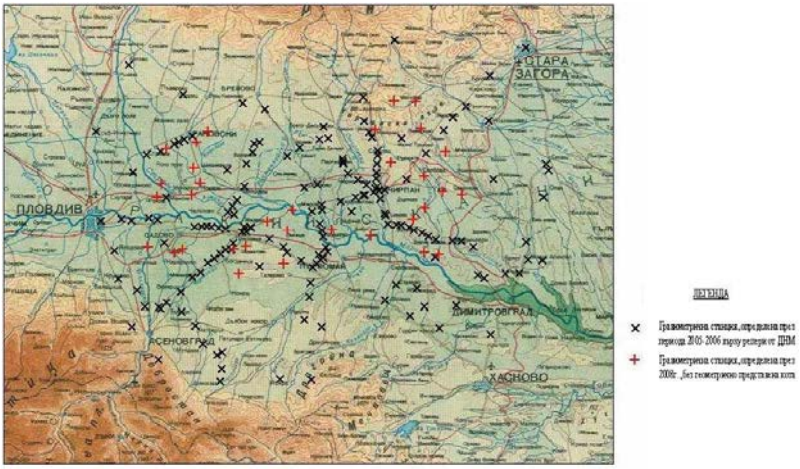
Измерванията през 2005 г. са проведени с два еталонирани гравиметра Scintrex CG-3 и руския гравиметър GAK-7T по 109 репери от Държавната нивелачна мрежа (ДНМ) I и II клас. Измерванията в изследвания район са привързани към гравиметрични станции от Основната гравиметрична мрежа на България в градовете Пловдив, Стара Загора, Поповица и Братя Даскалови. Така районът на изследването е заключен между паралелите $41^{0}54'$ и $42^{0}26'$ и меридианите $24^{0}44'$ и $25^{0}41'$. [9]

През 2006 г. са осъществени нови измервания за сгъстяване на гравиметричната мрежа в района с прецизния електронен гравиметър Scintrex CG-5 и руския гравиметър GAK-7T, като броят на станциите с прецизно определена сила на тежестта е значително увеличен. [7]

При първите две кампании измервания (2005-2006 год.) местата на гравиметричното измерване са избирани в близост до репери от ДНМ, като е отчитана разликата във височината между гравиметъра и нивелачния репер с оглед обезпечаване геометричното определяне на

станцията във височинно отношение.

За по-детайлно локализиране на главните разломи в района Чирпан – Пловдив през 2008 г. са осъществени нови прецизни измервания със Scintrex CG-5 и GAK-7T в централната зона между градовете Чирпан и Пловдив, които измервания не са направени върху точки с прецизни геометрично известни надморски височини.



Фиг. 2.2 Гравиметрична станция с прецизни гравиметрични измервания на БАН 2005-2006 год., (черен цвят) и измерени през 2008 год. без геометрично представена кота (червен цвят) използвани при измерването, представени върху извадка от топографска карта в М 1:500 000

Източник - Института по Геофизика, Геодезия и География (ИГГГ) при БАН.

Обработка на данните

В работата е направена обработка на предоставените данни за измерената реална сила на тежестта, от представените гравиметрични станции. Данните са обработени до получаване на аномалии Буге, като тук е описан използваният алгоритъм за получаването им.

За определяне на нормалната сила на тежестта, както и аномалиите на силата на тежестта, са използвани праметрите на геодезическа референтна система G R S WGS'84.

Аномалиите Буге са получени по следната формула:

(1)
$$\Delta g_B = g + (0.3086 - 0.0419\sigma) * H - \gamma_0$$

където за средна плътност на Земята □, е приета □□2.670 / sm^2 .

За района на България емпирично е получена стойност за плътността на земни маси □□2.300 g / sm^2□□и в работата аномалиите Буге са пресметнати по двете стойности, като е направено сравнение на резултатите на получените стойности.

Нормалната сила на тежестта на повърхността на елипсоида □$_0$ е определена по формулата на Пицети в сиситема WGS'84. Формулата представя □$_0$ като продължение към височината на изследваната точка чрез развитие в Тейлоров ред:

(2)
$$\gamma_0 = \frac{9.78032677114 * (1 + 0.00193185138639 * \sin^2 \phi)}{\sqrt{(1 - 0.00669437999013 * \sin^2 \phi)}}$$

където □ е геодезическата ширина (в градуси) за всяка гравиметрична станция.

Използва се формулата на Хелмерт „1901-1909" за нормалната сила на тежестта при елипсоида с развитие в ред на Тейлор на нормалната сила до първи ред. За нормалния вертикален градиент се взема:

(3) $$\left(\frac{\partial y}{\partial H}\right) = -0.3086 mGal / m$$

(4)

$$\gamma_N = \gamma_0 + \left(\frac{\partial y}{\partial H}\right)_0 * H + \frac{1}{2} * \left(\frac{\partial^2 y}{\partial H^2}\right) * H^2 + \left[\frac{1}{6}\left(\frac{\partial^3 y}{\partial H^3}\right) * H^3\right]$$

(5) $$\Delta g_B = g - \partial g_B - \gamma_N$$

За установяване местата на главните разломи от земетресенията на 14 и 18 април 1928 година са използвани резултатите от изчислените аномалии Буге за района, тъй като при тях е премахнато смущението от топографския слой, който значително променя на аномалното поле.

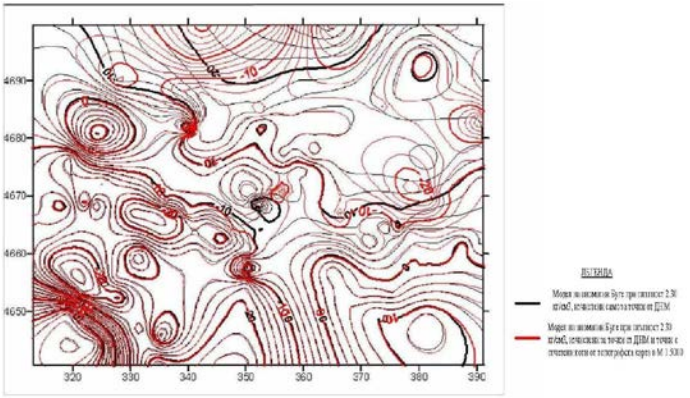
Съставени са нови карти на аномалията на Буге със сечение 2mGal за двете плътности□ □2.300 g / m^2 (фигура 2.4) и за плътност□ □ 2.670 g / m^2 (фигура 2.5) съответно емпирично определена за България и средна плътност за земната кора.

Установени са линейни гравиметрични контрасти в латералното изображение на аномалиите на Буге, които се свързват с главните разломи в Горнотракийската низина, активирали се по време на земетресенията на 14 и 18 април 1928 г.

За изследваната територия са изчертани две сравнителни карти (фигура 2.6), които са наложени една върху друга. На първата карта (изобразна чрез черни изолинии) е изобразено полето на аномалии Буге, изчислено от точките, измерени през 2005 и 2006 год. Тези точки са измервани в близост до репери от Държавната нивелачна мрежа и за тях се разполага с прецизно определени геометрични коти.

На втората карта е показано полето на аномалиите Буге, изчислени чрез множество от 198 точки – 170 от тях измерени в първите 2 експедиции, а останалите 28 в третата експедиция през 2008 год. 28-те точки са с отчетени коти от топографска карта в М 1:5000.

От направеното сравнение е видно, че в двете полета имат доста съществени разлики в околностите, където са добавените точки. Получените различия означават, че изчисленото поле с помощта на всички разполагаеми точки съвсем не е близо до необходимата точност и не може да бъде използвано за практически цели.



Фиг. 2.6 Сравнение на аномалии Буге, изчислени с добавени точки с отчетени коти от топографска карта в М 1:5000, с аномалии Буге, получени от гравиметрични измервания, извършени само върху точки от Държавната нивелация, при плътност 2.30 кг/см3.

Източник - Института по Геофизика, Геодезия и География (ИГГГ) при БАН.

Съставена е и карта на аномалиите «свободен въздух», представена за сравнение върху извадката от геоложката карта на България (Чешитев и др.1989) в М 1:500 000 (Фигура. 2.7). Не се наблюдава съществена разлика във връзката на анамалиите Буге с геоложката основа и тази на аномалиите свободен въздух с регионалната геология.

На фигура 2.8. са представени получените аномалии Буге при плътност 2.30 g/sm^2 върху геоложката карта на България (Чешитев и др.1989) в М 1:500 000. Установени са линейни гравиметрични

контрасти на аномалиите на Буге, които могат да се свържат с главните разломи в Горнотракийската низина, активирали се по време на

земетресенията на 14 и 18 април 1928 г. получени в (Dimitrov et al. 2009).

На фигура 2.9 са предсавени получените аномалии Буге при плътност 2.67 g/sm^2 върху извадка от топографската карта на България в М 1:500 000. Наблюдава се много добро съвпадение на контрастите в анамалиите Буге с релефа, както при Асеновградския разлом, които е по-малък и не е обект на това изследване, така и при Поповишкия и Чирпанския разломи.

На фигура 2.10 е представана крайната карта на аномалиите Буге с цветова скала и хипсометрично оцветяване, както и изолинии през 2 mGal, получено от това изследване. Нанесени са получените от изследването съществени нарушения в земната кора в района – главните сеизмогенни разломи в Горнотракийската низина. Получените разломи са изчертани с плътни прави линни, съответно със зелен цвят за разлома активирал се при труса от 14 април и с червен цвят – за разлома активирал се на 18 април. Така получените разломи са близки до разломите получени от Димитров (2009)[4] от геодезически данни за ко-сеизмични премествания и моделиране. При разлома на труса от 18 април се получи разлика от няколко градуса в ориентацията на разлома спрямо, разлома определен в Димитров (2009). Получените от изследването разломи имат по-голяма дължина от тези представени в Димитров (2009).

При съставянето на карти на аномалии Буге на района е избрано сечение от 2 mGal с оглед на големия обхват на обекта. Високата точност на данните позволява изготвяне на карта със сечение през 1 mGal, но картата изготвената не е читаема, тъй като изолиниите се получават твърде на гъсто и картата не е публикувана в дипломната работа.

Анализът на получените карти на аномалиите Буге позволи да се установят линейни гравиметрични контрасти в латералното изображение на аномалиите на Буге, които се свързват с главните разломи в Горнотракийската низина, активирали се по време на

земетресенията на 14 и 18 април 1928 год.

Изработените карти на аномалиите “Буге” (със сечение 2 [mGal]), установиха аномалии, които могат да се свържат с границите на Горнотракийския грабен и се свързват с главните разломи, активирали се при земетресенията от Април 1928 г.

За детайлното локализиране на разломите са изготвени напречни профили, отчитащи релефа и аномалиите Буге. Избрани са по 5 профила, пресичащи зоните на съществените контрасти в аномолиите Буге и напречно на двата главни разлома, показани са на фигура 2.11.

Профилите са именувани Профил 14-1 до 14-5 и Профил 18-1 до 18-5, съответно отнасящи се за разломите от земетресенията на 14 и 18 април. Напречните профили са през 9 км за разлома, активирал се на 14 април и през 10 км за разлома на труса от 18 април. Профилите са перпендикулярно на направлението на тектонското нарушение и имат дължини по 20 км от всяка страна на разлома.

На фигурите с напречните профили са показани също местата на установените разломни структури и използваните напречни профили за установяване местата на главните разломни структури. Показан е също интервала на отчитане на стойностите за изготвяне на профилите.

От напречните профили за детайлно локализиране на главния разлом на труса от 14 април 1928 г. се наблюдава най-рязка и контрастна промяна в аномалията Беге и профила на релефа при профил 14-2. С отдалечаване от този профил промяните в аномалиите и релефа са по-слабо изразени, на ясно забележими.

Изготвените профили за разлома от 18 април са с по-ясно изразен контраст и разко повишаване на аномалията Буге при екстремно понижение на релефа, което е най-силно изразено при профил 18-5. Профил 18-1 е по-къс от останалите, тъй като не се разполага с данни за аномалиите и релефа по цялата му дължина.

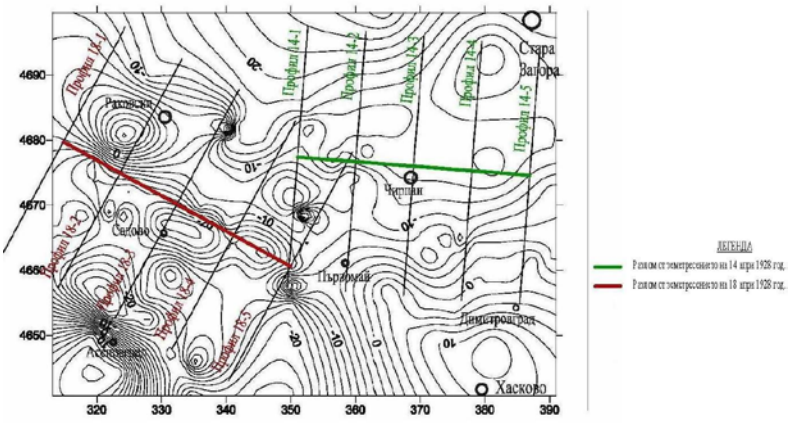
С червена начупена линия е изобразено местоположението на разлома, установено по геодезически данни /Димитров 2009/. От

направените профили е видно, че разломът от 18 април се маркира леко изместен на юг спрямо картирания от геодезическите изследвания. Това обстоятелство се дължи на факта, че в дълбочина разлома преминава в посока юг – югозапад.

Фигура 2.12 и 2.13 са изчертани напречни профили на тектонски разкъсвания от трусовете съответно на 14 и 18 април 1928 г. Профилът на аномалиите Буге е представен със зелена плътна линия на фигура 2.12 и със синя плътна линия на фигура 2.13, профилът на релефа с кафява линия, а с начупената вертикална начупена линия се изобразява местоположението на разлома според получените резултати от други негравиметрични изследвания за установяване местоположенията на разломите.

От напречните профили за детайлно локализиране на главния разлом на труса от

18 април 1928 г. се наблюдава най-рязка и контрастна промяна в аномалията Буге и профила на релефа при профил 18-2 и 18-3, който са най близо до епицентъра на земетресението от 18 април.



Фиг. 2.11 Изчислени аномалии Буге от прецизните гравиметрични измервания през 2 mGal, при плътност 2.30 кг/см3 – определена стойност за района на Чирпан – Пловдив, с нанесени получените места на разломите и напречните профили, използвани за детайлно изследване, в координатна система UTM, зона 35.

Източник - Института по Геофизика, Геодезия и География (ИГГГ) при БАН.

Заключение

Геодезическите изследвания на съвременните движения на земната кора, предизвикани от сеизмотектонски причини са важна част от изучаването на сеизмогенните зони. Геодезическите измервания позволяват да се определи и проследи пространственото положение на материализирани върху земната повърхност контролни точки. Установените закономерности в тяхното преместване в пространството и в развитието на бързите и бавните движения, дава възможност да се опознаят процесите на натрупване, освободаване и пренос на тектонските напрежения.

Геодезическите изследвания позволяват да се изучат сеизмогенните зони и физическите процеси, водещи до силни земетресения.

Литература:

1. Андреев А. *"Съвременни методи за локално моделиране на геоида"*, Шумен 2008г.

2. Андреев А. "*Ръководство за упражнения по физическа геодезия"*, ВТС 1989г.

3. Григоров Ив., "*Установяване наличието на разломни структури по резултати от гравиметрични измервания",* 2009 София;

4. Димитров Д., "*Геодезически изследвания на сеизмогенни зони",* 2009 София;

5. Димитров Л., "*Гравипрouване",* Техника, 1976;

6. Зидаров Д. П. "*Обратна гравиметрична задача в геопроучването и*

геодезията", БАН, 1984 София;

7. Михайлов Е., Димитров Д., Стоянов Л., Еверхард М., *"Гравиметрични аномалии в района на земетресенията от Април 1928 г. (Чирпан – Пловдив)",* Geosciences, 2006 София;

8. Михайлов Г., *"Анализ и оценка на гравиметричните данни в България –Автореферат",* 2011 София;

9. Михайлов Е., *"Гравиметрични поправки при високоточни измервания на силата на тежестта",* 2005 София;

10. Михайлов Е., Димитров Д., Беляшки Т. *"Гравиметрични работи за геодезически цели в Република България",* БАН, 2008 София;

11. Стойнов Вл., Пенева Ел. *"Физическа геодезия",* УАСГ, 2002 София;

12. Стойнов Вл., *"Физическа геодезия",* Техника, 1974 София;

13. Сборник доклади, *"Геодинамични изследвания, свързани със земетресенията от 1928 г. в Чирпан-Пловдив",* БАН, 1998 София;

14. Hofmann-Wellenhof B., Moritz H. *"Physical Geodesy* Springer-Verlag Wien", 2005 Виена;

АКТИВНАТА СТРАТЕГИЯ ЗА УПРАВЛЕНИЕ НА ПРОТИВОДЕЙСТВИЕТО НА ПОСЕГАТЕЛСТВА СРЕЩУ БИЗНЕС ОРГАНИЗАЦИЯТА - СЪЩНОСТ

ХРИСТО А. ХРИСТОВ

A DEFINITION OF THE ACTIVE STRATEGY FOR MANAGEMENT OF COUNTERACTION TO ENCROACHMENTS ON BUSINESS ORGANIZATION

HRISTO A. HRISTOV

ABSTRACT: *Strategies about counteraction to encroachments on business organization are scientifically considered and analytically well-founded and they have been realized by consistently and systematically enforcement of mechanisms and procedures for protection and control that are directed to restricting negative influence of existing threats and encroachments. This defines taking a decision about strategy for management of counteraction to encroachments on business organization as one of the most difficult management tasks that has ever been done on circumstances of complex, dynamic and variable security environment.*

KEY WORDS: *company security environment, strategies about security, active and passive strategies, security environment, security environment, management, business organization, protection, encroachments, counteraction.*

Рационалният избор на алтернатива за действие на дадена социална организация в конкретна среда за сигурност се извършва въз основа на определяне на оптималния възможен брой алтернативи, между които се осъществява избора и на прилагане на система от критерии за сравнение на вариантите за действие.

Стратегиите за противодействие на посегателства са научно обосновани и аналитично аргументирани и се реализират чрез последователно и системно прилагане на механизми и процедури за защита и контрол, насочени към ограничаване на негативното влияние на съществуващите заплахи и посегателства.

Затова вземането на решение за избор на стратегия за управление на противодействието за социалната организация е една от трудните

управленски дейности, осъществявани в условията на сложна и динамично променяща се среда за сигурност.

В изследването ще се изследва основно активната стратегия за организиране на противодействието срещу посегателства на фирмената сигурност, наречена в практиката стратегия за външна сигурност[1].

По принцип пасивната стратегия действа предимно във вътрешната среда, разчитайки на традиционните способи за физическа и персонална защита. Под вътрешна среда следва да се разбират тези организационни и кадрови параметри, които са свойствени за компанията – корпоративни традиции, култура на работното място, етични принципи, професионално ниво на ръководители и изпълнители, взаимодействие между отделните структурни звена, физическо разположение на обектите за защита, културни традиции и отношение на персонала към проблемите на сигурността и т.н.

При активната стратегия на противодействие, бизнес организациите имат добре развита структура за сигурност, което ги поставя в категорията на добре защитените. Те си поставят за цел не само защита на собствените интереси, касаещи пасивната стратегия, но и придобиване на информация за средата, в която фирмата действа. При тях се създава организация за обработка на информацията още в суров вид, успоредно с процеса на нейното придобиване. И в този случай възложител и получател на разузнавателния продукт е службата за сигурност на компанията. Целта е готовият продукт да послужи за надеждното организиране на противодействието, целящо недопускане реализирането на посегателства срещу бизнес организацията. Щом се появят допълнителни изисквания при организиране на противодействието, процесът започва отново. В известен смисъл, поради единство на процесите по сигурността, контраразузнавателната и разузнавателна дейност в тези компании се обединяват в един общ цикъл. Това се улеснява от създадената обратна връзка.

Основните фактори, определящи последователността на предлаганата интегрирана проактивна стратегия на противодействие са:

висшият мениджмънт на компанията; параметрите на вътрешната среда на компанията; параметрите на външната среда, в която компанията функционира; защитата на компанията (пасивен контраразузнавателен цикъл); проактивна защита на компанията (активният контраразузнавателен цикъл); обратната връзка (за пасивния и активния цикъл).

При проактивната стратегия задачите се поставят от службата за сигурност на фирмата. Когато ръководството на службата за сигурност постави задача, засягаща параметрите на външната среда на

компанията, тогава влиза в действия активният (контраразузнавателен) цикъл на сигурност. В тези случаи, обикновено се изисква придобиване на информация за различните параметри на външната среда, която има множество фактори. За да се премине към оперативна дейност, е наложително първоначално да се определи каква информация се изисква, в какъв обем, за колко време трябва да се придобие информацията и източниците, от които тази информация ще се търси.

Фиг. 1. Интегриран контраразузнавателен цикъл

Изяснявайки обема на наличната и липсващата информация, фирмената служба за сигурност преминава към етапа на нейното придобиване. Съществен момент на този етап е правилната преценка за времето, което трябва да се отдели за процеса на търсене. Ако използваме опита на някои от водещите компании, времето за търсене не трябва да бъде повече от това за анализ на цялата налична информация. Когато процесът не се регулира по този начин, съществува опасност от увличане в търсенето и загъване в излишна и, до голяма степен, ненужна информация.

След обработка и анализиране на получената информация се изготвя аналитичен продукт, въз основа на който се вземат решения, касаещи противодействието. Окончателната преценка на извършеното противодействие може да се направи, след като се видят резултатите от взетите въз основа на продукта решения. По точи начин интегрираният контраразузнавателен цикъл се затваря виж.фиг.1. [2].

Реализирането на проактивната стратегия за сигурност на търговското предприятие става посредством някои основни дейности, които са изброени и описани в следващото изложение.

1. Формиране на проактивна контраразузнавателна политика на фирмата

Фиг. 2. Функции на контраразузнаването на фирмата в процеса на придобиване на информация за външната среда и нейното оперативно използване

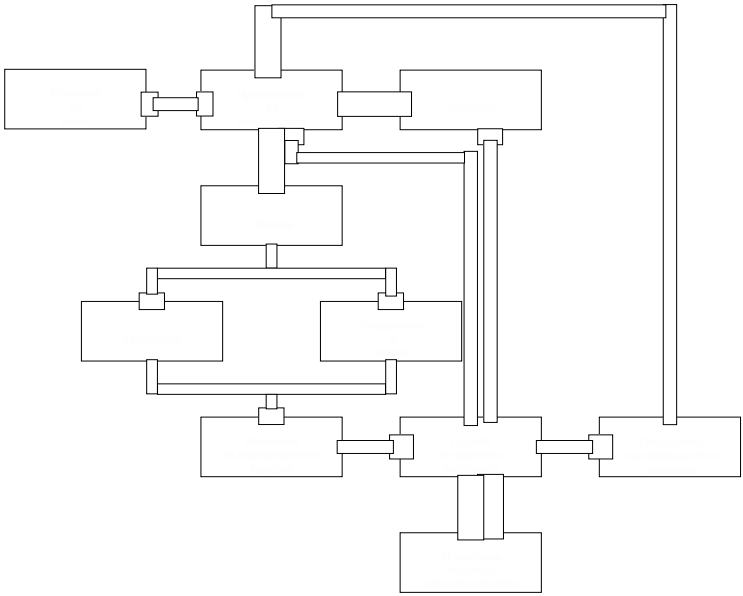
Тази политика се формира от службата за сигурност на бизнес организацията, на база планираните задачи и разбирания за организиране на противодействието. Проактивната стратегия на фирменото контраразузнаване се изгражда така, че да подпомага управлението на противодействието срещу посегателства на фирмената сигурност. Нейната основна задача е целенасочено системно изучаване на външната среда на фирмата с цел своевременно установяване на заплахи за организацията.

Резултатите от контраразузнавателната дейност на това равнище трябва да помогнат на ръководството на фирмата при определянето на действията на конкурентите, свързани с деянието нелоялна конкуренция, икономическите и пазарните фактори, демографията, новостите в законодателството и правните изисквания. Всичко това има

за цел да подпомогне службата за сигурност за своевременна реакция на фирмата към промените в околната среда с цел неутрализиране на потенциални посегателства срещу фирмата.

„Процесът на формулиране на контраразузнавателните задачи, по които службата за сигурност на фирмата трябва да работи, планирането на тяхното изпълнение и оползотворяването на крайния продукт е посочен на фиг. 2.”[3].

Правилната организация на собствена проактивна контраразузнавателна дейност се предопределя от цикъла на фиг. 3.



Фиг. 3. Проактивен контраразузнавателен цикъл

Той обхваща:

а) определяне на необходимостта от сведения;

б) организация на ресурсите и придобиване на информация;

в) обработка и анализ на придобитата информация с цел установяване заплахи за фирмата;

г) планирани мерки за противодействие.

д) обратна връзка, обезпечаваща модификацията на отделните етапи от цикъла, когато това е необходимо. По този начин

целият цикъл се усъвършенства в съответствие с възникването на нови потребности.

2. Установяване на контакти и взаимодействие

Установяването на контакти, връзки и познанства (или ползването на вече създадени) се извършва с цел изграждането на „симпатизанти" в обществено-политическото и икономическото пространство, съпричастни или с положително отношение към цялостната дейност на фирмата или по конкретни въпроси, представляващи в отделни случаи и взаимен интерес или от национална за икономиката значимост. Това е от особена важност за корпорации, холдинги, асоциации и други, които са основни или главни производители или дистрибутори на важни за здравето или бита на човека продукти, както и производители, важни за икономиката на страната.

3. Проучване на потенциални клиенти и доставчици

По отношение на това направление е излишно да се подчертава колко важно е търговското дружество да е в състояние предварително и с голяма степен на достоверност да оценява надеждността на клиентите, като се вземат всички необходими мерки за свеждане до минимум на нормалния стопански риск.

Задължение на структурата за сигурност е да осигури максимално достоверна информация както за някои фактически прояви, така и за истинските намерения на такъв род клиенти. Защото тяхното поведение в този случай може да бъде твърде различно – от прикрито, документално удостоверяващо техните затруднения, до грубо укривателство както на ресурси, така и на лицата, които са пряко отговорни за това.

Ненадеждните делови партньори се определят по следните признаци:

- допускат неедноктратни провали при сделки с други партньори;
- несвоевременно и некачествено изпълняват условията по договори;
- имат лоша репутация в деловите среди;
- обременени са с големи дългове;
- към тях са предявени различни съдебни искове;
- проявяват слабост към хазарт, алкохол, наркотици;
- водят разгулен живот;
- обграждат се с криминално проявени лица;
- проявяват пренебрежително отношение към авторското или патентно право;
- служат си с подкупи и използват нелоялна конкуренция;

- умишлено протакат деловите преговори и т.н.

Некредитоспособен е този партньор, който няма реална възможност да възстанови размера на получения кредит. Под реална възможност се разбира истинността на задължителните гаранции, които кредитираният предоставя на кредитора.

Некредитоспособният партньор се характеризира с:

- неакуратност при изплащане на стари кредити;
- влошено текущо финансово състояние;
- извършване на банкови операции с необезпечени кредитни ресурси;
- нецелево използване на кредитните средства;
- опит за измама на партньора при изпълнение на условията по договора и пр.

При посочените условия и информация фирмата може да изгражда взаимоотношения с клиенти, партньори или съдружници по определени направления на основата на взаимно доверие или на обоснована предпазливост и вземането на съответните защитни мерки във връзка с нея.

4. Проучване на конкуренти

Конкурентът може да бъде и лоялен. В този случай търговското предприятие трябва да извлече ползи от неговото съществуване. Добре е да се възложи на служителите от структурата за сигурност не само да съберат пълна информация за лоялните конкуренти, но и да установят личен контакт с тях.

Необходимо е да се проучат възможностите и нагласата на конкурентите за евентуални съвместни действия на пазара, когато важни обстоятелства налагат това. Решението за принадлежността на дадено търговско предприятие към някоя от формиралите се групи трябва да се извършва от служителите на структурата за сигурност след внимателна оценка на всички данни и обстоятелства.

5. Придобиване на информация за факти и обстоятелства, които способстват за сключването на изгодни договори

Добре функциониращата система за придобиване на информация може да съдейства за постигане на по-изгодни условия, като преди сключването на конкретна сделка предостави полезна информация за икономическата среда, в която работи контрагентът или за наличието на конкурентни оферти от друг контрагент.

Особен акцент на дейността по предотвратяване на потенциалното влияние на източници на заплаха върху социалната организация, са проактивните действия (общи и специални), спрямо

източника при разкриване на признаци за насочеността му срещу организацията.

Общите превантивни действия са насочени към постигане на промени в средата, в условията и предпоставките и обстоятелствата, довели до формирането и развитието на субекта или ситуацията в съответен източник на заплаха.

Специфичните превантивни действия са фокусирани върху конкретно идентифициран източник на заплаха. Целта е, на база познаване характеристики и признаци за проява на източника на мотивацията и способностите му за проява, да се въздейства активно спрямо източника на заплаха и той да бъде елиминиран или да се изведе от състояние, позволяващо му да оказва негативно влияние върху социалната организация. Поставянето на източника на поегателства в невъзможност за негативно въздействие върху социалната организация е постижимо при детайлно познаване на източника на заплаха, отчитането на взаимната проникнатост и зависимост на източника с други източници на заплаха в сложната среда за сигурност и прилагане на последователни проактивни действия. Тези проактивни действия могат да включват ограничаване или елиминиране на неговата финансова и логистична база на съществуване, лишаване от ресурси с критично значение за дейността му (материални, финансови, човешки, информационни) и т.н.

Основната идея на превантивната дейност е постигане на своевременно и надеждно активно въздействие върху източника на посегателства преди осъществяване на негативното му влияние спрямо организацията.

Прилагането на стратегията за проактивно противодействие може да постигне желания положителен ефект само при реализацията на методологически обосновани последователни действия, а не при хаотично реагиране на въздействие на видовете посегателства. Примерната методология за изпълнението на стратегията за проактивно противодействие може да включва: приоритизиране на действията, оценка на препоръчаните механизми и процедури за защита и контрол и избор на подходящите за реализацията на стратегията, определяне на отговорностите, разработване на плана за прилагане, прилагане на механизмите и процедурите, оценка на остатъчния риск за организацията.

Прилагането на научнообоснованите съвременни технологии за вземане на управленско решение за избор на подходяща стратегия за управление на противодействието, разработването и прилагането на обективни критерии за избор на алтернатива, способстват за намаляване

на несигурността, при която функционира социалната организация и благоприятстват постигането на висока полезност и рационалност на процеса по управление, с цел гарантиране изпълнението на мисията на организацията.

Планирането, организирането и изпълнението на стратегията по управление на противодействието могат да бъдат разгледани, както като отделни етапи на процеса по управление, така и като цялостен етап в изпълнение на взетото решение за действие, с цел гарантиране надеждността на функциониране на социалната организация.

Изпълнението на избраната стратегия за управление на противодействието е дейност по практическа реализация на взетото решение. То е концентриран израз на цялостната политика по управление на противодействието, на търсенето на действена, проактивна позиция спрямо предизвикателствата и заплахите на съвременната среда за сигурност, на опита за изграждане на нова философия и култура на отношение към динамичните промени, към сложността и хаоса.

Ефективността на изпълнение на взетото решение за проактивно управление на противодействието е в пряка зависимост и е определена от ефективността на всички предходни етапи и дейности на процеса на управление. Извършването на детайлно идентифициране на заплахи и посегателства, на обективен анализ и оценка на посегателствата, научно обосновано и адекватно на промените вземане на решение за избор на стратегия за проактивно противодействие, задълбочено планиране и организиране на дейностите, са основата, на която се реализира изпълнение.

Творческото мислене и интуиция на стратегическото ръководство не са достатъчни за ефективно изпълнение на решението за избор на проактивна стратегия за управление на противодействието. Необходимо е постигане на промяна в мисленето на целия човешки потенциал на социалната организация, разбиране че промените в средата за сигурност и съвременните предизвикателства, заплахи и посегателства представляват незащитеност не само за изпълнението на мисията на социалната организация, но биха застрашили и индивидуалната сигурност на персонала. Дейността по предотвратяването на посегателства и защита на сигурността е отговорност на всички и е споделена тежест и ангажимент, чиято реализация би допринесла за съвкупното неутрализиране на видовете посегателства.

В крайна сметка, можем да определим активната стратегия за управление на противодействието като средство за справяне с динамичните промени в средата за сигурност и развитието на

асиметричните заплахи и посегателства, чрез систематичен процес на прилагане на активна управленска политика, на целенасочено проактивно въздействие спрямо източници на заплаха с насоченост срещу сигурността на дадена социална организация, застрашаващи изпълнението на мисията й.

Въз основа на изложението могат да бъдат направени следните изводи:

1. Активната стратегия за управлението на противодействието срещу посегателства е комплексен подход, който може успешно да бъде приложен в сферата на сигурността на бизнеса, за надеждно противодействие на съвременните посегателства и заплахи и за изграждане на гъвкава динамична система за сигурност, гарантираща изпълнението на мисията на организацията.

2. Реализацията на ефективна стратегия за управление на противодействието в сферата на сигурността изисква изграждане на култура в организацията за оценка важността на противодействието и необходимостта от управлението му с усилията на целия персонал. Необходимо е строгото диференциране на отговорностите по разработване и прилагане на политиката по управление на противодействието и обучението на персонала са определящи за постигане на ефективно противодействие на видовете посегателства и заплахи.

Литература:

1. Сандев,Г. „Стратегии за сигурност на фирмата",Университетско издателство „Еп.Константин Преславски" Шумен.2005. с.12. и Василев,Ем. „Фирмена сигурност". Труд, 2000. с.67-99.
2. Начев, Й. „Конкурентно разузнаване". Сиела. 2007. с.234.
3. Сандев,Г. „Стратегии за сигурност на фирмата",Университетско издателство „Еп.Константин Преславски" Шумен.2005. с.12. и Василев,Ем. „Фирмена сигурност". Труд, 2000. с.54.
4. Слатински, Н."Същност, смисъл и съдържание на сигурността**".** „Военно издателство" ЕООД http://www.vi-books.com -2011.
5. Василев,Ем. „Фирмена сигурност". Труд, 2000. С.
6. Сандев, Г. Сигурност на организациите. Университетско издателство „Еп.Константин Преславски" Шумен.2012. ISBN 978-954-577-621-2.

Доктор Христо Атанасов Христов, главен асистент в катедра ,,Управление на системите за сигурност'', Шуменски Университет ,,Епископ Константин Преславски'', hristov63@abv.bg, тел.0889/816 612.

ИЗУЧАВАНЕ НА СОЦИАЛНАТА ОРГАНИЗАЦИЯ - ЕЛЕМЕНТ ОТ ОРГАНИЗАЦИЯТА НА ПРОТИВОДЕЙСТВИЕТО НА ПОСЕГАТЕЛСТВА СРЕЩУ ФИРМЕНАТА СИГУРНОСТ

ХРИСТО А. ХРИСТОВ

CARRYING OUT RESEARCH ON SOCIAL ORGANIZATION – AN ELEMENT OF ORGANIZATION ABOUT COUNTERACTION TO ENCROACHMENTS ON COMPANY SECURITY

HRISTO A. HRISTOV

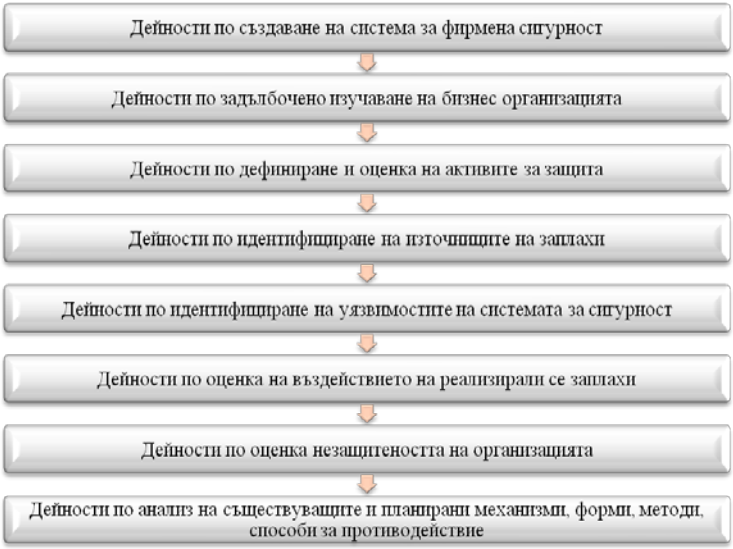
ABSTRACT: *The organization about counteraction to encroachments on company security is extremely important landmark in the process of managing business organizations and this landmark is described as complex and compound by nature and including determine all-bounded activities and procedures. Simultaneous and precise doing of each activity is a prerequisite about achieving high stage of objectivity of analysis and valuation about company indefensibility and creation of preconditions about rationality of process of organizing counteraction. The main activity in this process is the profound study of social organization that is also the subject of scientific research in this report.*

KEY WORDS*: The system – company security, valuation of assets, sources of threat, vulnerabilities, threats, indefensibility, mechanisms, structure, methods, contrivances for counteraction, security environment, management, business organization, protection, encroachments .*

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

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

- създаване на система за управление на фирмена сигурност;
- задълбочено изучаване на социалната организация;
- дефиниране и оценка на ценностите и активите за защита на организацията – кои и какви ресурси трябва да се защитят;
- идентифициране на източниците на заплаха на дефинираните активи – от какво трябва да се защитят ценностите и активите и каква е вероятността конкретната заплаха да се реализира;
- идентифициране на уязвимостите на системата за сигурност на организацията – уязвимите места, които могат да бъдат атакувани;
- оценка на въздействието, което реализирали се заплахи оказват на организацията – какви могат да бъдат последиците за организацията при реализиране на дадена заплаха (несанкциониран достъп, промишлен шпионаж, разкриване на конфиденциална информация), включително и последствия за организацията от реализацията на дадена заплаха в дългосрочен план (загуба на имидж, загуба на доставчици и пазари, финансови и материални загуби, фалит и др);
- оценка на незащитеността на организацията, чрез използване на количествени и качествени способи;
- анализ на съществуващите и планирани механизми, форми, методи и способи за противодействие и защита.



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

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

В организацията на противодействието на посегателства три от основните дейности – характеризиране на социалната организация, идентифициране на заплахите и идентифициране на уязвимостите са с определящ характер, представени на фигура. 2.

Фиг. 2 : Технологична схема на три от основните елементи на организацията за противодействие на посегателства в сферата на сигурността

Предмет на изследване в настоящият доклад е задълбочено изучаване на социалната организация.

Задълбоченото познаване на социалната организация, на нейната същност, мисия, цели, задачи е основна предпоставка за успешното дефиниране на активите за защита и идентифициране на уязвимостите на системата. Без наличието на детайлна информация за всички

функции и дейности на организацията, не може да се разчита на надеждно установяване на всички заплахи, произтичащи от организационната активност. Необходимо е наличие на задълбочено познаване на средата, в която оперира социалната организация. Притежаването на информация за основните характеристики на политическата, социална, законова и културна среда би позволило формирането на обективно познание за условията на функциониране на организацията и адекватно идентифициране на заплахите и посегателствата.

Принципното разглеждане на управлението на противодействието в сферата на сигурността, като компонент на стратегическото ръководство, определя необходимостта характеризирането на социалната организация да се осъществява в строго съответствие с развитието на стратегическата обкръжаваща среда.

Високата сложност на средата за сигурност и динамиката на процесите в нея оказват изключително високо и, често, критично влияние не само в процеса на комуникации на социалната организация и средата, но и в развитието и същностната им определеност. Липсата на обективно познание за промените в средата и на характеристиките на социалната организация, би довело до неадекватност на отражението на ситуациите, събитията и процесите в пространството и до неефективност, дори до невъзможност за управление на противодействието от проявата им. Управлението на противодействието е един от подходите за постигане на устойчиво развитие на социалните организации и обществото в сложната и хаотична среда за сигурност.

Обективното характеризиране на социалните организации е основен елемент в идентифицирането на посегателствата и е съществена предпоставка за ефективност на процеса на управление на противодействието. Без задълбочено познаване на същността, структурата, характеристиките, мисията, целите, основните функции и т.н. на социалната организация, е невъзможно да бъде определена нейната незащитеност.

„Социалната организация е обединение от хора, реализиращи мисия или постигащи цел и действащи на основата на общоприети правила и процедури” [1].

„Социалните организации" са социални феномени, създадени за реализация на определени функции, чрез използване на дадени ресурси, в името на постигане на предварително набелязани цели" [2].

„Социалните организации" са съставени от хора, между които има съществени различия в оценките, надеждите, възприятията и идеите, но те са обединени от общи интереси" [3].

„В условията на сложна и динамично променяща се обкръжаваща среда, за реализацията на мисията на социалната организация е от особено значение „постигането на качествено нови функционални възможности в цялото, които са немислими за съставляващите го отделни части", т.е. чрез постигане на синергичен ефект" [4].

Познаването не само на отделните структурни компоненти на социалната организация, но преди всичко на степента на постигане на синергизъм в дейността й, е от съществено значение за обективното характеризиране на организацията. „Синергизмът на организациите е смисълът на тяхното създаване и мярка на ефективността им" [5].

Чрез синергизма организацията не само придобива качествено нови възможности за функциониране, но в процеса на постигане на целите си се сблъсква с нови, непредсказуеми ситуации и заплахи. В този динамичен процес на развитие и социална реализация организацията се изправя пред нови рискове, чието управление е в зависимост от оптималното познаване на възможностите й.

Управлението на противодействието има за основна принципна цел осигуряване на способностите на организацията да изпълни своята мисия. Всяка организация има своя мисия и цялата управленска активност е насочена към постигането й.

„Мисията, по своята същност, е фундаменталната цел за създаване и функциониране на организацията. Мисията е основата, върху която се дефинират общи интереси, ценности, намерения, цели и приоритети. Определянето на мисията на социалната организация е творчески процес, в който изключително значение имат както знанията и уменията на ръководителите на различни управленски нива, така и споделяните от тях ценности. Добре формулираната мисия, според Кембъл и Яенг, трябва да включва четири елемента, които са в основата на модела на Ашридж – основна цел, стратегия, стандарти на поведение и ценностна система. Основната цел трябва да даде ясна представа за

причината за съществуване на организацията, която може да бъде разглеждана в тесен и широк аспект. Стратегията определя пътя за реализация на основната цел и границите на дейност на организацията. Стандартите превръщат основната цел и стратегия от интелектуални продукти в действащи инструменти, като определят правилата за действие в организацията. Със стандартите на поведение е пряко свързана и ценностната система, възприета от организацията – споделяните виждания и морални принципи, за изграждане на организационната култура" [6].

Целите на организацията произтичат от мисията й и са предварително определени, в съответствие със сложната същност и динамични промени на средата за сигурност.

Детайлното познаване на мисията и целите на организацията позволява извършването на обективно идентифициране, анализ и оценка на посегателствата и прилагане на съответни стратегии за управлението на противодействието.

Целите на организацията трябва да се разглеждат в тяхната динамика, защото промените в средата и ресурсната недостатъчност може да доведат до модифициране или предефиниране на целите. Отчитането на тези промени е от съществено значение за обективното идентифициране на посегателствата.

От изключително значение за адекватното характеризиране на социалните организации е задълбоченото познаване на обкръжаващата среда, в условията на която съществува и функционира организацията.

Динамиката и сложността на обкръжаващата среда изискват анализа и оценката на средата да бъдат осъществени както чрез диференцирано разглеждане на всеки един от компонентите й, така и отчитайки комплексното им влияние върху социалната организация. Всеки един от компонентите на средата влияе с различна интензивност и посока върху елементите и дейностите на социалната организация и формира условия, възпрепятстващи изпълнението на мисията и целите на организацията или благоприятстват постигането им.

Комплексното въздействие на средата върху дейността на социалната организация трябва да бъде оценявано при отчитане динамиката на развитие на компонентите на средата не само в национален, но и в регионален и глобален мащаб. Процесите на

глобализация, на взаимна проникнатост и зависимост на явленията, събитията и процесите, определят изключително голямото многообразие на начини, форми, средства на въздействие и подценяването на някои от елементите би довело до необективност на оценката за степента на незащитеност от проявата им.

„Съвременната наука дефинира най-общо седем вида функции на организациите – планиране, координация, набиране на действащи звена, ръководство, комуникации, вземане на решения и контрол" [7]. Задълбоченото познаване на всяка една от тези функции и осъществяването на конкретните дейности при използване на определен ресурс, би позволило извършването на своевременно и надеждно идентифициране на посегателствата, произтичащи от изпълнението на дефинираните дейности. Въпреки многообразието на дейностите, те могат да бъдат систематизирани и класифицирани по различни признаци, с цел създаване на условия за по-ясно и по-пълно определяне на същността и структурата на конкретните дейности и зависимостта и взаимодействието им при изпълнение на мисията на организацията. Възможно е групиране и разглеждане на дейностите като стратегически, оперативни, финансови, интелектуални, защитни и т.н.

Стратегическите дейности са насочени към постигане на дългосрочните стратегически цели на организацията и заплахите за тях могат да произтичат от глобални промени в политическата, законовата и социална среда.

Оперативните дейности са свързани с текущата активност на организацията и заплахите произтичат от ежедневния сблъсък на организацията с проблеми в стремежа за постигане на оперативните и стратегически цели.

Финансовите дейности са насочени към ефективно управление и контрол на финансовите ресурси на организацията и заплахите са свързани с промените в икономическата среда на функциониране на организацията.

Дейностите в интелектуалната сфера са тези, свързани с ефективно управление и контрол на интелектуалния потенциал на организацията и заплахите са определени от посегателства върху интелектуалната собственост, нарушения в организацията и използването на интелектуалния ресурс и т.н.

Защитните дейности обхващат целия спектър от организационна активност, насочени към създаване на условия за гарантиране надеждното функциониране на всички структурни звена и организацията като цяло. Рисковете при осъществяването на тези дейности са свързани с ненадеждно и неефективно изграждане на системите за сигурност на организацията, водещи до поява на уязвимост на различни източници на заплаха.

Възможно е систематизиране на дейностите по различни други признаци, но този процес трябва да е целенасочен, да търси опростяване, а не допълнително усложняване на процедурите по идентифициране на посегателствата от конкретните видове организационна активност.

За постигане на висока степен на обективност на идентифицирането на посегателствата е необходимо детайлно да се познават ресурсите, използвани от социалната организация за изпълнението на мисията ѝ. Съвременната стратегическа среда се характеризира със системен недостиг на ресурс и прилагането на научнообосновани стратегии за ресурсното осигуряване на разглежданата организация е с определящо значение за ефективното им използване. В условията на ресурсен дефицит за функциониране на организациите, особена значимост придобива прилагането на подходи за неутрализиране на рисковите фактори за организациите и за минимизиране на неблагоприятните последици от проявата им.

При ефективно прилагане на подхода за управление на противодействието, не само се намалява необходимостта от насочване на допълнителни ресурси в сфери на дейност на организацията, изложени на рисково въздействие, но се постига оптималното им използване за максимизиране на резултатите от организационната активност.

Основните ресурси, необходими за функционирането на социалната организация могат да бъдат класифицирани като човешки, финансови, технологични, информационни и материални. В процеса на идентифициране на заплахите и уязвимостите трябва да се постигне оптимално познаване на същността, конкретната и необходима наличност на ресурси, количественото им и качествено измерение, допустими критични нива за изпълнение на мисията и целите на организацията и т.н. Всеки един от ресурсите има важна роля за

ефективното функциониране на организацията, но с определящо значение е човешкия фактор.

Човешкият фактор е от изключително значение не само поради характеристиката си като основен двигателен компонент на дейността на организацията, но и предвид огромния потенциал за усъвършенстването му като ресурс. Недостигът на ресурси налага оптималното използване на всеки основен ресурс и човешкия фактор, заедно с информационния ресурс е най-сериозен потенциал за развитие и постигане на реален принос за повишаване на ефективността на организацията и надеждно изпълнение на мисията й.

Задълбоченото познаване на текущото състояние и прогнозите за развитие на човешкия фактор позволява да се направи обективна оценка на ролята му за изпълнение целите на организацията и да се идентифицират заплахите и уязвимостите, произтичащи от дейността й. Това би повишило ефективността на разработваните стратегии за управление на противодействието и би позволило оптимално използване на потенциала на човешкия фактор в реализацията на тези стратегии.

Управлението на противодействието като подход позволява, чрез детайлно идентифициране същността и характеристиките и чрез своевременно и обективно определяне влиянието на човешкия фактор върху дейността на организацията и заплахите и уязвимостите от проявата, да се въздейства превантивно за неутрализиране на негативния ефект за организацията. С това се създават условия за активно въздействие върху човешкия фактор, което е насочено към постигане на позитивна промяна в характеристиките му и оптимизиране на използването му за изпълнение на целите на организацията.

Общите характеристики на социалната организация са структура, големина и вид на ръководството. Структурата се дефинира като организационна рамка, която идентифицира съставните части и установените взаимоотношения. Големината е отражение на влиянието на околната среда и възможностите за постигане на целите и мисията на организацията. Ръководството на организацията се разглежда като последователност от управленски процеси на наблюдение, ориентиране, вземане на решение, комуникация и контрол.

Детайлното познаване на същността и характеристиките, на мисията и целите, на ресурсното осигуряване на социалната

организация позволява извършването на обективно идентифициране на заплахите и уязвимостите за организацията и създаване на условия за ефективно управление на противодействието. Неотчитането или подценяването на определени дейности и характеристики и на посегателства, произтичащи от проявата им, би възпрепятствало комплексното осъществяване на отделните етапи на управление на противодействието и би довело до невъзможност за изпълнение на основната идея на подхода – принос в стратегическото ръководство на организацията.

Извършването на обективно характеризиране на социалната организация, като стъпка в процеса на организиране на противодействието, е основа за ефективно осъществяване на следващите дейности по дефиниране и оценка на ценностите и активите за защита, идентифициране на заплахите и идентифициране на уязвимостите на организацията.

Литература:

1. /Webster's Third New International Dictionary, Massachusetts, 1986, p 1590/.
2. Семерджиев, Ц., Стратегическо ръководство /лидерство/, Софттрейд, София, 2000.с.319.
3. Шаламанов В., Реинженеринг на планирането на отбраната, Военен журнал, 1999.с.10.
4. Хакен Г., Синергетика, М., 1980.с.226.
5. Семерджиев, Ц., Стратегическо ръководство /лидерство/, Софттрейд, София, 2000.с.320.
6. Cambell, A, and Yeung,S.,Creating a sence of mission,Long Range Planning, 1991.pp 149-152.
7. Sherman C., The Uncommon Leader, Part 3, Chicago,1988.p.3

ТЕРОРИЗЪМ И ПРОТИВОДЕЙСТВИЕ

КАЛИН ИВАНОВ КРЪСТЕВ

TERRORISM AND COUNTERACTION

KALIN IVANOV KRASTEV

ABSTRACT: *Acts of International terrorism are related to commit terrorist acts (conduct terrorist operations) on the territory of two or more States , that its objects are in the international space. Depending on the goals to be achieved and the results of acts of international terrorism level can reach strategic dimensions. After September 11, 2001 - terrorist operation against the United States and the subsequent large-scale terrorist attacks worldwide terrorism has become a global threat, and with good reason can be defined as global terrorism. Modern terrorism is constantly showing their abilities, forming growing and permanent specific, non-traditional threat globally. Threat - real, not virtual. In all cases, however, this threat is vulnerable and can be neutralized. But only on condition that we know well the nature of the problem.*

KEY WORDS: *terrorism, counter terrorism, political terrorism, counteraction, violence, threats, global counterterrorist strategy, ethno-religious terrorism, counter-terrorist operations raiding, The system of preventive measures.*

„*Всички хора се раждат свободни и равни в своето достойнство и права. Те са дарени с разум и съвест и трябва да постъпват в отношенията си един към друг в дух на братство*" [1].

В условията на глобални предизвикателства пред човечеството и безпрецедентно многостранно взаимодействие между правителства, народи, общности и организации, тероризмът е онова социално явление, което предизвиква най-сериозна загриженост и представлява най-значима заплаха за националната, регионалната и международната сигурност. Именно заплахата, застрашаването и насилственото въздействие върху противостоящата страна са особеностите, характеризиращи тероризма като явление. Затова свидетелства и

етимологията на самото понятие, произхождащо от латинската дума "*terror*" - страх, ужас. Ефектът и последствията от дейността на терористичните мрежи засягат непосредствено и най-развитите държави, като възпрепятстват устойчивото и демократично развитие на гражданските общества и постигането на стабилен и мирен свят чрез интеграция и взаимоизгодно сътрудничество между отделните нации.

В същото време дългогодишните усилия на политици, експерти и учени да достигнат до общо разбиране за корените, същността и характерните черти на понятието **тероризъм** засега не са се увенчали с успех. Разнообразните литературни и историко-психологически, описателни и функционални, статистически и военно-технически определения за този неконвенциален феномен на политическо насилие често допринасят за разгаряне на нови дискусии с лансиране на още по противоречиви и противоречащи си интерпретации. В първите две издания /1984г.-1988г./ на авторитетното справочно издание за политическия тероризъм под редакцията на известния експерт на ООН по тази проблематика Алекс Шмид са предложени 109 различни дефиниции за явлението, разпределени в 22 по-общо категории. Двадесет години по- късно авторите на поредното преработено издание на същия сборник споменават вече за 123 обяснения на термина политически тероризъм [2]. Проблемът с дефинирането на тероризма понякога изглежда неразрешим дори в рамките на една отделна държава, в която различните специализирани правителствени агенции използват свои специфични определения. В САЩ, например, съществуват определени нюанси във възприетите официални дефиниции от Конгреса, Държавния департамент, ФБР, ЦРУ и Пентагона [3].

В последните 40 години международната общност в лицето на най- представителните свои междуправителствени организации /ООН, Съвета на Европа, НАТО, ЕС и др./ се опитва също безуспешно да постигне консенсус за определението *тероризъм*. Уникалната световна среща на над 170 държави и правителствени ръководители в рамките на 60-ата Юбилейна сесия на общото събрание на ООН през септември 2005 г., откроi същностните различия и гледни точки по този проблем между отделни групи държави. Постигнатото съгласие в раздела за тероризма от приетата резолюция на ОС на ООН № A/60.L/2005 подобно на одобрената година по- късно „Глобална контратерористична стратегия" на ООН предполага съзнателно едно много дипломатично и твърде общо описание на причините формите и проявленията на тероризма [4]. Няколко са ключовите дилеми в различните разбирания за същността на тероризма, но преди всичко те се отнасят до границите

между тероризма и другите форми на политическо насилие /национално освободителна борба, съпротивително въстание, партизанска война и т.н./.

Съвременната историография за тероризма открива корените на това обществено явление в предходни исторически епохи. Така например, за първообраз на етно-религиозния тероризъм се посочват „зелотите" от I век от н.е. и „хашашините" от XI-XIII век, за родоначалници на политическия тероризъм в Европа се разглеждат терористите анархисти от XIX век, а за предтеча на съвременния държавен тероризъм е представян „революционният якобински терор" от края на XVIII век и неговия идеолог Максимилиян Робеспиер [5].

През XX век спектърът от мотиви за използване на тероризма като средство за политическа борба се разширява. Ако дотогава на него се е гледало като на саможертва в името на някакви идеали, то за формиращите се крайно леви и крайно десни терористични формирования тероризмът се превръща в способ за самоутвърждаване. Проявленията на „*черния терор*" на фашистите и неонацистите, не се различават съществено. И за едните и за другите тероризмът е не само *мощно оръжие, инструмент, средство за борба срещу властта,* но и *средство за спечелване и задържане на властта*. В средата на XX век тероризмът все по-отчетливо започва да се използва от държавите и техните правителства **за** постигане на политически цели във вътрешно и външнополитически план - възниква т.нар. държавен тероризъм**.** Типични примери за това са фашистка Германия и Съветския съюз по времето на управлението на Сталин. Държавната подкрепа на дейността на терористичните организации е характеризирана ясно от Д. Уолкъм - *„При воденето на скрита война чрез тероризъм, кръвта винаги остава само по ръцете на фанатиците, а не и по ръцете на техните истински господари*"**.**

Един от най-сериозните нерешени проблеми, свързани с безопасността, с които човечеството навлезе в XXI век се оказа тероризмът. След трагичните събития от 11 септември 2001 г. светът вече не е същият. Терористичната атака в сърцето на Америка и последвалите я атентати в Испания, Англия, Беслан и много други места по света показаха, че заплахите и рисковете пред международната сигурност в началото на новото хилядолетие са разнообразни и нетрадиционни, че заплахите са глобални и имат трансграничен характер. Нито една страна не е застрахована от тях, нито една държава не може да се справи сама с тези заплахи и рискове. В годините от 2001 до днес терористичните действия се активираха до степен на

терористична война. Борбата срещу тероризма придоби първостепенно значение в цял свят.

Всичко това промени схващанията за сигурността изобщо, за ролята и отговорностите на системите и институциите за сигурност. Най-важният извод от случващото се през последните години е, че срещу глобалния тероризъм следва да се действа глобално, че той може да бъде спрян само със съвместните действия на целия демократичен свят. Днес главното предизвикателство пред човечеството е да не допусне превръщането на тероризма в "хронична болест" на новия век, както и неутрализирането на асиметричните заплахи за всяка една страна, за нейните граждани, обекти и интереси. [6].

Стратегията на международния тероризъм включва:

- водене на психологическа война с цел да покаже на света уязвимостта на всяка държава, колкото и могъща да е тя;
- обявяване на свещена война ("Джихад"), за да се предизвика сблъсък на цивилизации в глобален план и да се придаде религиозна окраска на чисто терористични цели;
- опити за сриване на световната икономика, разбиване на икономическото доверие в САЩ и най-развитите държави;
- предизвикване на енергийна криза;
- създаване на масова психоза от използването на биологически, химически или токсични вещества;
- заплахи от извършване на атаки срещу информационните и компютърни системи;
- внасяне на сериозни смущения в транспортните комуникации, застрахователното дело и др.

Асиметричният характер на терористичните действия позволява със сравнително малко средства и хора да бъдат нанасяни значителни поражения не само в материален и физически , но и в психологически план и може да направи неефективна военната мощ на съответната държава.

Разширяването на географията на международния тероризъм го превръща в опасност за сигурността и на Балканите поради съществуващите сложни междуетнически и религиозни проблеми, значителното влияние на организираната престъпност., активността на албанските радикални организации, стремежът на терористичните организации да създадат своя мрежа в района, износът на дейности на фундаменталистки структури от нестабилни региони (Близкия Изток и Кавказ), нелегалното производство и търговия с наркотици, които по различни канали да се транспортират през Балканите към Европа.

Сериозен рисков фактор представлява дейността на различни фундаменталистки неправителствени организации и асоциации, които имат седалища в почти всички балкански страни и поддържат връзки с терористични и престъпни структури от цял свят (включително "Ал Кайда").

Независимо, че понастоящем липсва директна заплаха от действия на международни терористични организации срещу Република България, активизирането на тероризма в глобален мащаб повишава рисковете и за нашата страна.

Превръщането на тероризмът и организираната престъпност в проблем номер едно и основен рисков фактор за националната сигурност принуждава правителствата на повечето страни в света (включително и във България) да предприемат безпрецедентни мерки в борбата с тях - ограничаване на демократичните права и свободи на личността (по-широко използване на специални разузнавателни средства), ограничаване достъпа до информация от различен характер, искане на доказателства за произхода на доходите, премахване на банковата тайна и т.н.

Всичко това в съчетание с корупцията на всички нива, изтичането на национални капитали, високата безработица, инфлацията, различните видове контрабанда и т.н, генерира социално напрежение в обществото и се отразява негативно върху националната сигурност и са реална заплаха за нея.

Борбата с тероризма е огромно предизвикателство, защото тя не само обединява демократичния свят, но поражда проблеми, които могат да го разединят.

„Война с тероризма" или „Борба с тероризма"? „Войната" предполага и прилага Law of War, законите на Войната, а „Борбата" - законите на Мира, Law of Peace. През отговора на въпроса - дали тероризмът е война или е престъпна дейност преминава разделителната линия между възгледите за средствата на борбата с тероризма в САЩ и Европа. Според САЩ това е война с тероризма и трябва да се води главно с армия и със специални части. Според Европа това е борба с тероризма и трябва да се води основно с полиция и със специални служби.

Тероризмът е най-значимият проблем на сигурността днес. При съвременните условия тероризмът се глобализира, т.е. добива транснационални измерения, при което нарастват неговата агресивност и жестокост. Съвременните терористи отчетливо проявяват липсата на категорията *„невинност*", т.е. за тях виновни са всички граждани на демократичното общество, които не са с терористите. В този аспект

тероризмът наистина се явява глобална заплаха за световната демократична общност.

Вниманието по отношение противодействието на тероризма, следва да се насочи към необходимостта от нов дух, философия и подход към нетрадиционния характер на заплахата и нейната асиметричност по отношение на класическите форми на заплахите за националната и международна сигурност. Тероризма непрекъснато показва възможностите си, формира нарастваща и постоянно действаща специфична, нетрадиционна заплаха в глобален мащаб. Заплаха – реална, а не виртуална. Във всички случаи, обаче тази заплаха е уязвима и може да бъде неутрализирана, но само ако добре познаваме същността на проблематиката. Задължително условие за постигане на успех в борбата с тероризма е отказването от прилагане на двоен стандарт при формирането на определение и обединяването около обща стратегия за противодействие. Военното решение не е и не може да бъде единствено и основно средство за постигане на успех.

Подобно на причините за поява и развитие на тероризма, противодействието срещу него следва да има подчертано комплексен характер. Наложително е разграничаването на същността на понятията тероризъм и прояви на терористичната дейност, което до голяма степен влияе върху избора на подхода, формите, методите и средствата за противодействие[7].

Стратегическият характер и глобалните измерения на съвременния тероризъм предполагат и специфичен стратегически подход, чието начало и основна цел следва да се насочат към елиминиране на причините за поява на явлението. Противодействието трябва да започва с нанасяне на удар по ембриона на тероризма [8].

Защитата на живота и здравето на гражданите от терористични атаки е от изключително значение. Те се защитават чрез система за национална сигурност, която е необходимо постоянно да се изменя според обстоятелствата. Част от тази система са действията за борба с тероризма. Детайлното планиране на тези действия може да предпази гражданите от стремежа на терористични организации да установят своята власт политическа, икономическа или духовна;

Анализа на същностните характеристики на тероризма води до заключението, че това явление е много добре организирано и за да му се противодейства е необходимо да се организират също толкова добре правозащитните организации. Те трябва да бъдат една крачка пред терористичните формирования, а не след тях, но се оказва, че това не е много лесно за изпълнение.

Тъй като тероризмът все повече придобива глобален характер, мерките за защита на гражданите трябва да включат превантивни и отговарящи удари срещу терористична инфраструктура, разположена далеч от мястото на провеждане на терористични атаки. Много често тук се използват контратерористичните рейдови операции, които проникват на територията, където действат терористичните организации, нанасят внезапни удари и бързо се оттеглят.

В глобален мащаб борбата срещу тероризма се заключава в няколко основни големи групи от превантивни мерки със задължително условие за комплексно прилагане:

- **политически** (решения, воля, обща стратегия, дипломация, сътрудничество, отговорност);
- **икономически** (осигуряване, подпомагане, ограничаване);
- **финансови** (пресичане, ограничаване, контратрансфериране, осигуряване);
- **оперативни** (разузнаване, контраразузнаване, военни действия за унищожаване и ограничаване, наказателно правни за възмездие):

Системата от превантивни мерки, от една страна, затруднява и ограничава терористичната дейност, а от друга - създава благоприятни условия за използване и ефективно осъществяване на оперативните мерки. Оперативните мерки на специализираните служби заемат важно място в рамките на общата система от мерки на държавата в борбата с тероризма [9]. Значението на този тип мерки нараства във връзка със засилването на конспирацията в дейността на терористичните организации и групи. Под оперативна мярка следва да се разбират действия в рамките на законово определените функции и задачи на специализираните служби, при които се прилагат оперативни средства и способи, включително секретен апарат (агентура) и специални разузнавателни средства. Оперативната мярка като целенасочено действие се основава на оценка на оперативната обстановка, прогнозиране на тенденциите в нейното развитие и произтичащите заплахи и опасности от терористични атаки.

Оперативната система от мерки на специализираните служби за гарантиране сигурността на обектите на терористичната дейност изпълнява две функции: от една страна, тя има за цел да създаде надеждна защитна бариера, която затруднява и пресича опити за терористични атаки.

Разглежданата система от оперативни мерки условно се разделя на две групи:

а) **мерки от общопревантивен характер за гарантиране сигурността на защитаваните от терористични актове обекти:**

сгради на държавни ведомства, електроцентрали; предприятия от военнопромишления комплекс, особено важни лица (very important persons - VIP) и др.;

б) **мерки, непосредствено насочени към разкриване, предотвратяване и пресичане на терористичната дейност.**

Двете групи мерки са взаимосвързани, но в същото време всяка от тях има определена насоченост.

Предназначението на мерките от първата група е да предотвратяват, затрудняват и ограничават терористичната дейност на евентуален неустановен конкретно противник срещу защитаван обект. Оперативната дейност в това направление предполага използването както на гласни (административни и профилактични), така и на негласни (оперативни) мерки.

Предназначението на мерките от втората група е непосредствено водене на борбата с терористичната дейност, разкриването, предотвратяването и пресичането на планове и опити за осъществяване на терористични актове. Това са мерки, при които се използват методите на агентурно проникване в терористичните групи и организации, при които се цели постигането на оперативно наблюдение и контрол на дейността на терористите, с оглед своевременното пресичане на действия по осъществяване на терористични актове.

В специализираната литература често под оперативни мерки се разбира само тази втора група агентурно-оперативни мерки.

В зависимост от териториалната сфера на прилагането им, системата от оперативни мерки за борба с терористичната дейност може да бъде също разделена на две групи:

а) **система от мерки, провеждани зад граница** (агентурно проникване в терористични организации, в центрове за обучение на терористи, в организации и групи, оказващи логистична подкрепа на терористи и т.н.);

б) **система от мерки, използвани на територията на отделната защитавана държава** (недопускане проникването на терористи в съответната страна, организиране на агентурна защита на обектите на терористичен интерес и пр.)

- **правни** (наказателноправни, наказателнопроцесуални, административноправни и международноправни).
- **логистични.**

Особено внимание следва да се отдели на ролята на човешкия фактор и огромното му значение за изпълнението на политическите решения. Без високо подготвени, квалифицирани и специализирани

хора прилагането на обема от дейности, особено от групата "оперативни" е невъзможно.

Дори в условията на високотехнологичния XXI век ролята на човешкия фактор е доминираща, особено в областта на разузнаването.

Въз основа на изложението, могат да се направят следните изводи и заключения:

За да се направи анализ на тероризма е необходимо да се познава логиката на терориста. В този смисъл е полезно за бъде разгледана удивителна изповед на терориста-теоретик Рикардо Гарсия Дамборенеа, смятан за идеолог на баската терористична организация „*ЕТА*" – Тероризмът отдавна е станал интернационален, той "*няма свое лица или нация"*. Това е много важна констатация, но все пак тя има определена декларативност, тъй като не можем да отречем, че заедно с "*просто тероризъм*" има и много специфичен "*арабски тероризъм*". И причините за този специфичен "*национален оттенък*" досега не са разкрити.

Тероризмът е асиметрично насилие срещу реда на световното статукво и следствията от него. Но статукво и ред също не могат да се налагат с насилие над тези, които не са питани и канени при създаването на дефинитивни ценностни правила. Не може неизбиран от никого световен връх да казва кое е добро и кое - лошо.

Тероризмът е част и инструмент и на световната организирана престъпност. А нейното съществуване без съмнение отдавна е елемент на скритата част от световното управление. Организираната престъпност се крепи на три кита - *престъпни икономически отрасли; проникването в официалните икономически, финансови и социални отрасли; регулираното насилие*.

Тероризмът трудно може да бъде победен с военни средства и бази в наречените за рискови региони. Но базите и военното присъствие могат да осигуряват други интереси на господстващите в света държави

Литература:

1. Т. Трифонов, А. Пейчев, Тероризмът. Теоретично изследване, Фондация „Национална и международна сигурност", София, 2003 г. с. 134

2. Alex Schmid and Albert Jongman, Political Terrorism: A New Guide to Actors, Authors, Concepts (Harvard University Press, 2005), p. 40-42;

3. Report of the U.S. State Department "Patterns of Global Terrorism";

4. UN A/RES/60/1. 2005 Word Summit Outcome, p. 22-23, A/RES/60/288 The United Nations Global Counter-terrorism Strategy, p. 1-3;

5. История на тероризма от Античността до Ал Кайда, под редакцията на Жерар Шалиан и Арно Блен (София: Леге Артис, 2005);

6. Досев, Н., Сандев Г. „Тероризъм и противодействие” с.1;

7. Константинов, Е., Симеонов, Л. Европейска сигурност и противодействие на тероризма. София, 2002.

8. Мирчев, М. Борбата с тероризма и участието на въоръжените сили в антитерористични операции. // В. журнал, № 6, 2003

9. Христов, Х. Доклад на тема:„Особености на организацията и управлението на оперативното противодействие на посегателства срещу фирмената сигурност”. Сборник научни трудове от Юбилейна научна конференция „10 години от създаването на НВУ „В.Левски” Том.4, проведена в ” НВУ „В.Левски” на 14-15.06.2012год..

ПОНЯТИЕ ЗА НАЦИОНАЛНА СИГУРНОСТ. РАЗБИРАНЕ НА НАЦИОНАЛНАТА СИГУРНОСТ КАТО СПОСОБНОСТ НА ДЪРЖАВАТА ДА ЗАЩИТИ НАЦИОНАЛНИТЕ СИ ИНТЕРЕСИ

КАЛИН ИВАНОВ КРЪСТЕВ

CONCEPT OF NATIONAL SECURITY. UNDERSTANDING OF THE NATIONAL SECURITY AS THE STATE'S ABILITY TO PROTECT ITS NATIONAL INTERESTS

KALIN IVANOV KRASTEV

ABSTRACT: *National security are the measures taken by a country to ensure their survival and safety. National security involves stopping attacks - inside (internal) and outside (external), as well as the protection and welfare of the citizens. Republic of Bulgaria appears as the geopolitical center of the Balkan region, which intertwine almost all important aspects of international relations in Southeast Europe. In continental term, however , the geopolitical situation of our country is the source of more problems than benefits. Bulgaria has emerged as part of the southern sector of Europe where historical practice problems interstate complex political, economic , territorial, ethnic and religious backgrounds are the basis of a number of potential sources of tension that at any time can become a risk factors not only for her safety but also that of the entire region.*

KEY WORDS: *national security, national interests, risks, threats, security environment, nation, protection of classified information, a concept of national security, national security system, information sources, sources of external threat, internal sources of threat, political and military situation, major risk factors, NATO.*

Проблемите на сигурността обективно са в центъра на общественото внимание. Те засягат защитата на интересите на личността, на социалните групи и на националната общност като цяло.

В самото начало на XXI век експертите по национална сигурност със закъснение разбраха, че светът е поставен в условия на неочаквана

глобална несигурност. На 11 септември 2001 г. в Ню Йорк и Вашингтон и след това в Мадрид през 2004-а и в Лондон през 2005-а съвременният международен тероризъм категорично демонстрира окончателното „детрониране" на старата представа за сигурността. Осъзнаването на новата несиурност доведе до появата на нова парадигма, която постави нови изисквания към преодоляването на заплахите и рисковете, появяващи се в обикновено неустойчива, бързо изменяща се, трудно преодолима и неовладяна среда.

Новата парадигма на сигурността императивно и непрекъснато поставя въпроса за нов подход при анализа на рисковете и заплахите в средата за сигурност. Налагането на новата парадигма съвпадна неслучайно с един друг процес – глобализацията. Определящ фактор в нея е революцията във високите технологии, особено в областта на информатиката, и навлизането им във всекидневния бит на хората (масови мобилни комуникации, Интернет, компютърна техника и пр.). Под влияние на информатиката и високите технологии средата за сигурност придоби ускоряваща се динамика, която допринесе за нарастване на неопределимостта на случващото се. [1].

Сигурността е елементарна форма на битийност в онова, което бива назовано теория на националната сигурност, сигурността е нейно базисно понятие [2], потребно също, както човешките потребности в мотивационната теория. Изпитването на потребност от сигурност не означава самата сигурност Човекът или общността от хора не удовлетворяват своите потребности сами по себе си – техните потребности биват удовлетворявани във взаимодействие със средата. Следователно в познавателен и практически смисъл сигурността би следвало да бъде разкрита и постигната в активното отношение човек – среда.

Разграничават се „Субективна и обективна сигурност", като обективната сигурност се свързва с отсъствието на заплаха (за ценностите на системата), а субективната – с отсъствието на страх от заплаха (че тези ценности ще бъдат атакувани). За да има истинска сигурност, трябва да са налице и обективната, и субективната сигурност" [3].

Накратко: **сигурността е проявявано качество на взаимодействие, при което дадена система запазва своята специфика**. Затова сигурността е толкова относителна, не принадлежи на нито една система, а единствено на взаимодействието между системи, трудно е определима като понятие и проява, защото се проявява винаги в отношение, но не и във всяко отношение, а в отношение спрямо дадена конкретна система. [4].

Логично следва въпросът "**Какво е национална сигурност?**" Доколкото вече е известно какво е сигурност, търсенето на отговор следва да се насочи към това, какво представлява нацията, която е генератор и потребител на сигурността и разбирането за която би следвало да бъде отразено в разбирането за национална сигурност.

Бенедикт Андерсън откроява четири основни характеристики на нацията: ограниченост, общност, суверенитет и въобразеност. [5].Обединяващата черта на четирите характеристики е тяхното осъзнато субективно изживяване както от отделния човек, така и от човешката общност.

Антъни Смит дава определение за нацията като „наименовано население, което споделя обща историческа територия, общи митове и исторически спомени, масова публична култура, обща икономика и общо юридическо право и задължения на всички членове". Смит констатира и че независимо от начина си на формиране „по принцип нацията трябва да съчетае две измерения, едното е гражданско и териториално, а другото – етническо и генеалогично". [6].

Със Закона за защита на класифицираната информация (ЗЗКИ) на практика се въвежда ограничаване на правото за достъп до информация, предвидено в чл. 41 на Конституцията на Република България, в който се казва: „*Всеки има право да търси, получава и разпространява информация. Осъществяването на това право не може да бъде насочено срещу правата и доброто име на другите граждани, както и срещу националната сигурност, обществения ред, народното здраве и морала*"[7]. Това ограничение е основано на защита на „Националната сигурност". От разбирането на това какво е национална сигурност, зависи и доколко ще се ограничава правото на достъп до обществена информация. Това понятие за пръв път получава правна дефиниция именно в ЗЗКИ, § 1, т. 13 от допълнителните разпоредби, която: „*Национална сигурност" е състояние на обществото и държавата, при което са защитени основните права и свободи на гражданите, териториалната цялост, независимостта и суверенитетът на страната и е гарантирано демократичното функциониране на държавата и гражданските институции, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива*" Концепцията за национална сигурност, както и няколко закона определят информационната сигурност като национален интерес. Спрямо методите за гарантиране на националната сигурност на държавата, организационната структура и принципите на действие на системата за национална сигурност могат да се изброят следните критични области:

- Информационните източници на Министерството на отбраната, Щаба по отбрана, щабовете на видовете въоръжените сили и научноизследователските звена; информация и факти /данни за подготовката и провеждането на оперативни и стратегически планове, разполагането на войски и мобилизацията, тактико-техническите характеристики на оборудването;

- Информационните ресурси на военнопромишления комплекс, както и за промишления потенциал и количеството налични суровини и материали; информация за основните насоки на разработките на оборудване за въоръжените сили;

- Системата за командване и управление на страната, личния състав и оръжейните системи, както и информационната им поддръжка;

- Морално-психологическото състояние на въоръжените сили;

- Информационната инфраструктура (контролни точки и връзки, релейни точки, тропосферни и спътникови комуникации), включително и комуникациите с други министерства.

Източници на външна заплаха за националната сигурност на страната са:

- Всички видове разузнавателна дейност;

- Информационно-техническа дейност като електронна война и методи за проникване в компютри;

- Психологически операции на възможни противници както чрез специални дейности, така и чрез средствата за масови комуникации;

- Дейности на чуждестранни политически и икономически структури, които са насочени срещу интересите на държавата в сферата на отбраната;

Съществуват и вътрешни източници на заплаха на сигурността, а именно:

- Нарушаване на установените комуникации и информационни средства в щабовете и учрежденията на Министерството на отбраната;

- Преднамерени и непреднамерени грешки на персонала на информационната система със специална значимост и предназначение;

- Информационно-пропагандна дейност на организации и личности, насочени срещу интересите на правителството, които водят до снижаване на боеспособността и боеготовността на въоръжените сили;

Всички тези заплахи са особено значими при влошена военнополитическа ситуация.

На основата на концептуалните методи се структурират целите при гарантиране на националната сигурност на държавата, например цели, произтичащи от практически задачи, правилно оценяване на

информационните заплахи и техните източници. Методите от тази област служат за усъвършенстване на средствата за защита на информационните източници от несанкциониран достъп чрез разработване на защитени системи за командване и управление и повишаване на надеждността на компютърните ресурси. На основата на организационните методи се формира оптимална структура и състав на функционалните органи на системата за национална сигурност и се координира тяхното взаимодействие, усъвършенстват се методите за стратегическата и оперативна дезинформация, разузнаване и електронна война и се развиват методи и средства за активно противодействие на информационно-пропагандни и психологически операции на възможен противник.

Концепцията за националната сигурност на Република България представлява официално приети политически виждания за защита на българските граждани, общество и държава от външни и вътрешни заплахи от всякакво естество, при отчитане на наличните ресурси и съобразяване с нивото на гаранциите, които дават световната, евроатлантическата и европейската система за сигурност и стабилно развитие. Съгласно тази концепция, национална сигурност има, когато са защитени основните права и свободи на българските граждани, държавните граници, териториалната цялост и независимостта на страната, когато не съществува опасност от въоръжено нападение, насилствена промяна на конституционния ред, политически диктат или икономическа принуда за държавата и е гарантирано демократичното функциониране на държавните и гражданските институции, в резултат на което обществото и нацията запазват и увеличават своето благосъстояние и се развиват. Българските граждани, обществото и държавата имат задължения, записани в Конституцията и законите на страната, сами да са създатели и гаранти на своята сигурност. Едновременно те са взаимносвързани потребители на сигурност, при които нарушаването на безопасността на който и да е от тях нарушава безопасността на останалите. Те съставляват заедно единната структура за сигурност на България. Сигурността е гарантирана, когато страната успешно реализира националните интереси, цели и приоритети, и при необходимост е в състояние ефективно да ги защити от външна и вътрешна заплаха. Равнището на сигурност се определя от степените на защита и на ефективно реализиране на интересите на българските граждани, общество и държава, които в съвкупност съставляват националните интереси. Интересите на българските граждани са в реалното гарантиране на конституционните права и свободи, личната безопасност, повишаването на качеството и равнището на живота, на

социално и здравно осигуряване. Интересите на гражданското общество са в утвърждаването на демокрацията, гражданския контрол върху институциите и свободата на сдружаване, в правата на религиозните, етническите и малцинствените групи, в съхраняването на националните духовни и културни ценности и традиции. Интересите на държавата изискват защита на Конституцията, суверенитета и териториалната цялост на страната, постигане на политическа и финансова стабилност на икономическото и социалното развитие, строго спазване на правовия ред, равнопоставеност и взаимноизгодно международно сътрудничество.

Три са основните фактори на националната сигурност на България:

- степента на развитие и ресурсите на страната;
- ефективността на външната и вътрешната ú политика, и
- участието на България в колективните системи за сигурност и икономическо развитие.

Съобразно Конституцията на Република България отговорности за националната сигурност на страната имат Президентът, Народното събрание и Министерският съвет. Президентът възглавява Консултативния съвет за национална сигурност, чийто статут е определен със закон. Народното събрание осъществява законодателното изграждане на системата за национална сигурност. Чрез своята постоянна Комисия по национална сигурност, контролира изпълнителната власт и специалните органи на сигурността, относно законосъобразност и ефективност на действията им и ефективно използване на ресурсите, оценява политически опасностите. Чрез своята постоянна Комисия по външна и интеграционна политика, контролира изпълнителната власт в областта на външните аспекти на националната сигурност. Министерският съвет на основата на тази концепция и в изпълнение на възложените му от Конституцията на Република България отговорности в областта на сигурността с доклад пред Народното събрание ежегодно посочва рисковете за страната и дава оценка за степента на защита на националните интереси. Министерският съвет разпределя ресурсите на страната за повишаване степента на защита на националните интереси. Министерствата и ведомствата в рамките на своята компетентност разработват и реализират стратегии и програми за най-ефективно използване на политическите, военните и икономическите ресурси на страната. В изпълнение на функциите си Министерският съвет се подпомага от Съвет по сигурността в състав: министър-председателя, министъра на външните работи, министъра на отбраната, министъра на вътрешните

работи, техни заместник-министри, началника отбраната на Българската армия и ръководителите на разузнавателните и контраразузнавателните служби. Президентът лично или чрез свои представители може винаги да участва в работата на съвета и по всяко време да изисква от него информация. Съветът по сигурността:

- обобщава, анализира и прави изводи от цялата текуща информация за рисковете пред националната сигурност и дава професионална оценка и прогноза за динамиката на опасностите;
- планира конкретни мерки за неутрализиране на опасностите и предлага решения в условия на криза;
- координира плановете на специалните органи за добиване на информация и дава становища по разпределението на ресурсите;
- разработва и предлага на Министерския съвет годишен доклад за националната сигурност.

Президентът, председателят на Народното събрание и министър-председателят, изхождайки от основните цели и задачи, свързани със сигурността на страната, са заявители на информация в Съвета по сигурността. Съветът по сигурността представя равна по обем и еднаква по съдържание информация на Президента, председателя на Народното събрание и министър-председателя. Гражданският контрол върху държавната политика за сигурност и органите, които я изпълняват, се гарантира от Конституцията и законите на страната.

Динамичното развитие на военнополитическата обстановка в региона доведе до изменения и в естеството и значението на дестабилизиращите рискови фактори и заплахи и за сигурността на Република България.

В чисто теоретичен план те могат да бъдат класифицирани:

- по място (вътрешни и външни);
- по характер (военни и невоенни);
- по време (трайни и временни);
- по области на въздействие {политически, социално-икономически, информационни, екологични, демографски, хуманитарни, етно-малцинствени и религиозни);
- по степента на тяхното проявление и въздействие (реални или потенциални, преки или косвени) и др.

Това разграничаване е условно, още повече, че част от тях се проявяват комбинирано (например като външни и невоенни, трайни, косвени и др.). В някои случаи комбинираното им и едновременно действие допълнително може да усложни и дестабилизира обстановката не само в национален, но и в международен мащаб. Характерно за

съвременната военнополитическа обстановка е възникването предимно на вътрешни, а не на междудържавни конфликти.

Основните рискови фактори, които имат едно или друго въздействие върху стабилността и сигурността в региона, включително и за сигурността на Република България понастоящем са:

- особеното геостратегическо положение на страната;
- съществуващите конфликти и потенциално кри шепи райони в Югоизточна Европа, някои от които се намират в непосредствена близост до границите на страната;
- действията на международни и регионални терористични формации и организирани престъпни групи и проявите застрашаващи сигурността, правата и свободата на гражданите;
- дисбалансите във въоръженията и състоянието на въоръжените сили на страните от региона и неравнопоставеността им по отношение на гаранциите за тяхната национална сигурност;
- социално-икономическите проблеми и неблагоприятната за България демографска характеристика;
- заплахите за информационната сигурност;
- възможните природни бедствия, мащабни промишлени и екологични аварии и катастрофи и др.

Обектите срещу които могат да бъдат насочени някои от рисковете и заплахите за националната сигурност са практически във всички области, но като основни могат да бъдат посочени:

- политическата и държавната система на страната;
- стопанската и финансова стабилност;
- отбранителната система и структурите за сигурност;
- единството на нацията, нейните духовни и културни ценности;
- междуетническите отношения и религиозната търпимост;
- елементи от външната политика;
- отношенията ни с конкретна страна или организация (съюз), които са приоритетни за нас;
- информационната система на страната;
- стратегическите инфраструктурни обекти, (транспортни и комуникационни възли, енергийни трасета и др.), в. т.ч.. военни обекти;
- екологично опасни обекти и др.

Политическата нестабилност на Балканите в резултат на тлеещите етнически конфликти и гранични спорове, на възникването на нови държави след разпадането на бивша Югославия, е реалност чието развитие в близка перспектива е повлияно от редица комплексни фактори и по тази причина е трудно предвидимо. Кризисното развитие на обстановката в някои части на Балканите, показва особеното

значение на етническите и религиозните противоречия и на предизвиканите от тях дезинтеграционни тенденции върху вътрешната стабилност на някои от страните. Крайният национализъм също остава рисков фактор за стабилността в Югоизточна Европа. Неустойчивото икономическо развитие на повечето страни в региона, породено от финансовите, стопанските и социалните затруднения и проблеми, безработицата и емиграцията увеличава заплахите за жизнено важните инфраструктури и преди всичко за информационните системи. Динамичното развитие на световното информационно общество увеличава рисковете за проникване, манипулиране и унищожаване на информационните масиви с цел извличане на представляващи интерес данни и информация и за парализиране на дейността на държавни и частни институции. Заплахи произтичат и от засиления интерес на терористични и други престъпни организации към поддържането и използването на такива масиви. Разпространението на опасни технологии и преди всичко на компоненти за оръжия за масово унищожаване е сериозна заплаха за сигурността, тъй като създава предпоставки за държави, терористични и престъпни организации да се снабдяват, разработват и търгуват с технологии и компоненти за производство на ядрени, химически и биологически оръжия и технологии с двойна употреба. Активизирането на международния тероризъм засилва рисковете от използването на такива оръжия срещу граждани и обекти в различни райони на света. Предизвикателство за националната сигурност на България е и трафика и търговията на хора. Налице е тенденция за засилване на миграционния поток към Западна Европа, САЩ и Канада на граждани от страните на Азия и Африка. Наблюдава се усложняване на обстановката във всички гранични райони, където се изграждат и функционират канали за прехвърляне през граница на нелегални емигранти. Бежанските и имиграционни проблеми (особено актуален проблем към настоящият момент за Република Бълария), натрупани през последните години на кризи и военни конфликти, генерират нестабилност и непредвидимост заради липсата на средства и достатъчна воля за тяхното разрешаване. Перспективата за интегриране на нашата страна в ЕС и отпадането на визовите ограничения прави бежанския проблем и нелегалната миграция сериозна заплаха за сигурността на нашата страна. Те, както и нелегалната миграция са сериозна заплаха, поради използването на региона и като транзитен и като „подкрепителен" пункт по пътя към Западна Европа. Близостта и влиянието на кризисно протичащите процеси в Източното Средиземноморие, Близкия изток и Кавказ, чрез възможността за износ от тях на организирана престъпност,

наркотрафик, религиозен екстремизъм, засилена емиграция, както и проблемите в двустранните отношения между някои от държавите в региона, задържат развитието на връзките и в една или друга степен влияят върху интересите и сигурността на България.

Сериозно предизвикателство за националната сигурност на нашата страна и борбата срещу новите заплахи в света и региона ще продължи да бъде трафикът на наркотици и оръжие, нелегалните канали за който преминават през Балканите и територията на нашата страна. Тероризмът и организираната престъпност се превръщат в първостепенна заплаха за политическата стабилност и националната сигурност. Извършените терористични атентати в САЩ, Русия, Турция, Испания и др. страни показаха уязвимостта на демократичните общества от асиметричните заплахи и това, че националната сигурност на която и да е страна, включително и на България, в досега влагания в това понятие смисъл, не може да бъде гарантирана напълно и със самостоятелни усилия.

Близостта и влиянието на кризисно протичащите процеси в Източното Средиземноморие, Близкия изток и Кавказ, чрез възможността за износ от тях на организирана престъпност, наркотрафик, религиозен екстремизъм, засилена емиграция, както и проблемите в двустранните отношения между някои от държавите в региона, задържат развитието на връзките и в една или друга степен влияят върху интересите и сигурността на България.

Борбата срещу тероризма е голямата война на нашето съвремие. Тази война е уникална спрямо войните досега и не прилича на никоя от тях.

Въз основа на изложението могат да се направят следните изводи и заключения:

С приемането на Република България за член на НАТО през 2004г., у нас е налице нова военнополитическа и военностратегическа среда с ново, по-високо състояние на сигурност и с нови, по-високи отговорности, а именно:

От пролетта на 2004 г. върху сигурността на България влияние оказват колективните гаранции и задължения по силата на Вашингтонския договор;

В общата система за сигурност военният фактор продължава да играе определяща роля в тясна връзка с дипломатическите, политическите и икономическите фактори;

Новите рискове и заплахи на XXI-ви век изправят пред нови предизвикателства националната сигурност на Република България и Българската армия;

Назрява необходимостта от нови концептуални и доктринални документи и планове за реализирането им, съответстващи на отговорностите от членството в НАТО и рисковете и заплахите на XXI-ви век.

Основните мисии на Въоръжените сили на Република България в тази нова среда, трябва да бъдат: отбранителна; подкрепа на международния мир и сигурност и принос към националната сигурност в мирно време.

За изпълнение на отбранителната си мисия, Въоръжените сили ще провеждат отбранителна операция на собствена територия или друга съюзническа територия, в отговор на военна криза за защита на териториалната цялост и независимост на страната, както и тази на други съюзнически държави;

За изпълнение на мисията, подкрепа на международния мир и сигурност, Българската армия осигурява формирования в състава на многонационални сили или самостоятелно за провеждане на операции по поддържане на мира, мироналагащи, хуманитарни и спасителни операции извън територията на страната. Сега, след като вече сме член на НАТО, тези подразделения ще бъдат ядрото на силите, които страната ще предостави за участие в пълния спектър от мисии на Алианса. Същите са основният компонент от силите за развръщане (Deployable Forces).

За изпълнение на мисията принос към националната сигурност в мирно време Българската армия ще поддържа определено ниво от основни сили за отбрана (In Place Forces), с които ще бъде гарантирана националната сигурност и териториалната цялост на страната, както и за подпомагане на населението при бедствия, аварии и катастрофи, борбата с тероризма, организираната престъпност и трафика на наркотици, хора и оръжия и провеждане на операции по издирване и спасяване.

Важна задача, произтичаща от членството ни в НАТО и свързана с националната сигурност, е актуализацията на правно-нормативната база.

Обществените отношения, свързани със сигурността, отбраната и с Въоръжените сили на Република България се уреждат с конституцията на страната, Закона за отбраната и Въоръжените сили (ЗОВС) и с отделни закони и нормативни актове за някои от структурите на системата за сигурност.

Новите реалности в света, в Европа, натрупаният от страната ни международен авторитет и последователната ú принципна политика на добросъседство и сътрудничество са важна предпоставка за успешното отстояване на националните интереси и сигурност. Съществуващите днес рискове и заплахи за националната сигурност изискват съвършено нов тип образование и обучение на командирския и редовия състав на Българската армия, адекватни на променената стратегическа среда и новите мисии. Във фокуса на този процес следва да бъде развитието на ново поколение командири, способни да действат в усложнената стратегическа среда, както и в условията на пълноправното членство на страната в НАТО. Настъпилите промени налагат разработването на нова концепция за национална сигурност, военна доктрина и национална военна стратегия. Те ще наложат промени в отделните доктрини за използването на войските и силите на оперативно и тактическо ниво.

От всичко това следва изводът, че на този етап и през следващите години Република България ще отстоява своите интереси в сложна глобална и регионална среда на динамично променящи се и трудно предвидими предизвикателства.

Л и т е р а т у р а:

1. Rogers, Paul. International Security in the Early Twenty-First Century (2000). HTNL, www.ciaonet.org, 07.06.2006

2. Слатински, Н. Измерения на сигурността София, 2000, с. 184;

3. Христов, Х. и Н. Тодоров Доклад на тема: „Теоретични подходи относно проблематиката на сигурността". В: Сборник трудове на научна конференция „Научна сесия 2013". ФАПВОКИС на НВУ, Шумен, 2013, с.2;

4. Гюров, Р. Към анализа на сигурността (в контекста на контраразузнаването). Фондация „Национална и международна сиурност", библиотека „Сиурност" София, 2011, с. 77;

5. Андерсън, Бенедикт. Нации и национализъм. Москва, 2002, с. 416;

6. Смит, Антъни. Национална идентичност. София, 2000, с. 296;

7. Концепция за национална сигурност, приета с решение на 38 НС от 16.04.1998г. (ДВ, бр. 46/22.04.1998г.).;

8. Закон за защита на класифицираната информация, § 1, т 13 от Допълнителните разпоредби

СТЕГАНОГРАФИЯ – ИЗКУСТВОТО ДА СКРИВАМЕ ИНФОРМАЦИЯ

СВЕТЛИН ПЛ. ИЛИЕВ, ДОНИКА В. ДИМАНОВА

STEGANOGRAPHY - THE ART HIDDEN INFORMATION

SVETLIN PL. ILIEV, ANELIA V. STAMENOVA, DONIKA V. DIMANOVA

ABSTRACT: *Nowadays disclose more personal information about themselves than before. As a result, the number of potential threats of theft of such personal data increase. Also, continuous, new methods used for this purpose.*

KEYWORDS: *information, threats, theft.*

В днешно време разкриваме много повече лична информация за себе си, в сравнение с преди. В резултат на това, броят на потенциалните заплахи от кражба на тези лични данни се увеличи. Също така, постоянно се появяват нови начини, използвани за тази цел. Проблемът идва в това, че освен общодостъпната информация излагаме на риск и данни, които искаме да останат в тайна (типичен пример е обсъждането на нов бизнес проект или изпращането на PIN код или парола на някой наш близък). Криптографията е наука, която ни дава решение на проблема, но и тя има слабости. Ако някой следи нашата кореспонденция, то той ще види, че изпращаме криптирана информация и ще се опита да разбере каква е тя. Какво е решението на проблема или по-точно – как да предаваме информация, без това да е видно за останалите?

Стеганография – изкуството да скрием информация. Стеганография, в буквален превод означава “тайнопис”. Тази наука изучава начините да скрием дадено съобщение (данни). Не трябва да се бърка с Криптографията, тъй като там става въпрос за промяна на информацията, с цел тя да не може да бъде възстановена в оригиналния си вид от неоторизирани лица. Все пак, често се използва съвкупност от Криптография и Стеганография.

Едни от първите примери за Стеганография са от времето на древна Гърция. Може би най-интересният пример от тогава е следният: Когато някой иска да предаде тайно съобщение, той обръсва главата на вестоносеца и записва съобщението на темето му. След като косата му порасне той отива до получателя, където пак обръсва главата си, за да може съобщението да бъде прочетено. Така при евентуално залавяне на вестоносеца няма да се разбере, че има съобщение.

В днешно време, голяма част от информацията, която изпращаме е чрез Интернет, а самата тя се съхранява в компютъра ни. Това води до развитие на Стеганографията и до появата на нови решения на проблема за скриването на данни. Въпреки това, все още Стеганографията се използва и за друг вид носители на информация. Като цяло използването ѝ, без значение дали в компютрите или не, е доста рядко явление. Въпреки това, този метод на защита на данните е доста ефективен по простата причина, че е доста трудно да се разбере, че тази информация (която сме скрили) я има.

Нека се запознаем с основните способи за скриване на съобщения. Остава обаче уговорката, че могат да бъдат измислени безброй много други начини за това.

Един пример, който може би почти всички от вас са виждали в някой филм. Дадено съобщение е скрито в статия или в книга на определена страница. За да бъде прочетено, трябва да се прочетат например първите букви от всеки ред или нещо подобно. Това е доста добър начин, тъй като се използва нещо съществуващо, при това нещо масово. Това осигурява липсата на подозрения, че изпращаме съобщение на някой. Естествено, възможни са много различни вариации на този метод – четене през ред, през дума и така нататък.

Друг пример, който е бил използван през Втората Световна Война е писането с невидимо мастило. Съобщенията са били записвани на празен лист хартия като след това обикновено са записвали маловажна или фалшива информация с нормално мастило (има и варианти, при които са оставали листовете празни). Така при прихващане на писмото, съобщението не е било видимо. Обичайни невидими мастила са били урина, мляко и оцет. При нагряване тези течности потъмняват и така се разчита написаното. В днешни дни има различни невидими мастила. Обикновено те се виждат при облъчване с различна светлина, на какъвто принцип са и част от защитите на ценните книжа и документите за самоличност. [1][3]

Още един метод (използван от ученици и студенти по време на изпит) е скриването на съобщения (или пищови) в различни предмети. Пример са химикалките с навит лист хартия в тях. Друг вариант е изписването на текст върху сканиран етикет на бутилка от минерална вода. Естествено има и десетки други варианти, които са близки до тези. В това отношение изобретателността на учениците и студентите не е за подценяване!

Нека разгледаме и основните начини за Стеганография при работа с цифрова информация. Остава уговорката, че други методи също могат да бъдат измислени.

Без значение каква е информацията, в компютъра тя е в цифров вид. Представена е от определен брой единици и нули (битове). Това е и причината да можем да скриваме всякакъв тип информация. Въпреки това, за Стего-среда (средата, в която е скрита информацията) не може да се използват всички видове файлове (някои не позволяват да бъдат променяни). Също така, различните типове файлове, които стават за Стего-среда, могат да скрият различно количество информация в себе си. [2][3]

Има няколко основни начина за скриване на информация в друг файл, както и няколко основни файлове, които се използват за "носители" на съобщението.

Най-често използваните Стего-среди са изображенията. Там се използва методът на най-малко значещия бит (LSB – Least Significant Bit). Идеята се състои в това, че при много малка промяна на цвета на дадена точка, окото не усеща разликата.

Най-добре това се осъществява с използване на 24 Bit BMP (Bitmap) изображение. Там, всяка точка от картината се определя от едно 24 битово число (224 броя единици и нули), съставящо три числа за всеки от цветовете червен, зелен и син, всяко представено от едно 8 (28 броя единици и нули) битово число. Последната цифра, от всяко от тези три числа, се променя, като в тези битове се записва скритата информация. Това, че за всеки от трите цвята отговаря по едно 8 битово число означава, че всеки един от тези цветове има 256 различни стойности. При промяна на последния значещ бит, се преминава от една стойност към съседната (пример: RGB=(123,022,112), а след промяната ще е RGB1=(122,021,113)). Това означава, че промените са толкова малки, че окото ни не може да забележи разликата. Нека да направим една проста сметка: Ако имаме едно 3-мегапикселово изображение

(съставено от приблизително 3,000,000 пиксела) и сме променили последните значещи битове на всеки цвят от всеки пиксел, то ние сме използвали 3 x 3,000,000 = 9,000,000 битове, което е около 3 Mbit (384 kB). [1][2]

Възможно е да използваме и по повече от един бит от всеки цвят, но това води до по-сериозна разлика в оригинала на изображението и картинката със скритата информация. Това е проблем, тъй като вече може да се забелязва тази разлика. Предимството на този метод е, че големината на файла не се променя. Също така, при други формати, като JPG например, количеството информация, която можем да вмъкнем е по-малко, тъй като там е по-различна структурата на файла. Там данните са компресирани, поради което е и по-малкия обем на файла. Важно е да знаем, че при обработката на даден файл (промяна, компресия и други), то най-вероятно скритото съобщение ще се заличи.

Методът на най-малко значещия бит (LSB – Least Significant Bit) или негова разновидност (промяна на по-голяма част от информацията) може да се използва и в друг тип файлове. Във видео файловете можем да променим малко всеки един кадър, като така окото няма да забележи разликата, но ще успеем да вмъкнем друга информация. Също така, в текстовите документи можем да скрием съобщение като добавим излишни интервали или табулации. Така общият вид на документа няма да се промени, но ще сме записали (незабелязано при това) и друга информация. [1]

Друг способ, който се използва за Стеганография е вмъкването на информация в даден файл (Injection). При него вмъкваме съобщението си във файла, като така увеличаваме размера му. Този метод също може да се използва при изображения. Идеята тук е, че в даден файл добавяме информацията, която искаме, без да го повреждаме. В резултат на това ще имаме по-голяма картинка например, която ще е същата като оригинала, но ще съдържа в себе си и нашето съобщение.

Методът на вмъкването на информация в даден файл (Injection) също може да се използва и за друг тип файлове. Пример може да се даде със звуковите такива. При тях може да се добави шум, който да представлява скритата информация. Тук количеството данни, което можем да скрием е относително по-малко, тъй като ухото е доста чувствително (по-чувствително от окото) и по-лесно усеща разликите.

Освен по тези начини, Стеганографията може да се извършва и по време на изпращане на данни. Тогава се използват транспортните

слоеве (също така може да се използва транспортния слой при mp3 файл). Пример за това е пренасянето на данни по време на Интернет-телефония. Различни изследвания показват какво количество информация може да се изпрати по време на Интернет-разговор. Интересен пример е за изследване колко информация може да се изпрати чрез технологията VoIP (Voice over Internet Protocol). Установява се, че за 13 минутен разговор (използвайки Skype) може да се предадат около 1,3 Mbit скрити данни. [2]

Къде намира приложение Стеганографията? Освен в прикриването на лична информация и защитата на ценни книжа, Стеганографията намира приложение и в "маркирането" на различни файлове. Пример за това е електронният подпис. Той представлява информация, която е вмъкната в картинка, песен, видеоклип или някакъв друг файл. Целта на тази информация е да покаже кой е автора или собственика, а по същество този метод за "подписване" на файлове е Стеганография. Също така, друга разновидност е не вкарване на допълнителна информация, а изменяне на част от файла. Пример може да се даде със снимка, на която даден участък е напълно черен. Върху него може с малко по-светъл цвят (сив, но близък до черния) се напише например името на автора. С "невъоръжено" око няма да може да забележим надписа, но при достатъчно приближение (и евентуална компютърна обработка), и ако знаем къде да търсим, ще можем да го открием. Предимството на този метод е, че е по-устойчив на различни манипулации с файла.

Относно това как, на практика, да скрием информация в даден файл. Има много програмни решения, които използват различни методи за да осъществят това. Естествено в зависимост от това кой метод ползвате, какви файлове използвате за Стего-среди и какво количество информация искате да скриете, резултатите ще са различни. Може да се получи така, че да има видима разлика при използване на картинка или песен, може размерът на файла да се е увеличил много и т.н.. Трябва сами да прецените за вашите нужди кое е най-удачно. [2]

Също така, съществуват и много програми за Стеганализ (процес на откриване на скрита информация). В зависимост от метода на "замаскиране" на данните, анализът може да е с различна успеваемост. Също така, понякога се налага Стеганализ да правим ние.

Важно е да се отбележи, че Стеганографията често се използва заедно с Криптографията. В тези случаи съобщението се криптира, а

след това се скрива. Всичко това се прави с цел ако бъде намерено това съобщение да не може (или да е много трудно) то да бъде прочетено. [1][2] [3]

Когато искаме да изпратим съобщение, което да достигне само до определен човек, трябва да вземем мерки за защитата на тези данни. Стеганографията ни дава начин да го постигнем, тъй като хората, които е нежелателно да видят съобщението, дори няма да разберат, че има такова.

Благодарности

Този доклад е подкрепен по Проект BG051PO001-3.3.06-0003 “Изграждане и устойчиво развитие на докторанти, постдокторанти и млади учени в областта на природните, техническите и математическите науки”. Проектът се осъществява с финансовата подкрепа на Оперативна програма „Развитие на човешките ресурси”, съфинансирана от Европейския социален фонд на Европейския съюз.

ЛИТЕРАТУРА :

1. URL: http://diit.sourceforge.net/examples.html
2. Steganography An Art of Hiding Data - Shashikala Channalli, Ajay Jadhav, 2012г.
3. Aproaches for stego defense of sensitive information from inside leakage,Stanev S.,Christov Ch.,Dimanova D. Journal scientific and applied research, vol.4, 2013г. ISSN 1314-6289 (под печат).

КРИЗАТА КАТО СОЦИАЛНО ЯВЛЕНИЕ И ФАКТОР, ВЛИЯЕЩ ВЪРХУ СЪСТОЯНИЕТО НА НАЦИОНАЛНАТА СИГУРНОСТ

Доника В. Диманова

CRISIS AS A SOCIAL PHENOMENON AND FACTOR AFFECTING THE NATIONAL SECURITY

Donika V. Dimanova

ABSTRACT: *Crises occur objectively and logically as a consequence of social and natural disasters, leading to radical changes in social relations. Because of the enormous resources required for their master, crises directly affect the vital and fundamental parameters of the public who are in direct relation to the national security of the country. One of the main causes of the state is the need to ensure public safety. We can therefore say that the crisis is a factor affecting the state of national security.*

KEYWORDS: *Crises, factor, security.*

Въведение

Кризите възникват обективно и закономерно, като следствие от социални и природни катаклизми, водещи до радикални промени в обществените отношения. Поради това те приемат най – различни форми – обществено – икономически, политически, военни и т.н. В настоящия доклад ще разгледаме кризата като социално явление и като фактор върху състоянието на националната сигурност.

От древността множество необичайни и внезапно възникващи природни бедствия и космически катаклизми, се отличават от всички останали с това, че надхвърлят границите на човешкото знание и възможности за въздействие върху тях. Размаха, неизбежността и разрушителната мощ на природните явления, които водят до възникване на катастрофални щети ги определят като значима заплаха за човечеството, по отношение изграждането на способности за овладяване на последствията от тях. През последните десетилетия все по – често възникват събития, причинени от действия или бездействия на човека. Всички катастрофи и аварии са уникални и на пръв поглед вследствие от множество случайни събития. В този смисъл можем да

кажем за кризата, че е носител на цивилизационен потенциал, даващ възможност за разрешаване или трансформиране на конфликтите в човешките обществени системи.

Изложение

В различните направления на науката понятието "криза" се интерпретира по различен начин, в зависимост от това, каква сфера от обществения живот е засегната от дестабилизиращи явления и каква е причината за тяхното възникване и развитие.

Кризата е социален феномен, който в същността си е комплекс от събития, явления и взаимовръзки.

За пръв път понятието "криза" се е използвало в областта на международните отношения, където кризите изобилстват и се развиват във военни конфликти, характеризиращи се като сериозна заплаха за обществата и държавите. В началото на 21 век термина „криза“ започва да се използва в по-широк смисъл и се свързва със специфични обществени състояния, предизвикани от природни бедствия, големи катастрофи, социални катаклизми и дори политически кризи. В неговите характеристики вече се влага и елемент на неопределеност, което изключително много затруднява определението на кризата като явление, свързано със специфични обществени отношения.

Съгласно Закона за управление при кризи, кризата се определя като: "…промяна на установеното състояние на живот, обхванала територии, обекти, сектори и сфери на икономиката и обществения живот или околната среда, предизвикана от човешка дейност или природни явления, в резултат на която условията за съществуване и за осъществяване на дейност в променената среда са силно нарушени..."

В социологията, кризата се разглежда като форма на нарушаване на нормалния ритъм на живот на индивида и обществото. В социалната психология терминът „криза“ се употребява и като синоним на обществен стрес, паника, нарушение на традиционния обществен живот, насилие или потенциално насилие, криза в системата от ценности и т.н.

Георги Йолов определя кризата като връхна точка на възможно най – опасното и носещо определени рискове съчетание на обективни реални условия на живот и дейност, при които "хората са притиснати плътно от всички страни от заплахата както за живота си, така и за материалните и духовни ценности, които притежават" [4].

Многоаспектността на кризата предопределя и различните подходи при определяне на нейната терминологична същност. Кризата е състояние на човека или на дадена система, което е различно от

обичайното, нормалното или равновесното. При "критични състояния, които засягат мнозинството членове на обществото: войните, икономическите и природните катастрофи, резките политически промени от типа на революциите и други сродни събития, създаващи еднозначно емоционално преживяване и оценъчно отношение; всички те в определено социално време представляват социален проблем, споделян от масите" [3].

Актуалността на проблемите, свързани с определянето на кризите като социално явление и уреждането на обществените отношения, възникнали по повод на тяхното предотвратяване и овладяване е в това, че кризата е значимо социално явление, при което се активират значителни обществени ресурси и се засягат основни ценности на хората.

Кризата е феномен и е уникална в своята същност, като се характеризира с изключителна неопределеност. Поради това тя трудно може да бъде моделирана с цел извличане на конкретни закономерности, свързани с процеса на нейното появяване и развитие.

В средата на управлението, кризата може да се дефинира като процес, предизвикан от многобройни, неопределени, необичайни или внезапно възникнали събития и ситуации, при които съществува заплаха за живота, здравето, собствеността и статута на хората и организациите, като те не разполагат с необходимите ресурси за неутрализиране на рисковете и заплахите на средата, в която съществуват [1].

Особеностите на кризата, могат да се обобщят в няколко основни характеристики:

- неочакваност;
- висока степен на неопределеност в първоначалния момент на възникване на кризата;
- необходимост от бърза реакция при настъпване на кризисното събитие;
- недостиг на време за вземане на обосновани решения;
- паника и стрес, съпровождащ всяка криза;
- предизвиква бърза ескалация на събитията;
- застрашава живота, здравето и сигурността на хората, статута на организацията.

Кризата се характеризира с пространствени, времеви, комуникационни и социални параметри – зона на кризата, периода на нейното действие, обществени настроения и нагласи, засегнати от

кризата общностни групи от хора обособени по териториален, етнически, институционален или друг признак. По отношение на определянето на кръга на засегнатите групи от населението – това зависи от вида на кризата и нейния размах.

Кризите е възможно да се класифицират по определени признаци и съгласно различни критерии. Класификацията им е условна, тъй като ако определим една криза като икономическа, то тя притежава както социални и психологически, така и културни измерения.

В зависимост от начина на възникване и тяхната продължителност могат да се разграничат три типа кризи:

- внезапно възникващи кризи – породени са от неочаквани събития и ситуации, при което предупредителния етап на кризисния процес е пренебрежимо малък. Това са катастрофални земетресения, големи пожари, големи наводнения, промишлени аварии, катастрофи, терористични актове. Този тип кризи не могат да бъдат предвиждани с достатъчна вероятност, предполагаща предприемането на конкретни управленски действия за намаляване на последиците от тях.
- кризи възникващи след наличие на предупредителен период – този тип кризи могат да бъдат прогнозирани и при тях е възможно да се предприемат конкретни управленски действия за намаляване на рисковете на средата и последствията от възникване на кризата. При тях се разполага с повече време за събиране и анализ на информация и непосредствено планиране, но ситуацията може внезапно да се изостри след дълги периоди на относително спокойствие. Такъв тип кризи могат да възникнат при: етнически проблеми; бежански потоци; необходимост от хуманитарно подпомагане на големи групи от хора; културни сривове; икономически, социални и религиозни проблеми; екологични катастрофи; вируси; компютърен тероризъм; неудовлетвореност на служителите, нисък морал, сексуално насилие на работното място, злоупотреба с имущество, злоупотреба с информация и др. Развитието им е вследствие от възможни две причини: при неблагоприятно развитие на възникнали вече ситуации и инциденти и като следствие от липса на достатъчно управленски ресурси за предотвратяване на съществуващи рискове и заплахи.
- периодично повтарящи се – проявяват се периодично (всеки месец или всяка година), въпреки положените усилия. Такива кризи са свързани със смяна на "поколенията" в обществени дейности изискващи опит и рутина (политика, култура, спорт, специални служби и др.) или слухове и спекулации в медиите, които често преекспонират в общественото информационно пространство проблеми и факти в контекста на актуалното за деня.

Предвид спецификата на войната като тип криза с най – висока степен на интензивност, характеризираща се с всеобхватност, изразходване на огромни ресурси и предизвикана с цел постигане на стратегически цели, кризите се делят на: криза с военен характер и криза с невоенен характер.

Изхождайки от сферата на обществения живот, в която се е проявила криза, те могат да бъдат: военни; технологични; информационни, финансови, икономически, политически, екологични, културни, личностни и др.

В зависимост от това къде възниква кризисното събитие и в каква степен корелира то със самата система, кризата може да бъде: вътрешна за системата – неудовлетворени служители и външна за системата – информационна криза.

В зависимост от обществената структура, в която се проявяват параметрите на кризата, могат да бъдат: общински, областни, национални, регионални и международни.

В зависимост от обхвата на разпростиране кризите биват: индивидуални, фирмени или институционални, браншови, локални и всеобхватни.

Според продължителността на действие: краткосрочни, средносрочни и продължителни.

По критерий за институционална компетентност за осъществяване на общата координация на силите и средствата при овладяване на кризисни ситуации могат да се определят няколко нива на намеса:

- дейността по овладяване на кризисни ситуации, възникнали вследствие бедствия, аварии и катастрофи на територията на една община се ръководи от кмета но общината.
- дейността по овладяване на кризисни ситуации, възникнали вследствие природни бедствия, аварии и пътно – транспортни катастрофи, проявяващи се на територията на една област се ръководи от областния управител.
- в случаите, когато кризата се развива на територията на две и повече области е целесъобразно взаимодействието и координацията на силите и средствата, участващи в овладяването на кризата, да се осъществява от министъра на съответното компетентно министерство или ведомство.

Определянето на кризата като особено състояние на обществото, изискващо_предприемането на специфични действия за овладяване на рисковете и заплахите на средата, предполага дефиниране на понятия като: риск, катастрофа, извънредна ситуация, кризисна ситуация и

критична ситуация. Тези понятия са много прецизен индикатор за типа на настъпилото събитие и възникналите последствия, а доколко са свързани със заплаха за живота, здравето и нормалното съществуване на хората, в основата на тяхното разбиране стоят понятията: риск, опасност, катастрофа, бедствие.

Бедствието по своя смисъл се приближава значително да съдържанието на понятието катастрофа. Бедствието се свързва с човешки жертви, разрушения и поражения по инфраструктурата вследствие на природни явления. Социалният аспект на понятието може да се търси в неговите последици, върху обществото и психофизическото състояние на отделния човек. Съгласно Закон за защита при бедствия, „бедствие е събитие или поредица от събития, предизвикани от природни явления, инциденти, аварии или други извънредни обстоятелства, които засягат или застрашават живота или здравето на населението, имуществото или околната среда ...”.

Основният въпрос при изследването на катастрофата е дали тя е природно или техногенно явление. Катастрофата е набор от събития, притежаващи специфични характеристики: причинява значителни щети (материални, социални и екологични); възникват внезапно или преминават бързо от етап в етап; съществува възможност за предприемане на реални мерки за намаляване на последиците от тях, както преди, така и след възникването им.

Под катастрофа в българският език се разбира "неочаквано нещастие, бедствие, събитие с трагични последици" [6].

В Закона за държавните резерви и военновременните запаси катастрофата е дефинирана като: " събитие, явление или процес на действието на разрушителни сили, довели до мащабни тежки или унищожителни последствия, жертви, наранявания, разрушения и повреди, изискващи незабавни и възстановителни интервенции".

Катастрофата е внезапно събитие, съпроводено с тежки последствия, жертви, наранявания, разрушения и повреди, които причиняват загуби, налагащи незабавна локализационна, спасителна намеса в широк мащаб [7].

Явлението „катастрофата" е възможно да се изследва в три направления:

- резултат от външни фактори;
- следствие от вътрешни (социални) фактори;
- като начало на процес характеризиращ се като неопределен.

Според Карл Пеланда, каквито и да са подходите те се обединяват около нейните специфични свойства: "катастрофата е резултат от негативни социални или природни катаклизми; тя е

ситуация на колективен стрес в общността; представлява противоречие между способностите за справяне с деструктивните фактори и тяхното негативно влияние" [1,13].

Гаро Мардиросян дефинира катастрофата като "ситуацията, настъпваща при такива изменения на обкръжаващата ни среда, което застрашава живота ни или влияе неблагоприятно върху дейността ни". Катастрофата може да бъде предизвикана както от внезапни стихийни бедствия, така и от бавни дълговременни явления и процеси [2].

Опасността е природно явление или събитие, причинено от човешката дейност, което може да причини вредни последици за населението и имуществото му, околната среда, икономиката и културните и материалните ценности.

Ситуацията в същността си отразява обективното, моментно състояние, в което се намира отделния човек или система. Терминът произлиза от лат. "situs"- разположен и означава " съвкупност от обстоятелства, положение или състояние " [1].

Под „ситуация“ в психологическия смисъл разбираме динамична, внезапно изменяща се система от взаимни отношения между човека и други елементи на неговата околна среда, при което човекът е субект и съставна част на тази система. Динамиката и внезапността на измененията в системата са особено силни в районите на бойните действия, както в районите на стихийните бедствия, катастрофи и аварии.

Според Г. Йолов ситуацията е обективна, реална проява на определен комплекс условия на природата и обществената среда, която изисква отношението и участието на оказалите се в нея личности [5].

Ситуация с кризисоопределящи параметри е възможно да настъпи, вследствие на:

- натрупването на множество нерешени проблеми и конфликти;
- вземането на управленски решения, при които не са адекватно оценени възможностите на системата и степента на риска, водещи до ескалиране на социален конфликт;
- настъпване на природни бедствия, промишлени аварии и катастрофи, както и терористични действия.

Извънредната ситуация в българския език се определя като: "състояние, положение което се случва извън определения ред или програма и по своя характер е необикновено, особено, специално, изключително" [6].

Извънредната ситуация може да се определи също като състояние на дадена система, което е различно от обичайното и предполага особени, необичайни действия за излизане от него. Често като

извънредна се възприема такава ситуация, която: винаги включва заплаха; описва се от явления, които са редки по своя характер; хората нямат създадени навици да реагират или опит в справянето с възникналия проблем; голямо разнообразие. Тя е неочаквана, внезапно възникнала рискова обстановка, характеризираща се с неопределеност и сложност на вземане на решение, конфликтност и стресово състояние на хората, често с човешки жертви. Вследствие на нея възниква необходимост от допълнителен разход на човешки и материални ресурси за преодоляване на последствията от възникването ѝ.

Дефинирането на понятието „извънредна ситуация“ дава възможност за извеждане на конкретни критерии за разпознаване на онези явления и събития, които принуждават определена обществена система да предприема специфични и неотложни действия за справяне със възникналата ситуация. Тя може да е следствие както от природни явления, промишлени аварии и катастрофи, така и от нарушаване на нормалния ритъм на функциониране на дадена система вследствие социални явления като протести, масова психоза, нарушен институционален климат и т.н. Следователно появата на извънредна ситуация има потенциал да предизвика развитието на криза, която може да се определи като внезапно възникваща. Извънредната ситуация има времеви, пространствени и социални измерения и в повечето случаи хората и управленските обществени структури нямат изградени стереотипи за поведение в такива условия на средата. За овладяване на такива ситуации се налагат действия, които изискват друг тип поведение и различен от нормално прилагания режим на работа и обществен ред. В тази връзка наличието на извънредна ситуация, в зависимост от нейните характеристики може да предизвика обявяване на "извънредно положение" смисъла на чл. 84 т. 12 от Конституцията на Република България или "кризисно положение" съгласно разпоредбите на Закона за управление при кризи [1].

Кризисната ситуация по същност се доближава до извънредната ситуация, като разликата е в начина на възникване и развитие, и във факторите и явленията които я определят. Съгласно Закона за държавните резерви и военновременните запаси "Кризисна ситуация възникна вследствие действието на разрушителни или агресивни сили при бедствия, аварии и катастрофи, епидемии или други събития".

Тъй като липсва критерий за отличаване на кризисната ситуация и кризата като явления, често термина криза се използва за определяне и на не дотам значими инциденти.Такива са пожари, промишлени аварии и катастрофи чиито размах не предполага предприемането на мащабни действия за ликвидиране на последствията, а жертвите и материалните

загуби са незначителни. Възникналата ситуация може да придобие параметри, превишаващи възможностите на организациите да се справят с нея, и се налага привличането на допълнителни ресурси за това, но не можем да определим случващото се като криза. Кризисната ситуация няма този комплексен характер който характеризира кризата. Тя може да възникне в отделна сфера от обществения живот, да се развие както в процеса на кризата така и без да е обвързана конкретно с нея. Параметрите на кризисната ситуация могат да предизвикат ескалиране на рисковете и заплахите на средата вследствие което да възникне криза. Кризисната ситуация може да възникне преди случването на някакво събитие, вследствие ясно дефинирани рискове и заплахи, които ако не бъдат овладени или неутрализирани могат да доведат до появата на криза [1].

Критичната ситуация от своя страна се определя от състоянието на граничния параметър на критерия за възникване на кризисна ситуация. Той е детерминиран от наличието на собствени ресурси в системата за овладяване на възникналата ситуация. Ако има наличие на такива ресурси ситуацията следва да се определи като критична, а ако се налага използването на външни за системата ресурси, като кризисна.

Общото между всички изброени по – горе понятия е, че те са социална конструкция възникнала в резултат на различни по характер причини: природни, антропогенни и техногенни. Основата за разбирането на тези явления е понятието "риск".

В българския език под "риск" се разбира: "възможна опасност, действие наслука" [6].

Директивата Севезо II определя риска като „вероятността от специфично въздействие, настъпващо в рамките на определен период от време или при определени обстоятелства“. Като такъв, рискът е сложна функция от опасности, свързани с определена система. Приемливостта на определени рискове зависи от много аспекти, такива като контрол, страх, знание, доверие.

По смисъла на Закона за управление на кризи – "Риск" е вероятността за настъпване в определен период от време на прогнозирано събитие, оказващо негативно въздействие върху населението, територията, околната среда, културните и материалните ценности.

Понятието „риск“ в буквален превод означава вземане на решение, резултатът на което не е известен, той е несигурен. Неопределеността, е осъзната и се възприема като заплаха за случване на нещо, свързано с отделния човек или обществена група. Най – широко разпространеното разбиране за риска е като вероятност за

настъпване на неблагоприятно събитие и/или загуба. Риска е явление, чиято същност е решението. Превръщайки се в реалност той придобива характера на катастрофа, кризисна ситуация или криза.

Заключение

Кризите, поради огромните ресурси необходими за тяхното овладяване, пряко влияят върху основни, жизненоважни параметри на обществото, които са в пряка зависимост с националната сигурност на страната. Една от главната причина за възникване на държавата е потребността да се гарантира сигурността на обществото. Следователно можем да разглеждаме кризата като фактор, влияещ върху състоянието на националната сигурност. Равновесното състояние на обществото, в рамките на националната държава се основава на няколко основни фактора зависими от времето и установените, посредством конституцията и законите обществени отношения. Тези фактори са:

- постигнатото съгласие в обществото по жизненоважните за него въпроси, по отношение на националната сигурност;
- създадените и ресурсно осигурени обществени организации от структури, гарантиращи определено състояние на обществен ред и сигурност на обществото;
- гарантираните основните права и свободи на гражданите от правораздавателните, правоохранителните и правозащитни органи;
- не е нарушено икономическото и социално статукво в обществото на големи групи от хора, поради което няма наличие на масови протести и безредици.
- животът, здравето и собствеността на членовете на обществото не са засегнати или застрашени от сбъдването на случайно събитие обусловено от природни бедствия, космически катастрофи и технологични аварии, изразено с вероятността за възникването им;
- заплаха от навлизане на територията на страната на големи групи от чужденци, търсещи хуманитарна закрила ; бежански и емигрантски потоци;
- терористични актове, свързани с големи разрушения, човешки жертви или заплаха за живота и здравето на много хора;
- нелегален трафик на ядрени материали и радиоактивни вещества или нерегламентирано посегателство върху такива, при което се създават рискове и заплахи за живота и здравето на големи групи от хора и др.

Страните от ЕС все повече си сътрудничат в областта на „сигурността”, като си предоставят информация, свързана с рискове от кризи и подпомагане на спасителни действия при възникнали природни бедствия. Проведени от ООН и други международни организации анализи подчертават растящата уязвимост по отношение на бедствия, вследствие на нарастващата интензивност при използването на земята, промишленото развитие, експанзията на градовете и изграждането на инфраструктура.

Отговорностите за управлението на кризи и бедствия са различни за всяка страна и могат да бъдат делегирани на няколко министерства и ведомства. Освен тях НАТО и Европейският съюз споделят общи ценности и работят съвместно в операции за реагиране при кризи и бедствия. Съвместявайки граждански и военни инструменти за управление на кризи и реагиране при бедствия, НАТО допринася ефективно за прилагане на всеобхватен подход. Съществуват ред причини, поради които превенцията на бедствия е намерила своето място на общоевропейско ниво. Една от тях е, че кризите и бедствията не се съобразяват с националните граници и могат да имат транснационален мащаб. Те могат да имат отрицателен ефект върху политики на Общността като тези в областта на селското стопанство и инфраструктурата. Икономическите последствия от тях могат да имат негативен ефект и върху икономическия ръст на отделни региони в ЕС.

Действията на ниво ЕС и НАТО трябва да допълват националните мерки и да се съсредоточат върху области, в които общият подход е по – ефективен отколкото отделни национални подходи, въпреки че не трябва да се забравя, че превенцията е основно национална отговорност.

Благодарности

Този доклад е подкрепен по Проект BG051PO001-3.3.06-0003 “Изграждане и устойчиво развитие на докторанти, постдокторанти и млади учени в областта на природните, техническите и математическите науки”. Проектът се осъществява с финансовата подкрепа на Оперативна програма „Развитие на човешките ресурси”, съфинансирана от Европейския социален фонд на Европейския съюз.

Литература:

1. Специализиран курс за управление при кризи и кризисни ситуации, Лъчезар Милушев.

2. Екокатастрофи, Г. Мардиросян, ИК "Ванеса", София 1995г.

3. Социална психология на масовото поведение, Д. Градев, УИ "Св. К. Охридски", София 2000г.
4. Личността в критични ситуации, Г. Йолов, Партиздат, София 1975г.
5. Критични ситуации и масовата психика, Г.Йолов, София 1973г.
6. Български тълковен речник, Андрейчин, Георгиев и др. 4. изд. София, НИ, 2003г.
7. Национална система за управление на кризи.
8. Концепция на центъра за изследване и усъвършенстване на способностите на НАТО за управление на кризи и реагитране при бедствия, Март 2013г.
9. Подход на Общността за превенция на природни и причинени от човека бедствия, COM(2009) 82, Брюксел, 23.2.2009г.
10. Закона за управление при кризи, бр. 102 / 2006 г.
11. Закон за защита при бедствия, бр. 80 / 2011 г.
12. Закона за държавните резерви и военновременните запаси, бр. 9 / 2003 г.
13. C.Pelanda, Disaster and Order: Theoretical problems in Disaster Reserch, 1982г.

БИБЛИОТЕКА ЗА ИНФРАСТРУКТУРАТА НА ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ (ITIL)

Валентин Д. Стоянов

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

Valentin D. Stoyanov

ABSTRACT: *The Information Technology Infrastructure Library (ITIL) is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published in a series of five core volumes, each of which covers an ITSM lifecycle stage. ITIL underpins ISO/IEC 20000 (previously BS15000), the International Service Management Standard for IT service management, although differences between the two frameworks do exist.*

KEY WORDS: *Service Support, Service Delivery, Planning to Implement Service Management, Application Management, ICT Infrastructure Management, Security Management, The Business Perspective, Software Asset Management*

ITIL (на англ. IT Infrastructure Library) е библиотека за инфраструктурата на информационните технологии (произнася се «айтúл»). ITIL е колекция от специализирани методологически принципи, синтезирани от най-добрите практики, с цел да се оптимизират процесите за ИТ услуги.

За произхода на ITIL съществува много истории. Не е сигурно до колко и кои от тях са верни, но в един детайл историите са единодушни - началото на ITIL е положено във Великобритания в средата на 80-те години на миналия век. Някой от тези истории са наистина поучителни, за което си заслужава да се преразкажат.

Тачъризъм в действие

В средата на 80-те години на XX век във Великобритания администрацията на Маргарет Тачър решава да провери състоянието на правителствените ИТ като извърши масов одит във всяко министерство, институция и държавна агенция. Целта е повишаване на ефективността и драстично намаляване на разходите за поддръжка на ИТ. За целта

правителството се консултира с външни одитори, от които получава отговор, че такава проверка може да бъде направена само ако за текущото състояние на ИТ може да се направи съпоставка с общоприети управленски принципи за всяка от използваните дисциплини в ИТ. Такива към момента липсват и това дава първият тласък за генезиса на ITIL.

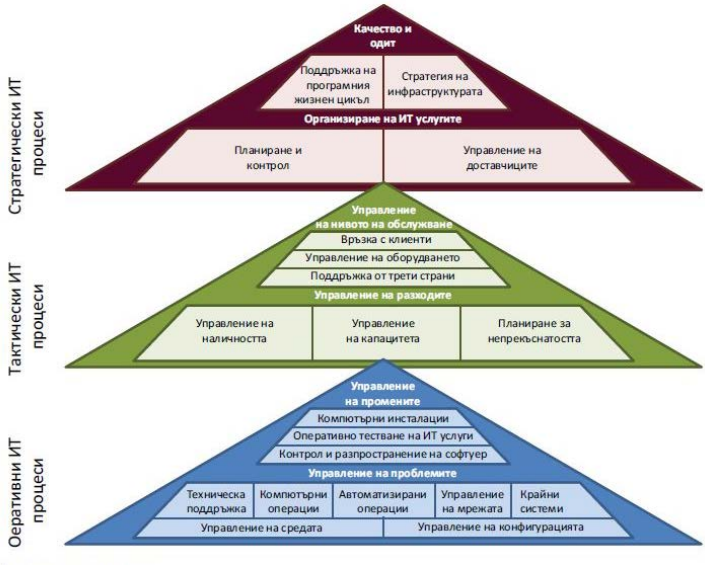
Фолклендската война

Друга версия твърди, че методиката е създадена в следствие на войната за Фолклендските острови между Аржентина и Великобритания, приключила през 1982 г. Между това стълкновение и краят на Втората световна война Обединеното кралство не е участвало в сериозни военни конфликти. Като следствие нуждата от прецизност и координация между отделните институции силно се подценява и от там с десетилетия комуникационните и информационни технологии на правителството се развиват безразборно и безпринципно. Ефектът от хаотичното внедряване на ИТ е изпитан най-силно от военноморските сили на Великобритания по време на войната, когато те трудно успяват да координират съвместните дейности и логистика дори вътре между различните части на флота. Когато започва подготовката за войната с Аржентина, става ясно че нещо трябва задължително да се направи, за да бъде поставено под контрол бързото проникване на ИТ в институциите. Това поставя началото на създаването на ITIL.

Мегапроектът на IBM

В средата на 80-те от IBM се свързват с администрацията на Тачър, за да проверят как би се приела идеята за поемане на ИТ услугите на държавните агенции от специализирани структури на компанията. В отговор на това от правителството поставят на IBM въпроса за очакваните разходи по начинанието, а от IBM пристъпват към проверка на състоянието на правителствените ИТ. Резултатът от проверката обезсърчава IBM, които се завръщат на масата за преговори вече с липсващо желание поради откритите от тях високо ниво на сложност, липсата на централизирана система за управление, силното разминаване между процесите и различното ниво на зрялост в отделните институции. Тази констатация дава основание на правителството да отдели средства и повери на Централната компютърна и телекомуникационна агенция (Central Computer and Telecommunications Agency - CCTA) задачата за осъществяване на проект, целящ откриване на върховите достижения в управлението на ИТ и на достъпните чрез тях услуги. Проектът продължава 4 години,

като напълно ангажира с работа 11 експерти. През 1989 год. излиза първата книга от колекцията, обобщаваща резултатите от изследването, която е в областта на управлението на нивото на услугите. Последен през 1994 год. излиза материалът за управление на наличността. Първоначалната цел на проекта е резултатът от изследването да се ползва единствено от правителството на Великобритания, но обикалящите различните държави консултанти споделят натрупания опит с бизнеса, от където в последствие се стига до световната популярност на методиката.



фигура 1: Модел на ITIL v1

Истинската история на методиката

Макар и различни, между тези истории липсва истинско противоречие, а в известен смисъл може да се приеме,че те дори се допълват.

ITIL започна съществуването си като GITIMM (Government Information Technology Infrastructure Management Method - Метод за управление на инфраструктурата от информационна технологична на правителството) в ССТА, която през 2000 год. е погълната от Бюрото за държавни поръчки на Великобритания (Office of Government Commerce - OGC).

ITIL е разработен от английския Център за Правителствена Търговия за оптимизация на ИТ услугите в публичната администрация на Обединеното Кралство. Понастоящем поредицата се издава от британската правителствена агенция Office of Government Commerce (OGC) и формално принадлежи на кралския дом на Англия, в частност - на сегашната кралица. Използвана от стотици организации по цял свят, ITIL философията се разраства благодарение на насоките и принципите описани в ITIL-книгите, базирани на най-добрата практика на частната индустрия и публичната администрация. ITIL услугите включват обучение, сертификация, консултиране, софтуер и имплементация.

В края на 80-те и началото на 90-те години ССТА управлява бюджет от над 8 милиарда паунда (спрямо сегашния курс еквивалентни на 9 144 427 480 EUR). Според разкази на няколко от участниците в проекта (Алън Нанс, Айвър Макфарлейн, Брайън Джонсън и Жан Ван Бон), основание за инвестирането в методиката освен подобряването на ефективността на работа и управлението на активите е идеята за „пробиране на пазара" - концепция, зад която стои желанието публичния сектор да се поучи от частния сектор по въпросите на управлението на ресурсите.

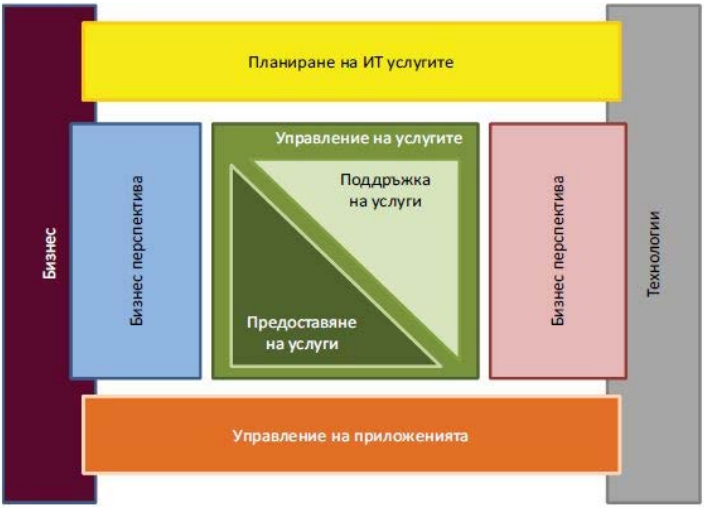
В разговор в коридор на агенцията Джон Стюард (ръководител в ССТА) и Рой Дибли (също от ССТА) решават, че със създадената колекция от над 30 книги GITIMM е по-близо до библиотека от добри практики, отколкото до метод за управление. В резултат на бързо взетото от двамата решение в крайната документация "MM" е сменено с "L" от Library (библиотека), а "G" бива случайно изпуснато. Така се стига до познатата днес абревиатура ITIL. Първоначалните стъпки по създаването на методиката се извършват още през 1985 год. от Уили Карол, Петер Скинер, Невил Грийнхал и други неизвестни днес ИТ експерти. Като основополагащ камък в началния градеж се използва ISMA (Information Systems Management Architecture) на IBM, но след сериозно допълнително финансиране проектът се разраства и включва проучване на добрите практики в ИТ в още над 50 фирми от частния сектор. Проучването се провежда под формата на изследване на казуси в различни сектори на икономиката, а резултатът е набор от добри практики, превърнали се в де-факто стандарт за предоставяне на ИТ услуги, приложим далеч извън рамките на правителството на Великобритания.

От средата на 90-те години на миналия век методиката започва да набира все по-голяма популярност и да се прилага масово от много компании по различните краища на света. Тази популярност и продължаващото й усъвършенстване не са само следствие от голите

ентусиазъм и вдъхновение на създателите на методиката, а в по-голяма степен резултат от планирани и координирани усилия за популяризирането и утвърждаването ѝ на международно ниво. Не на последно място за това е също и съзряната възможност за печалба чрез превръщането в бизнес на обучението и сертифицирането на знанията от методиката. Според Алън Нанс два фактора имат водеща роля за световното утвърждаване на методиката днес: предвиденото и осъществено по време на проекта създаване на добри учебни материали, а също и ентусиазма на група холандци, които през 1991 год. ползват ITIL за създаването на процесен модел IPW в KPN - водещ в страната телеком, които в последствие стоят в основата при създаването на itSMF (IT Service Management Forum).

В края на 80-те ССТА е подложена на множество атаки по няколко направления - от една страна в правителството от лобисти на множество компании, които се стремят към поемане на изпълняваните от централната агенция услуги (съответно и на свързания с това бюджет), а от друга и от останалите институции в правителството, които се стремят към независимо и децентрализирано управление. В крайна сметка агенцията е закрита и по този начин концепцията за въвеждане на централен правителствен орган за управление на ИТ е загубена. Това забавя не само теоретичното развитието на ITIL, но и прилагането на методиката в практиката, докато върви борбата между различните институции за това коя от тях каква част от процесите и услугите да поеме. В някои случаи постигнатото е трайно загубено, като например частта за управление на информационната сигурност. По време на разработването на методиката звеното за ИТ сигурност към ССТА предоставя основната част от знания по въпросите на сигурността, но след това изисква и налага секретност на тази част като част от собствената си борба за преразпределяне на свързаните със сигурността задължения.

През 1992 г. излиза версия 2, в която броят на документите е ограничен до 7, допълнени през 2002-а с още един документ под формата на изведената като самостоятелна дисциплина Управление на сигурността. През 2005 г. след сериозно преработване методиката излиза под версия 3, съставена от 5 концептуално нови части, където от процесно-ориентирана тя е трансформирана в предоставяща ценности.



фигура 2: Модел на ITIL v2

Поуки и уроци.

От историята на ITIL могат да се направят много полезни изводи в поне няколко направления - за необходимостта от развитие, за ползата от далновидност на ръководството и др.

Поуки за правителството:

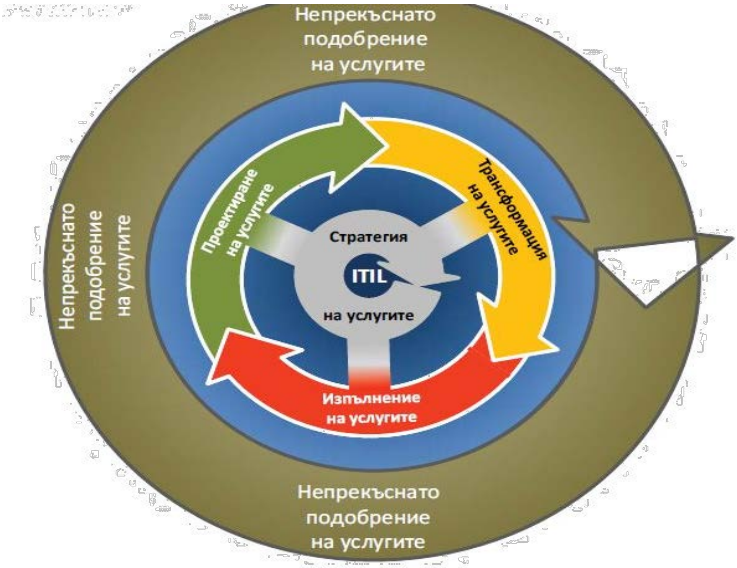
Публичния сектор може да се поучи от частния сектор и в това няма нищо непрестижно, а партньорството може да е изгодно и за двете страни.

Отговорното управление на бюджета и ресурсите изисква систематичност и високо ниво на постоянен контрол, за целите на който трябва да се разчита на обективен, прозрачен и проследим модел на управление.

Информационните технологии са в основата на управлението на всеки съвременен процес - от изпълнението на поставена профилирана задача, до вземането на информирано решение по стратегически инициативи.

Далновидността и подкрепата на държавата за натрупване на експлицитни знания позволява със сравнително малко но фокусирани средства да се постигнат полезни за цялата общественост качествени нови знания.

Оптималното управление е свързано с ефективност на дейностите и с баланс между вътрешните и външни интереси, а успехът със силно и зряло държавническо управление.



фигура 3: Модел на ITIL v2

Поуки за бизнеса:

Насърчаването на служителите в търсене, разработване и прилагане на добри практики, е полезно, тъй като може да доведе до създаване на качествено различие и репозициониране на компанията както спрямо останалите конкуренти в сегмента, така и в отношенията й с правителствените институции.

Дългосрочната печалба е зависима не от доминиращата роля на монополист, а от тази на надежден партньор, спазващ законите и етичните норми на професията.

Бизнесът има възможностите, а правителството потенциала да утвърди масовото използване на добри практики, т.е. успехът може да е резултат единствено от съвместните им действия.

Поуки за професионалиста:

Никой няма монопол над знанието. Въпреки голямото количество теории формулирането на нова модел или методика е винаги възможно,

а тяхната обективност, приложимост и полза зависят пряко от прилагането на научен подход при разработването им.

Възможностите на отделния специалист са ограничени, но работата в група позволява както съкращаване на времето, така и разделението, а от там профилирането, тясното специализиране и натрупване на експертиза по определена тема и въпрос.

Познанието на добрите практики в професионалната дисциплина, а не обвързването с конкретен доставчик, е в основата на конвертируемостта на професионалиста.

Историята на ITIL е история на съзряването на съвременната цивилизация и нейното преминаване от индустриалната към информационната ера на човечеството. Историята на ITIL също така демонстрира как факти и митове могат да бъдат съчетани, за да се постигне по-добро разбиране и успешност в прилагането на модели от добри практики. Тези модели са приложими не само в управлението на ИТ, но и за всяко подчинено на предоставянето на услуги управление както в частния, така и в публичния сектор, защото по своята същност това са информационни процеси - нито повече, нито по-малко.

Днес ITIL е стандарт, който се използва от организациите в целия свят.

На негова основа е разработен английския стандарт BSI15000, който практически без промени е утвърден като международен стандарт под названието ISO 20 000.

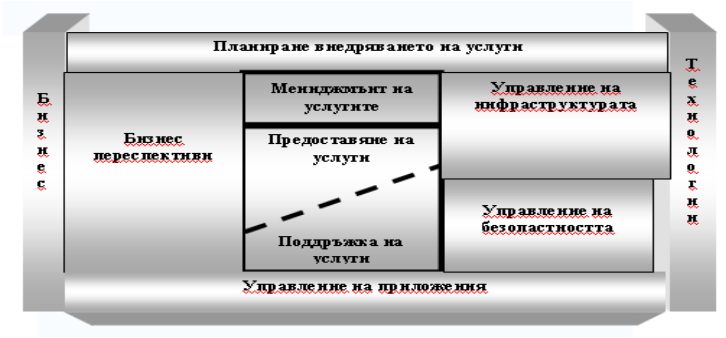
Принципи на модела ITIL \ ITSM :

-Основна задача на ИТ службата е съпровождане съществуващата ИТ-инфраструктура, а не разработка на собствени решения. Практиката показва че ИТ обслужващи бизнес процесите в организацията трябва да се базират на промишлени, т.е. покупаеми решения.

-ИТ службата обслужва бизнес подразделенията, с основна цел - удовлетворяване потребностите на бизнеса на организацията.

-Продуктът на ИТ службата не се явява информационна система, а ИТ услуга. Тези продукти се оценяват не само по предоставяната функционалност, но и по качеството на обслужване.

-Ефективността на ИТ службата се постига, само, ако на взаимодействието с бизнес подразделенията се придаде пазарен характер.



фигура 4: Принципи на модела ITIL \ ITSM

Структура.Текущата редакция на ITIL включва осем книги: Поддръжка на услуги (Service Support); Предоставяне на услуг (Service Delivery); Планиране внедряването на услуги (Planning to Implement Service Management); Управление на приложения (Application Management); Управление инфраструктурата на инофрмационно-коммуникационни технологии (ICT Infrastructure Management); Управление на безопасността (Security Management); Бизнес-перспектива (The Business Perspective); Управление конфигурациите на ПО» (Software Asset Management).

Процесен подход [5]. Моделът ITIL/ITSM описва не организационни единици и техните функции, а процеси. Практиката показма, че в съвременната ИТ служба процесния подход довежда до значително по-големи резултати от вякаква реорганизация.

Процесен модел. В процесният модел ITIL са включени следните процеси на управление на ИТ:

Йерархични нива	Процеси
Стратегическо	Планиране внедряването на услуги Planning to Implement Service Management
Тактическо	Предоставяне на услуги Service Support
Оперативно	Поддръжка на услуги Service Delivery
Изпълнително	Управление на инфраструктурата ICT Infrastructure Management

Таблица:1

Базови процеси

Най-известната част от ITIL — десет базови процеса, осигуряващи поддръжката и предоставянето на ИТ сервизите (IT Service Management или ITSM) :

Service Management (често - IT Service Management - ITSM) описва сервизния подход за предоставяне на ИТ-услуги. Включва:

Service Support – процеси за поддръжка на ИТ-услуги и повишаване качеството на тяхното предоставяне;

Service Delivery – процеси за създаване, предоставяне и управление на набор от услуги.

ICT Infrastructure Management – основа за осигуряване функционирането на техническите ресурси, на които се базират услугите.

В заключение предимства от използването на ITIL се свеждат до: Челен опит, проверен на практика от световните лидери; Ясно и разбираемо представяне качеството на услугите; Натрупване и използване на знания; Разработени методологии за оказване на услуги; Постигане на гъвкавост и мащабируемост; ИТ-инвестиции, базирани на доверие.

Преимущества от ITIL за потребителите на ИТ службите са: - Предоставянето на ИТ-услуги е по-ориентирано към потребностите на потребителите; Договарянето на качеството на услугите подобрява взаимоотношенията с потребителите; Услугите се описват точно (на езика на потребителя) и с необходимата степен на детайлизация; Прозрачно качество и цена на услугите; Ясна схема на взаимоотношения с потребителите; Подобряване ефективността от използване на ИТ.

Преимущества от ITIL за ИТ службите са свързани със: Оптимизиране на ИТ процесите, което създава основа за аутсорсинт на ИТ услуги; Изграждане на по-ефективна, рационална и ориентирана към корпоративните цели структура; Целенасочено управление на ИТ за постигане на промени; Активно участие на ИТ службата във внедряване на стандартите от серията ISO-9000.

Литература и ползвани източници:

1. Шаламанов, В., Реинженеринг и информационни технологии, Военен журнал 4/1998.
2. Шаламанов В., Реинженеринг на планирането на отбраната, Военен журнал, 1999.

3. Семерджиев, Ц., Информационна война, Софттрейд, София, 2000 г.
4. Млеченков, М. Учебно пособие –„Методика за разработване на система за информационна сигурност" – Шумен 2010.
5. Станев,С.,Х.Христов и Д.Диманова Доклад на тема: „IT – стеганографията и новите предизвикателства към системите за сигурност". В: Сборник трудове на XI международна конференция "Сигурността в Югоизточна Европа – в търсене на интелигентни решения".Секция 2, София, 2013 (под печат);
6. http://cio.bg/3053_itil__prikazki_s_pouki&ref=more;
7. http://cio.bg/1507_itil_v3;
8. http://bg.wikipedia.org/wiki/ITIL;
9. http://tuj.asenevtsi.com/Inf%20tehnologii/IT020.htm;
10. http://magazine.techwork.bg/archives/1502/all/1.

ИЗМАМИ С ЕВРОПЕЙСКИ ФОНДОВЕ- ИЗКУСТВЕНИ УСЛОВИЯ И ФУНКЦИОНАЛНА НЕСАМОСТОЯТЕЛНОСТ

Юлиян Н. Марков

ARTIFICIAL CONDITIONS AND FUNCTIONAL DEPEND

Yuliyan N. Markov

ABSTRACT: *Without prejudice to specific provisions, no payments shall be made to beneficiaries for whom it is established that they artificially created the conditions required for obtaining such payments with a view to obtaining an advantage contrary to the objectives of the support scheme.*

KEY WORDS: *anti-fraud strategy**,** prevention and detection of fraud**,** risk analyses, investigations**,** awareness-raising and training**,** sanctions**,** recovery**,** **national security system,** ethics and integrity*

Финансовият ресурс, заделен за Р. България от общия бюджет на ЕС, е значителен. Р. България може да се възползва от този ресурс за националната и регионална икономика чрез инвестиции в областта на инфраструктурата, околната среда, селското стопанство, развитието на бизнеса, обучението и иновациите. Един от ключовите фактори за успеха на Кохезионната политика на ЕС е децентрализираната система за управление на средствата и споделената отговорност между ЕК и държавата-членка. Програмите се управляват на национално и регионално ниво, така че за финансиране да се избират **най-добрите** и **най-необходимите** проекти. Много са ключовите участници във веригата на управление и контрол на европейските средства, което повишава съответно рисковете от грешки.

Ето защо, очакванията на европейските данъкоплатци към всяка държава-членка са да разполага с добър административен капацитет и адекватна законодателна и вътрешна уредба, които да гарантират законосъобразното и ефективно разходване на средствата от ЕС.

Българските бенефициенти и администрация, както тези във всяка друга държава-членка на ЕС, трябва да спазват своите задължения относно управлението на средства от ЕС.

Държавите-членки отговарят за създаването на системи за управление и контрол, които са в съответствие с изискванията на ЕС за проверка на ефективното функциониране на системите чрез одит на съответните органи, за предотвратяване, откриване и коригиране на нередности и измами. В случай на нередност или съмнения за измама, ЕК трябва да бъде информирана в съответствие с процедурите за докладване, определени в Регламент (ЕО) № 1828/2006 на Комисията.

Независимо от това дали нарушението е неумишлено или умишлено (измама), засегнатите разходи трябва да бъдат изключени от съфинансирането от бюджета на ЕС.

За да се класифицира като измама, случай със съмнение за измама трябва да се определи като „измама“ с определение на Съда (присъда).

Един от най-сериозните проблеми, както за администрацията така и за бенефициентите използващи съфинансиране от ПРСР е изискването да не се допуска финансиране на проекти и заявления за подпомагане в случай, че се установят изкуствено създадени условия с цел получаване на предимство в противоречие на целите на мярката/схемата за подпомагане. Това е така защото както в европейското така и в националното законодателство няма ясна дефиниция на понятията: **изкуствено създадени условия**; **функционална несамостоятелност**; **изкуствено разделяне на проекти**. Също така не са посочени другите изисквания, освен формално установените изкуствени условия за да бъде юридически стабилна издадена заповед за отказ от финансиране на проект или заявление за подпомагане.

Тези проблеми са довели до голям брой грешки, както от страна на ДФ „Земеделие“ при издаване на заповеди за отказ от финансиране, така и от страна на бенефициентите, които са подценили заплахата да не получат съфинансиране от ЕС и националния бюджет, което от своя страна в повечето случаи води до много сериозни финансови проблеми за бенефициентите, в повечето случаи водещи до банкрут [1].

Изложеното по-горе води до категоричния извод, че темата е особено актуална, значима и изисква сериозен и задълбочен научен анализ и изследване.

Най-сериозни проблеми във връзка с изкуствените условия и функционална несамостоятелност са установени при прилагането на мярка 312 от ПРСР и по-конкретно при изграждане на фотоволтаични централи за добив на електроенергия. При тези проекти най-ярко се открояват „изкуствените условия“ и функционалната несамостоятелност. Затова ще се спра именно на пример за такива

проекти за да изясня принципно проблема, след което ще го разясня и за други схеми и мерки за подпомагане.

Правна уредба

Правото на Съюза

Регламент (ЕО) № 1698/2005 на Съвета от 20 септември 2005 година относно подпомагане на развитието на селските райони от Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР) (ОВ Ь 277, стр. 1; Специално издание на български език 2007 г., глава 3, том 66, стр. 101) [4] определя правилата за подпомагане от този фонд. Разпоредбите за прилагането на този регламент се съдържат в Регламент № 65/2011.

По схемата за помощ по ос 3 относно качеството на живот в селските райони и разнообразяване на селската икономика член 52, буква а), подточка и) от Регламент № 1698/2005 предвижда:

„Помощи за създаване и развитие на микропредприятия с оглед насърчаване предприемачеството и създаване на благоприятна икономическа среда".

Член 4, параграф 8 от Регламент 65/2011 [3] има следното съдържание:

„Без да се засягат специфичните разпоредби, не се извършват плащания на бенефициери, за които бъде установено, че изкуствено са създали условията, необходими за получаване на такива плащания с оглед да получат облага в противоречие с целите на схемата за подпомагане“.

Българското право

В чл. 2 от Наредба № 29 от 11 август 2008 г. за условията и вида за предоставяне на безвъзмездна финансова помощ по мярка „Подкрепа за създаване и развитие на микропредприятия“ от Програмата за развитие на селските райони 2007-2013 г. (Държавен вестник бр. 76 от 29 август 2008 г.) в редакцията й от 20 юли 2010 г.[2], в сила към момента на настъпване на фактите, които се разглеждат в настоящия труд, се уточнява:

Подпомагат се проекти, които допринасят за постигане целите на мярката.

Целите на мярка 312 от ПРСР са:

1. насърчаване на растежа и създаване на нови работни места в микропредприятия за неземеделски дейности в селските райони,
2. насърчаване на предприемачеството в селските райони,
3. насърчаване развитието на интегриран туризъм в селските райони“.

Член 4, алинея 2, точка 10 от тази наредба предвижда, че не се предоставя финансова помощ за производство и продажбата на енергия от възобновяеми източници с капацитет на инсталацията над един мегават.

По силата на член 6, ал. 2 от Наредба № 29:

Финансовата помощ за проекти за производство и продажба на енергия от възобновяеми енергийни източници е в размер на 80% от одобрените разходи, но не повече от левовата равностойност на 200000 евро.

Член 7, параграф 2 от Наредба № 29 има следното съдържание:

„Финансовата помощ не се предоставя на кандидати/ползватели на помощта, за които бъде установена функционална несамостоятелност и/или изкуствено създаване на условия, необходими за получаване на помощ, с цел осъществяване на предимство в противоречие с целите на мярката“.

В точки 30 и 31 от допълнителните разпоредби от Наредба № 29 се уточнява:

„30. ‚Изкуствено създадени условия" е всяко установено условие по смисъла на чл. 4, т. 8 от Регламент № 65/2011.

31. „Функционална несамостоятелност" е изкуствено разделяне на производствени и технологични процеси в различни проекти или установяване ползване на обща инфраструктура, финансирана от ПРСР (Програма за развитие на селските райони), с цел осъществяване на предимство в противоречие с целите на мярката по ПРСР".

Изкуствени условия

Дружество „АЛФА“ подава до ДФЗ-РА заявление за финансиране на проект за изграждане на фотоволтаична централа по мярка 312 „Подкрепа за създаване и развитие на микропредприятие" от Програмата за развитие на селските райони.

Г-н Христов е упълномощен да представлява „АЛФА“ ЕООД, а едноличен собственик и управител на това дружество е г-жа Христова. **Тези две лица са в брак.**

Към подаденото от „АЛФА“ ЕООД заявление за финансиране са приложени, **първо**, договор за наем на земя между „АЛФА“ ЕООД“ и г-н Христов и г-жа Христова, собственици на този имот, върху който трябва да се изгради фотоволтаичната централа. **Второ**, към заявлението е приложен акт за сключен договор за продажба на вещно **право на строеж** между **„БЕТА" ЕООД**, чийто едноличен собственик и управител е **г-н Христов**, и **„АЛФА“ ЕООД.**

При разглеждане на заявлението на **„АЛФА“ ЕООД**, ДФЗ-РА установява, че съответният недвижим имот се намира **между други два**

имота, за които са поискани помощи по същата програма за два проекта, идентични с този на „АЛФА“ ЕООД. Г-н Христов и г-жа Христова са **собственици на тези два други имота**. **Правото на строеж върху тях също е продадено от „БЕТА" ЕООД.**

Изпълнението на трите проекта е поверено на едно и също дружество — „3 Д" ООД.

С оглед на тези обстоятелства и на факта, че в трите проекта за фотоволтаична централа се сочи **едно и също седалище**, с решение от 9 септември 2011 г. изпълнителният директор на ДФЗ-РА отказва съфинансиране на инвестиционния проект на **„АЛФА“ ЕООД** поради установена функционална несамостоятелност и/или изкуствено създаване на условия, необходими за получаване на помощта, с цел осъществяване на предимство в противоречие с целите на мярката.

Изпълнителният директор на ДФЗ-РА приема по-конкретно че **с проекта на „АЛФА“ ЕООД се цели заобикаляне на ограничението за максимално финансиране за отделен проект, а именно равностойността на 200 000 евровбългарски лева.**

„АЛФА“ ЕООД подава жалба срещу отказа на ДФЗ-РА до Административен съд София-град.

Тази юрисдикция смята, че решението по делото, с което е сезирана, зависи от тълкуването на понятието „изкуствено създаване на условия" по смисъла на член 4, параграф 8 от Регламент № 65/2011.

Тя подчертава, че българската администрация тълкува понятието в **широк обхват**, като се основава на **правната свързаност между субектите**, **идентичността на проектите** и **еднаквите седалища** на съответните дружества.

Практиката на ВАС е ориентирана към тълкуване на понятието „изкуствено създаване на условия" в по-тесен смисъл. Според тази практика простото наличие на общи факти не е достатъчно да обоснове съществуването на изкуствено създадени условия. Всъщност ВАС изисква ДФЗ-РА да докаже **умишлена координация** между юридическите лица и/или трето лице с цел осъществяване на предимство **в противоречие с целите на мярката.**

При така установената фактическа обстановка се налагат следните:

Основни въпроси

1) Как следва да се тълкува понятието „изкуствено създаване на условия" в светлината на разпоредбата на член 4, параграф 8 от Регламент 65/2011?

2) Член 4, параграф 8 от Регламент 65/2011, следва ли да се тълкува в смисъл, че се противопоставя на член 7, алинея 2 от Наредба

№ 29, според която финансова помощ не се предоставя на кандидати/ползватели на помощта, за които бъде установено изкуствено създаване на условия, необходими за получаване на помощта, с цел осъществяване на предимство в противоречие с целите на мярката?

3) Член 4, параграф 8 от Регламент 65/2011 следва ли да се тълкува в смисъл, че се противопоставя на съдебната практика в Република България, според която изкуствено създаване на условия за получаване на облага в противоречие с целите на мярката, е налице в хипотезите на правна свързаност между заявителите?

4) Използването от различни кандидати - самостоятелни правни субекти на съседни самостоятелни поземлени имоти, които преди подаването на заявленията са представлявали един поземлен имот, и установена фактическа свързаност, като например едни и същи пълномощници, оференти, изпълнители, седалища и адреси за кореспонденция на кандидатите, представляват ли „изкуствено създаване на условия"?

5) Следва ли да бъде установена умишлена координация между субектите кандидати и/или третото лице спрямо тях, с цел осъществяване на предимство за един конкретен субект кандидат?

6) В какво се изразява облагата по смисъла на член 4, параграф 8 от Регламент 65/2011, в частност следва ли да се изразява в създаването на няколко по-малки инвестиционни предложения, с цел един конкретен кандидат да получи по всички от тях, финансиране в максималния размер от 200 000 евро, макар и тези предложения да са формално подадени от различни кандидати?

7) Член 4, параграф 8 от Регламент 65/2011 следва ли да се тълкува в смисъл, че се противопоставя на съдебната практика в Република България, според която фактическият състав на нормата включва кумулативно наличието на три условия: [първо] наличие на функционална несамостоятелност и/или изкуствено създаване на условия, необходими за получаване на помощта, [второ] горното да е с цел осъществяване на предимство и [трето] това да е в противоречие с целите на мярката?".

Предварителни бележки

Повдигнатите въпроси се отнасят, от една страна, до условията за прилагане на член 4, параграф 8 от Регламент № 65/2011, а от друга страна, до начина, по който тази разпоредба се тълкува в българското законодателство и българската съдебна практика.

Поради това първо следва да се разгледат заедно първи и от четвърти до седми въпрос, а след това да се отговори на втория и на третия въпрос.

По първи и от четвърти до седми въпрос

С тези въпроси по същество се иска да се установи, какви са условията за прилагане на член 4, параграф 8 от Регламент №65/2011.

В самото начало следва да се отбележи, че ДФ „Земеделие“ отказва да одобри представения от „АЛФА“ ЕООД инвестиционен проект, с който то кандидатства за помощи за създаване и развитие на микропредприятия с оглед насърчаване предприемачеството и създаване на благоприятна икономическа среда, тъй като това дружество искало да злоупотреби с помощ, отпусната на основание на схема за подпомагане от ЕЗФРСР.

Съгласно постоянната съдебна практика обаче приложното поле на регламентите на ЕС не може да бъде разширено до такава степен, че да обхване и **злоупотребите** на икономическите оператори.

Инвестиционният проект на „АЛФА“ ЕООД формално отговаря на всички условия за кандидатстване за помощ за създаване и развитие на микропредприятия по силата на член 52, буква а), подточка ii) от Регламент № 1698/2005, както и на националното законодателство.

При тези обстоятелства, съгласно установената съдебна практика в Р. България за да се докаже наличие на злоупотреба от страна на потенциален бенефициер на такава помощ, от една страна, е необходима **съвкупност от обективни обстоятелства, от които следва, че въпреки формалното спазване на предвидените в съответната правна уредба условия целта, преследвана с тази правна уредба, не е постигната**, и **от друга страна, е необходим субективен елемент, изразяващ се в намерението да се получи предимство от правната уредба на ЕС, като изкуствено се създават условията, необходими за неговото получаване.**

Наличието на тези два елемента следва да се установи от администрацията, като доказването трябва да е съгласно правилата на националното право, стига да не се накърнява действието на правото на Съюза.

Именно в този контекст следва да се тълкуват понятията „изкуствено създаване" на условията, необходими за получаване на плащане, и „облага в противоречие с целите" по смисъла на член 4, параграф 8 от Регламент №65/2011.

Първо, когато става въпрос за **обективния елемент**, следва да се припомни, че по силата на съображение 46 от Регламент № 1698/2005 целта на схемата за подпомагане на селските райони от ЕЗФРСР по-

конкретно е да допринесе „за разнообразяване на селскостопанските дейности към неселскостопански и за развитие на неселскостопанските отрасли, за насърчаване на трудовата заетост, … и инвестиции за по-голяма привлекателност на селските райони с цел обръщане на тенденциите за икономически и социален спад и обезлюдяване на районите".

По-конкретно, целта на член 52 от Регламент № 1698/2005, въз основа, на който се иска подпомагане за разглеждания инвестиционен проект, е да се подкрепят мерките за разнообразяване на селската икономика и в него са предвидени помощите за създаване и развитие на микропредприятия с оглед насърчаване предприемачеството и създаване на благоприятна икономическа среда.

В този контекст Наредба № 29 предписва ограничения във връзка с финансирането от ЕЗФРСР на инвестиционни проекти, свързани с производство и доставка на енергия от възстановяеми източници, които са от категорията, подпомагана по посочените в член 52 от Регламент № 1698/2005 мерки. Така, от една страна, максималният размер на финансирането от ЕЗФРСР е ограничен до 200 000 EUR на бенефициер. От друга страна, финансирането е единствено за електроцентрали с максимален капацитет от 1 мегават.

От решението за отказ се установява, че е отказано финансиране от ЕЗФРСР за проекта фотоволтаична централа на „АЛФА“ ЕООД, тъй като ДФ „Земеделие“ приема, с оглед на обстоятелствата, че това дружество имало намерение да заобиколи предвидените в националното законодателство ограничения, като се е споразумяло с трети лица, самите те кандидатстващи за разглежданата помощ по схемата за подпомагане от ЕЗФРСР, изкуствено да разделят **един-единствен проект на три по-малки проекта.**

Само по себе си това обстоятелство обаче не позволява да се изключи, че представеният от „АЛФА“ ЕООД проект ще допринесе за постигане на посочените в Регламент № 1698/2005 цели.

В това отношение, ако упрекваме „АЛФА“ ЕООД, че иска да заобиколи ограниченията във връзка с размера на допустимите проекти и с максималния размер на помощта за един бенефициер, трябва да проверим дали това желание за заобикаляне на ограниченията води до невъзможност за постигане на посочените в чл. 52, буква а), подточка ii) от Регламент № 1698/2005 цели.

При това положение би трябвало по-конкретно да вземем предвид определението за микропредприятие, чието създаване и развитие са цел на помощта, посочена в чл. 52 от Регламент № 1698/2005, което определение може да се изведе от член 2, параграф 3

от приложението към Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. относно определянето на микропредприятията, малките и средните предприятия (ОВ L 124, стр. 36).

Второ, във връзка със **субективния елемент** трябва да определим действителното съдържание и значение на спорното заявление за финансиране.

Когато определяме това съдържание и значение, сред фактическите обстоятелства, които можем да вземем предвид, за да установим, че необходимите условия за получаване на плащане от ЕЗФРСР са изкуствено създадени, са **връзките от правно, икономическо и/или лично естество между лицата**, участващи в съответната операция по инвестиране.

Наличието на този субективен елемент може да бъде потвърдено и ако се докаже тайно съглашение, което може да приеме формата на умишлена координация между различни инвеститори, кандидатстващи за помощ по схема за подпомагане от ЕЗФРСР, особено когато инвестиционните проекти са еднакви и между тях съществува географска, икономическа, правна и/или персонална връзка.

Трябва да приемем обаче, че не може да бъде отказано финансиране на проект, когато съответните инвестиции могат да се обосноват по друг начин, а не само с плащането по схемата за подпомагане по ЕЗФРСР.

Поради това член 4, параграф 8 от Регламент 65/2011 трябва да се тълкува в смисъл, че условията за прилагането му имат обективен и субективен елемент. Във връзка с обективния елемент трябва да разглеждаме обективните обстоятелства в конкретния случай, въз основа, на които може да се направи извод, че целта, преследвана със схемата за подпомагане от ЕЗФРСР, няма да може да бъде постигната. Във връзка със субективния елемент трябва да разглеждаме обективните доказателства, които позволяват да се направи изводът, че с изкуственото създаване на необходимите условия за получаване на плащане въз основа на схемата за подпомагане от ЕЗФРСР, кандидатът за това плащане е смятал единствено да получи облага в противоречие с целите на тази схема. В това отношение можем да се обосновем не само с обстоятелства като правните, икономическите и/или личните връзки между лицата, участващи в сходните инвестиционни проекти, но и на улики, свидетелстващи за наличието на умишлена координация между тези лица.

По втория и третия въпрос

С втория и третия въпрос по същество искаме да се установи дали член 4, параграф 8 от Регламент №65/2011 трябва да се тълкува в

смисъл, че не допуска, от една страна, национална правна уредба, съгласно която финансова помощ на основание на схема за подпомагане от ЕЗФРСР не се изплаща при функционална несамостоятелност на инвестиционния проект, и от друга страна, установената съдебна практика, съгласно която изкуствено създаване на условия за получаване на облага е налице при правна свързаност между кандидатите за такава финансова помощ.

Както посочих по-горе, за прилагането на член 4, параграф 8 от Регламент № 65/2011 е необходимо да са налице както обективен, така и субективен елемент.

При това положение, независимо че сме установили обстоятелства във връзка със съществуването на правна свързаност между кандидатите за помощ, дори функционална несамостоятелност на различните разглеждани инвестиционни проекти, които наистина са белези, въз основа на които може да се приеме, че необходимите условия за получаване на плащания по смисъла на член 4, параграф 8 от Регламент № 65/2011 са изкуствено създадени, това все пак не изключва необходимостта тази преценка да се извърши с оглед на всички обстоятелства в конкретния случай.

По-конкретно, трябва да се уверим, че от всички обективни елементи по разглежадния случай се установява, че основната цел при избора на условията, свързани с разглежданите инвестиционни проекти, е плащането на помощите въз основа на схемата за подпомагане, без да е налице никаква друга причина, свързана с целите на посочената схема.

В заключение, подкрепени и от Решение по Дело C-434/12 на Съда на Европейския съюз от 12.09.2013 г. [5] можем да обобщим:

Член 4, параграф 8 от Регламент (ЕС) № 65/2011 на Комисията от 27 януари 2011 година за определяне на подробни правила за прилагане на Регламент (ЕО) № 1698/2005 на Съвета по отношение на прилагането на процедури за контрол, както и кръстосано спазване по отношение на мерките за подпомагане на развитието на селските райони, трябва да се тълкува в смисъл, че условията за прилагането му имат обективен и субективен елемент. Във връзка с обективния елемент трябва да разглеждаме обективните обстоятелства в конкретния случай, въз основа, на които може да се направи извод, че целта, преследвана със схемата за подпомагане от Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР), няма да може да бъде постигната. Във връзка със субективния елемент трябва да разглеждаме всички обективни доказателства, които позволяват да се направи изводът, че с изкуственото създаване на необходимите условия за получаване на плащане въз основа на схемата за подпомагане от

ЕЗФРСР кандидатът за това плащане е смятал единствено да получи по-голяма облага от максимално допустимата, в противоречие с целите на тази схема. В това отношение можем да се обосновем не само с обстоятелства като правните, икономическите и/или личните връзки между лицата, участващи в сходните инвестиционни проекти, но и на улики, свидетелстващи за наличието на умишлена координация между тези лица.

Член 4, параграф 8 от Регламент № 65/2011 трябва да се тълкува в смисъл, че не допуска да бъде отказано плащане по схемата за подпомагане от Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР) единствено поради това че инвестиционен проект, който кандидатства за подпомагане по тази схема, е функционално несамостоятелен или че съществува правна свързаност между кандидатите за такова подпомагане, при това без да се вземат предвид другите елементи по конкретния случай.

На основание на гореизложените съображения можем да изведем следните

Изводи:

1. Липсата на ясна дефиниция в Европейското и националното законодателство на понятията изкуствено създадени условия, функционална несамостоятелност и изкуствено разделяне на проекти води до противоречиво тълкуване от страна на ДФ „Земеделие“, бенефициентите и съдебните органи.

2. Непълното и неточно формулиране на целите на отделните мерки и схеми за подпомагане от Програмата за развитие на селските райони, както и по другите програми, схеми и мерки, води до изключително трудно доказване на противоречието с тези цели, а от там и на изкуствено създадени условия.

3. Субективната преценка на обективните доказателства за умишлено договаряне и координация между бенефициентите с цел получаване на финансова помощ по-голяма от максимално допустимата по мярката, без да е установена стабилна административна и съдебна практика създава условия за противоречиво тълкуване. Това от своя страна позволява да се предприемат противоречиви действия и/или бездействия, които могат да доведат до: грешки и корупционни действия от страна на държавните органи и до измами от страна на бенефициентите.

4. Изкуственото създаване на условия е измама по смисъла на определението за измама на ЕС, но в българския НК няма разпоредба, която да съответства на този деяния. Единствено чл. 321 би могъл да се обсъжда, но до момента ДФ „Земеделие“ няма информация за

образувано досъдебно производство по този текст на основание изкуствено създадени условия.

5. Изкуственото създаване на условия с цел получаване на финансова помощ по-голяма от максимално допустимата е сериозна и опасна заплаха за националната сигурност. Това е така, защото при някои от установените случаи лицата, които ръководят и координират действията на групата се опитват да получат 10 и повече пъти максимално допустимата помощ, която примерно за 312 мярка е 200 000 евро.

6. Предвид гореизложените слабости и пропуски, организирани престъпни групировки са се насочили и се опитват да използват програми, схеми и мерки съфинансирани от ЕС и националния бюджет от една страна за извличане на големи и лесни печалби, а от друга за „изпиране на пари“ придобити от други престъпни дейности.

Действия, които трябва да се предприемат:

1. Ясно дефиниране на понятията изкуствено създадени условия, функционална несамостоятелност и изкуствено разделяне на проекти в националното законодателство.

2. При изготвяне на новите програми, схеми и мерки за подпомагане от ЕС за следващия програмен период 2014-2020 г. целите им да се формулират адекватно, ясно и пълно.

3. Отправяне на искане за изготвяне и постановяване на тълтувателно решение на Върховния касационен съд и указания на Главния прокурор на Р. България по отношение на изкуствено създадени условия.

4. Провеждане на специализирани обучения на служителите от държавната администрация и бенефициентите по отношение на изкуствено създадени условия с цел избягване и недопускане на грешки от двете страни.

5. Популяризиране на влезли в сила решения на съда и постановления на прокуратурата по случай с изкуствено създадени условия.

Литература:

1. Христов, Х. Доклад на тема: „Ролята на организацията и управлението на оперативното противодействие за разкриване и неутрализиране на посегателства срещу фирмената сигурност”. Научна конференция „Защита на информацията –състояние и перспективи”, проведена в НВУ „В.Левски” - Факултет „Артилерия, ПВО и КИС”, на 07-08.06.2012год. –докладът е публикуван в сборник научни трудове в направление „Държава и сигурност”.

2. НАРЕДБА № 29 от 11.08.2008 г. за условията и реда за предоставяне на безвъзмездна финансова помощ по мярка "Подкрепа за създаване и развитие на микропредприятия" от Програмата за развитие на селските райони за периода 2007 - 2013 г.
3. Регламент (ЕС) № 65/2011 на Комисията от 27 януари 2011 година за определяне на подробни правила за прилагане на Регламент (ЕО) № 1698/2005 на Съвета- стр.2 позиция [4]
4. Регламент (ЕО) № 1698/2005 на Съвета от 20 септември 2005 година относно подпомагане на развитието на селските райони от Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР)
5. Решение по Дело С-434/12 на Съда на Европейския съюз от 12.09.2013 г.

ПРОЦЕС НА ДЕФИНИРАНЕ НА ЧУВСТВИТЕЛНАТА ИНФОРМАЦИЯ, КАТО ЕЛЕМЕНТ ОТ НАЦИОНАЛНАТА СИСТЕМАТА ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА

Стоян Г. Тонев

PROCESS OF DEFINING THE SENSITIVE INFORMATION AS AN ELEMENT OF THE NATIONAL SYSTEM FOR PROTECTION OF THE INFORMATION

Stoyan G. Tonev

ABSTRACT: *The management of the sensitive information are contemporary approach whose application in the sphere of the security allow realization to complex counteraction to multiform and interdependence and interlinks sources to risk and threat, which are factor for reliability prevention to negative influence toward National security to Republic of Bulgaria.*

KEY WORDS: *Information security; Politics safety; Sensitive information*

II.

През последните години, с новите модели на общуване, активно се намесиха средствата за масова комуникация и обхванаха три четвърти от населението на Земята и така съдържанието и същността на обществения живот и развитието на информационно общество доведоха

до въвеждането и използването на нови понятия като „свързано общество" и „чувствителна информация".

Основното, което е характерно за свързаното общество е, че то разкрива нов вид връзки между хората и между институциите – връзки, базирани на споделянето на чувствителна информация.

Чувствителната информация е стратегически актив[2]. Както всички други организационни активи, този актив е ценност и, следователно, трябва да бъде добре защитен. Това е особено важно в днешната сложна и динамично променяща се среда, в която чувствителната информация е изложена на множество разнообразни заплахи.Чувствителната информация съществува в много форми по вид носители, предаване и обменена. Обмена и промените, свързани с интереса към чувствителна информация стават много бързо и това, което вчера е било писък в технологичната мода и представлява интерес, утре може да бъде „детронирано" и да влезе в музея.

Каквато и форма да приеме чувствителната информация, тя винаги трябва да бъде защитена от деструктивно въздействие. [3]

Посредник в общуването между хората станаха комуникационните и компютърните средствата за мобилна, интернет връзка и др. Отношенията, които се създават зараждат и развиват ново общество, с гъвкави и динамични общувания, ограничени във времето, пространството и начина на изразяване. В потвърждение е изводът, на агенцията за маркетингови и социални проучвания „Алфа Рисърч" през септември 2012 г, че все по-ниските цени на комуникации, в съчетание с растяща популярност на социалните мрежи, ни изправя пред истински бум на мобилен пренос на данни в страната. [4]

Промяната в механизмите на обмен на чувствителна информация трансформира традиционния тип общество в общество от нов тип, с по-голямо разнообразие във взаимоотношенията и нов начин на създаване и натрупване на богатство. [5]

Като резултат от увеличения брой връзки в заобикалящата ни среда за сигурност, [6] нараства все повече необходимостта и от по-точни критерии за персонификацията на лицата, с които се обменя чувствителна информация. През последните години използването на комуникациите, компютрите претърпяха драстична промяна. Гръбнакът на информационното общество-интернет, е емблематична рожба на конвергенцията[7].

Това гарантира още по-динамично развитие на информационните и комуникационните технологии през следващите няколко години, което ясно се откроява от „Digital Agenda", водеща инициатива в рамките на стратегията „Европа 2020" [8]. Съвременните технологии направиха възможно свързването чрез Интернет на компютри от всяка точка на земното кълбо в обща мрежа, бъдещи и анонимни[9] мрежи, носещи със себе си проблеми, свързани с адресното пространство.

В свързаното общество хората, познанието, връзките и информацията са в непрекъснат обмен, което позволява по-бързо развитие и динамика провокираща креативността и тя тласка и изисква иновации, неспирна трансформация и по-висока ефективност[10]. Чрез новите технологии географските и културните бариери се преодоляват лесно и дори падат, а комуникациите, широколентовия интернет и „облакът" показват нови хоризонти на развитие.

Анализът на съвременните социални отношения показва, че с нарастване мащабите на анонимно рутиране [11] на чувствителна информация както между отделните структури на дадена социална организация, така и между партньорите в дадена сфера на обществена активност.

Дефицитът на понятието „чувствителна информация” се съдържа под различна форма в българското законодателство, както следва и разпространението му е забранено и ограничено със закони, заповеди или други административни разпореждания:

- Закона за статистиката[12];
- Закона за съдебната власт[13];
- Закона за кредитните институции[14];
- Закона за защита на личните данни;
- Закона за здравето;
- Наказателния кодекс;
- Наказателно-процесуалния кодекс[15];
- Семейния кодекс;
- Закона за адвокатурата[16];
- Закона за достъпа до обществена информация;
- Данъчно-осигурителния и процесуален кодекс;
- Закона за защита на конкуренцията;
- Закона за експортния контрол;
- Закона за електронните съобщения;
- Закона за специалните разузнавателни средства;
- Непубличните регистри, определени от законодателя;
- Географската информационна система (ГИС);
- Правно-информационната система;

- Шенгенската информационна система.ШИС (SIS);
- ЕСГРАОН – Единната система за гражданска регистрация и административно обслужване на населението.

Всички тези закони са подчинени на принципите, залегнали в Конституцията на Р. България и по-точно в чл. 34, ал. 1 „правото за свободна и тайна кореспонденция и на други съобщения”.

Чувствителната информация и поддържащите процеси, системи и мрежи са важни активи на всички организационни структури.

Много информационни системи не са проектирани да осигурят сигурност на чувствителната информация. Сигурността, която може да се постигне чрез технически средства, е ограничена и трябва да бъде поддържана чрез съответни управленски решения и установени процедури.

Определянето на това кои видове контрол трябва да се използват, изисква грижливо и детайлно планиране и отчитане на характеристиките на системата за сигурност.

Управлението на сигурността на чувствителната информация изисква задължително участие на всички служители в организационната единица. То може да изисква участие на акционерите, доставчиците, трети страни, контрагенти. Може, също така, да бъде необходим съвет на експерт от външна организационна единица, предвид спецификата на чувствителната информация, ползвана в публичния сектор[17]

От гледна точка на използваните предмети за записване и пренасяне на информация, включително негласно, те се произвеждат, държат и търгуват свободно. Те са част от бита на гражданите, без

формалности, тъй като придобиването им не е подчинено на специален или разрешителен режим.

Необходимо е да се изясни, могат ли те да послужат за извършване на престъпление по българското законодателство във връзка с чл. 339а от НК.

По принцип, неприкосновеността на личния живот може да се засегне негласно и с такива общодостъпни средства, като се събере съответната информация.

Необходимо е българското законодателство да претърпи изменение в насока: „Който противозаконно използва техническо средство за негласно събиране на информация, свързана с неприкосновеността на физически и юридически лица, на жилището, на кореспонденцията, на собствеността и на други съобщения, носи наказателна отговорност", защото това е чувствителна информация. В потвърждение на това, при законно използване на специални разузнавателни средства (СРС) в чл. 33 от закона на Специалните разузнавателни средства (ЗСРС) законодателят е предвидил регламент, че на лицата, на които са станали известни факти и сведения за специални разузнавателни средства, използвани при условията и реда на закона за СРС, както и събрани данни, са длъжни да не ги разпространяват. [18]

Възможно е да се изведе изводът, че използването и прилагането на СРС представлява дейност, с която се реализира държавна принуда по отношение на конкретни правни субекти. Целта е предотвратяване, разкриване и доказване на тежки престъпления, което обуславя социалната ценност на принудата и нейната достъпност, във връзка със конституционните права и свободи на гражданите, във

връзка с чл. 34, ал. 1 от КРБ[19]. В тези случаи информацията не е класифицирана, но попада в категорията „чувствителна информация".

Интерес представлява изпълнителното деяние под формата на „използване" на техническо средство без надлежно разрешение и събраната информация, съгласно закона на Специалните разузнавателни средства.

Необходимо е българското законодателство да разграничи ограниченията, свързани със събиране на информация с разрешения, както е по чл. 13 от ЗСРС и събирането на такава от частни физически и юридически лица. В потвърждение на нуждата от това, са материалите по досъдебно производство под № 759/2004 г. на Окръжна следствена служба – гр. Русе по водено наказателно производство срещу румънски гражданин, използвал скрита видеокамера за негласно видео и звукозаписване на чувствителна информация от критичната инфраструктура на Р. България. Във връзка с подобни казуси, се налага експертното становище, [20] че събирането на информация от частни лица с използване на технически средства трябва да се отдели в самостоятелен състав и то има място в глава 3 от НК, наред с престъпленията, свързани с нарушаване неприкосновеността на жилище, помещение, превозно средство, кореспонденция и е чувствителна информация, за която не е определен ред за защитеност.

Непрекъсваемостта и неприкосновеността на кореспонденцията при използване на комуникациите трябва да се осигурява и от правораздавателната система с предвиждане на съответни наказателни мярка и за всеки, който противозаконно отвори, подправи, скрие или унищожи или вземе чужда кореспонденция, без значение на материалния носител, с цел да узнае или промени нейното съдържание

или да узнае неадресирано до него съобщение и т.н., което е чувствителна информация.

В българската нормативна база са налице характеристики за забранен обмен на чувствителна информация между определени субекти на обществото. В потвърждение на това са разпоредбите на Комисията за защита на конкуренцията[21] (КЗК), която на основание чл. 60, ал. 1, т. 24 от Закона за защита на конкуренцията (ЗЗК) регламентира, че „Информацията, чийто обмен между конкуренти може да се счита за забранен, най-често се обозначава с понятието „стратегическа" или „чувствителна" търговска информация".

В становище Българската Народна Банка (БНБ) заявяват, че в Централния кредитен регистър (ЦКР) се съхранява „изключително чувствителна [22]по своя характер информация" и определя реда за ползването й.

Дефинирането на понятието „чувствителна информация" е осъзнато и използвано от изпълнителната власт, като в потвърждение на това е Заповед [23]на заместник министър-председателя на Р. България, който създава междуведомствена работна група за преглед и оценка на нормативната уредба, регламентираща взаимодействието между службите за сигурност и обществения ред в Р. България при „нематериален" трансфер на технологии – понятие, използвано в ЕС, „неосезаем" трансфер на технологии – понятие, използвано в САЩ и „неосъзнат трансфер" на технологии, използвано в Р. България.

След анализ и съпоставка на действащото законодателство на Р. България и Европейския съюз, междуведомствената работна група е изготвила доклад с предложени дейности, засягащи БАН и висшите училища за определяне необходимостта от дефиниране на понятието

„чувствителни информации", дейности, процедури, както и научни области, в които се обучават студенти/докторанти от рискови държави и нуждата от оптимизиране на проблема със системата за издаване на визи за такива.

Горното потвърждава необходимостта от дефиниране на чувствителната информация в Р. България и необходимостта от изясняване и уеднаквяване на обмена на чувствителна информация между конкуренти, като форма на хоризонтално сътрудничество между конкуренти и икономически ползи.

Обменът на информация между субекти, които оперират на едно и също ниво от веригата на производство, дистрибуция и контрол на определени продукти (стоки или услуги), формиращи самостоятелен пазар, представлява форма на хоризонтално сътрудничество между конкуренти в публичния сектор.

Обменът на информация може да създаде предпоставки за адаптиране на предлагането на стоки или услуги, спрямо търсенето, както и за подобряване на стопанската ефективност на ОЕ, опериращи на съответния пазар, за повишаване на информираността на новонавлизащите субекти и на инвеститорите, които желаят да се установят на пазара в публичния сектор[24].

Обменът на информация може, също така, да бъде от полза и за потребителите, посредством намаляване на разходите им за търсене, което по директен начин води до повишаване на тяхното благосъстояние. Обменът на пазарна информация, който повишава прозрачността на пазара, е полезен за ефективната конкуренция, доколкото не води до създаване на условия за съгласувано или координирано пазарно поведение на участниците на пазара.

Съществуват определени видове информация, която ако бъде обменена и достъпна за участниците на пазара, би довела до превишаване на благоприятното равнище на прозрачност на пазара и до ограничаване на конкуренцията между предприятията, които участват на пазара като конкуренти. В този смисъл, обменът на информация не трябва да води до намаляване на стимулите за предприятията да следват конкурентно поведение на съответния пазар и да премахва или да намалява значително стопанския риск, произтичащ от неизвестността, относно актуалното или бъдещото пазарно поведение на конкурентите и планираните от тях маркетингови стратегии.

Понятието за „обмен" на чувствителна информация, по своята конкурентно правна същност, представлява форма на хоризонтално сътрудничество между конкурентни обекти и субекти в публичния сектор, чрез което те си предоставят, пряко или непряко, едностранно или двустранно, минали, текущи или бъдещи данни, относно съществените икономически параметри на своята стопанска дейност, а именно:

- *ценови параметри* (Счетоводен отчет, група 21 от Закона за счетоводството, [25] прилагани цени, механизъм на ценообразуване, себестойност на предлаганите продукти, търговски отстъпки, структура на разходите за производство и реализация и др.) или
- *неценови параметри* (маркетингови стратегии, рекламни кампании, промоции, намерения за позициониране на нови продукти, навлизане на нови пазари, отношения с други предприятия и др.).

III. Понятието за обмен на чувствителна информация „*между конкуренти*” представлява, преди всичко, интерес от гледна точка на правото на конкурентите да обменят информация между ОЕ.

„Предприятие” е всяко физическо, юридическо лице или гражданско дружество (неперсонифицирано образувание), което извършва стопанска дейност, независимо от правната и организационната си форма[26]. Съгласно константната практика на ЕК и Съда на ЕС (СЕС) „предприятие” е всяко образувание, ангажирано в осъществяване на стопанска дейност, независимо от правния му статут и начина, по който се финансира. В този смисъл, предприятието се дефинира чрез своя функционален характер, който изисква съответното образувание да извършва „стопанска дейност”.

„Стопанска дейност” е дейността на предприятия, резултатите от която са предназначени за размяна на пазара[27]. Съгласно правото на ЕС в областта на конкуренцията, „стопанска” е всяка дейност по предлагане на стоки или услуги на пазара. Тази дейност се осъществява по такъв начин, че по принцип да е от естество в публичния сектор, водещо до реализиране на печалба в частен интерес, без обаче да е необходимо такава печалба да е реално реализирана.

Дефиниране на понятието „чувствителна информация” е осъзнато и използвано от съдебната власт, като в потвърждение на това са дела на Върховния административен съд [28]

Обобщавайки гореизложеното, може да се направи извода за необходимостта от дефинирането й, както и даване на примерно научно/работно определение за чувствителна информация.

Чувствителната информация е вид жизненоважен актив за физическите и юридически лица и субекти със стопанска и нестопанска цел, който актив трябва да бъде адекватно управляван, умело защитен, с

цел недопускане накърняване на личното достойнство, финансово ощетяване на юридическите и физически субекти и гарантиране непрекъснатост на работния процес на организационната единица и конкурентно начало.

Очевидно, предвидените в нашето законодателство правно-фактически основания за ограничаване на основите права и целите, които законът предвижда чрез тях, съответстват на тези, посочени в Европейската конвенция за защита на правата на човека и основните свободи, в решения на Европейския съд за правата на човека и други международни актове[29].

Налага се изводът, че държавната има ангажименти към дефиниране на чувствителната информация в едно демократично общество, в интерес на националната сигурност и икономическото благоденствие на Р. България

Гореизложеното налага извода, че в публичния сектор се използва терминът „чувствителна информация", обменя се между различни субекти на обществото и, въпреки липсата на дефинирано понятие и маркиране на чувствителната информация, има изисквания за нейния достъп и разпространение.

Литература:

1.Информация – всяко знание, което може да бъде съобщено под каквато и да е форма, ДВ.103/2004 г.

2. Актив (осезаем и неосезаем) – всичко, ценно със стойност за организацията (ISO/IEC 13335-1:2004).

3. Виж.чл.4, ал.1, т.10 от Закона за Държавна Агенция Национална Сигурност (ЗДАНС)

4. Проучване на „Алфа Рисърч” през септември 2012 г., отразено в сп. Икономика – бр.20, декември 2012 г. www.ekonomymagazine.bg

5. Алвин и Хайди Тофлер, Революционното богатство. С Обсидиан, 2007 г.

6. Среда за сигурност – съвкупност от вредни въздействия върху страна, които оказват влияние върху стабилността и живота на гражданите, обществото и държавата.

7. Състояние на приближаване на сходства – становище на ексминистър Антони Славински – преподавател в Нов Български университет и председател на Асоциация „Телекомуникации” в сп. Икономика-бр.20, декември 2012 г.

8. сп. Икономика – бр.20, декември 2012 г. www.ekonomymagazine.bg

9. Анонимник [4] – това е HTTP прокси, който филтрира идентифициращата заглавна част и адреса на изпращача от Web-браузъра. Анонимникът предлага бърз начин за анонимно сърфиране без да се разкрива тяхната идентичност. Смесената топология и маршрут се състои от единствен възел – Анонимизиращ сървър. Силните страни са ниско закъснение, лесно внедряване и повишаване на анонимността. Слабите страни са невъзможност за криптиране, защита на влизането и скритост на пренасочването.

10. Ефективност – взаимовръзка между получения резултат и използвания ресурс 3.2.15. (ISO 9000:2005)

11. Анонимно рутиране с динамичен източник (Anonymous Dynamic Source Routing-AnonDSR) е протокол по заявка за смесена onion мрежа, без разкриване на съседните възли, с крипто защита за получателя.

12. Чл.27,ал.5 от Закона за статистиката

13.Чл.64 от ЗСВласт

14. Касаеща банковата тайна

15. Чл.179 от НПК

16. Касае адвокатската тайна
17. Х. Христов. Доклад „Посегателства срещу лични данни в организацията– специфични аспекти”.Сборник трудове НК „Защитата на личните данни в контекста на информационната сигурност”.Секция „Държава и сигурност”. ФАПВОКИС на НВУ, Шумен,2013 (под печат);

18.Закон за СРС чл.33

19. Бояджиев Н., Сп. „Съвременно право”, кн.5, 1999 г., стр.48

20. Велчев Б., Сп. „Съвременно право” кн.I, 2005 г., стр. 71

21. Решение № 1778 от 20.12.2011 г. Комисията за защита на конкуренцията
22. по решение № 1068/15.10.2009 г по преписка с вх. № КЗК751/17.08.2009 г.на БНБ до КЗК

23. Заповед № I-з-793/23.03.2011 г. на заместник министър-председателя и министър на вътрешните работи на Р. България

24. Подробности в Решение № 1778 гр. София, 20.12.2011 г. на КЗК

25. Закона за счетоводството

26. По смисъла на § 1, т.7 от ДР на ЗЗК

27. По смисъла на § 1, т.13 от ДР на ЗЗК

28. Решения на Върховния административен съд но дела № 9578/2010 г., и № 2931/2011 г.

29.Рашков, Б. Специални разузнавателни средства УИ, Св. „Кл. Охридски – 2010 г., стр.327

АКТУАЛНИ АСПЕКТИ НА УПРАВЛЕНИЕ НА ЧУВСТВИТЕЛНАТА ИНФОРМАЦИЯ, КАТО ЕЛЕМЕНТ ОТ НАЦИОНАЛНАТА СИСТЕМАТА ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА

Стоян Г. Тонев

TOPICAL ASPECTS OF THE MANAGEMENT OF SENSITIVE INFORMATION AS AN ELEMENT OF THE NATIONAL SYSTEM FOR PROTECTION OF THE INFORMATION

Stoyan G. Tonev

ABSTRACT: *Increasingly often talk about information management and how accurate and timely information is a key element of making important and adequate solutions. The information is defined as the diversity , the result of interaction of objects. In worldly aspect - for each person the information is the information about the world around him and processes occurring there , entering the brain from many sources and in different forms . As a result of carried out there interactions form the structure of human knowledge. Management policy of sensitive information can and should be part of the common security of the information of both the EU and NATO and the Republic of Bulgaria.*

KEY WORDS: *Aspects of the management, sensitive information, management systems, anonymous routine, security, strategic asset, organizational security, information systems, proportionality, hostile environment*

През 70-те години на миналия век приоритет на академичните звена в световен мащаб са били осигуряване продуктовата сигурност, добива и преработката на нефт или друг стратегически продукт. С развитието на IT-технологиите съществено внимание е отделено на информационната сигурност и най-вече на т.нар. „системи за управление на чувствителна информация". Това не е случайно, тъй като по дефиниция - информационната сигурност е „степен на сигурност на системата за управление на чувствителна информация" която е прилагана от малко на брой организационни единици /ОЕ/. Последното се определя от факта, че информацията се разпространява неравномерно и в световен мащаб представлява силно зависим източник- актив, подпомагащ придобиването и управлението на финанси и капитали. Поради което управлението на чувствителна информация е изключително важен елемент за една държава, организация и в много висока степен засяга проблемите на националната сигурност, суверенитета и независимостта им.

В процеса на глобализация, ненадеждната защита и управлението на чувствителната информация води до отслабването на държавата, чрез две основни следствия:

- бързото нарастване на трансграничната престъпност и

- глобализацията на престъпността превръща се в сериозно предизвикателство към сигурността на личността, Държавата и общностите в съвременния свят.

Стратегически приоритет на правителството на Р. България след влизането ни в Северноатлантическия алианс и Европейския съюз бе изграждането на унифицираща законодателна и институционална база в Р. България в областта на защитата и управлението на

чувствителната, и по-специално на класифицираната информация. Целта бе дефиниране по нов начин приоритетите и основните понятия, определяне на компетентни органи и регламентиране на отговорности и правомощия, детайлно уреждане на принципите за защита и управление на класифицираната информация приведена в съответствие с политиката и стандартите на НАТО и ЕС, както и за изпълнението на споразуменията по сигурност между Р. България с ЕС, НАТО и с други страни - членки и партньори. Политиката за сигурност при управление на чувствителната информацията може и трябва да бъде част от обща политика за сигурност на информацията както е в ЕС, НАТО така и трябва да е в Р. България.

В тази връзка, приетият през 2002 г. закон за защита на класифицираната информация (ЗЗКИ) създаде нова регулаторна рамка, съобразена с принципите за изграждане на модерната демократична държава в тази област. Законът въведе нови понятия като "класифицирана информация", "физическа сигурност", "индустриална сигурност" "документалната сигурност" и др., дефинирани като основни за закона разпоредби, напълно съответстващи на стандартите на НАТО и на Европейския съюз.

Управлението на видовете защита на класифицираната информация и оценката на възможностите за защита на класифицирана информация е сложен процес, свързан със събиране, обработка и анализ на разнородна и голяма по обем информация. Той като неотделим елемент от системата на защита на класифицираната информация е един от основните фактори- нейната сигурност. В организационните единици се прилага утвърден модел на процес на защита и управление на класифицирана информация. Действащата процедура за определяне на

сигурността, често се определя, като трудоемка и тромава. В този аспект, прилагането на информационните технологии води до рязко увеличаване на обема от информация, която се обработва и използва за определено време. Това налага необходимостта да се анализира съществуващата практика и да се предложи нов, ефективен модел за оптимизиране дейностите по защита и управление на Чувствителната информация.

Оценката на мотивите определят това изследване за изключително актуална и значима. Нейното разработване осигурява компенсирането на съществуващите дефицити, в теоретично и практично отношение, в организацията по управлението на чувствителната информация, което ще осигури:

1.установяване на общи процедури по управление на чувствителната информация и нейната надеждност и защитеност;

2. създаване на оптимизиран модел за управление на чувствителната информация за надеждност спрямо сега действащия модел в ОЕ;

3.разработване и внедряване на система за ефективно управление на чувствителната информация и повишаване на непрекъсваемостта за надеждност на бизнес организациите, която ще:

- изключва субективизма при управление на чувствителната информация;
- разпределение на чувствителната информация по различни направления;
- уеднаквяване на групи информации като чувствителна информация за по лесно управление;

осигурява на информационен масив от база данни, които да могат да се анализират и да послужат за управление на рискови и заплахи за адекватна контраразузнавателна дейност по наблюдение, разкриване, противодействие, предотвратяване и пресичане на замислени, подготвени или осъществявани посегателства срещу бизнес организациите касаещи националната сигурност.[2]

- **Целта** на изследването е на основата на обзорния анализ и на съществуващия опит и на специализирани публикации, да се обоснове теоретично, проектира и предложи модел за внедряване на процеса по **управление на чувствителната информация** и защита й, както и използване на различни технологии, с които да се осигури повишаване на оперативността при обработката, съхранението и обмена на чувствителна информация.

За постигането на тази цел в изследването е залегнало решаването на следните научноизследователски **задачи**:

- оптимизиране на процеса по управление на чувствителната информация по изведени приоритетни критерии;
- -изследване на подсистемата за надеждно управление на чувствителната информация, в контекста на общата теория на системата за сигурност на информацията, и определяне на нейния обхват;
- -анализ на възможностите на информационните техники и технологии за усъвършенстване и оптимизиране на

процеса по защита на чувствителната информация на отделните ОЕ;

- разработване на модел за защита на чувствителната информация и прилагането й в работата на организационните единици;

Обект на изследването е системата за управление на чувствителната информация на база законодателството на страната в условията на реално членство на Р. България в ЕС и пълноправен член на НАТО.

Предмет на изследването е оптимизиране на процеса по управление на чувствителната информация като елемент от националната система за защитата на класифицираната информация.

Хипотезата на изследването е разработване и внедряване на модел на процеса за надеждност при управление на чувствителната информация, което ще доведе до стандартизиране на процесите в модела, а от там оптимизиране и автоматизиране на процеса по надеждна защита на чувствителната информация.

Управление на чувствителната информация може и следва да се разглежда като система. Изхождайки от общото определение, че системата е множество от елементи, които се намират в отношения и връзки помежду си и образуват определена цялост, може да се направи извода, че системата за надеждно управление на чувствителната информация трябва да притежава следните характеристики:

- наличие на връзки и отношения между образуващите я елементи;

- неразривно единство със средата, във взаимодействие, с която системата изразява своята цялост;
- разглежда се като система от по-висок порядък, докато нейните елементи могат да бъдат системи от по – нисък порядък;
- поведението й е подчинено на постигане на определена цел;
- цялостното й функциониране е резултат от взаимодействието на всичките й елементи.

В съответствие с гореизложеното, в изследването е приложен системен подход, който цели максимално обхващане и разглеждане на вътрешните и външни връзки за системата за надеждно управление на чувствителната информация, като подсистема на националната системата за защита на класифицираната информация и националната сигурност.

Наред с тези класически методи в изследването са използвани и включени:

1. Проучване на документи – събрани са и са проучени основни нормативни документи. В по- тесен план, свързани с надеждност при управление на чувствителната информация, а в по – широк със системата за национална защита на класифицираната информация и системите на НАТО, ЕС и ООН;

2. Събеседване с експерти. Проведени са срещи, обсъждания и интервюта със специалисти в областта на защита на класифицираната информация в НАТО, ЕС и ООН;

3. Използван е *структурен анализ,* предложен е обзор на системата за надеждно управление на чувствителната информация и след това тя е детайлизирана; *функционален анализ*, с помощта на който

са изследвани динамичните характеристики на системата; *информационен анализ*, чиято цел е изследването на количествените и качествени характеристики на чувствителната информацията, използвана в системата;

Създадени са модели, с цел преодоляване на разнообразията на изследваната система;

Чувствителната информация, като стратегически актив[3] е ценност и трябва да бъде добре защитен. Това е особено важно в днешната сложна и динамично променяща се среда, в която чувствителната информация е изложена на множество разнообразни заплахи. Сигурност.[4], защита и система за управлението на чувствителната информация са фундаментални понятия, които изграждат цялата концепция за постигане на конкурентно предимство.

Анализът на съвременните социални отношения показва, че с нарастване мащабите на анонимно рутиране.[5] на чувствителна информация, както между отделните структури на социалната организация, така и между партньорите, нарастват рисковете, свързани с опазване репутацията на организациите, а също така и рисковете, имащи непосредствено отношение към тяхната стабилност.

Налага се изводът от специалистите, работещи по поддържане на мрежови системи, че с обмена на чувствителна информация, може да се очаква нарастване на рисковете от срив и несанкциониран достъп до чувствителна информация.

Предизвиква тревога фактът, че голяма част от организациите.[6] нямат план за действие при срив на информационната система, обработваща чувствителна информация и сроковете за нейното възстановяване могат драстично да се разминат както с надеждите на

ръководството, така и с очакванията на потребители, подизпълнители, партньори и др.

Макар в последно време на въпросите, свързани с рисковете за информационната сигурност, да се обръща все по-сериозно внимание, практиката показва, че реалните действия по управление.[7] на чувствителната информация много често са непоследователни и недостатъчни. В резултат на такова отношение, много ръководители на организационни структури.[8] прекалено късно откриват, че икономическите резултати от инвестициите в сферата на информационната сигурност са далеч от очакваните, поради неадекватни действия, съчетани с: подценяване на проблемите на информационната сигурност при работата и обучението на персонала; неподготвеност за работа с външни лица; липса на процедури за тестване за устойчивост, дискретност, оперативност и надеждност на при работа с чувствителна информация, като в потвърждение на това е работата на публичните администрации, отказващи да използват комуникационните системи на държавната администрация и активно използват нелицензирани и незащитени доставчици. Тази неподготвеност за работа в конкурентна и/или враждебна.[9] среда поставя на решаването на актуален и значим проблем за гарантиране на информационната сигурност и защита на чувствителната информация от нерегламентиран достъп.

Предстои компютърните услуги, чрез новото явление „cloudcomputing” .[10], да се присъединят към списъка на комуналните услуги и следващите предизвикателства да са в сферата на интерфейса „човек-информационните и комуникационни мрежи и чувствителна информация” и управлението да става чрез говор, поглед, мисъл, което

ще е доказателство за реализирането на „глобален изкуствен интелект”, който предстои да бъде обект на изследване от гледна точка на сигурността. Една от основните насоки на работа е обезпечаване на „глобалния изкуствен интелект” при управление на чувствителна информация, като подготовката трябва да започне веднага е чрез правилната организация на собствена проактивна контраразузнавателна дейност в ОЕ.[18].

Чувствителната информация съдържаща се в българското законодателство се управлява по различен начин в различни, закони, заповеди или други административни разпореждания. Всички тези закони са подчинени на принципите, залегнали в Конституцията на Р. България и по-точно в чл. 34, ал. 1 „правото за свободна и тайна кореспонденция”.

Информационната сигурност на чувствителната информация е такова състояние на организационната единица, в което е необходимо да се осигурява, поддържа и гарантира, непрекъснатост на работните процеси, минимизация на рисковете за организацията и максимизиране на възвращаемостта на инвестициите.

Гореизложеното недвусмислено потвърждава необходимостта от информационна сигурност при управление на чувствителната информация.

Определянето, оценката, постигането, поддържането и подобряването на сигурността на чувствителната информация са съществени за повишаването на конкурентоспособността, финансите, доходността, за спазване на законите и поддържане на добрия имидж за организационната единица.

Много информационни системи не са проектирани да осигурят сигурност на чувствителната информация. Сигурността, която може да се постигне чрез технически средства, е ограничена и трябва да бъде поддържана чрез съответни управленски решения и установени процедури.

Управлението на чувствителната информация изисква задължително участие на всички служители в ОЕ, доставчиците, трети страни и контрагенти. Отчитайки тези особености, изследването се насочва към управлението на чувствителната информация, касаеща физически и юридически лица и съгласно законодателството ни, като такива са определени личните данни, банкова, адвокатска, търговската, производствена, следствената, статистическа и др тайни на осиновяване и завещанието, данъчната, осигурителна, служебна, здравната, информация, актовете на съда, картелните споразумения, списъка със стоки и технологии с двойна употреба, информацията в публични и непублични регистри и др.

Интерес за изследването представляват информационните системи в, които се управлява чувствителна информация и това са:

Географската информационна система (ГИС), която е съвкупност от софтуер, хардуер, данни, процедури и обучени кадри за създаване, манипулиране, съхраняване, анализ и визуализация на пространствено определени данни.

Правно-информационна система е програма базирано в интернет приложение, даващо достъп до база данни от документи, най-вече с юридическа насоченост.

Шенгенската информационна система, ШИС (SIS), с данни за над 1 млн за хора и предмети,за изгубени вещи или хора, заповед за

арестуване, откраднато или присвоено огнестрелно оръжие, изгубени или, откраднати документи за самоличност.[11].

ЕСГРАОН е абревиатура на Единна система за гражданска регистрация и административно обслужване на населението, създадена през 1977 г. с ПМС №15 на НРБ.

Горепосочените информации не попадат под защита на ЗЗКИ и това изисква друг вид защита на информация, определена като чувствителна за личността и обществото.

В законодателството на Р. България не е изяснен елементът „информация”[12], който е с много широко съдържание и прилагането му, във всички случаи, може да доведе до колизии – например „ако без знанието на който и да е, се направи негласно записване с техническо средство на магнитен или лазерен носител на” информационна емисия на публична медия, към която лице проявява интерес, съставът на престъпление по чл.339а от НК не конкретизира в тази насока, че с изпълнителното деяние се събира не всякаква информация, а само свързаната със защитени от Конституцията основни права.[13].

Възможно е да се изведе изводът, че прилагането на СРС представлява дейност, с която се реализира държавна принуда по отношение на конкретни правни субекти с цел предотвратяване, разкриване и доказване на тежки престъпления, което обуславя социалната ценност на принудата и нейната достъпност, във връзка със конституционните права и свободи на гражданите, във връзка с чл. 34, ал. 1 от КРБ.[14] В тези случаи информацията не е класифицирана, но попада в категорията „чувствителна информация”и трябва да се управлява като такава.

Управлението на „чувствителна информация” не е управление на “некласифицирана информация”, и не подлежи на свободно разпространение. С чувствителната информация се означава информация, която не е класифицирана, с която се работи по-свободно, но която също така не подлежи на свободно разпространяване и с нея следва да се запознават лица, чиито служебни задължения налагат това. Информация, маркирана като чувствителна, се оповести само със съгласието на автора на документа, но единствено авторът на документа е оправомощен да променя маркировките й.[15].

Сигурността на чувствителната информация, като вид жизненоважен актив налага и определени ограничения на свободния достъп и разпространението й, която трябва да бъде адекватно управляван, умело защитен, с цел недопускане накърняване на личното достойнство, финансово ощетяване на юридическите и физически субекти и гарантиране непрекъснатост на работния процес на организационната единица и конкурентно начало. Ограниченията в европейското и българското законодателство задължително трябва да бъдат съобразени с принципа на пропорционалност и на допустими ограничения и свобода на ползване на информация. Същото е регламентирано и в международни актове.[16] и е основополагаща практика на европейските институции. Известно е, че същността в управлението на чувствителната информация е осигуряване на относително съответствие, баланс, равновесие между обществения интерес от прилагане на ограничителни мерки и достатъчната и необходима степен на засягане на съответните основни права така, че с въздействието върху тях да не бъде нарушено, а защитено съдържанието на чувствителната информация.

Принципът за пропорционалност в българското законодателство е изразен в разпоредбите на чл. 40, ал. 1 от Закона за електронните съобщения по следния начин: „исканията на Комисията за регулиране на съобщенията за предоставяне на информация трябва да бъдат пропорционални на целите, за които са направени".

Предвидените в нашето законодателство правно-фактически основания за ограничаване на права и целите, които законът предвижда, съответстват на , посочени в Европейската конвенция за защита на правата на човека и основните свободи, в решения на Европейския съд за правата на човека и др. международни актове.[17]

Особен акцент на дейността по предотвратяване на потенциалното влияние на източници на заплаха върху социалната организация, са проактивните действия (общи и специални), спрямо източника при разкриване на признаци за насочеността му срещу ОЕ.[18].

Налага се изводът, че държавната намеса за защита на чувствителната информация е необходима в едно демократично общество, в интерес на националната сигурност и обществения ред, на икономическото благоденствие на Р. България на правосъдието, морала и здравето, подчинено на цялостната концепция за постигане на конкурентно предимство за предотвратяване на деструктивни въздействия и разкриване на извършени или подготвяни престъпления за ОЕ.

Л и т е р а т у р а:

1.Информация – всяко знание, което може да бъде съобщено под каквато и да е форма, ДВ 103/2004 г.

2. Актив (осезаем и неосезаем) – всичко, ценно със стойност за организацията (ISO/IEC 13335-1:2004).

3. Сигурност – Сигурността се дефинира, като „достигнато състояние, при което посочена информация, материали, персонал, дейности и съоръжения са защитени", Съвместна доктрина на НАТО за разузнаване, контраразузнаване и сигурност (AJP 2.0), www.his.com

4. Анонимно рутиране с динамичен източник (Anonymous Dynamic Source Routing-AnonDSR) е протокол по заявка за смесена onion мрежа, без разкриване на съседните възли, с крипто защита за получателя.

5. Организация – съвкупност от помещения, съоръжения и хора с разпределени отговорности, пълномощия и взаимовръзки, 3.3.1, (ISO 9000:2005)

6. Управление – съвкупност от координирани дейности за ръководене и контрол на дадена организация 3.2.6 (ISO 9000:2005)

7. Организационна структура – разпределение на отговорности, помещения и взаимовръзки между хора 3.3.2. (ISO 9000:2005)

8. С Враждебна среда се означава „противник" или воюваща страна в конфликт, в който Алианса е директно въвлечен или като трета страна – подробности в „Съвместна доктрина на НАТО за разузнаване, контраразузнаване и сигурност" (AJP 2.0), www.his.com

9. Подробности в сп. Икономика – бр.20, декември 2012 г.- стр.89, www.ekonomymagazine.bg

10.Чл.360 от НК – Който разгласи сведения от военно, стопанско или друго естество, които на са държавна тайна, но чието разгласяване е забранено със закон, заповед или друго административно разпореждане, се наказва с лишаване от свобода до една година или пробация.

11.http://bg.wikipedia.org/w/index.php?title=Шенгенска_информационна_система&oldid=5485913“

12. Визира се чл.24 и чл.25 от Закона за Специалните разузнавателни средства

13. Велчев Б. Сп. „Съвременно право”, кн.I, 2005 г., стр.70

14. Бояджиев Н., Сп. „Съвременно право”, кн.5, 1999 г., стр.48

15. Документална сигурност в рамките на НАТО – Семинар на ДКСИ 2012 г.

16. Подробно виж „Всеобща декларация за правата на човека”, „Европейската конвенция за защита на правата на човека и основните свободи”

17.Рашков, Б. Специални разузнавателни средства УИ, Св. „Кл. Охридски – 2010 г., стр.327

18. Христов Х.Атанасов, „Активната стратегия за управление на противодействието на посегателства срещу бизнес организацията - същност”- главен асистент в катедра ,,Управление на системите за сигурност’’, Шуменски Университет ,,Епископ Константин Преславски’’, hristov63@abv.bg.

ГОДИШНИК

НА ШУМЕНСКИЯТ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

ТЕХНИЧЕСКИ НАУКИ

Т. IV Е

Формат 16/80/84

ISSN 1311-834X

Универистетско издателство
“Епископ Константин Преславски“ 2014