ГОДИШНИК

НА ШУМЕНСКИЯ УНИВЕРСИТЕТ

„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Т. XII Е

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

ANNUAL

OF KONSTANTIN PRESLAVSKI

UNIVERSITY OF SHUMEN

Vol. XII E

FACULTY OF TECHNICAL SCIENCES

Университетско издателство

„Епископ Константин Преславски“

Шумен, 2022

ISSN 1311-834X (print)
ISSN 2815-4703 (online)

ГОДИШНИК

НА ШУМЕНСКИЯ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Т. XII Е

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

ANNUAL

OF KONSTANTIN PRESLAVSKI
UNIVERSITY OF SHUMEN

Vol. XII E

FACULTY OF TECHNICAL SCIENCES

Университетско издателство
„Епископ Константин Преславски“
Шумен, 2022

Настоящият годишник съдържа статии и студии за 2022 г. от Факултета по технически науки

РЕДАКЦИОННА КОЛЕГИЯ

ISSN 1311-834X (print)
ISSN 2815-4703 (online)

СЪДЪРЖАНИЕ

ГЕОДЕЗИЯ С ГРАВИТАЦИОННА ГРАДИОМЕТРИЯ, Красимира К. Кирилова 5

ИНТЕГРИРАНЕ НА ДАННИ ОТ НАЗЕМНО ЛАЗЕРНО СКАНИРАНЕ ВЪВ ФОТОГРАМЕТРИЧНА ОБРАБОТКА, Кирил Ф. Янчев 10

МОДЕЛИРАНЕ НА ОБУЧАВАЩА ИГРА ЗА ТСР МЕХАНИЗЪМ, Валентин Т. Атанасов 15

ПЛАНОВА И ВИСОЧИННА ГЕОДЕЗИЧНА ОСНОВА ЗА ТОПОГРАФСКА СНИМКА НА РЕКИ И ВЪТРЕШНИ ВОДОЕМИ, Евгени Гр. Стойков 21

ЗА МРАВКИТЕ И ЛОГИСТИКАТА, Светлозар П. Стоянов, Йорданка И. Янкова-Йорданова 27

ЗА НЯКОИ ЖЕЛЕЗНИ СПЛАВИ, СТОМАНИ И ЧУГУНИ, Светлозар П. Стоянов, Георги П. Георгиев 34

АКТУАЛНИ АСПЕКТИ НА РИСКОВЕТЕ ОТ ИЗПИРАНЕ НА ПАРИ, Цвета Т. Маркова, Николина М. Маркова 38

ИДЕНТИФИКАТОР НА ПОЗЕМЛЕН ИМОТ. СЪЩНОСТ И ПРЕДНАЗНАЧЕНИЕ, Мирем Е. Ниязи-Юсуф 46

ВЛИЯНИЕ НА РАЗНОТОЧНАТА КАДАСТРАЛНА КАРТА ВЪРХУ ПОТРЕБИТЕЛИТЕ НА КАДАСТРАЛНИ ДАННИ, Мирем Е. Ниязи-Юсуф 50

ПОСЛЕДИЦИ ОТ ВЪЗМОЖНОТО ИЗПОЛЗВАНЕ НА ТАКТИЧЕСКО ЯДРЕНО ОРЪЖИЕ В УКРАЙНА Оценка на политическите, военните и екологичните ефекти, Андрей Н. Михайлов 54

ПРОЕКТИРАНЕ И РАЗРАБОТКА НА СТЕНД ЗА ИЗПИТВАНЕ НА МЕХАНИЧНА УСТОЙЧИВОСТ НА ВОДОСЪДЪРЖАТЕЛИ, Милен К. Петков, Пламен Л. Рибарски 70

ИМПЛЕМЕНТАЦИЯ НА BEAGLEBONE BLACK ЗА УПРАВЛЕНИЕ НА СЕРВОМОТОР С ЕНКОДЕР, Милен К. Петков 81

ПРИСВОЯВАНЕ НА ДЪЛЖИНА НА ВЪЛНАТА ЗА WDM МРЕЖИ, Цветослав С. Цанков, Екатерина М. Христова 87

ОТНОСНО ПРОГНОЗИРАНЕТО НА ПОЯВАТА НА ГРЕШКИ В ПРОГРАМНИЯ КОД НА СОФТУЕРНИТЕ СИСТЕМИТЕ ЗА УПРАВЛЕНИЕ, Атанас Начев 92

ОСНОВНИ ИЗИСКВАНИЯ КЪМ ЕКРАНИРАНЕТО, КАТО ПОДХОД ЗА ЗАЩИТАТА НА ИНФОРМАЦИЯТА ЧРЕЗ ОГРАНИЧАВАНЕ НА ВЛИЯНИЕТО НА ПАРАЗИТНИТЕ ЕЛЕКТРОМАГНИТНИ ИЗЛЪЧВАНИЯ, Атанас Начев 97

ОТНОСНО УНИВЕРСАЛНОСТТА НА ВЕРОЯТНОСТНАТА ИНТЕРПРЕТАЦИЯ НА ИНФОРМАЦИЯТА, Анита Димитрова, Атанас Начев 101

СТРАТЕГИЯ ЗА СИГУРНОСТ НА ОБЩИНА ШУМЕН 2022-2028 г. Усъвършенстване и ефективно поддържане на системата за сигурност на Община Шумен, Илиана К. Симеонова 108

АВТОМАТИЗИРАНО УПРАВЛЕНИЕ НА МРЕЖОВА ИНФРАСТРУКТУРА ЧРЕЗ РАМКАТА ЗА МРЕЖОВА АВТОМАТИЗАЦИЯ ANSIBLE, Мустафа Б. Узун, Валентин Т. Атанасов 117

WDM СПОСОБ ЗА УВЕЛИЧАВАНЕ ПРОПУСКАТЕЛНАТА СПОСОБНОСТ НА КАНАЛА, Екатерина М. Христова, Цветослав С. Цанков 125

ПРЕНОСИМИ СИСТЕМИ ЗА ИНДУСТРИАЛЕН КОНТРОЛ И УПРАВЛЕНИЕ, Христо Х. Хадживанов 132

ИСТОРИЧЕСКО РАЗВИТИЕ НА ФОТОГРАМЕТРИЯТА В БЪЛГАРИЯ, Найлян М. Салиева 143

МОДЕЛИРАНА СИГУРНОСТ В КОДИРАНЕТО НА КОМУНИКАЦИОННА МРЕЖА, Даниел Р. Денев 153

ПРОУЧВАНЕ НА КАЧЕСТВОТО НА ДАННИТЕ ПРИ ЦИФРОВА ОБРАБОТКА НА АКУСТИЧНИ СИГНАЛИ, Даниел Р. Денев, Цветослав С. Цанков 162

ПОДДЪРЖАНЕ НА РАБОТНАТА ГЕОДЕЗИЧЕСКА ОСНОВА (РГО) В АКТУАЛНО СЪСТОЯНИЕ, Стефан Д. Добрев 175

МАРШРУТИЗАЦИЯ ПРИ WDM МРЕЖИ, Екатерина М. Христова, Цветослав С. Цанков 179

ОСНОВНИ ЕЛЕМЕНТИ НА ФИРМЕНАТА СИГУРНОСТ, Цветелина И. Методиева, Велимира К. Канчелова, Георги Жеков 188

ТЕОРЕТИЧНИ АСПЕКТИ НА СИГУРНОСТТА, Цветелина И. Методиева, Велимира К. Канчелова 193

КОРПОРАТИВНА СИГУРНОСТ И ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД НЕЯ, Велимира К. Канчелова 198

МРЕЖОВА ЗАЩИТА, Димитър Р. Илиев 206

ГЕОГРАФИЧЕСКИЕ АСПЕКТЫ РОССИЙСКО-УКРАИНСКОГО КОНФЛИКТА (ДНЕПР), Мирослав Н. Кацаров 209

COUNTERMEASURES FOR PROTECTION OF INFORMATION IN THE COMPUTER SYSTEMS, Veselin Kr. Raynov, Ilko Sr. Marev, Svetlin E. Stefanov 219

TECHNICAL DEVICES AND PROTECTION SYSTEMS, Veselin Kr. Raynov, Ilko Sr. Marev, Svetlin E. Stefanov 224

ГЕОДЕЗИЯ С ГРАВИТАЦИОННА ГРАДИОМЕТРИЯ

Красимира К. Кирилова

GEODESY WITH GRAVITY GRADIOMETRY

Krasimira K. Kirilova

ABSTRACT: *Space gravity gradiometers have been in development for decades. The recent success of the GOCE space mission (van der Meijde et al 2015) has stimulated new ideas and new approaches to gravity gradiometry that have aided studies of the Moon (Carroll 2011), Mars (Cuperus et al 2009) and other planets. The gravity gradient tensor contains information about the local gravity field, which is the source of many problems of geodesy and geophysics.*

KEYWORDS: *Tensor, gravity gradiometry, gradient.*

Въведение

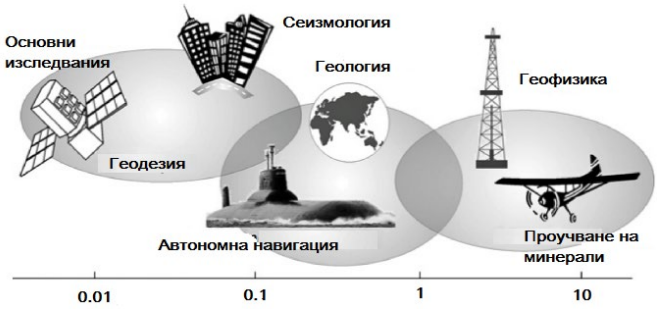
През второто десетилетие на XX век за определяне на компонентите на тензора на градиентите на силата на тежестта са разработени специални гравитационни градиометри и методи за измерване. Разработването на такива устройства е доста трудно и бавно поради факта, че изискванията за точност са много високи, около 10^{-9} от измерените стойности. До средата на XX век са използвани торзионни везни на Етвьош. През 70-те години във връзка с бързото развитие на ракетните и космическите технологии се появяват инерциални измервателни системи с наноразмерна точност на наноразмери. Появява се възможност не само да се създаде устройство за измерване на градиентите на движеща се среда, но и да се разделят инерционните и гравитационните ускорения. Появява се нов раздел на гравиметрията - градиометрия, която започна да се развива бързо, като се разделя на наземна, самолетна и спътникова градиометрия [2,3].

Целта на доклада е да представят изходните предпоставки на т. нар. гравитационен градиометър с пълен тензор (Full Tensor Gradiometry - FTG), способен да измерва всички компоненти на градиента на силата на тежестта, което води до генерацията на гравитационни градиометри FTG ™.

Корпорацията *Lockheed Martin* (преди това Bell Aerospace) е инициатор на практическата гравитационна градиометрия от преди около 50 години. Това довежда до така нареченото Falcon ™ - генериране на гравитационни градиометри, което все още се разглежда като водеща гравитационна градиометрова технология в света (*Dransfield u Christensen 2013*). В Lockheed Martin (американска компания) се разработва т. нар. гравитационен градиометър с пълен тензор (Full Tensor Gradiometry - FTG), способен да измерва всички компоненти на градиента на силата на тежестта, което води до генерацията на

гравитационни градиометри FTG ™. Той беше приет в търговска версия на Bell Geospace, Inc. и понастоящем е достъпен за крайните потребители (Murphy 2010).

Съществува огромен интерес от използването на такава модерна технология за стратегически търговски приложения. Фигура 1 показва графично представяне на различни приложения на гравитационната градиометрия.



Фиг. 1. *Приложения за гравитационна градиометрия, сравнени по скалата на чувствителност, която е необходима за дадено приложение. Тези от крайната лява страна са 1000 × по-чувствителни от тези в най-дясната част [7].*

Космическите гравитационни градиометри се разработват от десетилетия. Неотдавнашният успех на космическата мисия на GOCE (van der Meijde et al 2015) стимулира нови идеи и нови подходи към гравитационната градиометрия, подпомогнала изследванията на Луната (Caroll 2011), Марс (Cuperus et al 2009) и други планети.

1. Изходни предпоставки

Нека се предположи, че потенциалът на планетата (Земя) се определя от силата на тежестта [1,5]

$$W\left(\bar{r}\right) = U\left(r\right) + Q\left(r\right) + ..., \qquad (1)$$

където $U\left(r\right)$ е потенциал на силата на привличане; $Q\left(r\right)$ - центробежния потенциал (потенциалът на привличане от Луната и Слънцето, приливния потенциал и т.н. не се вземат предвид)

Тогава градиента на Земния потенциал $W\left(\bar{r}\right)$ има вида

$$\nabla W = \left(\frac{\partial W}{\partial x} \quad \frac{\partial W}{\partial y} \quad \frac{\partial W}{\partial z} \right)^T \qquad (2)$$

и той е идентичен с ускорението на силата на тежестта, т.е.

$$\overline{g} = \nabla W = \left(g_X g_Y g_Z \right)^T . \qquad (3)$$

В произволна ортогонална координатна система, векторът на ускорението на силата на тежестта $\overline{g}$ може да се разглежда като тензор от ранг 1 – вектор (големина, посока), имащ само физически координати, тъй като поради ортогоналността на системата, нейните ковариантни и контравариантни координати съвпадат с физическите [1,5]. Като се използва правилото за прилагане на оператора ∇ (набла) към тензор от ранг 1, се получава тензора на първите производни на компонентите на вектора на ускорение на силата на тежестта или въз основа на (2), (3) - вторте производни на потенциала на силата на тежестта *W*. Предмет на изследването на градиометрията се явява градиентът на силата на тежестта $\overline{g}$, тоест изразът:

$$\nabla \overline{g} = \nabla \left(\nabla W \right) = \begin{pmatrix} \frac{\partial^2 W}{\partial x^2} & \frac{\partial^2 W}{\partial xy} & \frac{\partial^2 W}{\partial xz} \\ \frac{\partial^2 W}{\partial y \partial x} & \frac{\partial^2 W}{\partial y^2} & \frac{\partial^2 W}{\partial yz} \\ \frac{\partial^2 W}{\partial z \partial x} & \frac{\partial^2 W}{\partial z \partial y} & \frac{\partial^2 W}{\partial z^2} \end{pmatrix} = \begin{pmatrix} W_{xx} & W_{xy} & W_{xz} \\ W_{yx} & W_{yy} & W_{yz} \\ W_{zx} & W_{zy} & W_{zz} \end{pmatrix}. \qquad (4)$$

Тензорът на градиентите на ускорението на силата на тежестта съдържа пълна информация за локалното гравитационно поле. Той описва структурата на полето чрез неговата кривина, позволява да се определят функциите $U\left(C_{nm} S_{nm}\right), \mathrm{Q}\left(\omega_{\oplus}\right)$ и други чрез решаване на задачи на диференциалната геометрия, което дава възможност да се прехвърлят измерените стойности на силата на тежестта $\overline{g}$ в съседни точки. От измерените градиенти може да се определят кухини и структурата на вътрешния строеж на измереното тяло.

Основният недостатък на наземната градиометрия е влиянието на близки и далечни зони, чиито маси са доста трудни за отчитане, следователно е необходимо да се изчисли гладък градиент на силата на тежестта (обикновено вертикалния му компонент) въз основа на трансформация на полето.

Градиенти на нормалното поле на силата на тежестта и аномалии на градиента. Разликата между реалния (*W*) и нормалния потенциал на силата на тежестта се нарича аномален потенциал (*T*) и се дефинира с уравнението:

$$W\left(\overline{r}\right) = U^0\left(\overline{r}\right) + T\left(\overline{r}\right). \qquad (5)$$

Необходимостта от разделяне на потенциала на нормален потенциал (U) и смущаващ (T) се обосновава с добрата апроксимация на реалния потенциал от нормалния и с възможността за работа със сравнително малки стойности при изчисление на величините, свързани със смущаващия потенциал.

В геодезическата система на повърхността на общоземен геоцентричен референтен елипсоид се определят следните стойности на нормалните градиенти [Торге, 1999]:

$$U^0_{xx} \approx U^0_{yy} = 1540 \ \ ns^{-2}; \qquad U^0_{yy} - U^0_{xx} = 10,4 \cos\varphi \ \ ns^{-2}$$

$$U^0_{zz} = \frac{\delta\gamma}{\delta z} = 3086 \ \ ns^{-2}; \qquad U^0_{zx} = \frac{\delta\gamma}{\delta x} = 8,1 \sin 2\varphi \ \ ns^{-2}; \ \ U^0_{xy} = U^0_{zy} = 0$$

Измерените градиенти с нормална сила на тежестта могат значително да се различават от дадените стойности поради привличането на топографски маси, близки до точката, в която се определя тензора. Отклонението от нормалната стойност на W_{zz} в умерено планинския терен на Централна Германия достига до $\pm 1400 \ \ ns^{-2}$; след въвеждането на корекции за релефа, отклоненията остават, но намаляват до стойност $\pm 300 \ \ ns^{-2}$ [4];

Ако от W израз (5) се изключи градиента на нормалното поле на силата на тежестта, тогава се получава смущаващия потенциал

$$T\left(r\right) = W\left(r\right) - U^0\left(r\right). \qquad (6)$$

От израз (6), като се приложи два пъти оператора ∇, се получава тензора на градиентите на гравитационното смущение

$$\nabla\left(\nabla T\right) = \begin{pmatrix} T_{xx} & T_{xy} & T_{xz} \\ T_{yx} & T_{yy} & T_{yz} \\ T_{zx} & T_{zy} & T_{zz} \end{pmatrix}. \qquad (7)$$

Статистическите характеристики на тензора (7) могат да се опишат с помощта на глобалния модел на силовите дисперсии на аномалиите на силата на тежестта. За земната повърхност са получени следните средноквадратни стойности на съставните градиенти на компонентите на градиента на силата на тежестта (Таблица 1) [6]:

$$\sigma\left(T_{zx}\right) = \sigma\left(T_{zy}\right) = \pm 59 ns^{-2};$$

$$\sigma\left(T_{zz}\right) = \pm 84 ns^{-2}.$$

Таблица 1. *Зависимоста на средната квадратна грешка от височината и точността на измерванията*

Височина (km)	$\sigma\left(T_{zz}\right)\ ns^{-2}$	Точност на измерването ns^{-2}
1	±40	±10
10	±10	±1
250	$\pm 0,3$	$\pm 0,01 \div 0,0001$

Заключение

За начало на градиометрията се счита създаването на устройство от унгарския учен Р. Етвьош, наречено „торзионни везни“ с тестови маси, разположени на различни височини, което дава възможност да се определят хоризонталните градиенти на ускорението на силата на тежестта. Създаването на различни видове гравитационни градиометри (транслационни или ротационни) с помощта на нанотехнологии (т.е. от ускорителните единици) дава възможност за измерване на всички компоненти на тензора на градиентите на ускорение на силата на тежестта (тензор на Етвьош).

ЛИТЕРАТУРА

[1] Кирилова К., „Основни концепции за спътникова гравиметрия – спътникова гравитационна градиометрия и спътниково проследяване“, Университетско издателство “Епископ Константин Преславски“, 177 стр., ISBN 978-619-201-415-5.

[2] Кирилова К., Янчев К. Спътникова градиометрия – отлично допълнение към общия динамичен метод на космическата геодезия. Годишник на ШУ \" Епископ Константин Преславски\" Технически науки. Том X E, Шумен, Университетско издателство \"Епископ Константин Преславски\", ISSN: 1311-834X, стр. 153-159.

[3] Кирилова К., Янчев К. Градиометрични измервания с градиометър на борда. Годишник на ШУ \"Еп. К. Преславски\" Технически науки. Том X E, Шумен, Университетско издателство \"Епископ Константин Преславски\", ISSN: 1311-834X, стр. 159-163

[4] Торге В. Гравиметрия. –М.: Мир, ISBN 5-03-002809-9 (руск.) 1999. –429 с.

[5] Яшкин С. Н., «Спутниковая градиентометрия и системы спутник - спутник», ISBN 978-5-91188-020-0, М., МИИГАиК, 2009.

[6] Tscherning, C. C.: (ed.): Proceedings ofthe lntemational Symposium "Management of Geodetic Data", K0benhavn 24.-26. August 1981. Geod. lnst. M~dd. No. 55, K0benhavn 1981.

[7] Veryaskin, A., Gravity, Magnetic and Electromagnetic Gradiometry, 2018.

ИНТЕГРИРАНЕ НА ДАННИ ОТ НАЗЕМНО ЛАЗЕРНО СКАНИРАНЕ ВЪВ ФОТОГРАМЕТРИЧНА ОБРАБОТКА

Кирил Ф. Янчев

INTEGRATION OF TERRESTRIAL LASER SCANNING DATA INTO PHOTOGRAMMETRIC PROCESSING

Kiril F. Yanchev

ABSTRACT: *One of the main problems of terrestrial laser scanning data processing is low throughput. The subject of this report is the use of photogrammetric principles to process terrestrial laser scanning data. The essence of the idea of using photogrammetric principles lies in the transformation of ground laser scanning data into a set of virtual images corresponding to the central projection.*

KEYWORDS: *Terrestrial laser scanning, photogrammetric principles.*

Въведение

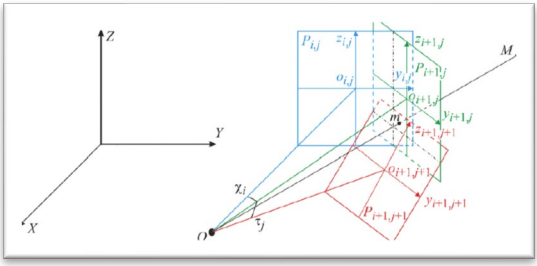
Един от основните проблеми на обработката на данни за наземно лазерно сканиране е ниската производителност. Така например в съществуващите софтуерни продукти времето, прекарано за изграждане на триизмерни модели или цифрови планове или чертежи на фасади, спрямо продължителността на лазерното заснемане е пропорционално ((5-9))/1. Това обстоятелство компенсира предимството на значителното намаляване на обема на работа на терен, което възпрепятства развитието на технологията за наземно лазерно сканиране. Поради това се предлага използването на фотограметрични принципи за обработка на данни от наземно лазерно сканиране.

Същността на идеята за използване на фотограметрични принципи се крие в трансформирането на данните от наземно лазерно сканиране в набор от виртуални изображения, съответстващи на централната проекция [4].

1. Описание на концепцията за използване на фотограметрични принципи при обработката на данни от лазерното сканиране

За да се реализира това мнение, сканирането трябва да бъде представено като набор от измерени посоки, т.е. група лъчи, които на определено разстояние f от точка O от равнината P, сякаш получаваме картина. В този случай един от лъчите, излизащи от точка O, трябва да пресича равнината P ортогонално (фигура 1). В този случай формираните плоски виртуални изображения отговарят на централна проекция.

Фигура 1 показва, че линейните елементи на външната ориентация за всички изображения, направени от една скенерна станция, са еднакви. Ъгловите елементи на външно ориентиране се различават по ъгли χi, τi, т.е. аргументите на матрицата на косинусите на посоката ще бъдат $\varepsilon + \tau i$, η, $\xi + \chi j$, където i = (0, 1, 2,…, n), j = (0, 1, 2,…, k).



Фиг. 1 *Формиране на изображения от данни от наземно лазерно сканиране*

Правоъгълните координати в изображението се изчисляват, както следва:

$$\left.\begin{aligned} x_{i,j} &= ftg(\varphi - \chi_i) \\ y_{i,j} &= ftg(\theta - \tau_j - 90) \end{aligned}\right\} \qquad (1)$$

За свързване координатите на точките на изображението с пространствените координати на съответните точки се използват уравнения за колинеарност [1, 2, 3]:

$$\left.\begin{aligned} y_{i,j} - y_0 &= f\frac{e_2(X_M - X_0) + g_2(Y_M - Y_0) + q_2(Z_M - Z_0)}{e_1(X_M - X_0) + g_1(Y_M - Y_0) + q_1(Z_M - Z_0)} \\ z_{i,j} - z_0 &= f\frac{e_3(X_M - X_0) + g_3(Y_M - Y_0) + q_3(Z_M - Z_0)}{e_1(X_M - X_0) + g_1(Y_M - Y_0) + q_1(Z_M - Z_0)} \end{aligned}\right\}, \qquad (2)$$

където:

x_0, y_0 – координати на центъра за проекция на изображението;

X_M, Y_M, Z_M – пространствени координати на точките на обекта.

За изображения, образувани от данни от наземно лазерно сканиране, x_0, y_0 са равни на нула.

В допълнение към вертикалните и хоризонталните ъгли, НЛС измерва разстоянието R, което е свързано с линейни елементи за външна ориентация и пространствени координати на точките на обекта, както следва:

$$R = \sqrt{(X_M - X_0)^2 + (Y_M - Y_0)^2 + (Z_M - Z_0)^2} \qquad (3)$$

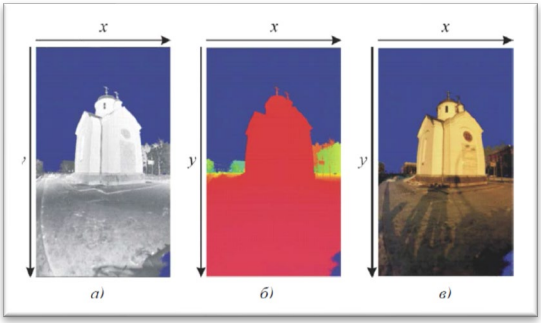
Израз (3) определя дължината на вектора на посоката до точката от обекта. Традиционно, за да го намерите, се използва двойка изображения с взаимно припокриване.

Въз основа на тази теория могат да бъдат създадени два вида изображения: аналитични и цифрови [5]. Първият изглед е показан в Таблица 1, където елементите на изображението са разстоянията, измерени от скенера. По-целесъобразно е използването на аналитични виртуални изображения за решаване на изчислителни проблеми, т.е. външна ориентация на сканирания, настройка на скан-триангулачни конструкции, внедряване на автоматични алгоритми за изграждане на триизмерни модели и др. В днешно време този тип от виртуални изображения може да се използва само за решаване на първите два проблема от изброените по-горе.

Таблица 1 *Пример за аналитично виртуално изображение на контролни точки*

номер на точка	x, mm	y, mm	R, m
Tar 4.5	42,184	–8,069	18,367
Tar 4.6	48,343	–8,176	18,520
Tar 5.1	–82,631	1,378	39,343
Tar 5.2	–81,466	1,437	40,550
Tar 5.3	–40,328	2,775	60,800
Tar 5.4	–37,899	2,722	60,815
Tar 5.5	5,081	1,900	58,258
Tar 5.6	7,813	1,812	58,024
Tar 5.7	24,393	–2,034	34,408
Tar 5.8	24,140	–2,222	32,550

За цифровото представяне на виртуални изображения се използват три характеристики като стойности на пиксели: интензитет, разстояние от скенера до снимания обект и реален цвят (Фигура 2).



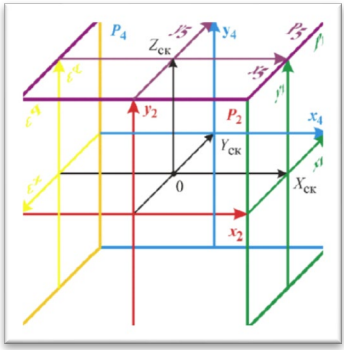
Фиг. 2 *Представяне на резултатите от наземно лазерно сканиране под формата на двуизмерни виртуални изображения: а) интензитет на отразения сигнал; б) разстоянието от скенера до снимания обект; в) реални цветове на обекта*

По-целесъобразно е да се използват цифрови виртуални изображения за автоматизирано декодиране, компресиране на изображения и изграждане на цифрови модели.

За практическото приложение на тази предложена теория възникват два въпроса: изборът на броя на кадрите и изборът на фокусното разстояние на виртуалните кадри.

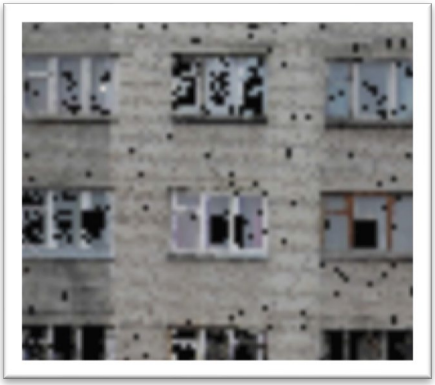
Изборът на броя на изображенията трябва да се реши по пътя на минимални разходи за преобразуване на данни и оптимално възприемане на данни. Въз основа на това е най-ефективно да се използват пет изображения на скенера, главните оптични оси, които са разположени за четири изображения в равнината на сканиране $X_{ск}Y_{ск}$ през 90°, а петото изображение е перпендикулярно на равнината $X_{ск}Y_{ск}$.

Това позволява да се покрие областта на сканиране на всички произведени скенери само с пет снимки. Тази схема за поставяне на виртуални изображения е показана на фигура 3.



Фиг. 3 *Схема за преобразуване на данните от скенера в пет виртуални изображения*

Подобна схема за поставяне на виртуални изображения не води до видими изкривявания, причинени от преизчисляване от сферична повърхност към централна проекция. По цялото поле на изображението тези изкривявания не надвишават 11% от размера на пиксела (фигура 4), което е визуално незначително. В този пример няма видими изкривявания, причинени от сферичността, за разлика от снимките, показани на фигура 2.



Фиг. 4 *Пример за виртуално изображение 90°×90° с цифрово наслагване*

Освен това изборът на такава схема за подреждане на оптични оси значително намалява времето за външна ориентация. Тъй като елементите на направляващата косинусова матрица за всички изображения, получени от една станция, са едни и същи и при преместване от изображение на изображение вътре в сканирането елементите на косинусовата матрица на посоката променят само своето местоположение и знак (Таблица 2), това значително намалява машинното време за математически операции, които могат да се извършват с виртуални изображения.

Таблица 2 *Изглед на матрицата от косинуси на посоката в рамките на едно сканиране за пет виртуални изображения*

номер на снимка	снимка 1	снимка 2	снимка 3	снимка 4	снимка 5
ъгъл на завъртане не снимката	$\chi = 0°$; $\tau = 0°$	$\chi = 90°$; $\tau = 0°$	$\chi = 180°$; $\tau = 0°$	$\chi = 270°$; $\tau = 0°$	$\chi = 0°$; $\tau = 90°$
вид на косинусиновата матрица	$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$	$\begin{vmatrix} -a_2 & a_1 & a_3 \\ -b_2 & b_1 & b_3 \\ -c_2 & c_1 & c_3 \end{vmatrix}$	$\begin{vmatrix} -a_1 & -a_2 & a_3 \\ -b_1 & -b_2 & b_3 \\ -c_1 & -c_2 & c_3 \end{vmatrix}$	$\begin{vmatrix} a_2 & -a_1 & a_3 \\ b_2 & -b_1 & b_3 \\ c_2 & -c_1 & c_3 \end{vmatrix}$	$\begin{vmatrix} a_1 & -a_3 & a_2 \\ b_1 & -b_3 & b_2 \\ c_1 & -c_3 & c_2 \end{vmatrix}$

Фокусното разстояние трябва да бъде избрано от по-нататъшните задачи, които трябва да бъдат решени. В първия случай, ако е необходимо изображения, получени от цифров фотоапарат да се наслагват върху виртуални изображения, т.е. да се получат виртуални изображения в реални цветове, тогава за тях е необходимо да се избере фокусно разстояние, равно на фокусното разстояние на насложеното цифрово изображения. Ако няма такава задача, тогава е по-целесъобразно да зададете кратно на 100.

Заключение

Казаното до тук дава основание да се заключи, че фотограметричните принципи за обработка на данни от наземно лазерно сканиране позволяват значително да се намали времето, прекарано на машината за конвертиране на виртуални изображения. Тъй като задачата за изчисляване на координатите на плоски виртуални изображения всъщност се свежда до изчисляване само на тангенси, т.е., като по този начин се намалява операцията на умножение по фокусното разстояние [4].

ЛИТЕРАТУРА

[1] Аналитические модели местности и снимков (макетные снимки) [Текст] / А. Н. Лобанов, В. Б. Дубиновский, А. И. Саранцев и др. – 2-е изд., пере-раб. и доп. – М.: Недра, 1989. – 140 с.

[2] Антипов, И. Т. Математические основы пространственной аналитической фототриангуляции [Текст] / И. Т. Антипов. – М.: Картгеоцентр – Геодезиздат, 2003. – 296 с.

[3] Лобанов, А. Н. Фотограмметрия [Текст]: учеб. для вузов / А. Н. Лобанов.– 2-е изд., перераб. и доп. – М.: Недра, 1984. – 552 с.

[4] Янчев, К. "Лазерното сканиране – постижимата прецизност в областта на фотограметрията, дистанционното наблюдение и геодезията", университетско издателство „Епископ Константин Преславски“, гр. Шумен, 2022, ISBN 978-619-201-573-2. 175 с.

[5] Янчев К., Кирилова К., Наземно лазерно сканиране. Шумен: Научна конференция с международно участие MATTEX 2022. Сборник научни трудове, Том 2, Шумен, ISSN: 1314-3921, стр. 226-230.

МОДЕЛИРАНЕ НА ОБУЧАВАЩА ИГРА ЗА TCP МЕХАНИЗЪМ

Валентин Т. Атанасов

LEARNING GAME FOR TCP MECHANISM MODELING

Valentin T. Atanasov

ABSTRACT: *Based on contemporary characteristic of the students which leading features has been formed by high technology environment, an game based approach in educational process is promoted. In this paper a modeling approach of learning game for TCP mechanism is presented. A learning game principles, paradigm and functional model are introduced.*

KEYWORDS: *Learning game, didactic model, educational process, system modeling, high interactive generation.*

Увод

Основавайки се на съвременната характеристика на обучаваните студенти[1,2,3], чиито водещи признаци са формирани от високотехнологоичното им обкръжение в съвременния свят и чиито възприятия са обусловени превалиращо от взаимодействието човек-машина, в настоящата статия се разглежда компютърна обучаваща игра(*обучаваща игра*) в учебния процес и прекият процес на нейното моделиране.

Обучението, базирано на игри все още се причислява към групата на иновативните подходи и без тенденция той да бъде отхвърлен[3] в бъдеше. Този подход не е самоцелен, а е в отговор на различните стилове на учене и предпочитания на дадено поколение обучавани. Това би включвало методи за комуникация, типове обратна връзка, степен на използване на технологии, дигитална социална свързаност[4].

Изследователите на обучаващи игри и тяхното приложение в лекционните зали, обаче, не могат да формират съществено окончателно заключение за ефективността и мотивацията на обучаваните в този игрово базиран процес, въпреки наличието на предпоставки, улесняващи обучението или учебния процес[5,6]. Основанието за приложението на обучаващи игри се опира на три фактора, влияещи върху разглеждания учебен процес – моделът на възприятия на съвременните обучавани[2], информационните и комуникационни технологии и произтичащите от това преки връзки с дигиталната същност на игрите[7].

В настоящата публикация се разглеждат принципите, парадигмата и функционалният модел на обучаваща игра, използваща TCP механизъм в компютърните комуникации. Една от основните цели на тази обучаваща игра е създаване на среда за обучение посредством игрови подход, с приложен дидактически модел.

Основни принципи в обучаваща игра за TCP механизъм

Водещ принцип при интегрирането на обучаващи игри в учебен процес, е че тези игри трябва да имат образователна цел, чието достигане се определя от ***дидактически модел с приложени педагогически принципи***[2].

Концептуализирано, в настоящата статия се представя подход за моделиране на обучаваща игра, определящ установяването на връзки между ненадеждни хостове и през ненадеждна Интернет комуникационна система, чрез използване на последователни номера, генерирани от управлявана с часовник схема, или т.н. „*тripътно ръкостискане*“. Поради възникването на механизми за атаки в TCP/IP базирани комуникации[8], се налага необходимостта от разработване на нов или изменението на съществуващ алгоритъм, съставляващ елемент от това трипътно ръкостискане. Един от тези алгоритми дефинира определянето на първоначален последователен номер (ISN). В настоящата статия не се разглеждат, респективно моделират, детайли в алгоритмите при определянето на ISN, а се извежда приложението на този ISN на абстрактно ниво, или иначе казано неговото предназначение.

Без да се омаловажава въпросът със сигурността на изградената комуникационна връзка, следва да се отбележи, че в бъдещите редакции на моделирането в разглежданата обучаваща игра, ще се включат операции, базирани на алгоритми, свързани със сигурността при определянето на този ISN. Това обстоятелство бива продиктувано от приетия тук когнитивен принцип в усвояването на нови знания, постановяващ „*От общото към конкретното*“, т.е. самият факт за използване на ISN следва да бъде валиден в когнитивен процес. А, на тази основа, в бъдещи етапи, да се разгръщат детайли, пряко обвързани с генерирането на ISN.

В този смисъл, първична цел на обучаваща игра в този мрежови домейн би следвало да бъде изграждането на устойчиви познания за процеса, установяващ връзка между непознати/ненадеждни хостове в TCP/IP базирана мрежова среда, допускаща възникването на събития, които биха могли да бъдат определени като „зловредни“ по отношение на поне една от предполагаемите две страни в тази комуникация.

Друг основен принцип при моделирането на обучаваща игра е разгръщане на ***игрово базиран учебен процес***, ***имплицитно свързан с теорията на потока***[9]. Съгласно тази теория се постига състояние на *завършена целеустременост* (autotelic) у обучавания, прилагащ игровия подход, когато предоставяните игрови възможности по отношение на функционалния, архитектурния, информационния, визуалния и потребителския дизайн съответстват на нивото на уменията на обучавания. Това се явява съществено обстоятелство, обуславящо достигането на ефикасност в учебния процес, базиран на обучаваща игра. На фигура 1 е представен модифициран вариант на модела, разглеждан в [9].

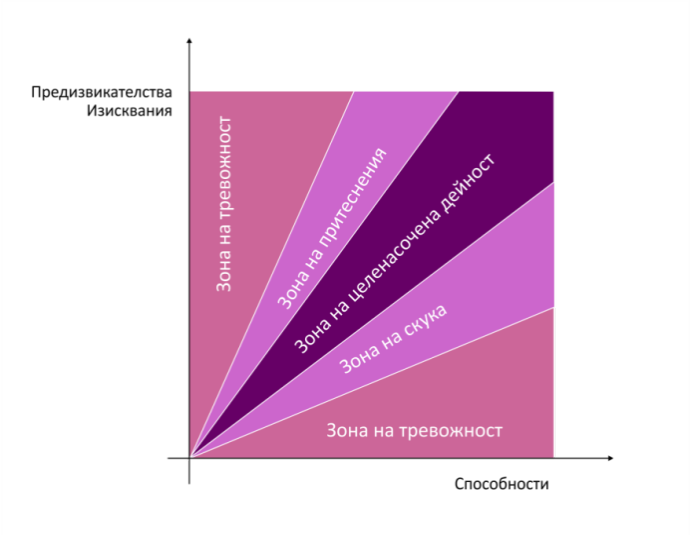
Парадигма на обучаваща игра за TCP механизъм

Може да бъде разглеждана следната комплексна парадигма на обучаващата игра, формализирана със средствата на предикатната логика.

$$\exists\, G_{learning}(d,t,i) \rightarrow (P_{actions}(t) = P_{actionscorrect}(t) + P_{actionserror}(t)) > 0 \rightarrow (A_{games}(t) = (A_{correcr}(t) + A_{error}(t))) \rightarrow P_{knowledge}(t) > 0, \quad (1)$$

където

$G_{learning}$ - Обучаваща игра за TCP механизъм.
d - Дидактически модел, интегриран в обучаващата игра.
i - Брой опити на обучавания с обучаващата игра за $i > 0$.
$P_{actions}(t)$ - Вероятност за функционално пълно множество от действия в обучаващата игра.
$P_{actionscorrect}(t)$ - Вероятност за правилни действия в обучаващата игра.
$P_{actionscorrect}(t)$ - Вероятност за неправилни действия в обучаващата игра.
$A_{games}(t)$ - Съвкупност от всички действия в обучаващата игра.
$A_{correct}(t)$ - Съвкупност от правилните действия в обучаващата игра.
$A_{error}(t)$ - Съвкупност от неправилните действия в обучаващата игра.
$P_{knowledge}(t)$ - Вероятност за получаване на знание посредством действия в игровия процес.



Фиг. 1. Зона на целенасочена дейност в обучаващата игра

Горното може да бъде формулирано по следния начин: Съществува такава обучаваща игра за TCP механизъм, при която има функционално пълно множество от правилни и неправилни действия, чието осъществяване би довело до когнитивен процес с вероятност по-голяма от нула, при поне един опит с тази обучаваща игра.

Следва да бъде отбелязано, че парадигмата дефинира изискване за придобиване на знания, както при правилни, така и при грешни игрови действия на обучавания. В този смисъл, следва да се разбира логиката при детерминирането на действието като грешно в контекста на причинно-следствената игрова връзка. Тоест, за да се постигне очакван игрови резултат(настъпи дадено игрово събитие), е необходимо действие, насочващо обучавания към текущи изводи, обусловени от неговите действия.

За пример би могло да се посочи следният фрагмент от игрови сценарий:

Ако обучаваният определи правилно „изисквания“ ISN в текущия игрови момент, то настъпилите игрови събития би следвало да утвърждават правилността на отговора чрез установяване на комуникационна връзка между двете устройства, последващото прехвърляне на данни към сървъра и стартиране на етап от стимулиращата игрова стратегия. Но, ако обучаваният установи, че не е изградена комуникационна връзка, няма прехвърляне на данни и не е стартиран никакъв етап от стимулиращата игрова стратегия, и съпътстващо има редукция на неговите игрови показатели, причината за това следва да бъде изрично ясна – неправилно определяне на ISN. Тази логическа обусловеност на действията следва дидактическия подход, интегриран в обучаваща игра, от една страна, а от друга е необходима валидност на теорията за потока[9].

Функционален модел на обучаваща игра за TCP механизъм

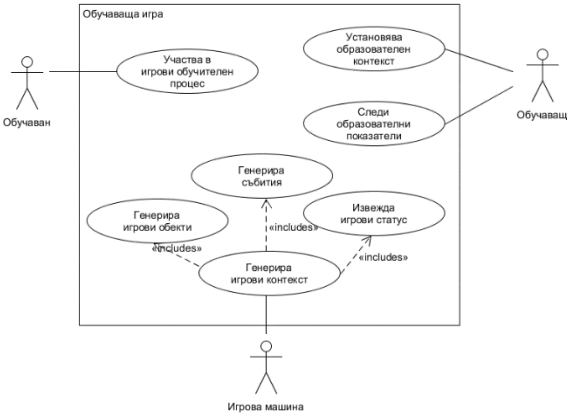
Систематизиран подход при изграждане на представа за функционирането на дадена система е нейното функционално моделиране. Взаимодействието с външни потребители(обучавани) следва да удовлетворява изискванията на тези потребители и то експлицитно в образователна среда. Добра практика при синтезирането на функционален модел са моделирането на взаимодействията между потребителите и системата, обособени в отделни случаи на употреба посредством използване на нотациите на унифицирания език за моделиране (UML)[10].

При използването на диаграми на случаи на употреба за разработваната обучаваща игра се формулира основен сценарий на успех.

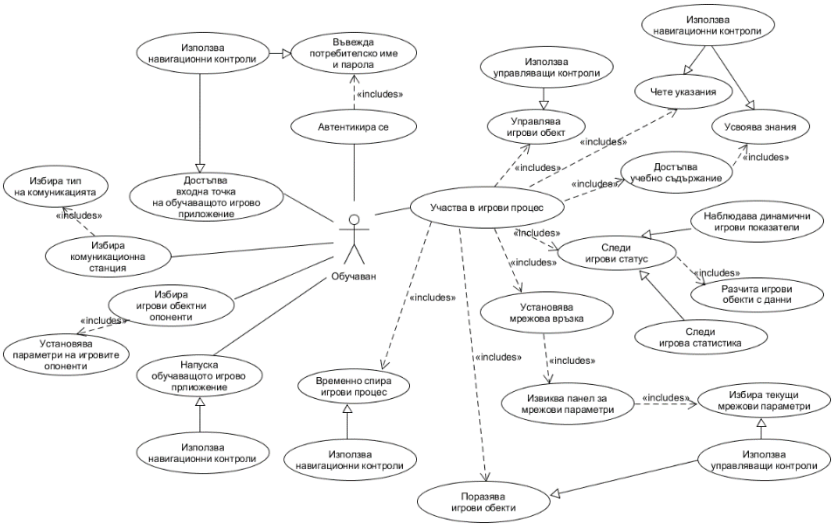
Обучаваният:

1. *достъпва приложението;*
2. *се вписва в системата;*
3. *избира тип на комуникацията;*
4. *избира комуникационна станция;*
5. *избира обектни опоненти;*
6. *установява игрови параметри;*
7. *започва игрови процес;*
8. *достъпва учебно съдържание;*
9. *достъпва указания;*
10. *следи игрови статус;*
11. *избира текущи мрежови параметри;*
12. *осъществява комуникационна сесия;*
13. *поразява игрови обекти.*

На фиг. 2 и 3 са представени случаите на употреба на обучаващата игра за TCP механизъм, като се разглеждат взаимодействията между системата и обучавания в определен контекст на употреба, параметри на игровото обкръжение и педагогически сценарий.



Фиг. 2.Функционален модел на обучаващата игра за TCP механизъм



Фиг. 3. Случаи на употреба в обучаващата игра за TCP механизъм (актьор обучаван)

Заключение

По своята същност разработката на обучаваща игра се опира на подхода за разработване на приложение, включваща основните етапи на даден процес на развойна програмна дейност. Поради широкото навлизане на технологии като повсеместен компютинг и мрежова свързаност е препоръчително интерфейсът на игровото приложение да се базира на УЕБ. Поради физическите ограничения за публикуване, не са представени по-разгърнати версии на моделите.

ЛИТЕРАТУРА

[1] Атанасов, В., „Измерване и оценка на образователна интерактивност на уеб базирани обучаващи приложения“, Международна научна конференция „Форум отбранителни технологии 2020“, 2020, стр.245-252, ISSN:2367-7902.

[2] Атанасов, В., „Алгоритъм и функционален модел за игрово базирана проверка на знания“, Годишник 2019, Издателство на Национален военен университет „Васил Левски“, Том I, 2019, стр.29-36, ISSN:1312 6148.

[3] Beloev, H., Smrikarov, A., Ivanova, A., Vassilev, T., Georgiev, T., Smrikarova, S., Ivanova, G., Stoykova, V., Ibryamova, E., Aliev, Y. and Zlatarov, P., A Vision of the University of the Future, In Proceedings of the 21st International Conference on Computer Systems and Technologies'20, 2020, pp.307-312, ISBN:9781450377683, doi:https://doi.org/10.1145/3407982.3408027.

[4] Brauner, Ph., Ziefle, M., Beyond playful learning – Serious games for the human-centric digital transformation of production and a design process model, Technology in Society, vol.71 article 102140, Elsevier Ltd., 2022, ISSN:0160-791X, doi: https://doi.org/10.1016/j.techsoc.2022.102140.

[5] Rahimi, S., Shute, V., J., Fulwider, C., Bainbridge., K., Kuba., R., et all, Timing of learning supports in educational games can impact students' outcomes, vol.190 article 104600, Computers & Education, Elsevier Ltd., 2022, ISSN:0360-1315, doi:https://doi.org/10.1016/j.compedu.2022.104600.

[6] Shorey, Sh., Chan, V., Rajendran, P., Ang, E., Learning styles, preferences and needs of generation Z healthcare students: Scoping review, Nurse Education in Practice, vol.57 article 103247, Elsevier Ltd., 2021, ISSN:1471-5953, doi:https://doi.org/10.1016/j.nepr.2021.103247.

[7] Mullen, J., Milechin, L., Milechin, D., Teaching and learning HPC through serious games, Journal of Parallel and Distributed Computing, vol. 158, Elsevier Ltd., 2021, pp.115-125, ISSN:0743-7315, doi:https://doi.org/10.1016/j.jpdc.2021.07.014.

[8] Gont, F., Bellovin, S., Defending against Sequence Number Attacks, Internet Engineering Task Force, 2012, ISSN:2070-1721, https://www.rfc-editor.org/rfc/pdfrfc/rfc6528.txt.pdf.

[9] Csikszentmihalyi, M., Flow: The Psychology of Optimal Experience, Harper Perennial Modern Classics, 2008, ISBN:978-0-06-133920-2.

[10] Fowler, M., UML Distilled: A Brief Guide to the Standard Object Modeling Language, Addison-Wesley Professional, 2018, ISBN-13: 9780134865126.

ПЛАНОВА И ВИСОЧИННА ГЕОДЕЗИЧНА ОСНОВА ЗА ТОПОГРАФСКА СНИМКА НА РЕКИ И ВЪТРЕШНИ ВОДОЕМИ

Евгени Гр. Стойков

PLANNING AND ELEVATION GEODETIC BASIS FOR TOPOGRAPHIC PHOTOGRAPH OF RIVERS AND INLAND WATERS

Evgeni Gr. Stoykov

ABSTRACT: *Geodetic networks in nature depend on many factors that ultimately determine their type and diversity. A major factor is the accuracy that they must satisfy when using them to solve various scientific and applied problems. The points of the supporting and working geodetic base form the so-called photographic base, from which a geodetic survey is carried out when creating a plan, map or digital topographic model.*

KEYWORDS: *Geodetic network, Photographic base, Plan, Map.*

Въведение

Вътрешните води на една държава представляват всички водни басейни, които са на нейната територия и до изходната линия, от която се измерва ширината на териториалното море.

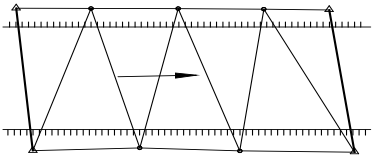
Проучването и заснемането на вътрешни водоеми се извършва при изработване на топографски план или карта на тези водоеми, при корекции на реки, изграждане на защитни диги, строителство на ВЕЦ, водоснабдяване на населени места, напояване и отводняване на големи райони, извършване на различни инженерно-строителни и монтажни работи по дъното на реки, езера, язовири, а също така и за поддържане на корабоплаването по вътрешните водоеми.

Плановата геодезична основа се състои от опорна и работна геодезична основа, включена в държавната геодезична мрежа. Изборът на метода за създаване на плановата основа зависи от размерите на района на снимката, характера на релефа, конфигурацията на водоема (язовир, река, езеро), който ще се заснема, застроеността, залесеността на района и т.н [1], [3].

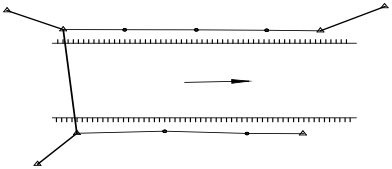
Изложение

Плановата опорна мрежа се създава като мрежа от триъгълници (фиг.1), чрез полигонометрични ходове (фиг.2), чрез верига от бездиагонални

четириъгълници (фиг.3), микротриангулация (фиг.4) и други геодезични построения.

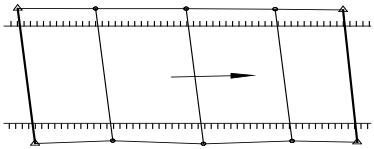


Фиг. 1. Мрежа от триъгълници

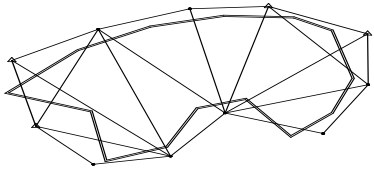


Фиг. 2. Полигонометричен ход

Точността в положението на новите точки трябва да отговаря на зададената, като всички етапи на проектиране, измерване, обработка на измерванията и изравнението по МНМК отговарят на посочените изисквания. Тази точност ще осигури изискванията на плановете и картите, за които тя се създава. Отделни опорни точки могат да се създават чрез прави, обратни и комбинирани засечки. Когато се заснемат малки части от реки или малки по площ водохранилища, координатите на точките от опорната геодезична мрежа се изчисляват в локална координатна система.



Фиг. 3. Верига от четириъгълници



Фиг. 4. Микротриангулация

Плановата работна геодезична основа се създава чрез полигонови ходове и мрежи и геодезични засечки, включени в опорната геодезична основа. Точността на работната геодезична мрежа се определя така, че да осигури точност ±1.5 mm в положението на заснетите точки, независимо от мащаба. Тази точност е достатъчна за проектиране на водохващания, корекции на реки и др. Когато тази основа се използва за снимка на широка ивица встрани от брега на реката, точността на плановата основа трябва да осигурява точността на топографските планове и карти на сушата [1], [3].

При условие че плановата работна основа се използва само за извършване на промерните измервания в реката, за които точността е до ±1.5 mm в мащаба на плана, средната квадратна грешка в положението на точките от работната основа трябва да бъде ±1.5 m за мащаб 1: 2 000, ±3.0 m за мащаб 1: 5 000 и ±5.0 m за мащаб 1 : 10 000. Най-често работната основа се създава чрез полигонови ходове

и микротриангулация. Дължините на полигоновите страни са до 200 – 300 m, като най-късата страна е 20 m, а най-дългата – 350 m [1].

Когато основата се създава чрез микротриангулация, ъглите трябва да бъдат между 30° – 150°, а страните да са по - големи от 150 m.

Плановата геодезична основа при снимки на магистрални канали се създава чрез полигонометрични ходове и чрез триангулация. Полигонометричните ходове са с дължина на страните от 0.5 до 1 – 2 km, които са включени в опорната геодезическа мрежа. Дължините на тези полигони достига до 15 – 30 km. Средните квадратни грешки на ъглите са 15^{cc} – 30^{cc}, а относителните грешки на полигонометричните ходове са от 1: 5 000 до 1:10 000. Когато плановата основа се изгражда като триангулация, дължините на страните са 1 - 5 km, ср.кв. грешка на измерен ъгъл е до 15^{cc} – 30^{cc}. При необходимост полигонометричните ходове и триангулачната мрежа се сгъстяват с теодолитни ходове с дължина на страните 200 – 500 m и относителна грешка 1: 2000. В някои случаи триангулацията може да се замени с микротриангулация с дължини на страните от 200 – 700 m и точност на измерените ъгли до 50^{cc} [1].

Снимките могат да бъдат [2]:

- Обща – при нея се изяснява общия характер на релефа на дъното;
- Подробна – извършва се в отделни райони с цел подробно заснемане на формите на релефа на дъното;
- Детайлна – прави се в отделни райони с цел да се покажат всички характерни форми на релефа с голяма подробност и точност.

За извършване на снимките се използват различни способи: промер, промер с инструментална оценка на релефа, площно обследване, аерофотоснимка, обследване с ехотралове и др [2].

Височинната геодезическа основа се създава чрез нивелачни ходове по дължината на реката, канала или чрез нивелачни мрежи.Тази основа се използва за извършване както на топографските снимки, така и за хидрографските измервания и снимки. Височините на точките от нивелачните ходове и мрежи се определят чрез геометрична и тригонометрична нивелация.

Класът на нивелачната мрежа се избира в зависимост от наклона на реката (табл. 1). Данните от тази таблица могат да се използват и при снимки на магистрални канали.

Таблица 1

Наклон на реката %	Клас на нивелацията
По-малко от 0.1	III клас
0.1-0.2	III клас
0.2-0.5	IV клас
Повече от 0.5	Техническа нивелация

Височинната геодезична основа при снимки на вътрешни водоеми се създава за:

- определяне на дълбочините на промерните точки;
- определяне на нивото на водата при хидроложките работи;
- определяне на нулите на водомерните постове;
- височинно привързване на инженерно – геоложките работи.

Етапите при създаването на височинната основа са:

- избиране, стабилизиране и извършване на нивелацията;
- създаване на водомерни постове и отчитане на нивото на водата;
- извършване на мигновени измервания и привеждането им към проектното ниво (нулата на дълбочините) на водата [1].

Избиране, стабилизиране на репери и извършване на нивелацията

Височинната мрежа се създава чрез трайно стабилизирани репери и временни репери. За да се осигури надеждно определяне на нивото на водата по цялото протежението на реката се избират и трайно стабилизират репери, Когато реката е с ширина до 600 – 800 m, тези репери се създават само от едната страна на реката, а при реки, по-широки от 800 m – по двата бряга, Изборът на местата на реперите зависи от геоморфоложките особености на брега. Реперите се стабилизират и нивелацията се извършва съобразно инструкциите за нивелация I – IV клас.

Временните репери сгъстяват височинната основа и се използват за определяне на нивото на реката. Тези репери се избират близо до водната линия и се стабилизират с дървени колове, бетонни блокчета, метални тръби, използват се опори на мостове, стълбове от електромрежата и други. Техническата нивелация се извършва чрез ходове, включени в нивелачните репери от по-висок клас или чрез нивелачни мрежи от затворени полигони [1].

Създаване на водомерни постове и отчитане на нивото на водата

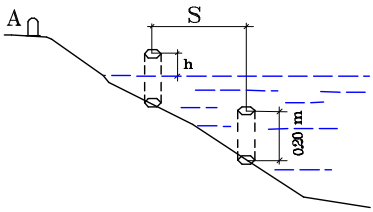
Релефът на дъното на вътрешни водоеми се изобразява с хоризонтали, изобати или чрез коти и дълбочини. Когато дълбочините се определят чрез промер, е необходимо да се знае нивото на водата. Нивото на водата и площта на водните басейни се определят чрез водомерни постове.

Водомерните постове се делят на основни, временни и подвижни.

Основните постове служат за непрекъснато регистриране на водното ниво и за осигуряване на хидроложка информация за вътрешните водоеми. В тях се поставя вертикална лата с деления през 2 cm, която се прикрепва неподвижно към масивни съоръжения на брега или във водата.

Нулата на латата е на 40 – 50 cm по-ниско от нивото на най-ниските води. Често в основните водомерни постове се поставят уреди за непрекъснато автоматично регистриране на нивото на водата, наречени лимниграфи. Котата на нулата на латата се определя чрез геометрична нивелация от най-близкия нивелачен репер [1], [3].

Временните водомерни постове се създават за по-детайлно измерване на нивото на водата в места с по-значително изменение на водния режим, в местата, където се трасират створовете за напречни профили на реката. Тези постове се стабилизират с колове през 60 – 80 m на различни нива по брега (фиг. 5) така, че горният край на по-ниско разположения кол да бъде на 0.20 m над терена. Котите на върховете на коловете се определят с геометрична нивелация от най-близкия репер. Нивото на водата се определя като се измери с милиметрова линия разстоянието *h* от кола, който е над нивото на водата [1].



Фиг. 5. Временните водомерни постове

Подвижните водомерни постове са лати или колове, които се поставят вертикално в района на снимката в защитено от вълнение място край реката, като нулата на латата (горния край на кола) се определя чрез геометрична нивелация. Котата на нивото на водата се отчита през 12 часа с точност до 1 cm.

Докато нивото на водата на морета, езера и язовири в няколко водомерни поста е приблизително еднакво, то нивото на водата в реките, поради наклона на реката, е различно. В реките се различават мигновено (работно) ниво и нула на дълбочините [1], [3].

Мигновеното (работно) ниво е нивото на водата в определен момент. В един и същ момент на различни водомерни постове по протежението на реката се определя котата на нивото на водата. При хидрографски снимки от мигновеното ниво се измерват дълбочините на точките до речното дъно, поради което това ниво се нарича още и работно.

За **нула на дълбочините** се приема нивото на водата към определен характерен момент на водния режим в зависимост от предназначението на плановете и картите. Най -често за нула на дълбочините се приема средното многогодишно ниво за летния период, най-ниското ниво или най високото ниво на водата в реката. Спрямо тази нула се надписват дълбочините на плановете и картите на вътрешните водоеми.

Във вътрешни водоеми, особено тези, които се използват за корабоплаване, вместо нула на дълбочините се използва т.н. проектно ниво. То се установява на базата на многогодишни наблюдения на водния режим на реката [1].

Заключение

Проучването на релефа при вътрешни водоеми (реки, язовири, езера и др.) се извършва с цел осигуряване на данни необходими при корабоплаване, инженерно-геоложки и хидротехнически проучвания, строителство на различни подводни и надводни съоръжения и др. Тези и други приложения на геодезията определят голямото значение на топографските планове и карти на вътрешните водоеми и свързаните с тях различни геодезични измервания и изчисления.

ЛИТЕРАТУРА

[1] Вълчинов В., Костадинов Т. Морска геодезия. София, УАСГ, 2000.

[2] Дачев Ю., Хидрографски системи, използвани за заснемане на релефа на дъното на българското черноморско крайбрежие, Списание „Геодезия, картография, земеустройство”, бр. 3 – 4, стр. 9 – 13, София, 2017, ISSN 0324-1610.

[3] Стойков, Е. Технически средства и системи при извършване на хидрографски измервания, Университетско издателство "Епископ Константин Преславски", Шумен, 2019, 177 стр., ISBN 978-619-201-334-9.

ЗА МРАВКИТЕ И ЛОГИСТИКАТА

Светлозар П. Стоянов, Йорданка И. Янкова-Йорданова

OF ANTS AND LOGISTICS

Svetlozar P. Stoyanov, Yordanka I. Yankova-Yordanova

ABSTRACT: *The current paper has a subject that is oriented towards the united systematic interrelatedness of the processes in the supply chain and the aim is to achieve effectiveness of the data in order to optimize the processes. In this relation, the aim is systematically, briefly and generally to present challenges and tendencies which the industrial companies face when achieving certain production provision.*

KEYWORDS: *Interrelatedness, Logistics, Implementation.*

Предмет на настоящата разработка е взаимосвързаността в единна информационна система на процесите по веригата на доставките.

Обект на предложената тематика е развитието в постигане на полезност от данните с цел рационализиране на процесите.

Целта на работата е систематизирано, накратко и в най-общ план да представи предизвикателства и тенденции пред индустриалните предприятия да постигнат съответна осигуреност на продукцията си.

Известно е че целенасоченото развитие на логистиката (тази част от управлението на веригата на доставките, която управлява ефективното и ефикасно право и обратно движение и съхранение на продукти и услуги и свързаната с това информация от мястото на зараждане до мястото на потребление с цел удовлетворяване на изискванията на клиентите) е в посоката на Индустрия 4.0, на Интернет на нещата и на Големите данни. Казаното предполага да се отбележи, че управлението на веригата на доставките е триединен процес на планиране, изпълнение и контрол (предварителен, текущ и последващ) на операциите по веригата на доставките, който има за цел да увеличи изгодата за крайните клиенти. В това направление доставчиците съединяват в единна информационна система (тя координира дейността на участниците, а това осигурява необходимия информационен обмен между тях, в резултат на който концепцията за управлението на веригата на доставките е приложима на практика) процесите по веригата на доставките (това е системата от организации, включени в процеса на създаването и реализацията на продуктите и услугите от пораждането им в стадия на добиване на суровините до тяхната доставка до крайния потребител) и така тази взаимосвързаност се анализира, допълва и търпи съответни промен [2, с. 38; 8, с. 25; 14, с. 271 – 272; 15, с. 7, с. 13, с. 18, с. 27, с. 33, с. 43, с. 48; 16, с. 64 – 65; 17, с. 40 (бел. 1), с. 147 (бел. 2) – 148 (бел. 1); 18, с. 255 – 256; 19, с. 12, с. 49, с. 186; 20, с. 44, с. 47 – 48, с. 52 – 53; 22, с. 11; 24, с. 31, с. 33, с. 38, с. 41; 25, с. 14 – 16; 27, p. 1; 28, p. 549 – 550; 29, p. 168].

По отношение на посочената взаимосвързаност проф. Михаел тен Хомпел от *Техническия университет – Дортмунд* (Федерална Република Германия, Дортмунд) посочва за образец принципа на предаване на информацията между мравките. Техният модел им дава възможност да устроят своето движение, впоследствие да бъдат анализирани възможните пътища и да се избере целесъобразният маршрут, ползван от целия мравуняк [2, с. 38; 9, с. 11 – 12].

Споменатият и известен метод на мравките (оптимизация с колония от мравки) [Ant colony optimization (ACO)] е характеризираща се с положително развитие съвкупност от начини и средства при извършване на определен тип дейност, т.е. различна степен на възможност за осъществяване на нещо, посредством подредена цялост от способи и похвати за пристъпване към определен сложен въпрос, който изисква разрешаване, а в случая решаване на изчислителни задачи, и който може да се сведе до откриване на добри пътища (най-къс или най-дълъг) през граф. Идеята е имитиране на поведението на мравките [те се движат по дъгите на граф, представляващ областта на възможните решения (фиг. 1.2), а стремежът на мравките е намиране на оптималното от тези решения (фиг. 1.3)], които координират своите действия благодарение на индиректната комуникация (мравките обменят информация индиректно, чрез полагане на феромон по пътя си), осъществявана с посредничеството на измененията на средата, в която те се движат. Това е самоорганизираща се система, основана на положителна обратна връзка (полагането на феромон привлича други мравки, които, следвайки следата, привличат други мравки) и на отрицателна обратна връзка (излиняването на пътя поради изпарение на феромона, което предотвратява системата да се препълни с информация и да се срине). В посока на казаното съществено е че индивидуално ограничените откъм когнитивни възможности мравки, взети заедно, откриват най-кратък път (фиг. 1.3) между източника на храната *[F]* и своя мравуняк *[N]*. Първата мравка (фиг. 1.1) установява източника на храна *[F]* по съответен начин *[a]*, като маркира пътя си, за да може да се върне, след което се завръща в мравуняка *[N]*, оставяйки след себе си следа от феромон *[b]* [1, с. 82 – 83, с. 84 (фиг. 2. 12), с. 86; 5, с. 16 – 17, с. 19, с. 21; 6, с. 33; 11, с. 4 – 6; 21, с. 17, с. 31; 23, с. 40, с. 41, с. 44, с. 45].

Представените постановки предполагат посочването на двата съществени акцента, т.е.:

а) вероятност на прехода – своето движение мравката осъществява от връх *[i]* до връх *[j]* на графа с различна степен на възможност за изпълнение:

$$p_{i,j} = \frac{(\tau_{i,j}^{\alpha})(\eta_{i,j}^{\beta})}{\Sigma(\tau_{i,j}^{\alpha})(\eta_{i,j}^{\beta})} \qquad (1)$$

където

$[\tau_{i,j}]$ е съответното количество феромон отговарящо на движението от връх *[i]* до връх *[j]*

$[\alpha]$ е величина за контрол на въздействието на $[\tau_{i,j}]$

$[\eta_{i,j}]$ е евристичната информация, която е предварително познание за задачата и в редица случаи е съчетание от величините на целевата функция и ограниченията

$[\beta]$ е величина за контрол на въздействието на $[\eta_{i,j}]$ [23, с. 47]

б) обновяване на феромона:

$$\tau_{i,j} = (1 - \rho)\tau_{i,j} + \Delta\tau_{i,j}^{k} \qquad (2)$$

където

[$\tau_{i,j}$] е съответното количество феромон отговарящо на движението от връх *[i]* до връх *[j]*

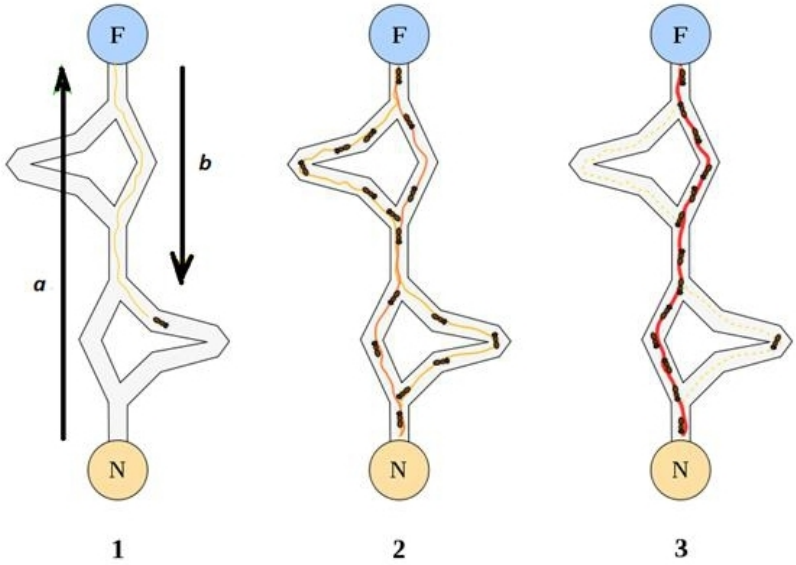
[ρ] е скоростта на изпарение на феромона

[$\Delta\tau_{i,j}^{k}$] е съответното количество новоотложен феромон от мравка с номер [k], традиционно представяно по следния начин:

$$\Delta\tau_{i,j}^{k} = \begin{cases} \frac{1}{L_k} (\text{при условие, че мравка с поредност } k \text{ премине по реброто } i,j) \\ 0 \qquad\qquad\qquad\qquad (\text{в противен случай}) \end{cases} \qquad (3)$$

където

[L_k] е стойността на целевата функция за решението, построено от *[k]* мравката, а (3) се отнася за случая на търсене на минималната стойност на целевата функция. При търсене на максималната стойност на целевата функция, в (3) е разположена стойността на целевата функция за решението, построено от *[k]* мравката, а не реципрочната ѝ стойност. Условие за построяване на решение от мравката (условие за край) е, когато е невъзможно добавяне на следващ връх в решението или това е, когато различната степен на възможност за следващо движение е равна на *[0]* [23, с. 47 – 48].



Фиг. 1. *Движение на мравчена колония [По Богданов, А. Решения в логистиката. Шумен, 2021, Печатна база на ШУ „Епископ Константин Преславски", с. 84 (фиг. 2. 12)]*

Казаното по-горе налага споменаването на т.нар. стигмергия, която е механизъм на непряка координация чрез околната среда, т.е. само мравка, която се намира на място, на което е положен феромон, получава информация от предходната мравка. Практически поради обратните връзки в системата, дори и слабите вариации в привлекателността на дадени пътища позволяват даден маршрут да бъде предпочетен, което с нарастващия брой на мравките, които го избират, води и до изявяването му като оптимален [1, с. 82 – 83, с. 84 (фиг. 2. 12), с. 86; 21, с. 17, с. 31; 23, с. 40, с. 41, с. 44, с. 45].

Посочената взаимосвързаност поражда и натрупва количество данни в мравешкото общество, а по същия начин и в човешкото общество. Проучвания сочат достигане на количество от 44 млрд гигабайта към 2020 г., което е почти 10 пъти повече, отнесено към първите месеци на 2016 г. Следователно данните се трансформират в съществено предимство за логистичната индустрия. В тази посока индустриалното предприятие [то е система, която определя начина на неговото управление (изграждане, функциониране и развитие)], което сполучи да придобие полезност от данните, напр. за рационализиране на процесите, ще е възможно да продължи да се котира [2, с. 38; 4, с. 29; 13, с. 91; 27, p. 1].

Индустриалните предприятия следва да постигнат осигуреност на продукцията си в бурно развиващата се електронна търговия, както споделя главният технолог в *Партньорска група Ерхард* (Федерална Република Германия, Бопард-Бухолц) Йенс Хайнрих, за да удовлетворят желанията на своите потребители. Пазарният растеж е следствие от все по-нарастващите потребителски желания и все по-нарастващата конкуренция. Това предполага необходимост от система за процесно изпълнение на веригата на доставки [Supply chain execution (SCE)]. Тя предоставя прозрачност в логистиката и използва събраните данни, за да оптимизира цялата верига и може да бъде сравнена с ERP [Enterprise resource planning (Планиране на ресурсите на предприятието)] системите, които са предназначени да автоматизират планирането, синхронизирането, контрола и анализа на бизнес процесите [2, с. 38; 3, с. 6 – 7; 4, с. 29; 7, с. 9; 8, с. 43 – 44 (фиг. 9); 10, с. 38; 12, с. 34 – 35; 26, p. 50; 27, p.1, p. 2].

Тенденцията е ежегодно нарастване в значителни размери на количеството данни. Посредством точните инструменти те могат да бъдат ползвани за бъдещи периоди. В тази посока анализът на бъдещите процеси следва да е неделима част от системата за процесно изпълнение на веригата на доставките. Именно изпълнението на веригата на доставките е едната част от триединния процес на управлението на веригата на доставките [2, с. 38 – 39; 27, p. 2 – 3].

Казаното се потвърждава от различни индустриални предприятия, които са разпознали съответния ефикасен процес на изпълнение. В тази посока и съответният софтуер за мобилни устройства е в синхрон с техните потребности. Споменатите индустриални предприятия са конкурентоспособни, а пример по отношение на това е т.нар. *Приложение за шофьор на камион Е+П* на *Партньорска група Ерхард*, което дава възможност за видимост на данните за поръчката, рационално пътуване и др. Информация или промени биват изпращани на мобилния телефон на шофьора. Използването на аналогични системи е възможно и в складовете, като предоставянето на изображения

значително ограничава неточности при изпълнение на поръчките. В тази посока Нилс Херцберг от *„Системи, приложения и продукти за обработка на данни“ АД* (Федерална Република Германия, Рейн-Некар-Крайс, Баден-Вюртемберг, Валдорф) допълва, че усвояването на знания за максимално оптимизиране на „пътя на мравките” в логистиката би ангажирало значителен бъдещ времеви период, което е предпоставка за разработване и на съответни типови предписания за изпълнение по определен начин [2, с. 39; 27, p. 3].

Представените дотук възгледи са подкрепени и от мнението на директора в *„Системи, приложения и продукти за обработка на данни“ АД за Югоизточна Европа и Общността на независимите държави* Александър Марочкин и експерта по продажби *за Централна и Източна Европа и Югоизточна Европа* в същото акционерно дружество Грегор Лонкар, които потвърждават, че взаимосвързаността в единна информационна система на процесите по веригата на доставките е предпоставка за видимост на всички дейности и конкурентоспособност на индустриалните предприятия. Посочената взаимосвързаност следва да се поддържа не само по отношение на веригата на доставките, но и на ниво управление на индустриалното предприятие [2, с. 38; 4, с. 29; 13, с. 91; 27, с. 1].

Обединяването и установяването на връзка между различните логистични процеси са подтик и възможност индустриалните предприятия да бъдат конкурентоспособни [2, с. 39; 27, p. 4].

ЛИТЕРАТУРА

[1] Богданов, А. Решения в логистиката. Шумен, 2021, Печатна база на ШУ „Епископ Константин Преславски”.

[2] Божилов, Н. Логистика 4.0 – данни, които говорят. – Списание „Транспорт и логистика”, Год. XII, Бр. 7, Септември 2016, София, „БТП – Българска транспортна преса” ЕООД, 38 – 39.

[3] Бонева, М., Петков, А., Недялков, А., Шелудко, И., Витлиемов, П. Приложение на интегрирани информационни системи за управление на процесите в организациите. Първо издание. Русе, 2017, Примакс ООД, Академично издателство „Русенски университет”.

[4] Василев, В. Как да изградим цифрова верига на доставки? – Списание „Транспорт и логистика”, Год. XVIII, Бр. 9, Ноември 2022, София, „БТП – Българска транспортна преса” ЕООД, 28 – 30.

[5] Георгиева, П. Генетичните алгоритми като средство за решаване на оптимизационни задачи. – Електронно списание „Компютърни науки и комуникации” на Център по информатика и технически науки на Бургаски свободен университет, Том 2, №3, Юли – Септември 2013, Бургас, Бургаски свободен университет, 16 – 23.

[6] Давидов, К. Управлението като теория породена от практиката. Шумен, 2020, Университетско издателство „Епископ Константин Преславски”.

[7] „Да изпреварим конкуренцията с bgERP”. Първо издание. Велико Търново, 2020, Експерта ООД.

[8] Драгомиров, Н. Информационни системи в логистиката – състояние и тенденции в използването. София, 2014, Издателски комплекс – УНСС.

[9] Желязкова, Д. Транспортът като ключова функция в логистиката. Варна, 2011, Издателство „Наука и икономика", Икономически университет – Варна.

[10] „Конвейерни системи за дистрибуционни и фулфилмънт центрове". – Списание „Инженеринг ревю", Брой 3, Май 2022, София, Издателска къща „Ти Ел Ел Медиа" ООД, 38 – 44.

[11] Марков, М. Лекции по Алгоритми. Работна версия 2021 година. София, 2021, Софийски университет „Св. Климент Охридски", Факултет по математика и информатика, Катедра „Математическа логика и приложенията ѝ".

[12] Николов, Д., Лазарова, М. Метаевристични методи за оптимизация при планиране на ресурси и управление на бизнес процеси. – Списание „Автоматика и информатика", Кн. №3, 2019, София, Съюз по автоматика и информатика „Джон Атанасов", 34 – 44.

[13] Николов, Х. Организационните структури в системите за управление – наука и практика в индустриалните предприятия. – Електронно списание „Диалог", Бр. 1, 31.03.2022, Свищов, СА „Д. А. Ценов" – Свищов, 82 – 100.

[14] Раковска, М. Теоретични аспекти на управлението на веригата на доставките. – Научни трудове на УНСС, Том 2, 2009, София, Университет за национално и световно стопанство – София, 247 – 290.

[15] Раковска, М. Управление на веригата на доставките. София, 2013, Издателски комплекс – УНСС.

[16] Раковска, М. Характеристики на управлението на глобалните вериги на доставките. – Списание „Икономически изследвания", Год. XIX, Кн. 1, 2010, София, Икономически институт на БАН, 61 – 100.

[17] Рибов, М. Дигитализацията – в преддверието на Индустрия 5.0. София, 2021, Издателски комплекс – УНСС.

[18] Рибов, М. Дигиталната трансформация. София, 2019, Издателски комплекс – УНСС.

[19] Рибов, М. Новите технологии. Следващото поколение. София, 2021, Издателски комплекс – УНСС.

[20] Тодоров, Ф.Проектиране на логистични системи. София, 2017, Издателски комплекс – УНСС.

[21] Трайков, М. Математически модели и алгоритми за предсказване на пространствената структура на протеини. Автореферат на дисертация за присъждане на образователна и научна степен „доктор". Благоевград, 2017, Югозападен университет „Неофит Рилски" – Благевград, Природо-математически факултет, Катедра „Информатика".

[22] Христов, В. Влияние на комплексното логистично обслужване върху развитието на взаимоотношенията с клиентите. Автореферат на дисертационен труд за присъждане на образователна и научна степен „доктор". Варна, 2018, Икономически университет – Варна, Факултет „Управление", Катедра „Маркетинг", Печатна база на Икономически университет – Варна.

[23] Шиндаров, М. Алгоритъм за оптимизиране по метода на мравките за построяване на безжични сензорни мрежи. Дисертация за придобиване на образователна и научна степен „доктор". София, 2014, Българска академия на науките, Институт по информационни и комуникационни технологии.

[24] Щерев, Н. Индустрията на България: между оценката на настоящето и очакванията за бъдещето. – Индустриален бизнес и предприемачество – иновации в науката и практиката, Сборник с доклади от международна научно-практическа конференция „Индустриален бизнес и предприемачество – иновации в науката и практиката" (финансирана по проект №НПК-237 със средства, отпуснати целево от държавния бюджет на Икономически университет – Варна за 2018 г.), Посветена на 70-годишнината от създаването на специалност „Индустриален бизнес и предприемачество" в Икономически университет – Варна, Варна, 2018, Печатна база на ИУ – Варна, Издателство „Наука и икономика", Икономически университет – Варна, 27 – 44.

[25] Щерев, Н. Индустрията на България: състояние, развитие и перспективи пред индустриалната политика. – Развитие на българската и европейската икономика – предизвикателства и възможности, Том 3, Сборник с научни изследвания от годишната конференция на Стопанския факултет на ВТУ „Св. св. Кирил и Методий", проведена на 17. – 18.10.2019 г. във Велико Търново, Велико Търново, 2019, (2020), Университетско издателство „Св. св. Кирил и Методий", 13 – 20.

[26] Kazakov, S. ERP systems in logistics and transportation. – International scientific refereed indexed online journal with impact factor "SocioBrains", 2020, Issue 69, 49 – 53, Smart Ideas – Wise Decisions Ltd., Bulgaria, Sofia.

[27] „Recognizing chances. Taking changes. Logistics 4.0 – smart, connected, digital". – Technical article, March 8th 2016, Boppard-Buhholc, (DE), Ehrhardt + Partner GmbH & Co. KG, 1 – 5.

[28] Sterev, N., Rosillo, H. Technology, innovations and industrial development. – Journal „Economic alternatives", Issue 4, 2019, Sofia, (BG), UNWE Publishing complex, 549 – 559.

[29] Vitasek, K. (compiler). Supply chain management. Terms and glossary. Laurel (Maryland, USA), 2013 (August), SOLE – The International Society of Logistics.

ЗА НЯКОИ ЖЕЛЕЗНИ СПЛАВИ, СТОМАНИ И ЧУГУНИ

Светлозар П. Стоянов, Георги П. Георгиев

FOR SOME IRON ALLOYS, STEELS AND CAST IRONS

Svetlozar P. Stoyanov, Georgi P. Georgiev

***ABSTRACT**: This article identifies the most important specifics of the iron-carbon system, the iron carbide, the iron graphite, the steel and cast iron. It analyses the previous research on the topic and focuses on the practical applications of these materials.*

***KEY WORDS**: Iron-carbon system, Iron carbide, Iron graphite, Steel, Cast iron, Practical application.*

Системата желязо-въглерод представя фазите (твърдите състояния) на желязото и неговите сплави във връзка с количеството на наличния въглерод [1, с. 15], като фазовата диаграма показва различните фази, които могат да съществуват в системата при различни температури и налягания, както и границите между тях. В тази посока съществените фази са:

• ферит – твърд разтвор на желязо и въглерод, който съществува при ниски концентрации на въглерод;

• аустенит – твърд разтвор на желязо и въглерод, който съществува при високи концентрации на въглерод;

• цементит – съединение на желязо и въглерод, което се образува, когато концентрацията на въглерод е между 0,8 и 6,67%.

Казаното предполага да се спомена и останалите елементи на структурата от фазовата диаграма на системата желязо-въглерод:

• перлит – евтектоид на метастабилната желязо-въглеродна система и представлява смес от два кристални вида: ферит (мек) и цементит (твърд).

• ледебурит – евтектум на метастабилната желязо-въглеродна система с 4,3% въглерод;

• графит – наблюдава се при стабилната желязо-въглеродна система, представлява една от двете кристални модификации на въглерода, като втората е диамантът.

Фазовата диаграма на системата желязо-въглерод показва също евтектоидната точка (0,8% въглерод) и евтектичната точка (6,67% въглерод), които са първостепенни в системата. Евтектоидната точка маркира границата между ферит и перлит (смес от ферит и цементит), докато евтектичната точка маркира границата между аустенит и цементит.

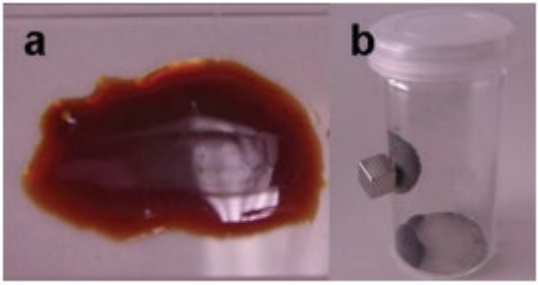
Железният карбид (Fe_3C) е химическо съединение, съставено от желязо и въглерод, известно още като цементит. Обикновено е сив или черен на цвят и се образува, когато желязото и въглеродът са в контакт при високи температури и налягания, а и обикновено се намира в малки, игловидни кристали.

Железният карбид се нарежда сред най-старите материали, известни на човечеството, като комбинацията от желязо и въглерод е открита още преди чистия метал и това, което древните култури са наричали „желязо“, в действителност е съставно съединение желязо/въглерод. Наличието на Fe_3C е потвърдено напр. в древната дамаска стомана [2], материал на 2500 години, използван за мечове и кинжали, поради специалните си свойства (напр. превъзходна твърдост и лекота).

Установен и представен е универсален начин за производство на значително разнообразие от метални нитриди и карбиди [3, 4], чиято ключова характеристика е образуването на гелообразен/стъклен изходен материал, съставен от полимерен комплекс между урея и металния прекурсор, който може директно да се преобразува с подходяща температурна обработка в съответните метални нитридни/карбидни наноструктури.

В стандартния експеримент на Джордано и др. [3, 4] претеглено количество твърд $FeCl_2{+}4H_2O$ се смесва с $Fe(CO)_5$ в моларно съотношение 2:1 и се разтваря в абсолютен етанол, което води до полупрозрачен тъмнокафяв разтвор. След това подходящото количество урея се добавя бавно към разтвора, за да се достигне крайното моларно съотношение урея/желязо (R) от 3. След разбъркване в продължение на 1 час и бавно изпаряване на разтворителя се образува тъмнокафяв гел (Фиг. 1a). Следва нагряване на пробите от гел при 700°C под поток от азот в продължение на 2 часа (плюс 1 час за достигане на крайната температура), като се получава (след охлаждане до стайна температура) сребрист/черен магнитен прах (Фиг. 1b).

Резултатът е „лесен за работа“ Fe3C прах, съставен единствено от наночастици, приготвен е по прост, бърз и сравнително евтин начин. От своя страна наночастиците са кристални, малки (вариращи от 5 до 10 nm в диаметър), суперпарамагнитни и стабилни при тежки химически условия. Комбинацията от изброените свойства прави тази система надеждна за различни приложения, напр. при съхранение на магнитни данни и за производството на нови ферофлуиди.



Фиг. 1. *a) оригиналният гел; b) суперпарамагнетични Fe3C наночастици след термична обработка*

Желязо-графитът е композитен материал, който се получава чрез комбиниране на желязо и графит, като графитните частици обикновено се добавят към желязото под формата на люспи или прахове. Композитите желязо-графит могат да бъдат направени чрез различни методи, като напр. прахова металургия, при която желязото и графитният прах се смесват заедно и след това

се пресоват в желана форма, или чрез инфилтрация, при която разтопеното желязо се излива в заготовка, направена от графит.

Желязо-графитните композити имат уникални свойства, които ги правят полезни в различни приложения. Графитните частици в композитния материал подобряват топлопроводимостта и електропроводимостта. Освен това, високата якост и устойчивост на желязото, съчетани с ниския коефициент на топлинно разширение и добрата обработваемост на графита, правят желязо-графитните композити полезни в приложения, където се изисква висока якост, устойчивост на износване и термична стабилност, като фрикционни материали, електроерозионна обработка и електромагнитни приложения.

Компактното графитно желязо (CGI) е вид желязо, което се използва в производството на двигателни блокове, цилиндрови глави и други компоненти за двигатели с вътрешно горене. Произвежда се чрез добавяне на графитни частици към желязото по време на процеса на леене, което подобрява здравината на материала, устойчивостта на износване и топлопроводимостта.

CGI е известно с неговото високо съотношение на якост към тегло, висока устойчивост и добра обработваемост.

Изследване на Сам и др. [5] установява, че CGI е поне 75% по-здраво от други сплави и е с поне 40% повече еластичност, когато се използва в дизеловите двигатели. Същото изследване показва, че дори и при слабо намаляване на количеството на титания (приблизително от 0,01 до 0,02%) води до намаляване на живота на режещите инструменти с 50%. Поради това и едно от заключенията на изследването е, че се налага въвеждането на инструменти за рязане с по-високо качество. В тази посока изследването на Гуо и др. [6] показва, че обработката с помощта на модулация (MAM) е доказана като ефективна за намаляване на износването на инструменти от кубичен борен нитрид (CBN) при обработка на CGI при високи скорости на обработка (500 м/мин).

Сплави до 2% въглерод се наричат стомани и се подразделят на следните групи:

• с по-малко от 0,008%C – ферит – технически чисто желязо;
• 0,008% до 0,83%C - подевтектоидни;
• 0,83%C – евтектоидна (перлитна) стомана;
• 0,83% до 2%C – надевтектоидна.

Една от най-употребяваните сплави на стоманата е неръждаемата стомана, характеризираща се с ниско съдържание на въглерод и съдържание на хром, от 10 до 30%.

В изследването „Неръждаема стомана в строителството: преглед на изследвания, приложения, предизвикателства и възможности“ [7] се описват някои от сферите, където неръждаемата стомата може да има съществено влияние:

• ядрени реактори – използването на модулни двуслойни композитни конструкции от неръждаема стомана-бетон- стомана може да намали времето за изграждане и да позволи по-тънка конструкция, отколкото иначе би се изисквало при използване на стоманобетон. Намаленото време за строителство често може да се окаже жизненоважно за търговската жизнеспособност на производството на ядрена енергия;

• производство на био-горива – типичното съоръжение за биогорива се състои от реактори, охладителни кули, котли, технологични тръби, технологични

и помощни помпи, резервоари за съхранение и топлообменни намотки и използва стотици тонове неръждаема стоманена ламарина, плочи и тръби.

Чугуните са желязо-въглеродни сплави със съдържание на въглерод от 2% до 6,67%. Според Български държавен стандарт (БДС) в зависимост от начина на термичната обработка ковкият чугун се дели на три групи:

• бял ковък чугун – КЧ35-4, КЧ40-5 (КЧ е ковък чугун; 50 е якост на опън; 5 е относително удължение в проценти);

• черен ковък чугун – КЧ30-6, КЧ35-10;

• перлитен ковък чугун – КЧ50-5, КЧ70-2.

Различни форми на чугун се намират в тръбите, машините, железопътната, автомобилната и енергийната промишленост, както и в готварството. Пазарният дял за пластичен чугун възлиза на около 25 милиона тона годишно въз основа на данните за Съединените американски щати (САЩ) за 2018 г. (Metalcasting Forecast and Trends, 2019), които със сигурност са представителни за световния пазар.

Една от употребите на чугун е в производството на дизелови двигатели. Независимо от навлизането на електрически автомобили на пазара, основен дял все още имат двигателите с вътрешно горене (90% от всички продажби) през 2020 г. [9]. От страна на търговските превозни средства, няма все още достатъчно добра алтернатива на дизеловия двигател за превоз на тежки товари на дълги разстояния и има широко разпространено мнение в индустрията, че дизеловият двигател ще доминира поне до 2040 г.

ЛИТЕРАТУРА

[1] William D. Callister, David G. Rethwisch. Materials Science and Engineering: An Introduction 9th Edition, Wiley; 9 edition (December 4, 2013), ISBN-13: 978-1118324578.

[2] A. A. Levin, D. C. Meyer, M. Reibold, W. Kochmann, N. Patzke, P. Paufl er, Cryst. Res. Technol. 2005, 40, 905.

[3] C. Giordano, C. Erpen, W.-T. Yao, M. Antoniett, Nano Lett. 2008, 8, 4659.

[4] C. Giordano, C. Erpen, W.-T. Yao, B. Milke, M. Antonietti, Chem. Mater. 2009, 21, 5136.

[5] Sahm, A., Abele, E., & Schulz, H. (2002). Materialwissenschaft Und Werkstofftechnik, 33(9), 501–506. doi:10.1002/1521-4052(200209)33:9 <501::aid-mawe501> 3.0.co;2-w.

[6] Guo, Y., Mann, J. B., Yeung, H., & Chandrasekar, S. (2012). Enhancing Tool Life in High-Speed Machining of Compacted Graphite Iron (CGI) Using Controlled Modulation. Tribology Letters, 47(1), 103–111. doi: 10.1007/s11249-012-9966-z.

[7] Anon, Stainless steel in construction: A review of research, applications, challenges and opportunities, Journal of Constructional Steel Research, Volume 64, Issue 11, 2008, pp. 1199 – 1206.

[8] Metalcasting Forecast and Trends, 2019. AFS, Schaumburg.

[9] Lacaze, J., Dezellus, O., 2021. Surface Tension, Interfacial Segregation and Graphite Shape in Cast Irons. Metallurgical and Materials Transactions B, Available Online at https://doi.org/10.1007/s11663-021-02352-x.

АКТУАЛНИ АСПЕКТИ НА РИСКОВЕТЕ ОТ ИЗПИРАНЕ НА ПАРИ

Цвета Т. Маркова, Николина М. Маркова

CURRENT ASPECTS OF MONEY LAUNDERING RISKS

Tsveta T. Markova, Nikolina M. Markova

ABSTRACT: *The report examines some aspects in the Action Plan to limit the risks of money laundering established by the National Money Laundering Risk Assessment prepared by a permanent inter-ministerial working group under Article 96 paragraph 1 of the Law on Measures Against Money Laundering.*

KEYWORDS: *risk assessment, money laundering.*

Увод

В България през 2012 г. е реализиран ръководен от Международния валутен фонд (МВФ) пилотен проект, чиято цел включва прилагането в множество държави на подход основан на риска, включително измерването на рисковете от изпирането на пари. За изработването на предварителната оценка е използвана методология разработена от МВФ. Беше направен основен извод, че големи количества финасови средства имат своя произход от ДДС измами. За справяне с този проблем между 2014 г. и 2018 г. бяха приети:

1. Стратегия за превенцията за изпиране на пари (2011-2015)
2. Стратегически насоки за превенция и противодействие на корупцията 2015-2020;
3. Стратегия за националната сигурност 2011-2020;
4. Актуализирана Стратегия за национална сигурност 2018-2025;
5. Интегрирана стратегия за превенция и противодействие на корупцията и организизираната престъпност;
6. Стратегия за превенция на престъпността (2012-2020);
7. Национална стратегия за киберсигурност "Кибер устойчива България 2020".

Доклад за Националната оценка на риска

Националната оценка на риска за 2019 г. приключва с Доклад, който по своята същност представлява инструмент за подпомагане на публичния и частния

сектор при формулирането за заплахите и мерките за борба с тях. С приемането на този доклад Република България изпълни изискванията на FATF* и на ЕС†

Докладът за Националната оценка на риска се предшества от анализ на рисковете от изпирането на пари, вклюващ анализи, както следва: на заплахите от предикатната престъпност, като основен източник на средства; на субектите, извършващи дейностите по изпирането на пари; на икономическите сектори, свързано с изпирането на пари; на финансовия сектор и на сектора на нефинансовите бизнеси и професии, които се използват за изпирането на пари; на трансграничните характеристики на изпирането на пари.

Националната оценка на риска регистрира тридесет и две рискови събития за изпиране на пари. Основните от тях са: Изпиране на пари от предикатни престъпления, извършени в България или в чужбина, свързано с организирана престъпност – наркотици, трафик на хора и данъчни престъпления, вкл. избягване на данъчни задължения, чрез използване на парични средства в брой; Изпиране на пари от корупция, вкл. имущество, придобито от незаконосъобразни обществени поръчки и фондове на ЕС чрез използване на "професионални перачи" и интегриране на ресурса във финансови инструменти, в юридически лица и недвижими имоти; Изпиране на пари от данъчни престъпления чрез подставени лица – местни и чуждестранни юридически лица при използване на схеми за разслояване; Интегриране на местни и чуждестранни лица на изпрани средства в строителството и в недвижими имоти, използвайки сивата икономика; Изпиране на пари, получени от предикатни престъпления чрез използване на небанкови инвестиционни посредници или на нерегулирана търговия с финансови инструменти; Изпиране на пари от избягване установяване на данъчни задължения и от измами с ДДС при търговията с храни и горива чрез подставени лица и "кухи" компании в корупционна среда и на фона на "сивата икономика"; Изпиране на пари от компютърни измами и измами тип "социално инженерство" чрез раслояване на средства; Като основен риск се наблюдава въвличането на задължени лица и професионалисти по Закона за мерките срещи изпирането на пари (ЗМИП) чрез злоупотреба с режимите на регистриране и лицензиране.

В изпълнение на Закона за мерките срещу изпирането на пари от март 2018 г.и на осн. Чл. 96 с Решение № 314 от 20.05.2019 г. на Министерски съвет, изменено с Решение № 523 от 02.09.2019 г. е създадена постоянна междуведомствена работна група за оценка и управление на риска, председателствана от от Директора на САД ФР – ДАНС, включваща директорите на съответните дирекции от ДАНС, МВР в лицето на Главна дирекция "Борба срещу организизираната престъпност", Главна дирекция "Национална полиция", НАП, Агенция "Митници", МФ, МП, ВКП, БНБ, КФН, КПКОНПИ. Националната

---

* Препоръка 1 на FATF

† Чл. 7 от Директива (ЕС) 2015/849 на Европейсския Парламент и на Съвета от 20.05.2015 г.за предотвратяване използването на финансовата система за изпирането на пари, за изменение на Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета и за отмяна на Директива 2005/60/ЕО на Европейския Парламент и на Съвета и на Директива 2006/70/ЕО на Комисията (ОВ, L 141/73 от 05.06.2015 г.)

оценка на риска е изготвена въз основа на информацията получена от всички посочени по-горе служби, органи и институции.

През 2019-2021 г. са предприети законодателни действия целящи ограничаването на рисковете констатирани в Доклада за националната оценка на риска сред които и, но не само "*законодателни и институционални действия за осигуряване на своевременен достъп до точна, подходяща и актуална информация за действителна собственост, съхранявана от централните регистри (което води и до своевременна идентификация на видни политически личности (ВПЛ) и техните роднини и близки сътрудници, когато участват в юридически лица като действителни собственици и на нерезиденти когато участват в юридически лица като действителни собственици*)". Информацията за действителна собственост се вписва в Търговския регистър и регистъра за юридическите лица с нестопанска цел, съответно Регистър БУЛСТАТ.

На следващо място, бяха предприети законодателни промени с цел гарантиране получаването на пълна и вярна информация за задължените лица по ЗМИП и от техните клиенти – юридически лица, които са собственост на близки сътрудници и роднини на видни политически личности (ВПЛ). Една от мерките например е задължението на БНБ от 2019 г.по чл. 56а, ал. 1 от Закона за кредитните институции да създаде електронна информационна система за банковите сметки и платежните сметки с IBAN (международен номер на банкова сметка) не само в банки, но и в дружества за електронни пари и платежни институции, за титулярите, пълномощниците, действителните собственици, за наематели на сейфове, респ. пълномощниците им. С установяването на това изискване всички лицензирани от БНБ платежни институции и дружества за електронни пари предоставят на регистъра информацията за своите клиенти. Задължените лица по ЗМИП ползват списъка с висши държавни длъжности на КПКОНПИ. Лицензионният и регистрационният режим като контролна функция на Комисията за финансов надзор предотвратяват риска от притежание на финасови институции от лица с престъпни прояви.

Промените в регулаторната рамка са насочени към минимализиране на предлагането на анонимни продукти чрез

- **Наредба № 3 на БНБ от 18.04.2018 г.относно условията и реда за откриване на платежни сметки, за изпълнение на платежни операции и за използване на платежни инструменти**, която регламентира уникалния идентификатор на платежната сметка за електронни пари. От 01.01.2020 г.платежните сметки се обозначават от доставчиците на платежни услуги с уникален IBAN.
- **Наредба № 12 на БНБ от 29.09.2016 г. за Регистъра на банковите сметки и сейфове.** След измененията от 10.09.2020 г. се регламентира пълният обем информация, която Регистърът предоставя относно всички реквизити на сметката.
- **Плащания в трети държави с анонимни предплатени карти** се приемат само ако тези карти отговарят на изискванията на чл. 24, ал. 1 и ал. 2 от ЗМИП.

С цел извършването на комплексна проверка в условията на физическо отсъствие на клиента задължените лица по ЗМИП са задължени да притежават вътрешни системи за идентификация, както и за проверка на идентификацията.[*]

С цел установяване на еднакво разбиране на понятието виртуална валута през 2020 г. беше въведена законова дефиниция в ЗМИП.[†] Тя гласи, че ***виртуална валута*** е цифрово представяне на стойност, която не се емитира или гарантира от централа банка или от публичен орган, не е свързана със законово установена валута и няма правния статут на валута или на пари, но се приема от ФЛ и ЮЛ като средство за обмяна иможе да се прехвърля, съхранява и търгува по електронен път. Чрез транспонирането на Петата Директива за мерките срещу изпирането на пари[‡] са въведени две нови категории задължени лица:

1.Лица, които по занятие предоставят услуги за обмяна на между виртуални валути и признати валути без златно покритие и

2.Доставчиците на портфейли, които предлагат попечителски услуги.[§]

За тези две нови категории задължени лица са приложими всички мерки – комплексна проверка на клиента, опростена и разширена коплексна проверка, собствена оценка на риска за изпиране на пари, подаване на уведомления за съмнителни клиенти и др.

Специално внимание е обърнато на дейността и контролните правомощия на Комисията за финансов надзор. С цел оптимизиране на контролната фунция на КФН през 2021 г. комисията е изготвила Наръчник относно сектор "Застраховане" за риск-базиран надзор за превенция на изпирането на пари и финансирането на тероризма. КФН събира информация веднъж годишно чрез използването на въпросник за прилагането на ЗМИП, ППЗМИП и Закона за мерките срещу финансиране на тероризма (ЗМФТ) и формуляр за статистическа информация. Направена е препоръка информацията да се събира два пъти годишно за сектор "Търговия с финансови инструменти". През същата 2021 г. Дирекция "Специфични надзорни дейности" е предприела още две други действия, а именно

- актуализиране на Вътрешните насоки за основан на риска надзор на банките и
- актуализиране на Методологията на БНБ за оценка риска на банките.

Банките предприеха също мерки в посока на институционалнато укрепване на техния капацитет. Увеличиха броя на служителите и проведоха обучения в звената за борба с изпирането на пари. Вложиха значителен финансов ресурс инвестиран за специализиран софтуер. БНБ въведе въпросник за рисковите фактори в областта на изпирането на пари, който платежните институции и дружествата за електронни игри попълват всяка година от 2019 г. На базата на получената информация от този въпросник БНБ прави анализ.

Ефективността на работата на САД Финансово разузнаване – ДАНС беше подобрена след влизане в сила на новия Закон за мерките срещу изпирането на пари чрез новата методология за оценка на риска на основа на опита придобит при използваната в периода 2011-2018 г.методология. Така методологията е била

---

[*] Чл.41, ал. 3 от Правилника за приложение на Закона за мерките срещу изпирането на пари;

[†] §1, т.24 от Допълнителните разпоредби на ЗМИП;

[‡] Директива (ЕС)2018/843 на Европейския парламент и на Съвета;

[§] Чл. 4, 38 и т.39 от ЗМИП;

актуализирана през 2019 г. САД ФР – ДАНС е въвела методология за оценка на риска на обменните бюра и критерии аз избор на лица за проверка.

На БНБ бяха възложени функции за надзорна дейност по ЗМИП относно кредитните институции, които извършват дейност на територията на Република България по смисъла на Закона за кредитните институции[*], както и клонове на кредитни институции от трета държава. Бяха възложени надзорни функции по ЗМИП и на КФН по отношение на другите доставчици на платежни услуги по смисъла на Закона за платежните услуги и платежните системи и техните представители[†].

През 2019 г. бяха въведени административно-наказателни правомощия за Държавната комисия по хазарта[‡], които през 2020 г. преминаха към Националната агенция за приходите.

В областта на засилване на сътрудничеството между различните надзорни органи са били подписани две инструкции за извършване на съвместни проверки от САД ФР-ДАНС и БНБ и от САД ФР-ДАНС и КФН, а от 2021 г. и инструкция за съвместни проверки на ДАНС и НАП.

САД ФР-ДАНС е издала през 2020 г. и през 2021 г. актуализирала указания за идентифициране на клиенти-ФЛ и указания за коплексна проверка на видни политически личности.

САД ФР-ДАНС е надзорен орган по мерките срещу изпиране на пари. Ефективният надзор изисква реален достъп до информация относно онлайн хазартните услуги. На 21.06.2021 г. е изтекъл срокът за подаване на информация за онлайн хазартните игри към централния сървър на на НАП. САД ФР-ДАНС има достъп до сървърите на три от седемте лицензирани лица, които организират онлайн хазарт. Направена е препоръка за повишаване на осведомеността при установяване произхода на средствата чрез комплексни съвместни проверки.

Изцяло нов момент в работата на надзорните и контролните органи беше установяване на сътрудничество между САД ФР-ДАНС с Висшия адвокатски съвет и Нотариалната камара чрез разработването на правила за адвокати и нотариуси зе целите на превенцията на изпирането на пари. Чрез обучения беше обърнато специално внимание на уведомления за съмнителни операции, сделки и/или клиенти за установяване произхода на средствата.

Друг аспект за повишаване на институционалния капацитет на САД ФР-ДАНС е разширяване сътрудничеството с професионалните организации на одитори и счетоводители. САД ФР-ДАНС е разработила примерни вътрешни правила. Има принципно два подхода по отношение на външните счетоводители, а именно: изработването на собствени вътрешни правила или допълването на примерните вътрешни правила със собствени оценки на риска.

Отдел "Икономическа престъпност и и сътрудничество" на Съвета на Европа съвместно с Междуведомствената работна група за Националната оценка на риска изпълняват проект, стартирал през 2020 г., финансиран по РЕГЛАМЕНТ (ЕС) 2017/825 от 17.05.2017 г.Проектът разработва анализи за

[*] Чл.4, т.1, предложение второ ЗМИП;
[†] Чл.108, ал. 6, т. 2 ЗМИП;
[‡] Чл. 108, ал. 6, т.3 ЗМИП;

сектора на виртуалните валути, схемите за инвестиции срещу гражданство и сектора на юридическите лица с нестопанска цел (ЮЛНЦ).

България е поела ангажимент да имплементира в националното законодатекство новите разпоредби на Европейския съюз – Регламент (ЕС) 2018/1672 на Европейския парламент и на Съвета от 23.10.2018 г., който се отнася до контрол на паричните средства, които се внасят в държава член на ЕС или се изнасят от нея, т.е. от ЕС. Разширена е представата за парични средства чрез обхващане на стоки като високоликвидни средства за съхраняване на стойност. В Регламент (ЕС) 2018/1672 е разширено понятието чрез включване на парични средства внасяни или изнасяни в ЕС посредством пощенски или куриерски пратки или като непридружен багаж, или товар в контейнери. В тези случаи се изисква от изпращача Декларация за оповестяване. Митническите органи имат паво да задържат паричната пратка ако липсва декларация или има съмнение, че те са от престъпна дейност.

ДАНС е предприела извършването на действия за разширяване на публично-частното партньорство. В раздел "Мерки срещу изпирането на пари и финансиране на тероризма" на страницата на ДАНС е публикувана Методология за оценка на риска на ЮЛНЦ.[*]

Специално внимание се обръща на въпроса за повишаване на информираността на обществото относно рисковете за изпиране на пари. КФН и САД ФР-ДАНС разработват материали за обучение, които предоставят на банките и всички задължени лица. БНБ лидерства процеса на законодателните промени.

Може да се направи извод, че обществото няма достатъчно информация относно търговията с ценни книжа, което е причина за големия брой измами от търговия с ценни книжа от нерегулирани субекти. Направен е извод в посока на необходимостта от повече информация на достъпно ниво за повишаване на културата в областта рисковете в областта на изпирането на пари.

САД ФР-ДАНС като финасово-разузнавателен орган е предприела редица оперативни действия за идентифициране на злоупотреби с финансови средтсва за изпиране на пари като резултат от депозити и теглене на пари в брой от банкови сметки на ЮЛ, измами с ДДС и регистриране на фиктивни обороти, използване на парични средства вместо банкови разплащания, сива икономика, трансграничен пренос на парични средства натрупани от престъпна дейност.

През програмния период 2014-2020 г. Европейската комисия беше отправила препоръка да се избягва концентрацията на средства в едни и същи бенефициенти. За изпълнение на тази препоръка бяха променени условията за кандидатстване. Беше въведено изискване към бенефициентите, които са спечелили проекти по програмата "Развитие на конкурентоспособността на българската икономика" над посочен праг да не могат да кандидатстват по Оперативна програма "Иновции и конкурентоспособност". Това ограничение даде възможност на повече ЮЛ и ЮЛНЦ да кандидатстват. Бяха намалени също така

[*] https://dans.bg/bg/msip-091209-menu-bul

административните процедури чрез въвеждането на електронно подаване на документи по проекти и електронното отчитане.

По "презумпция" процедурите по Закона за обществените поръчки (ЗОП) създават предпоставки за корупционни нагласи. Чрез въвеждането на електронно възлагане със законодателните промени през 2019 и 2020 г. се постави началото на преодоляване на проблемите в "in-house" процедурите или т.нар. "вътрешно възлагане" чрез отстраняване на непълнотите в ЗОП по препоръка на ЕК.

За оптимизиране на регулаторната рамка на търговията и преработката на нефтени продукти през 2019 г. е приет Закон за административното регулиране на икономическите дейности, свързани с нефт и продукти от нефтен произход (ЗАРИДСНПНП), които е насочен към гарантиране на по-голяма сигурност в търговията с нефтени продукти и респ.предвидимост и сигурност в енергетиката.

С цел увеличаване на административния капацитет през 2015 г. е създаден Междуведомствен център за контрол и надзор на дружествата търгуващи с акцизни стоки, който реално функционира от 2017 г. с участието на МВР, ДАНС, НАП и Агенция "Митници". Компетентността е в областта на разследването на данъчни престъпления.

Приет е План за изпълнение на мерки в отговор на препоръките и посочените предизвикателства в Доклада на Европейската комисия от 30.09.2020 г. относно върховенството на закона за 2020 г., Ситуация в областта на върховенството на закона в България. Планът е одобрен с Решение на Министерски съвет № 806 от 06.12.2020 г.

През следващата година е приета новата Национална стратегия за превенция и противодействие на корупцията в България* с Решение на МС № 235 от 19.03.2021 г.Въведени са седем приоритета:

1. Противодействие на корупционните престъпления;
2. Укрепване капацитета и подобряване работата на органите, натоварени с контролни и санкционни правомощия в администрацията;
3. Повишаване прозрачността и отчетността на местната власт;
4. Освобождаване на гражданите от "дребната" корупция
5. Създаване на среда за обществена нетърпимост към корупцията;
6. Своевременен отговор на необходимостта от актуализация на антикорупционните мерки, заложени в националната стратегия за превенция;
7. Противодействие на корупцията, включително в отговор на препоръки от международни институции.

Осъществяването на приоритетите се предхожда от Пътна карта, съдържаща мерки, действия, индикатори и срокове.

*Продължение на предишната Национална стратегия за превенция и противодействие на корупцията в България 2015-2020 г.

Предприети са действия, насочени към подобряване на сътрудничеството между ведомствата относно изпирането на пари чрез приемане на междуведомствени подзаконови нормативни актове.[*]

Изводи и препоръки

Разгледаните по-горе мерки представляват добра основа за постигане на значителни резултати в дейността на институциите, на държавните органи и органите от съдебната власт, насочена към превенцията и мерките срещу изпирането на пари. За постигането на видими резултати, които да бъдат реално усетени от обществото, трябва да се продължи процеса на надграждане на законовата и подзаконовата регулаторна рамка. Следва да продължат усилията в посока на укрепване на административния капацитет на органите. За установяване на обществено доверие към институциите в областта на превенцията и мерките срещу изпирането на пари, следва да бъде гарантирана тяхната деполитизация и независимост от политически фактори. Използването на органите, натоварени с функции срещу изпирането на пари за политическа репресия срещу опонента поставя под съмнение обективността и стабилността на актовете им. На следващо, но не на последно място е дейността по обучение, както на служителите и магистратите, така и повишаване информираността на цялото общество за непрестанните усилия с цел промяна на нагласите на всеки субект и изграждане на безкомпромисна обществена нетърпимост към всички форми и дейности насочени към изпиране на пари.

[*] Инструкция № 2 от 05.09.20218 г.за взаимодействие между КПКОНПИ и Прокуратурата на РБ по ЗМИП;
Инструкция № 1 от 08.04.2020 г. за взаимодействие между КПКОНПИ, МФ, МВР, ДАНД и Инспектората към ВСС;
Споразумение между Прокуратурата на Република България и Сметната палата от 15.01.2019 г.

ИДЕНТИФИКАТОР НА ПОЗЕМЛЕН ИМОТ. СЪЩНОСТ И ПРЕДНАЗНАЧЕНИЕ

Мирем Е. Ниязи-Юсуф

PROPERTY IDENTIFIER. NATURE AND PURPOSE

Mirem E. Niyazi-Yusuf

ABSTRACT: *The identifier is a unique number of the property, which is given to each immovable property - an object of the cadastre and includes the code of the settlement in whose territory the property falls, the number of the cadastral region on the cadastral map and the number of the land property.*

KEYWORDS: *cadastre, map, property identifier.*

Агенцията по геодезия, картография и кадастър дава идентификатор на поземлен имот и го нанася в кадастралния регистър на идентификаторите и промените им. Идентификаторът е уникален номер, чрез който поземленият имот се посочва еднозначно за територията на страната.

Идентификаторът се състои от три до пет цифрови полета, подредени по йерархични нива съгласно приложение № 1 от [4].

Йерархичните нива се подреждат в низходящ ред, както следва:

1. Първото поле на идентификатора се състои от 5 цифри. В него се записва кодът на населеното място съгласно Единния класификатор на административно-териториалните и териториалните единици (ЕКАТТЕ) на населеното място, на чиято територия се намира недвижимият имот;

2. Във второто поле на идентификатора се записва номерът на кадастралния район, който не може да бъде нула.

При създаване на кадастралната карта и кадастралните регистри с данни от картата на възстановената собственост при липса на дублиране номерата на масивите се приемат за номера на кадастрални райони.

3. В третото поле на идентификатора се записва номерът на поземлен имот, намиращ се в кадастрален район, чийто номер е записан във второто поле.

При създаване на кадастралната карта и кадастралните регистри с данни от картата на възстановената собственост при липса на дублиране номерата на имотите от картата на възстановената собственост се приемат за номера на поземлените имоти. Поземлените имоти в масив с номер „0“ (нула) в картата на възстановената собственост се включват към съседни на имота кадастрални райони.

При създаване на кадастралната карта и кадастралните регистри с данни от кадастралните планове при липса на дублиране планоснимачните номера на имотите се приемат за номера на поземлените имоти.

4. В четвъртото поле на идентификатора се записва номерът на сграда или номерът на съоръжение на техническата инфраструктура, в което има самостоятелен обект.

Сграда или съоръжение на техническата инфраструктура, в което има самостоятелен обект, разположени в повече от един поземлен имот и не може да се определи принадлежността им към поземлен имот, се номерират в обхвата на кадастралния район, като в третото поле на идентификатора се записва цифрата нула;

5. В петото поле на идентификатора се записва номерът на самостоятелен обект в сграда или в съоръжение на техническата инфраструктура.

Идентификаторът се изписва в кадастралния регистър на недвижимите имоти, в регистъра на идентификаторите и промените им, в официалните документи и справки, издавани от службата по геодезия, картография и кадастър и от Агенцията по геодезия, картография и кадастър, в част „А“ на партидите на недвижимите имоти от имотния регистър, в актовете, с които се признава или прехвърля правото на собственост или се учредява, прехвърля, изменя или прекратява друго вещно право върху недвижимите имоти, както и в други случаи, определени с нормативен акт.

При създаване на кадастралната карта и кадастралните регистри по реда на чл. 35 и 35а от Закона за кадастъра и имотния регистър (ЗКИР) идентификаторите се формират от правоспособното лице, определено със заповедта за създаването им, след съгласуване на проекта за определяне на кадастралните райони със службата по геодезия, картография и кадастър по местонахождение на обекта.

При създаване на кадастралната карта и кадастралните регистри по реда на § 33 от преходните и заключителните разпоредби към Закона за изменение и допълнение на ЗКИР (ДВ, бр. 57 от 2016 г.) идентификаторите се формират от Агенцията по геодезия, карто-графия и кадастър.

Идентификаторите на недвижимите имоти се одобряват със заповедта за одобряване на кадастралната карта и кадастралните регистри и се съхраняват в регистъра на идентификаторите чрез информационната система на кадастъра.

При поддържане на кадастралната карта и кадастралните регистри идентификаторите се генерират от информационната система на кадастъра. В проекта за изменение новите обекти на кадастъра имат временни номера, които са уникални за проекта.

Временният номер има йерархична структура се състои от две до пет цифрови полета, разграничени с точки, съгласно приложение № 2 от [4]. (фиг. 1)

Временните номера се заменят с идентификатори при въвеждане на проекта на проектно ниво в информационната система на кадастъра. Новите идентификатори се считат за одобрени след извършване на изменението в кадастралната карта и кадастралните регистри.

При поддържане на кадастралната карта и кадастралните регистри новите обекти на кадастъра получават нови идентификатори в случаите на:

1. разделяне или съединяване на съществуващи поземлени имоти, включително при нанасяне на имоти с възстановено или придобито по давност право на собственост, разделяне при отчуждаване на част от поземлен имот, индивидуализиране на урегулирани поземлени имоти по чл. 16 от Закона за

устройство на територията, индивидуализиране на имоти, които са предмет на прехвърляне или придобиване на право на собственост;

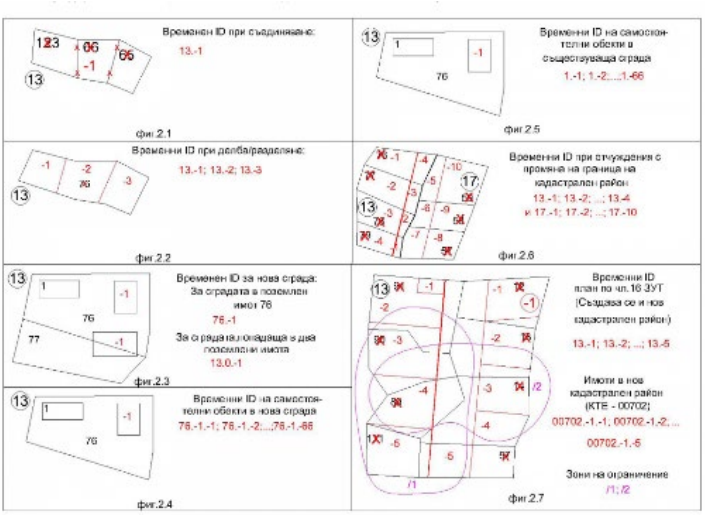
2. нанасяне на нови, както и разделяне/съединяване на съществуващи сгради, съоръжения на техническата инфраструктура, в които има самостоятелни обекти, или на самостоятелни обекти.

При поддържане на кадастралната карта и кадастралните регистри одобрените идентификатори не се променят при:

1. изменение на граница и/или очертание на съществуващите обекти в кадастъра;

2. изменения на трайното предназначение, начина на трайно ползване и адреса – за поземлен имот; брой етажи, предназначение и адрес – за сграда и съоръжение на техническата инфраструктура, в което има самостоятелен обект; етаж, брой нива в самостоятелния обект, предназначение, адрес, площ по документ – за самостоятелен обект;

3. изменения в данните за правото на собственост и други вещни права върху недвижимите имоти – обекти на кадастъра.



Фиг. 1 Временни номера на обекти на кадастъра в проекти за изменение на кадастралната карта

При промяна на граници на административно-териториални и териториални единици, извършена по реда на Закона за административно-териториалното устройство на Република България, която се изразява в промяна на ЕКАТТЕ, поради сливане, разделяне, присъединяване, отделяне или закриване на населени места или на части от тях, се променя първото поле от идентификаторите на всички имоти, които попадат в територията, предмет на изменението. В случай че има дублиране на номер на кадастрален район, се изменя и второто поле на идентификатора.

Кадастърът и имотният регистър са свързани чрез двустранна връзка въз основа на идентификатора на недвижимите имоти. Основните данни за недвижимите имоти в имотния регистър се получават от кадастъра. Данните за правото на собственост и другите вещни права върху недвижимите имоти в кадастъра се получават от имотния регистър.

Заключение

Идентификаторите на поземлените имоти имат изключително важно значение в областта на кадастъра. Те служат както за еднозначно посочване на поземлените имоти за територията на страната, така и за връзката между кадастъра и имотния регистър.

ЛИТЕРАТУРА

[1] Закон за кадастър и имотен регистър. ДВ бр. 34, 2000

[2] Наредба № РД-02-20-5 от 15 декември 2016 г. за съдържанието, създаването и поддържането на кадастралната карта и кадастралните регистри. ДВ. бр. 4, 2017

[3] Иванова, Ил. Ръководство за упражнения по кадастър

[4] Наредба № РД-02-20-3 от 29 септември 2016 г. за структурата и съдържанието на идентификатора на недвижимия имот и на номера на зоната на ограничение в кадастъра (обн. ДВ-брой: 80, от дата 11.10.2016 г.)

[5] Иванова, Ил. Кадастърът в България. Замисъл и изпълнение

[6] http://www.cadastre.bg/ - Агенция по геодезия, картография и кадастър

ВЛИЯНИЕ НА РАЗНОТОЧНАТА КАДАСТРАЛНА КАРТА ВЪРХУ ПОТРЕБИТЕЛИТЕ НА КАДАСТРАЛНИ ДАННИ

Мирем Е. Ниязи-Юсуф

IMPACT OF THE VARIOUS CADASTAL MAP ON THE USERS OF CADASTRAL DATA

Mirem E. Niyazi-Yusuf

ABSTRACT: *The accuracy of the cadastral map is defined as the correspondence of the real estate data that existed at the time of approval of the map to their actual condition.*

KEYWORDS: *cadastre, map, accuracy.*

Точността на кадастралната карта се определя съобразно чл.18 от Наредба № РД-02-20-5 от 15 декември 2016 г. за съдържанието, създаването и поддържането на кадастралната карта и кадастралните регистри, като съответствие на данните за недвижимите имоти, които са съществували към момента на одобряване на картата спрямо действителното им състояние. Точността на кадастралната карта обаче е и съответствие на границите със санкционираните от закона доказателства, установяващи данни за правото на собственост и другите вещни права. Необходимостта от такова съответствие произтича от самата същност на поземления имот, който съгласно чл. 24, ал. 2 от ЗКИР е тази част от земната повърхност с граници, съобразно правото на собственост [5].

Точността на нанесените в кадастралната карта поземлени имоти, сгради и съоръжения на техническата инфраструктура се определя чрез изчисляване на стойностите на:

1. Грешката в абсолютното положение на подробна точка (ΔS);
2. Грешката в разстоянието между две подробни точки (∂S).

Под "грешка в абсолютното положение на подробна точка" се разбира величината:

(1) $$\Delta S = \sqrt{(x - x_0)^2 + (y - y_0)^2}$$

където:

x_o, y_o са координатите на точката в кадастралната карта;

x, y - координатите на идентичната точка при контролно определяне чрез геодезично измерване и изчисление в координатната система на кадастралната карта.

Под "грешка в разстоянието между две подробни точки" се разбира величината:

$$\partial S = S - So,$$

където:

S_o е разстоянието между две произволно избрани подробни точки в един или съседни обекти (поземлени имоти, сгради или съоръжения на техническата инфраструктура) от плана или картата;

S - разстоянието при контролно измерване на място между идентичните подробни точки.

Допустимата разлика в площта, определена след контролно измерване на точките от границите на поземлен имот или сграда, се изчислява по формулата:

(2) $$m_{p_{доп.}} = 2\Delta S\sqrt{P}$$

където:

ΔS е величина, която зависи от точността на координатите на граничните точки на имота в m;

P - площта на имота в m^2.

Разликата в площта на имота, записана в кадастралния регистър на недвижимите имоти и в документа за собственост, не се счита за грешка и не е основание за изменение на кадастралната карта, ако грешките в абсолютното положение на подробните точки от границите на имота и грешките в контролните дължини отговарят на изискванията по чл. 18, ал. 4 или 5 от [2].

"Трайно материализирана граница" е граница, която може да бъде: стена на сграда; ограда, изпълнена от бетон, зидани камъни, тухли, метал с бетонна или каменна подземна основа; зидана или бетонна подпорна стена, суха зидария с височина на зида над 1,20 m и стена на масивно съоръжение или граница, означена с трайни знаци по реда на чл. 38, ал. 1, т. 23 КИР. [2]

"Нетрайно материализирана граница" е граница, която може да бъде: ограда, изградена от градински мрежи, суха зидария с височина на зида до 1,20 м, бодлива тел, жив плет, но с бетонирани бетонни или метални колове между тях или граница на обект на техническата инфраструктура.[2]

"Нематериализирана граница" е граница, която е определена с влязъл в сила план или карта, граница, одобрена или определена по реда на закон, вкл. границите на обектите на техническата инфраструктура и границите, представляващи структурни линии на естествени и изкуствени форми на релефа. [2]

Разноточната кадастрална карта оказва влияние върху :

- точността на отразяване на отделните обекти;
- точността при определяне на границите;
- точността при определяне на площите;
- грешна оценка на сградата.

Допустимите стойности на ΔS и ∂S за урбанизирани територии са:

а)за точки от трайно материализирани граници на поземлени имоти, сгради от основното застрояване и на съоръжения на техническата инфраструктура ΔS <= 30 cm и ∂S <= 20 cm;

За площ от 100 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}30\sqrt{100} = 6\ m^2$$

За площ от 500 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}30\sqrt{500} = 13{,}42\ m^2$$

За площ от 1000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}30\sqrt{1000} = 18{,}97\ m^2$$

За площ от 5000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}30\sqrt{5000} = 42{,}43\ m^2$$

За площ от 10000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}30\sqrt{10000} = 60\ m^2$$

b) за точки от нетрайно материализирани граници на поземлени имоти и постройки на допълващото застрояване ΔS <= 60 cm и ∂S <= 40 cm.

За площ от 100 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{100} = 12\ m^2$$

За площ от 500 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{500} = 26{,}83\ m^2$$

За площ от 1000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{1000} = 37{,}95\ m^2$$

За площ от 5000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{5000} = 84{,}85\ m^2$$

За площ от 10000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{1000} = 120\ m^2$$

Допустимите стойности на ΔS и ∂S за неурбанизирани територии са:

а)за точки от трайно материализирани граници на поземлени имоти, на масивни сгради и на съоръжения на техническата инфраструктура ΔS <= 60 cm и ∂S <= 40 cm;

За площ от 100 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{100} = 12\ m^2$$

За площ от 500 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{500} = 26{,}83\ m^2$$

За площ от 1000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{1000} = 37{,}95\ m^2$$

За площ от 5000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{5000} = 84{,}85\ m^2$$

За площ от 10000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 0{,}60\sqrt{1000} = 120\ m^2$$

b) за точки от нетрайно материализирани граници на поземлени имоти ΔS <= 120 cm и ∂S <= 80 cm;

За площ от 100 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 1{,}20\sqrt{100} = 24\ m^2$$

За площ от 500 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 1{,}20\sqrt{500} = 53{,}67\ m^2$$

За площ от 1000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 1{,}20\sqrt{1000} = 75{,}84\ m^2$$

За площ от 5000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 1{,}20\sqrt{5000} = 169{,}71\ m^2$$

За площ от 10000 m^2, допустимата стойност в площта ще бъде:

$$m_{p_{доп.}} = 2 * 1{,}20\sqrt{10000} = 240\ m^2$$

Заключение

При оформяне на данъчната и пазарната оценка на поземлените имоти, важна роля оказва и тяхната площ. Различната точност в урбанизираните и неурбанизираните територии води до икономически проблеми при извършване на сделки, особено при висока пазарна цена за 1 m^2.

ЛИТЕРАТУРА

[1] Закон за кадастър и имотен регистър. ДВ бр. 34, 2000

[2] Наредба № РД-02-20-5 от 15 декември 2016 г. за съдържанието, създаването и поддържането на кадастралната карта и кадастралните регистри. ДВ. бр. 4, 2017

[3] Иванова, Ил. Ръководство за упражнения по кадастър

[4] Иванова, Ил. Кадастърът в България. Замисъл и изпълнение

[5] Танев, Д. За точността на кадастралната карта, Нотариален Бюлетин бр. 2/2016 г.

[6] http://www.cadastre.bg/ - Агенция по геодезия, картография и кадастър

ПОСЛЕДИЦИ ОТ ВЪЗМОЖНОТО ИЗПОЛЗВАНЕ НА ТАКТИЧЕСКО ЯДРЕНО ОРЪЖИЕ В УКРАЙНА
Оценка на политическите, военните и екологичните ефекти

Андрей Н. Михайлов

CONSEQUENCES OF THE POSSIBLE USE OF TACTICAL NUCLEAR WEAPONS IN UKRAINE
Assessment of political, military and environmental effects

Andrey N. Mihaylov

ABSTRACT: *In the context of the complicated security environment in Europe due to the military aggression of the Russian Federation towards Ukraine, the potential threat of the use of tactical nuclear weapons by Russia is increasingly discussed. The eventual use of a tactical nuclear weapon in the Ukrainian theater of operations will be of a strategic nature for this conflict, and the power of the nuclear weapon will not be decisive for the consequences in a political aspect (except for the purely environmental ones, which are also the subject of consideration in the present study). The military effect of a tactical nuclear strike on a long front will not stop hostilities on all other fronts, only on the affected one, and will not lead to the immediate surrender of Ukraine. It may result in the blockade of certain Ukrainian military formations, a massive refugee flow, cutting off access to the Black Sea and reduced supplies, but it will not result in an immediate Russian victory. it is possible to induce a "radioactive migration" effect, i.e., young people of working and reproductive age to leave the region or the country forever. "Radioactive migration" will be triggered by any incident involving nuclear materials - this will not be a simple refugee flow from a local conflict, but a long-term migration process leading to the depopulation of entire areas. Radioactive contamination will certainly cause severe environmental consequences with long-lasting effects for Ukraine, Bulgaria and Romania.*

KEYWORDS: *nuclear weapons, indicators, effects, political and military consequences, Ukraine.*

В контекста на усложнената среда за сигурност в Европа, поради военната агресия на Руската федерация спрямо Украйна, все по-често се обсъжда потенциалната заплаха за употреба на тактическо ядрено оръжие от страна на Русия. Темата за възможните ефекти при употребата на ядрено оръжие в последните десетилетия беше обект на разглеждане единствено в научните среди и имаше теоретичен характер – запазена само за военни и за членовете на целеви аналитични групи, които да изградят математически и теоретични модели. Днес тази тема е широко обсъждана и може да се заключи, че ще става все по-актуална.

Участващите във войната държави имат излаз на Черно море, а това обстоятелство (заедно с географската близост до България) превръщат нашата страна в потенциално най-засегната от ефектите от употребата на ядрено оръжие. По този начин темата се превръща в болезнено актуална за нас и последиците от подобно катастрофално събитие ще бележат развитието на страната за десетилетия напред, насочвайки обичайния живот на гражданите в напълно непозната и опасна посока.

Войната не се развива по начина, по който вероятно е била планирана от страна на руското държавно и военно ръководство, т.е. няма бърз победен изход – опитът да се представи на света една агресивна война като освободителна беше гротеска и не се приема от демократичния свят. Негативният за Русия ход на бойните действия е възможно да доведе до решение за употреба на ядрено оръжие като средство за решаване с един удар на нереализираните (и военно нереализируеми) задачи. Безспорен е фактът, че употребата на ядрено оръжие (дори и тактическо) ще доведе до комплексни последици най-вече за Източна Европа, които може да бъдат обобщени в няколко категории.

На първо място това са политическите ефекти – ще бъде премината границата, която светът не желае да пресича – използване на неконвенционални поразяващи средства със значителна мощ. На второ място – военните аспекти на употребата на ядрено оръжие и възможността за прерастване на конфликта в паневропейски или световен. На трето място – екологичните и дългосрочни последици от радиоактивно заразяване, съпътствани от продоволствени и икономически ефекти за населението по целия свят. Комплексното разглеждане на тези групи ще даде възможност да се предвиди възможен сценарий за развитие на континента в условията на локална война с употреба на ядрено оръжие. Настоящата студия няма за цел да опише всички възможни ефекти, а по-скоро да маркира най-тежките последици за България и Европа при евентуална употреба на тактическо ядрено оръжие от страна на Русия.

Политически ефекти от употребата на ядрено оръжие

Обсъждайки политическите последици, следва да се посочи, че ходът и развитието на войната срещу Украйна ще бъдат определящи за решението на руското висше държавно и военно ръководство за употреба на ядрено оръжие. **При реализиране на мащабни настъпателни операции от украинска страна, сериозни загуби на личен състав на руските въоръжени сили и отвоюване обратно на значителни територии от Донецка и Луганска област, може да се заключи, че Русия би могла да счете използването на тактическо ядрено оръжие като военно-политически оправдан акт**. Провеждането на т.нар. референдуми в Луганска, Донецка, Запорожка и Херсонска област и присъединяването им към територията на Руската федерация, съгласно руските разбирания, ги превръщат в част от руската държава. Този акт, макар и непризнат от световната общественост, дава статут на украинските области като на субекти на Руската федерация и разпростира над тях всички средства за защита – включително и употребата на ядрено оръжие. От правна страна това би било своеобразно оправдание на Русия за евентуална дефанзивна употреба на неконвенционални средства, т.е. вероятно пред международната общественост да бъде представена версията, че това е защита на териториалната цялост на Федерацията. Подобна версия категорично няма да се приеме в международните

отношения, защото е правно необоснована, но ще намери прием в руското общество, особено в онези политически и обществени кръгове, искащи яростна ответна реакция на украинските действия.

Все по-често в изказванията на руския президент (както и на други политици в Москва) има съвсем открити заплахи за употреба на неконвенционални средства. Това означава, че тактическите ядрени оръжия са напълно приемливо и дори желано средство за определени кръгове в Русия. Съгласно разпоредбата на т. 19 от Основите на държавната политика на Руската Федерация в областта на ядреното сдържане (утвърдена с президентски Указ № 355/02.06.2020 г.) са налице две хипотези, които частично могат да намерят приложение в настоящата военно-политическа обстановка.

Първата е свързана с „*въздействие на противника върху критично важни държавни или военни обекти на Руската Федерация, извеждането от строя на които ще доведе до срив в ответните действия на ядрените сили*“, а втората е „*агресия срещу Руската Федерация с използване на обикновено оръжие, когато под заплаха е поставено съществуването на държавата*“. Посочените нормативни текстове трудно биха послужили за оправдание на тактически ядрен удар по територията на Украйна, защото досега няма поразени руски критично важни обекти, чието унищожаване да „доведе до срив в ответните действия на ядрените сили“. Именно това е вторият необходим елемент – заплаха срещу ядрените сили.

Руската военна доктрина разделя обектите на стратегически (категория I), оперативни (II категория) и тактически (III категория). От гледна точка на атаките над обекти на РФ, интерес представлява категория I. Това са важни стратегически обекти, поразяването на които в значителна степен ще намали отбранителната способност на страната, но също и категория II, обекти чието поразяване снижава бойните способности на въоръжените сили и изменя хода на операциите.

В категория I се включват: енергийни съоръжения (ядрени, ТЕЦ, водноелектрически централи); обекти на управление на водите (язовири на големи резервоари, шлюзове, канали); ядрени съоръжения с национално значение (АЕЦ, хранилища за ядрено гориво и др.); ядрени съоръжения на Министерството на отбраната (РВСН, 12 ГУМО, ВВС, ВМС); обекти на нефтохимическата промишленост; обекти с отбранително значение (отбранителни заводи, арсенали, бази, корабостроителници, хранилища за гориво и суров петрол); комуникационни съоръжения и информационни центрове; държавни органи; пунктове за управление на Генералния щаб на въоръжените сили, видовете въоръжени сили и родове войски; важни мостове и тунели по магистрали и железопътни линии. Макар и мостовете да са посочени като военни обекти, атаката на моста над Керченския проток, за която Русия обвинява Украйна, дори и да засяга важна транспортна инфраструктура не може да доведе до „оправдани ответни действия“ на ядрените сили, защото повреденият мост не довежда до потенциален срив на руските ядрени средства. **Затова отговор на атаката над моста с използване на ядрено оръжие ще е непропорционален и доктринално необоснован.**

Втората хипотеза заслужава повече внимание от правна страна, тъй като предполага, че „*под заплаха е поставено съществуването на държавата*“, ако руският политически и военен елит възприема държавното ръководство като

израз на самата държава, то широки антивоенни протести и политическа несигурност за управляващото ръководство може да се приемат в Русия и като заплаха за съществуване на държавата като цяло. Подобно приравняване на държавно ръководство с държава ще означава и наличие на обосновка за ядрен удар, съгласно т. 19, б. „г“ от Основите на държавната политика в областта на ядреното сдържане. **Затова по-голяма степен на риск се открива при хипотеза на защита на самата власт като такава**. Трябва да се отчита факта, че правната формулировка в политическия контекст винаги е била само удобна форма за обличане на волята на висшето ръководство и никога водеща сама по себе си.

Би могло да се направи заключение за това, че ядреното оръжие ще има повече политически ефекти, отколкото военно значение. Натрупването на успехи от страна на украинските въоръжени сили (нови атаки по Керченския мост, настъпления в Донецка и Херсонска област, придобиване на модерни военни способности и тяхното успешно прилагане), а също и протести в руското общество срещу режима ще са решаващите фактори за употреба на ядрено оръжие. Няма да се спираме на евентуални вътрешнополитически за Русия ефекти от евентуална ядрена атака, но те ще са основно насочени към консолидиране на руското общество около идеята за силна, непоколебима и решителна Русия – това ще бъде маската, зад която на руската общественост може да бъде поднесена идеята за превръщането на локалната война в ядрената такава. За да приеме едно общество радикалната стъпка, то следва тази идея месеци наред да бъде насаждана сред гражданите, за да започнат да я разбират като приемлива и търпима. Множество индикации в руските медии сочат, че на обществеността все по-често се дава тема за размисъл в тази насока, много политически коментатори, близки до руските силови кръгове, открито говорят и призовават за крайно военно решение. Това може да се оцени като стъпка към настройване на руското общество към по-агресивно отношение и приемане за допустимо използването на ядрено оръжие.

По отношение на вътрешнополитическите руски аспекти от използване на ядрено оръжие следва да се отчита и едно обстоятелство – предприетата мобилизация. Съдейки по информацията, постъпваща от социалните мрежи, мобилизацията не се осъществява с желаното от военното ръководство темпо. Независимо от това, очакваната групировка от мобилизирани [1] (над 300 000 души) следва да има готовност за участие в бойни действия към края на тази или началото на следващата година. Вероятно широкомащабно пролетно настъпление от страна на Русия е една от основните цели, доколкото към момента руските въоръжени сили не показват способност за успешно превземане на нови територии от Украйна, а есенно-зимния сезон не е подходящото време на годината за активни военни действия. Голямото количество мобилизирани, които се очаква да бъдат изпратени на фронта, може да бъде пречка за употреба на ядрено оръжие. Все още в руското общество съществува страх от ефекта върху населението при ядрено заразяване, породен от аварията в Чернобил. Този страх се проявява в цяла Европа и е основа за психологическия ефект от ядреното оръжие и загубата на обичайния начин на живот, утвърден в последните 75 години.

Ако бъде взето решение от страна на Русия за употреба на ядрено оръжие и на фронта са разположени мобилизирани военнослужещи, то може да бъде предизвикан страх у тях от факта, че следва да носят службата в географски

райони с високи или средни нива на радиоактивно заразяване. Близките и семействата на мобилизираните, с голяма степен на вероятност може да се предположи, ще се страхуват за здравето на мобилизираните (дори и да се върнат, последиците върху здравето на младите войници ще са негативни). Това може да предизвика остра вътрешнополитическа ситуация в Русия – разполагането на стотици хиляди мобилизирани на територията на Украйна или в близост до нея не се вписва в политическата логика за употреба на ядрено оръжие. **Изводът, който може да бъде направен е, че евентуална употреба на ядрено оръжие може да се очаква, ако на територията, подлежаща на поразяване, не се разположени много части и съединения, комплектовани от мобилизирани (или същите бъдат бързо изтеглени в дълбочина в границите на Русия)**.

Със сравнително приемлива степен на вероятност може да се предположи какви ще бъдат политическите последици от употребата на ядрено оръжие, но за момента на използването му може да се съди само по косвени признаци. **Няколко индикатора за предстояща употреба на ядрено оръжие биха били:**

а) **изтегляне на руските войски от определени райони**, което на пръв поглед би изглеждало тактически нелогично, но тези територии са „отстъпват“ с ясното съзнание, че ще бъдат подложени на радиоактивно заразяване;

б) **придвижване на войскови части, чиято основна задача е съхраняване, охрана и подготовка за употреба на ядрено оръжие от различни носители**. Това означава много внимателно наблюдение на частите и обектите на 12-то Главно управление на Министерство на отбраната с цел получаване на изпреварваща информация за доставяне на ядрени средства за поразяване до бойните части, които ще ги използват. Осъществяването на наблюдението е изключително трудна задача, тъй като една от основните цели на 12-то Главно управление на МО е да извърши скрито превозване на ядрените средства, като за целта има разработени мерки, охрана и маршрути, така че да не бъдат забелязани от технически средства за наблюдение;

в) **целенасочена работа сред мобилизираните и тяхното обучение за водене на бойни действия в условията на ядрен конфликт**, раздаване на предпазни облекла, противогази, медикаменти (ако са налични). Това са ясни признаци за предстояща употреба на неконвенционално оръжие, наред с трайното и последователно индоктриниране на населението по отношение на това, че единственият изход за „отбраняващата се Русия“ е неконвенционален отговор.

Не би могло да се оцени като надежден и навременен индикатор евентуална заповед от руското военно командване до частите за непосредствено използване на защитни облекла или противогази, тъй като с цел скритост на използването на ядрено оръжие тази заповед вероятно ще бъде дадена в последния възможен момент, т.е. в рамките на минути или час (дори и с цената на рискуване на здравето на военнослужещите, заповед може въобще да не бъде дадена на всички части или съединения).

Анализирайки публично достъпни източници, може да се заключи, че засега единствено обработването на общественото мнение в Русия е факт, тъй като отстъплението на руските въоръжени сили, по всичко личи, не е резултат от заповед на висшето държавно ръководство, а поради умелите действия на украинската армия и множеството грешки в руското военно командване.

Разглеждайки външнополитическите последици от употребата на тактическо ядрено оръжие следва да бъдат отбелязани няколко особено важни ефекта, които биха настъпили практически незабавно. На първо място, това е крайно острата осъдителна реакция на всички западни държави, това е предвидимо, но осъдителна реакция ще има и от държави, които поддържат по-неутрална и балансирана позиция спрямо войната на Русия срещу Украйна. Държави като Сърбия, Босна и Херцеговина и Турция няма как да приемат употребата на ядрено оръжие на континента поради очакваните екологични и икономически последици. Това означава, че Русия би загубила сравнително малкото си поддръжници или поне неутрално настроени държави. Пълната политическа изолация на Русия ще бъде факт следупотреба на ядрено оръжие и това ще е най-тежката последица – на практика ще се създадат условия за нова желязна завеса в Европа. През лятото и есента на 2022 г. държавите от Европейския съюз полагат усилия за намаляване до минимум зависимостта от Русия по отношение на доставки на газ, петрол, уран и други метали, но превръщането на войната в ядрена ще ускори и завърши този процес в много кратък срок. Ефектът ще бъде рязко отделяне на Европа от Русия във всички отношения – политически, икономически, движение на хора – това означава, че резултатът от употребата на тактическо ядрено оръжие ще бъде стратегически в политически аспект.

Ако руското държавно ръководство вземе решение за употреба на ядрено оръжие, то вероятно ще е чрез използване на оперативно-тактически ракети (възможно ОТРК 9К720 „Искандер-М“) или крилати ракети с морско базиране, мощността на бойната глава ще бъде в рамките на 5-10 килотона. Тази мощност може да се определи като тактическо ядрено оръжие, но изводът е, че политическите ефекти от неговата употреба далеч ще надхвърлят тактическия обхват. Вероятността от ескалиране на войната от локална (с употреба на ядрено оръжие) в паневропейска е значителна, защото използването на ядрено оръжие ще предполага реципрочен отговор – дори и да не е ядрен, а само конвенционален, то той ще доведе до скокообразно ескалиране. **Европейският континент ще понесе най-много загуби, но не по-малки ще бъдат и косвените щети за държави в Близкия изток и Африка, изразяващи се в продоволствена криза през 2023-2024 г. (реколтата от пшеница и слънчоглед в Украйна ще бъде компрометирана напълно).**

Заключението, което може да се направи е, че тактическото ядрено оръжие, използвано на украинския театър на бойни действия, ще има стратегически характер за този конфликт и мощността няма да е определяща за последиците в политически аспект (освен за чисто екологичните, на които ще се спрем по-късно). С голяма степен на вероятност може да се заключи, че руското държавно и военно ръководство знае за тежките последици от подобна стъпка и сериозните вътрешно- и външнополитически последици ще са основния възпиращ фактор към момента, това ще е така докато обстановката на фронта не бъде оценена като застрашаваща съществуването на политическата и военна система в Русия като цяло.

Няма данни за силно повишаване нивото на неодобрението на режима в Руската федерация към нива, които да водят до срив на политическата система. Мобилизацията категорично предизвика явно неодобрение, страх и отклоняване от военна служба на мъже в мобилизационна възраст, но все още е далеч от

нивата на търпимост на обществото и ще е нужно повече време за натрупване на критично недоволство. Опасността от загуба на съюзници за Русия ще е основният фактор, за да не прибегне до ядрена опция – дори режимите, които са умерени критици или скрити привърженици, ще са принудени да осъдят употребата на неконвенционални средства.

Следователно употребата на ядрено оръжие не е логически очаквана в много близка перспектива, но това може да се промени под въздействие на два фактора:

На първо място, сериозни загуби сред личния състав на въоръжените сили (особено сред мобилизираните наскоро), водещи до недоволство вътре в страната и срив в авторитета на армията, както и поразяване на критична руска (или окупирана) инфраструктура.

На второ място, лично решение на политическото ръководство. Последното е трудно предвидимо, тъй като попада в обхвата на психологическата оценка на конкретни личности и тяхното емоционално състояние, а не на обективни политически или военни фактори. В заключение на оценката за политическите последици за Руската федерация следва да се посочи, че те ще се изразяват в следното:

- Външнополитическа изолация – Русия действа в такава частично от анексирането на Крим през 2014 г., но използването на ядрено оръжие ще направи изолацията на Русия по-силна от тази в най-тежките години на Студената война. Международният авторитет на Русия ще бъде по-нисък от този на Северна Корея, изолацията й ще бъде дори по-сериозна именно поради употреба на ядрено оръжие срещу неядрена страна;
- Ще отпаднат всякакви ограничения за предоставяне на въоръжение за Украйна и тя ще получи много по-мощни системи за поразяване дори в дълбочина на руска територия, като пример може да се посочи, че ракетите за системите HIMARS вече няма да бъдат с ограничен обхват от 75-85 км., а вероятно ще се използват ATACMS с далечина на полета около 300 км;
- Загуба на съюзници – държавите от БРИКС и ШОС ще осъдят подобен ход, защото в противен случай биха били в една група с държава, прибегнала до офанзивна употреба на ядрено оръжие (дори и под благовидния предлог за защита на анексирани преди това чужди територии);
- Протести сред собственото население, породени от страх от радиоактивно заразяване, увреждане на личния състав от мобилизирани граждани, неадекватна защита на населението. Неконтролируем вътрешен мигрантски поток от западните граници на Руската федерация в източна посока към вътрешността на страната, обезлюдяване и огромно социално напрежение в анексираните области;
- Продоволствена и икономическа криза – реколтата от пшеница и слънчоглед на Украйна ще бъде напълно негодна за употреба, а това означава глобален недостиг на храни, особено в държави от Близкия Изток и Африка. Там Русия има традиционни съюзници и благосклонно настроени режими. Продоволствена криза ще бъде предизвикана и в Европа, тъй като реколтата и в тези държави ще бъде застрашена. Икономическите ефекти са трудно предвидими, но може да се посочи, че ще обхващат намаляване до минимум или пълно прекъсване на движението на стоки и суровини от/към Русия, а също и на

хора в Източна Европа. Туристическият бизнес в Европа и Черноморския басейн (в частност Румъния и България) ще бъде засегнат поне за десетилетие;

- Промяна на балансираната позиция на Турция спрямо Русия;
- По отношение на българо-руските отношения ефектът ще бъде също разрушителен, тъй като голяма част от нашето общество ще загуби всякакво положително отношение към Русия. Вероятно е да се задейства изключително остра обществена реакция, основаваща се на дълготрайните рискове за здравето на българските граждани от евентуално радиационно замърсяване. Вината ще бъде върху страната, използвала ядрено оръжие, но негативното отношение може да се пренесе и върху руските граждани живеещи в България, т.е. да се стигне до трайно враждебно отношение към тях;
- За България основните последици ще са в три направления: а) практическа загуба на статуса на туристическа страна, тъй като Черно море ще престане да бъде желана дестинация за каквито и да било туристи, поради потенциални рискове за здравето. Това ще доведе до значително спадане или напълно прекъсване на приходите от туризъм, а в резултат но това и вътрешно социално недоволство; б) продоволствен риск, тъй като реколтата е възможно да се окаже неизползваема и непродаваема; в) вътрешна миграция от североизточните области към югозападните;
- Доколкото България е член на НАТО и ЕС, нашата страна ще е обвързана с реакцията на тези международни организации, отговорът на нашите съюзници може да доведе до прекратяване на отношенията с Руската федерация или дори до тежка ескалация на войната със засягане на Черноморския басейн. Възможните опции не са много – ядрен отговор; отговор с обикновено въоръжение; невоенен отговор, т.е. пълна изолация. Дори и при неядрен отговор с обикновено въоръжение от страна на съюзниците Черно море ще бъде театър на бойни действия, а това означава сериозно засягане на корабоплаването основно от пристанище Варна, както и на търговската дейност;

На фона на описаните последици, от руска гледна точка, единствено оцеляването на режима, увеличаването на авторитета на въоръжените сили и мотивиране на най-остро настроените граждани са политическите „ползи“ при употреба на ядрено оръжие. **Сравнението на потенциалните негативни последици за Русия и евентуалните ползи за нея сочи превес на негативните последици, особено външнополитическите и икономическите**.

Горните изводи се базират на политическата логика и сочат, че към настоящия момент и при така създалата се обстановка на фронта е нецелесъобразно за Русия да използва тактическо ядрено оръжие, но не отчитат психологическите аспекти на членовете на политическия и военен елит, непредвидими по своята същност, особено при хипотези на украински удари върху знакови обекти от руската военна или цивилна инфраструктура и емоционално решение за запазване „престижа на руската армия“ и на политическото ръководство.

Военни ефекти от употребата на ядрено оръжие

Както посочихме по-горе, решението за употреба на ядрено оръжие от страна на руското държавно и военно ръководство може да се вземе при няколко обстоятелства – тежки загуби сред личния състав на руските въоръжени сили (особено сред мобилизираните наскоро), водещи до недоволство вътре в страната

и срив в авторитета на армията и политическото ръководство, както и поразяване на критична руска (или окупирана) инфраструктура.

1. Обективни индикатори (признаци) за предстоящо използване на ядрено оръжие. Доколкото не е известна с точност реалната воля на висшето държавно ръководство на Русия по отношение на използването на ядрено оръжие, може да правим заключения единствено въз основа на публичните изказвания. През последния месец те стават все по-заплашителни. Поради това е необходимо да се обърне внимание на обективни факти, които могат да послужат като база за оценка и демаскиращи признаци за предстоящо използване на ядрено оръжие. Сред тези обективни, изцяло военни, индикатори могат да бъдат:

- Установяване и разпознаване на носители на ядрено оръжие – това могат да бъдат оперативно-тактически ракетни комплекси (ОТРК) от различни типове (9К720 „Искандер – М“ или ТРК 9К79-1 „Точка-У“, за последната платформа е по-малко вероятно, поради по-малкия обхват и точност) и тяхното придвижване на потенциални стартови позиции. Съгласно публично достъпни данни ОТР 9К720 „Искандер“ може да носи една ядрена бойна част с мощност от 10 до 100 килотона, а Русия разполага с около 70 бойни глави;
- Проследяване разположението и движението на плавателни съдове в акваторията на Черно и Азовско море, които имат на борда си крилати ракети 3М54 „Калибър“. Именно тези системи (ОТРК „Искандер“ и крилати ракети „Калибър“) са най-вероятните носители поради три обстоятелства: а) те са сред системите с най-висока точност и тяхното кръгово вероятно отклонение от целта е сравнително малко. При използване на тактическо ядрено оръжие точността на носителя придобива решаващо значение, защото епицентъра на взрива е близо да предния край на собствените войски; б) пуск може да бъде осъществен от територията на Руската Федерация или от акваторията на Черно море без ядрената бойна част преди старта да напуска осигурените и проучени предварително позиции. Съгласно руската доктрина безопасна дълбочина за ядрените сили е от 75 до 450 км. от фронта, там са в безопасност от противникова авиация, дронове и малки ударни (диверсионни) групи. Затова може да се оцени, че евентуален пуск ще бъде извършен именно от дълбочина, но подбрана така, че времето на полета на носителя до целта да е сравнително кратко; в) кратко време за полет до поразяване на целта се налага, за да не може да реагират украинските средства за ПВО. Малко вероятно е да се използват носители с въздушно базиране като крилати ракети Х-55 и Х-102, тъй като носителите са стратегически бомбардировачи и лесно могат да бъдат установени, а основните и запасните им летища за базиране са известни и наблюдавани;
- Разпределяне сред личния състав на руските въоръжени сили на защитни облекла, противогази (включително изолиращи противогази) и друго защитно оборудване срещу оръжия за масово поразяване. Следва да се обърне внимание на вида на личните предпазни средства, ако се установи разлика в оборудването на едни части в това на други може да се достигне до заключение, че тези с по-съвременното оборудване ще бъдат разположени близо до епицентъра (или ще осъществят марш през заразена зона);
- Ускорена подготовка на частите за защита от оръжия за масово поразяване. Обективен индикатор би била заповед от командването за постоянно съхранение на противогаз от личния състав или раздаване на предпазни светлинни филтри за стъклата на противогаза срещу светлинното излъчване като

поразяващ фактор на ядрения взрив. Установяването на обстоятелството колко часа продължава подготовката на личния състав е показател за сериозността в намеренията да се използват неконвенционални средства;

- Създаване на организация и извършване на йодна профилактика сред личния състав;
- Насищане на частите с военно-медицински персонал, дозиметрични прибори и медикаменти;
- Наличие на множество прибори, комплекти и машини за дезактивация и дезинфекция (придвижване на авторазливни станции и цистерни);
- Активно придвижване на частите за радиационна, биологична и химическа защита и тяхното оборудване. От дислокацията и оборудването им може да се достигне до косвено заключение за направлението на ядрения удар, тъй като една от техните задачи ще е определяне на индивидуалната и групова доза на облъчването;
- Военно-тактически необосновано отстъпване на определени части от вече окупираните територии и/или изграждане на дълготрайни защитни съоръжения;
- Учения на военно-космическите сили за използване на ядрено оръжие, активиране на системите за защита на държавното ръководство в условията на ядрена война и центровете за оценка на ефектите от нея;
- Издаване на заповеди за промяна/повишаване на пределно допустимите дози и времето, което личният състав може да престои в заразена зона;

Така изброените индикатори (признаци) са примерни и неизчерпателни, като се счита, че особено важно е установяване движението на автомобилни военни колони, за които се предполага, че **превозват екологично опасни товари в граничните с Украйна райони**. Именно в тях може да се намират ядрените бойни глави. Пример за такъв транспортьор, който следва да е обект на специален интерес, е НГ9Т1-1/М01, конструиран на базата на военен триосен товарен автомобил, но снабден с бронирани екрани по бордовете. Наред с това ядрената бойна част изисква специална климатизация, което означава, че колоната ще включва множество подвижни работилници, автокранове и товарни автомобили, включително такива, осигуряващи температурен режим на съхранение и защита от статично електричество. Охраната на такива колони е значителна, маскировката също, а може да се предположи, че ще имат и въздушно прикритие от складовете/базите за постоянно съхранение до стартовата позиция на носителя. Логично е, че ще се движат няколко колони в различни направления в светлата и тъмна част на денонощието, но самия факт на движение на тези транспортни средства показва активна подготовка за използване на ядрено оръжие.

Разумно е да се предположи, че е необходима система от индикатори, а не само един, тъй като само един може да се използва и като демонстрация и политически инструмент. Някои от индикаторите вече са налице, като пример може да се посочи учението на руските ракетни войски със стратегическо назначение, завършило в средата на м. октомври, но те са форма на политическа демонстрация. Много по-сериозен индикатор биха били обвиненията на руската страна, че украинските въоръжени сили са атакували

обекти например в Белгородска област, т.е. на територията на Руската федерация, а не на окупираните украински области.

Само едновременно или последователно регистриране на индикатори може да доведе до обоснован извод за високо вероятно използване на ядрено оръжие.

2. Относно въпроса за тактическото ядрено оръжие, неговата мощност и решаваните задачи – в руската военна доктрина няма ясно посочване на мощността, която определя бойната част като тактическа. Избраната мощност може да има тактически характер за определени театри на бойни действия, но на други да не е така – това изцяло зависи от поставената задача и територията/акваторията, над която ще бъде използвано.

Оперативно-тактическото ядрено оръжие е предназначено за поразяване на цели в оперативна дълбочина на развръщането на войските на противника (до 500 км.) за изпълнение на бойни задачи. Тактическото ядрено оръжие е предназначено за поразяване на обекти в тактическа дълбочина на войските на противника (до 300 км) за изпълнение на бойни задачи. При определени условия тактическо ядрено оръжие може да се използва за изпълнение на оперативни или стратегически задачи. Оперативно и тактическо ядрено оръжие се намират на въоръжение на силите с общо назначение. **Ролята и задачите на тактическото ядрено оръжие в конкретната оперативна обстановка в южната част на Украйна са в три направления:**

а) Пресичане на настъплението на украинската страна;

б) Осигуряване на бърз пробив на руската армия в някое от направленията на фронта. Според избрания вид и мощност на ядрения взрив (наземен или въздушен) ще възникне въпроса за това, че руско настъпление ще предполага марш на войските през зони с радиоактивно заразяване;

в) Сковаване на украинските части и пресичане на достъпа до брегове на Черно море.

Руската доктрина допуска използване на ядрени боеприпаси с малка мощност при водене на бойни действия и поразяване на живата сила на противника в непосредствена близост. По поразяващи фактори тактическото ядрено оръжие не се различава от това със стратегическо предназначение – проявяват се познатите фактори като светлинно излъчване, електромагнитен импулс, ударна вълна, проникваща радиация и радиоактивно заразяване, но малката мощност ще обуслови по-различно проявяване на поразяващите фактори. Ударната вълна ще бъде слаба и общото й поразяващо действие ще има съвсем ограничен обхват. Същото се отнася и до светлинното излъчване, което ще се прояви за много кратко време и може да окаже въздействие, ако взривът и осъществен в тъмната част на денонощието.

Като пример за въздействието на ударната вълна може да се вземе взривът в пристанището на Бейрут, Ливан – на 04.08.2020 г. се взривява пристанищен склад с амониев нитрат, а мощността на взрива е изчислена на 1.1 килотона тротилов еквивалент. Кратерът, който се образува в резултат на експлозията е с диаметър около 120 метра, а повредените сгради са на разстояние приблизително километър. Може да се заключи, че това поражение от ударната вълна не би било решаващо, още повече, ако е извън урбанизирана територия. При тактически ядрен удар радиоактивното заразяване ще бъде основния

поразяващ фактор. В първите часове след взрива площта на заразяване няма да е много голяма и ще позволява обхождане от наветрената страна, по този начин руските войски биха постигнали две цели – задържане на украинските части и бързо обхождане на епицентъра, а същевременно и настъпление по незаразеното направление. Един от ясно изразените военни ефекти на използването на тактическо ядрено оръжие в Украйна е, че ще престане да има решаващо значение превземането на по-малки населени места като села и малки градове. Фронтът ще придобие общ и много по-стратегически характер като се обособят само две или три големи водещи направления, а бежанската вълна ще препятства движението на въоръжените сили на Украйна (тя ще се превърне от социално-икономически във военен фактор). Сценарият за използване на ядрено оръжие от територията на Беларус заслужава отделен анализ, но към настоящия момент може да бъде оценен като много малко вероятен.

Съгласно публични оценки [2, 8] в началото на 2022 г., че Русия разполага с приблизително 4477 бр. ядрени бойни глави, които са предназначени за всички видове носители. От това количество около 1588 бр. са за стратегически носители (основно междуконтинентални балистични ракети), а 1912 бр. са предназначени за тактически носители на ядрено оръжие. По други оценки [4] обаче е невъзможно да се прецени какво количество тактическо ядрено оръжие притежава Русия, оценките варират в много широки граници от 1000 до 3000 бр. (включително единиците на дългосрочно съхранение). Ядрените бойни глави за ОТР се изчисляват приблизително на 250-370 бр. като половината от тях се намират в Западния военен окръг. Това означава, че страната разполага със значителни запаси, разположени в множество бази за постоянно съхранение. Сравнително близо до границата с Украйна се намират Белгород-22 (в/ч 25624), Брянск-18 (в/ч 42685), Воронеж-45 (в/ч 14254), Можайск-10, Москва (в/ч 52025, 714 АХЯО). Изводът, който се налага е, че наличието на ядрена бойна част и съхранението ѝ не е проблем за руското военно ръководство, предизвикателство е подбор на носителя поради намаляващото количество нови ОТР и крилати ракети.

Военният ефект на един тактически ядрен удар по отношение на фронт с голяма дължина е, че няма да спре бойните действия по всички други направления, а само по поразеното и няма да доведе до незабавна капитулация на Украйна. Може да доведе до сковаване на определени украински части, огромен бежански поток, отсичане достъпа до Черно море и намаляване на снабдяването, но няма да резултира в незабавна руска победа.

Екологични ефекти от употребата на ядрено оръжие

Оценката на екологичните ефекти зависи от множество фактори, които по своята същност са главно метеорологични и географски. Основните фактори са посоката и силата на вятъра, характер и плътност на облачността и сезона. Географски най-трудно е да се оцени къде би бил нанесен евентуален ядрен удар, тъй като това зависи от конкретната обстановка на фронта. Мотивите за подбор на конкретно място могат да бъдат основно два:

а) Очакван военно-тактически ефект (поразяване на украински въоръжени сили и спиране на тяхното настъпление);

б) Стратегически – блокиране на излаза на Черно море на Украйна и сковаване на място на украинската армия. Според това кое съображение ще вземе превес ще се направи и избор от страна на военното и политическо ръководство на конкретна точка, в която евентуално да бъде нанесен удара.

Вземайки под внимание, че южното направление е от съществено значение за осъществяване на замисъла на Русия, както и поради факта, че там се осъществява настъпателна украинска операция за отвоюване на окупираните територии, може да се заключи, че **Херсонска област е вероятно да бъде избрана за атака**. Към настоящия момент фронтът в Херсонска област е с дължина около 150 километра, минавайки на около 25-35 километра западно от областния град. Евентуално използване на тактическо ядрено оръжие по херсонското направление (западно от Херсон) ще пресече действията на украинските въоръжени сили по възвръщане на областта и главния град, но това едва ли ще е основен мотив за избор на конкретно място. Водещо вероятно ще бъде отсичането на украинския достъп до Черно море, превръщайки Украйна в държава без излаз на море, тъй като радиоактивното заразяване ще обхване и южните части на съседните Николаевска и Одеска област. По този начин ще се създаде риск от блокиране на всякакви доставки по море към Украйна, а и масова евакуация на населението от областите към северозападните части на страната.

Ефектът върху околната среда при употреба на ядрено оръжие може да бъде разделен на краткосрочен и дългосрочен. Двете категории зависят от множество фактори, които не подлежат на точна оценка без да се знае географската позиция, която ще бъде обект на удара.

Пожарите, които със сигурност ще възникнат (при наземен и нисък въздушен ядрен взрив) са сред краткосрочните ефекти и зависят като интензитет от вида на горящия материал, същото се отнася и за отделянето на прах и пепел в атмосферата. Ако бъде поразен град, характерът на сградите и отделения от тяхното горене дим ще бъде различен сравнено с поразяване на цел в открита, степна или гориста местност. Обемът, масата и видът на издигащите се в атмосферата частици има значение за радиоактивната следа, която ще се образува в резултат на взрива. Потенциално значителна роля би имало поразяването на складове с гориво, което ще доведе до силни пожари с отделяне на голямо количество дим в атмосферата без възможност за тяхното овладяване, тъй като в условията на радиоактивно замърсяване пожарогасителната дейност ще бъде затруднена, ако не и невъзможна. Територията на Херсонска област е около 28 хил. км², а областта е разположена в степна зона по долното течение на река Днепър. **Степната зона и равнинният характер на релефа предполагат отделяне на голямо количество радиоактивни прахови частици и лесното им разпространение**. Липсата на планини и големи възвишения ще доведе до обширно заразяване на площи, а същевременно преобладаващите ветрове през есенно-зимния сезон са от североизток. Руската страна може да прибегне към използване на ядрено оръжие в тази част на Украйна именно поради това, че насочеността на вятъра не е към руска територия, а Кримските планини действат като своеобразен щит в югоизточно направление.

Скоростта на вятъра в района на северното крайбрежие на Черно море има изразен годишен динамичен ход с максимум в зимния сезон и минимум в летния, като варира усреднено от 3 до 6 м/сек. През зимата метеостанциите са отчитали и ветрове със значително по-големи скорости. Посоката на вятъра по

бреговете на Черно море се определя от разпределението на атмосферното налягане в различните сезони – през есенно-зимния сезон под влияние на циклонални области над морето преобладава пренос на северно континентални и дори полярни въздушни маси, съпроводени със североизточни и северни ветрове. **Това означава, че следата от радиоактивно заразяване ще има обичайната издължена елипсовидна форма насочена на югозапад към територията на Украйна, Румъния и България**. Посоката на вятъра е решаващ фактор за площта на заразената зона, основавайки се метеорологични данни от дългогодишно наблюдение на явленията в северното Черноморие може да се заключи, че основните екологични щети ще бъдат именно в южните области на Украйна, североизточните области на Румъния и на България.

През летния сезон посоката на ветровете е по-променлива и често от юг или югозапад. Това означава, че използването на ядрено оръжие и ефекта на разпространението на радиоактивния облак ще се определя от очаквания вятър през есенно-зимния сезон. Именно в този сезон е очаквано да се използват неконвенционални поразяващи средства, тъй като през лятото ветровете биха насочили радиоактивните въздушни маси и продукти от горене към територията на Русия.

Приемайки хипотезата, че се използва тактическо ядрено оръжие с мощност около 5 килотона, при въздушен ядрен взрив (на ниска или средна височина), то непосредствено ще бъде засегната атмосферата в диапазона 6-8 километра.

Продуктите от деленето на ядрения материал ще се пренасят по посока на вятъра и, ако приемем, че средната му скорост в района на северното Черноморие е около 5 м/сек от североизток, то ще достигнат територията на България след по-малко от 24 часа. Това води до извод за изключително кратко време за реакция от страна на България с цел защита на населението.

Изчислението е възможно да варира в широки граници, тъй като в конкретния ден силата и посоката на вятъра може да са различни, а и мощността и височината на взрива също. Скоростта на вятъра зависи от атмосферното налягане и характера на повърхността, последният фактор предполага значително увеличение на средната месечна скорост над открито море в сравнение с тази по крайбрежието. Това предполага, че пренасянето на радиоактивните частици във въздуха **може да стане и по-бързо от очакваното**. Наред с това при въздушните взривове на сравнително голяма височина не се образува облак от увлечен прах от земната повърхност и продукти на горенето в резултат на пожари на земята. Всъщност теоретичната оценка е затруднена, тъй като много фактори са променливи – скорост и посока на вятъра са основните (макар, че има данни от дългогодишни метео наблюдения и усреднени стойности), но и вида на ядрения взрив също е важен. При наземните и ниските въздушни взривове ще има значителни количества радиоактивен прах, а при въздушните (височинни) малко или никакъв. Това обаче не означава, че въздушният взрив няма да нанесе екологични поражения в дългосрочен аспект, защото радиоактивните материали ще бъдат в атмосферата и ще попаднат върху земната повърхност или в акваторията на Черно море.

Предвид изложеното се налага извода, че разпространението на изхвърлени в атмосферата радиоактивни вещества, се изразява в пренос по

посока на вятъра и в разсейване с процеси на атмосферна турболентна дифузия. Необходимо е много по-детайлно моделиране и компютърна симулация, но не може да се избегне заключението, че ще има отлагане и върху земната повърхност, водещо до радиоактивно замърсяване на почвата и подпочвените води. Дълготрайният ефект ще бъде пренасяне на вещества в хранителната верига, натрупването им в растителни и животински продукти и поради обективния факт, че ветровете над Черно и Азовско море през есенно-зимния сезон са от североизток, то България е вероятно да бъде засегната. Някои от съвременните ядрени боеприпаси са с управляема мощност, вариращa от няколко килотона до няколко стотици килотона, т.е. дори и мощността да е малка, то ядреният материал в бойната част е значителен. При взрив той ще бъде разпръснат в атмосферата, което ще увеличи радиоактивното заразяване.

Именно дълготрайният ефект може да се оцени като по-рисков при тактически въздушен ядрен взрив, радиационното заразяване ще обхване сушата, т.е. тревни площи, растителни култури, плодове, зеленчуци, фураж, а от там и животни (резултиращо в риск от заразяване на млечни и местни продукти). Последиците за здравето на населението ще зависят от това какъв обем предпазни действия бъдат предприети – именно тук е основната отговорност на централната и местната власт в нашата страна. Фактори като: решение за употреба на неконвенционално оръжие, неговата мощност, височина на използване и място са изцяло независещи от страни като България, но във властта на страната ни е навременно информиране населението, да се говори по темата, за да няма паника, а разбиране как да се извърши защитата. Това е основната цел на настоящия анализ – да предизвика професионална дискусия с оглед навременни и обмислени решения и подготвеност на населението.

Бихме искали да се спрем и на още един сценарий, който не предполага целенасочено използване на ядрено оръжие. Ако руската страна счете ядрения удар (дори и височинен с относително ниска степен на радиоактивно заразяване) за твърде рисков, може да използва косвено самото радиоактивно заразяване като оръжие. Това би могло да се осъществи, чрез **допускане на авария в ядрена централа и политически прехвърляне на отговорността на Украйна**. Най-близката до фронта е Запорожката ядрена централа. Авария (умишлена или по непредпазливост) в активната зона на някой от реакторите ще доведе също до заразяване, ако се стигне до разпръскване на радиоактивен материал, то заразяването ще е сравнимо с използване на тактическо ядрено оръжие с малка мощност. Дори и да не е предизвикана умишлено (към настоящия момент изглежда малко вероятно) авария в ядрена централа крие значими рискове. Няма да се спираме на психологическите ефекти от сценария „авария в атомна централа“, тъй като те трудно могат да бъдат описани, но е достатъчно да се посочи, че спомените за аварията в Чернобил са още много силни. Дори и да не е с мащабите на Чернобил, а далеч по-малък, то страхът сред хората ще е сравним – възможно е да се получи **ефект на „радиационна миграция“, т.е. млади хора в работоспособна и репродуктивна възраст да напускат областта или страната завинаги. Радиационна миграция ще се предизвика при какъвто и да било инцидент с ядрени материали – това няма да е обикновен бежански поток от локален конфликт, а дългосрочен миграционен процес, водещ до обезлюдяване на цели области.**

Използването на ядрено оръжие от руска страна няма да доведе до гарантирана победа във войната, а до нейната ескалация и тежки последици за Руската Федерация, някои от тях могат да бъдат предвидени и са очаквани, но други ще са резултат от променящата се обстановка.

Към настоящия момент не е много вероятно да се прибегне до такава радикална стъпка и не са налице комплексни обективни обстоятелства, които да свидетелстват за непосредствено предстоящ ядрен удар, въпреки агресивната реторика и ученията на ракетните войски със стратегическо назначение. Описаните последици са известни на руското държавно и военно ръководство и, независимо от агресивните изказвания, се осъзнават. Сценариите са много и няма да бъдат разглеждани в настоящия материал, но безспорен е факта, че наблюдението на обстановката и обективните индикатори ще продължат да бъдат основен инструмент в опита за предвиждане на действията на руската страна.

ЛИТЕРАТУРА

[1] Указ № 647/21.09.2022 на президента на Руската федерация „Об объявлении частичной мобилизации в Российской Федерации“

[2] Russia Military Power, Defense Intelligence Agency, USA, 2017;

[3] Konrad Muzyka, Russian Forces in the Western Military District, Rochan Consulting, CNA, 2021

[4] Vira Ratsiborynska, Daivis Petraitis and Valeriy Akimenko, Russia’s strategic exercises: messages and implications, NATO Strategic Communications Centre of Excellence, 2020

[5] Robert E. Berls Jr, Leon Ratz, Raising Nuclear Dangers/Рост ядерной опасности: оценка риска использования ядерного оружия в Евро-Атлантическом регионе, NTI, Washington, DC 2006, 2015

[6] Nonstrategic Nuclear Weapons, Congressional Research Service, https://crsreports.congress.gov, RL 32572 Updated March 7, 2022;

[7] Hans Kristensen. Non-Strategic Nuclear Weapons 2012, FSA, ISBN 978-1-938187-01-8

[8] Hans M. Kristensen & Matt Korda, Russian nuclear weapons, Bulletin of the Atomic Scientists 2022

[9] Hans M. Kristensen & Matt Korda, Tactical nuclear weapons, Bulletin of the Atomic Scientists 2019

[10] Field Manual FM 34-52, Washington, USA, DoD, 1992

[11] Field Manual FM 100-50, Nuclear Unit Operations in Combat USA, DoD, 1977

[12] Field Manual FM 101-31-1, Nuclear Weapons Employment, USA, DoD, 1977

[13] Gunnar Arbman, Charles Thornton, Russia’s Tactical Nuclear Weapons, Stockholm, 2005

[14] Л.Н. Репетин, В.Н. Белокопытов, Режим ветра над побережьем и шельфом северо-восточной части Черного моря, 2006

[15] Микола КУЛЬБІДА, ДСНС України, Інформаційна довідка Радіаційна ситуація в Україні 3-5 вересня 2022 р.

ПРОЕКТИРАНЕ И РАЗРАБОТКА НА СТЕНД ЗА ИЗПИТВАНЕ НА МЕХАНИЧНА УСТОЙЧИВОСТ НА ВОДОСЪДЪРЖАТЕЛИ

Милен К. Петков, Пламен Л. Рибарски

DESIGN AND DEVELOPMENT OF A STAND FOR TESTING THE MECHANICAL RESISTANCE OF WATER CONTAINERS*

Milen K. Petkov, Plamen L. Ribarski

ABSTRACT: *On the basis of the studies carried out, the shortcomings of the existing test methods have been pointed out and an innovative approach has been proposed using an air-water cylinder that can perform a huge number of cycles combined with easy, intuitive control. This bench is designed, developed and implemented based on the proposed approach.*

KEYWORDS: *test bench, high pressure, air-water cylinder.*

Въведение

Предназначението на стенда е да може циклично да натоварва водосъдържатели с налягане и за време, указано от стандарта EN12897и според декларираното от производителя на водосъдържателя. Според изискванията на стандарта EN12897 една тестова процедура продължава повече от 10 дни. В този дълъг период може да настъпят много непредвидени събития – прекъсване на електрозахранването, токови удари и т.н. които да направят резултатите от стенда невалидни. Поради тази причина беше проучен досегашния опит в тази насока и бяха идентифицирани слабостите и силните страни на известните досега методи. Друго важно изискване, на което трябва да се обърне внимание при проектирането на стенда е изпитване на повече от един водосъдържател, о то така, че да може да се провеждат независими един от друг тестове с по един водосъдържател или стринг от водосъдържатели [1, 4, 5].

Стендовете в експлоатация в момента използват двукамерен, пневматично-воден цилиндър с бутало. Предимството на този метод е че при правилно избран диаметър на цилиндъра от по-ниско пневматично налягане може да се създаде по-високо налягане на водата във водосъдържателя.

Съществен недостатък обаче е използването на движеща се бутална част. Често уплътнителите на буталото се повреждат по време на теста и това довежда до:

* Този труд се издава с частичната финансова подкрепа на проект РД-08-130/04.02.2021 от фонд „Научни изследвания“ на Шуменския университет „Епископ Константин Преславски“

- невалидност на теста;
- забавяне от две или три седмици за получаване на резултат (времето изминало от теста и времето за ремонт на цилиндъра);
- нужда от нов водосъдържател. Стандарта не позволява прекъсване на теста, отваряне на системата и продължаване от цикъла до който сме стигнали преди повредата на цилиндъра;
- проникване на вода в отделението за въздуха, като това може да доведе до засмукване на вода от компресора и повреда на скъпо оборудване.

Проектиране на стенда

Настоящият стенд се проектира в търсене на решение на гореизложения проблем.

Буталните цилиндри разчитат на бутало, което се движи през първия етап на цикъла, при отваряне на нагнетателни клапан в едната посока за да създаде налягане във водосъдържателя, а след това под действие на налягането създадено в първия етап се връща в първоначалната позиция, след като е отворен изпускателния клапан. Поради огромния брой цикли (до 100 000) и високото налягане, дори и минимални механични примеси водят до прекомерно износване на гумените уплътнители, като понякога буталните цилиндри не успяват да издържат дори един пълен тест (по-малко от 20 000 цикъла). Това забавя и без това дългата процедура на теста и внася съмнения в коректността на целия тест [2].

Помпите за виско налягане разчитат на помпа която създава нужното налягане и сложна система от управляеми клапани и вентили. При тази ситема задължително трябва да се предвиди ресийвър за изпусканото налягане. Сиситемата е доста сложна за проектиране, експлоатация, поддръжка и диагностика. Освен това е в пъти по-скъпа от традиционните цилиндри.

Решението е въвеждане на междинен буферен съд, който е напълнен с вода до определено ниво, а останалата част от обема е с въздух. Частта от буферния съд пълна с вода е много по-голяма от частта на въздуха. Това се прави защото свиването на водата при тези налягания е пренебрежимо малка в сравнение с това на въздуха. Обема на въздуха е точно изчислен и е синхронизиран с дебита на въздуха под налягане от външния източник така че свиването на въздуха да може да повиши налягането в буферния съд, съответно във изпитвания водосъдържател, в съответствие с градиента на нарастване на налягането зададен по стандарта EN 12897 [1, 2, 7].

Освобождаването на налягането трябва да се осъществи с изпускане на въздуха навън в атмосферата (околната среда). Това се прави защото така е много лесно да се контролира скоростта на намаляване на налягането.

Недостатък на този метод е нуждата от специален компресор за високо налягане. С напредването на технологиите обаче, компресорите за високо налягане стават все по-надеждни и все по-достъпни. А повишената надеждност на тестовата установка, предсказуемостта на времето за един тест и липсата на престои за ремонт са достатъчна отплата за по-високата цена на компресора.

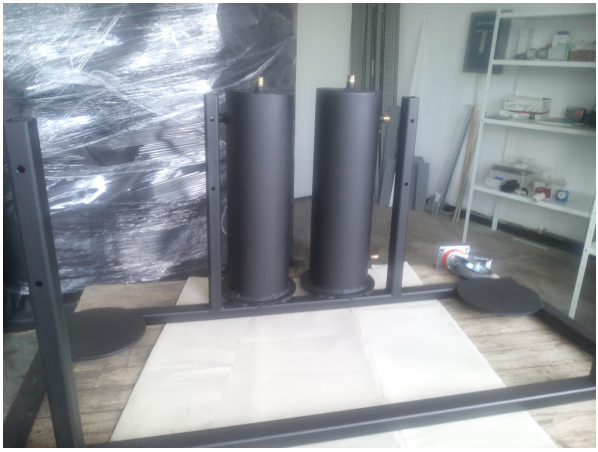
В крайна сметка беше проектиран иновативен въздушно-воден цилиндър, който да може да изпълнява огромен брой цикли комбиниран с лесно, интуитивно

управление. При проектирането е обърнато внимание и на основните принципи на човеко-машинния интерфейс [3].

Разработване и експлоатация на стенда

Стенда за изпитване на водосъдържатели е конструиран така че да покрива изискванията на стандарта EN12897. По този стандарт се изпитват бойлери с директно и индиректно загряване, с или без обезопасителен клапан и разширителен съд.

Стенда е изграден около здрава метална конструкция (Фиг. 1), която е способна да издържи собственото тегло на стенда и допълнителното натоварване от два 150 литрови водосъдържателя пълни с вода. Металната конструкция е прахово боядисана за да е устойчива на корозия и е поставена на колела (Фиг. 2) за по-лесна работа.



Фиг. 1. *Конструкция на стенда*

Фиг. 2. *Основа на конструкцията.*

Съставните части на стенда са:

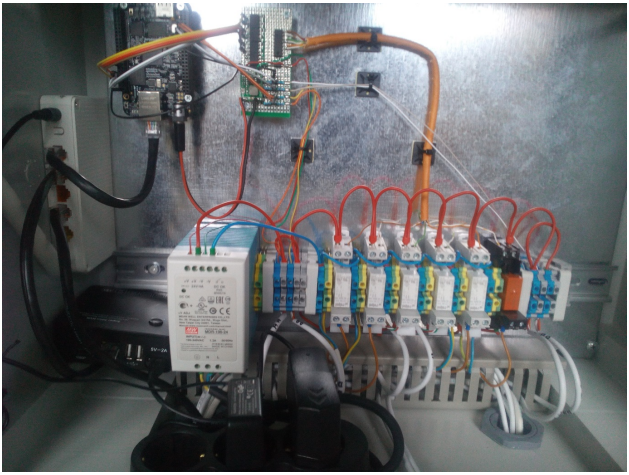
1. Метална поставка за водосъдържателя. Изработена от 5мм дебел стоманен лист. Здраво заварен към носещата конструкция (Фиг. 3).

Фиг. 3. *Метална поставка за водосъдържателя.*

2. Въздушно-воден цилиндър (Фиг. 4). Изработен със заварки от тръба с диаметър 125 мм и дебелина 5 мм и стоманени дискове с дебелина 5 мм. На две места на цилиндъра и на горния диск са заварени три щуцера завършващи с резба ½“. Самите цилиндри са здраво заварени към носещата конструкция. Всички заварки са направени с апарат за заваряване и от лицензиран заварчик. Здравината на въздушно-водните цилиндри е тествана с налягане 16 bar. Долния щуцер монтиран на страната на цилиндъра се състои от накрайник за бърза връзка, спирателен кран и филтър. Това е входа за водата за напълване на въздушно-водния цилиндър и водосъдържателя от външен източник. Горния щуцер монтиран на страната на цилиндъра е изхода на водата от въздушно-водния цилиндър към водосъдържателя. На него са монтирани манометър и трансмитер за измерване на налягането на водата в цлиндъра и водосъдържателя, обезвъздушителен клапан и гъвкава връзка за свързване с изпитвания водосъдържател. На щуцера заварен на горния диск са монтирани манометъра и трансмитера за измерване на налягането на въздуха, двата електромагнитни вентила (вертикално нагнетателния, хоризонтално изпускателния), регулатора за налягане със собствен манометър и двата пневматични вентила (най-горе вертикално нагнетателния, хоризонтално изпускателния). От тези два пневматични вентила се прави предварителната настройка на стенда. Върху нагнетателния пневматичен вентил е монтирана бърза връзка за свързване към източника на сгъстен въздух [3, 5, 6].

Фиг. 4. *Въздушно-воден цилиндър.*

3. Табло за управление съдържащо: едноплатков компютър BeagleBone Black, постоянно токово 24 V-тово захранване Meanwell, релета и платка за осигуряване на интерфейс между BeagleBone-а и свързаните устройства за измерване на физически величини (трансмитер за налягане) и управление на устройствата (електромагнитните клапан) (Фиг. 5).



Фиг. 5. *Табло за управление.*

4. Рутер за осигуряване на връзката между всички устройства (BeagleBone, лаптоп Asus, IP камера Megapixels и NVR Supermini).

5. Supermini NVR с възможност за управление на IP камерата и устройство за записи.

6. Уебкамера Megapixels за записване на процеса (Фиг. 6).

Фиг. 6. *Уебкамера.*

7. Резервно захранване UPS Eaton 850VA (Фиг. 7). Понеже един тест трае повече от 10 дни, ако има кратковременно прекъсване на захранването в рамките на тестовия период може да провали теста. Ако прекъсването на захранването е за по-дълго, резервното захранване дава възможност да се спре теста. След възстановяване на захранването теста се подновява. За да не се загуби бройката цикли до момента на спиране са предвидени механични броячи.

Фиг. 7. *Резервно захранване UPS Eaton 850VA.*

8. Механични броячи на цикли (Фиг. 8). Управляват се от BeagleBone-а и превключват в началото на всеки нов цикъл. Нулират се механично от копче на корпусът им.

Фиг. 8. *Механични броячи на цикли*

9. Алуминиева конструкция закрепена с болтове към металната носеща конструкция за монтаж на операторския плот (Фиг. 9).

Фиг. 9. *Алуминиева конструкция за монтаж на операторския плот*

10. ПДЧ плоскост за операторски плот (Фиг. 10)

Фиг. 10. *Плоскост за операторски плот*

11. Компютър ASUS за управление на процесите от оператора.
12. Монитор Philips за показване на SCADA
13. Докинг станция J5Create, модел JUD481 за осигуряване допълнителни интерфейси към компютъра и възможността за включване на допълнителни устройства.
14. Комплект клавиатура и мишка Dell, за операторски интерфейс.

Кратко описание на процеса

Въпреки че стендът се управлява от едно управление от едно електрическо табло, той е конструиран така че да позволява едновременно изпитване на два водосъдържателя. При определени обстоятелства няколко водосъдържателя могат да се свържат последователно и да се изпитват едновременно. Условието е да са с еднакви обеми, работни налягания и да са от

един вид (например: електрически, без разширителен съд и обезопасителен клапан). Постановка с така свързани водосъдържатели се нарича стринг.

Всяка система за изпитване се състои от въздушно-воден цилиндър, кранове за вода, кранове за въздух, регулатор за налягане на въздуха, електрически задвижвани пневматични вентили, манометри за вода и въздух и датчици за налягане на въздуха и водата.

При изпитването на водосъдържатели те се запълват с вода. Изпитването на налягане само с въздух би довело до същия резултат, но запълването с вода намалява риска при изпитване. Водата има много нисък коефицент на свиване и при внезапно спукване или разкъсване на водосъдържателя не довежда до рязко разширение на флуида, както би било с въздуха. Ако водосъдържателя е пълен с въздух под налягане, при спукването му се получава рязко разширение и ефект като при взрив. Докато ако водосъдържателя е пълен с вода ефекта при спукване е минимален – водата почти не променя обема си.

Основната част на изпитвателния стенд е въздушно-водния цилиндър. Уникалния и иновативен дизайн на стенда позволява изпитването да става без движещи се части, които намалява до минимум възможността от повреда или провал на теста поради износена част.

Преди старта на всеки тест е необходимо да се спази следната процедура и да се направят следните настройки:

1. Проверява се работното налягане на водосъдържателя, предписано от производителя.
2. Определя се изпитвателното налягане, според метода на изпитване, който ще ползваме (например 20 000 цикъла с 1,5 пъти номиналното налягане)
3. Настройва се регулатора за налягането на въздуха да отговоря на налягането определено в точка 2.
4. Според обема на изпитвания водосъдържател (или стринга от водосъдържатели) се отварят нагнетателния и изпускателния клапан, в такава позиция че да нагнетателния и изпускателния етап от изпивателния цикъл да имат продължителността от точка 4.3.3.1 на стандарта EN12897

След изпълнение на процедурата по предварителната подготовка и настройки се присъединява водосъдържателя към стенда. Водосъдържателя се поставя на мястото за изпитване и се укрепва срещу падане и накланяне. Към единия извод на водосъдържателя се присъединява изходящата от стенда гъвкава връзка, а на другия извод се монтира кран. Добра идея е след крана да се монтира маркуч или гъвкава връзка за отвеждане на водата при пълнене.

След като водосъдържателя е поставен на мястото за изпитване, надлежно укрепен и подготвен се пристъпва към напълване. Това става като към стенда се присъединява източник на вода под налягане. При съединяването става към най-долния отвор на въздушно-водния цилиндър. Отваря се кранът и започва пълнене с вода на водната част от въздушно-водния цилиндър и водосъдържателя. Пълненето продължава докато от изходящия кран на водосъдържателя потече стабилна струя вода, без балончета въздух. Това означава че водосъдържателя е пълен с вода. Тогава се затваря изходящия кран на извода на водосържателя. След това се затваря крана на входа на въздушно –водния цилиндър (Фиг. 11).

Фиг. 11. *Кран на входа на въздушно –водния цилиндър*

Така системата е пълна с вода при определено налягане и е готова за започване на същинската процедура по изпитването. Налягането не зависи от стенда и водосъдържателя, а от външния източник на вода, който използваме. Затова изпитвателната процедура започва с еднократно отваряне на изпускателния въздушен клапан за да се намали налягането до нула и така то да няма влияние по-нататък върху теста.

След стартиране на същинската процедура започва цикъл състоящ се от следните етапи:

1. Отваря се нагнетателния въздушен клапан. През регулатора за налягане на въздух, пневматичния нагнетателен кран и нагнетателния електромагнитен вентил нахлува въздух с определена скорост, като при правилни настройки (описани по-горе в текста) на 15-та секунда налягането в цилиндъра и водосъдържателя трябва да достигне точно определеното за изпитване (например 1,5 номиналното налягане).

2. След 15-та секунда (и достигане на тестовото налягане), електромагнитния клапан се затваря като прекъсва притока на въздух под налягане. Това е етапа на задържане, който трае също 15 секунди.

3. Отваря се изпускателния електромагнитен клапан. През пневматичния изпускателен вентил и електромагнитния изпускателен клапан, нагнетения въздух от въздушно-водния цилиндър се изпуска от околната среда. При правилни настройки за времето на изпускането (отново 15 секунди) налягането спада обратно до 0.

Промените в налягането се наблюдават на двата манометъра за налягане съответно на водата и на въздуха. За целите на теста налягането се отчита от трансмитери за налягане (отново един за водата и един за въздуха), като показанията им се показват на монитора на стенда и могат да бъдат записвани.

Регулатора за налягане също има манометър (Фиг. 12), но той показва само налягането до което е ограничена системата. Той служи за диагностика на външния източник на въздух под налягане (компресора). Ако налягането се промени (падне под настроеното тестово налягане) означава че има проблем с налягането и теста трябва да се спре.

Фиг. 12. *Регулатор за налягане*

Теста продължава докато се достигне един от следните резултати:

— Достигнат е броя цикли за съответния водосъдържател и съответното налягане (например 20 000 цикъла). В този случай се съставя протокол с положително становище, че водосъдържателя е издържал теста.

— Наблюдава се теч. В този случай се прави снимка на компрометираното място (заварка, ръб, огъвка и т.н) и се съставя протокол с отрицателно становище, че водосъдържателя не е издържал теста.

Стандарта EN12897 позволява известна вариативност в продължителността на етапите на цикъла на изпитване. За продължителността на етапите на един цикъл тук са избрани 15 секунди. Това е минималното време за един цикъл. Тази продължителност е избрана с цел спестяване на време (при 20 000 цикъла продължителността на теста е 250 часа) и доставяне на резултати по-бързо на Възложителя.

След стартиране на същинската част на изпитвателната процедура, контрола се поема от контролната част на стенда. В случая е използван едноплатков компютър BeagleBoneBlack. Той извършва следните действия:

1. Преди първия цикъл отваря за 2 секунди изпускателния пневматичен клапан за да изравни налягането на водата в въздушно-водния цилиндър и водосържателя с атмосферното.
2. Изпраща импулс към механичния брояч на импулси и отваря нагнетателния пневматичен клапан. Клетката от вътрешната памет, която съдържа броя цикли се увеличава с единица.
3. Изчаква 15 секунди, като през това време отчита нарастването на налягането на водата и въздуха във въздушно-водния цилиндър и водосъдържателя.

4. Затваря нагнетателния клапан
5. Изкачва 15 секунди.
6. Отваря изпускателния пневматичен клапан
7. Изчаква 15 секунди, като през това време налягането на водата и въздуха във въздушно-водния цилиндър и водосъдържателя трябва да спадне обратно до 0 bar.
8. Повтаря стъпки от 2 до 7 докато достигне тестовата бройка цикли или докато не се компрометира водосъдържателя.

Заключение

Представеният стенд е предназначен за циклично натоварване водосъдържатели с налягане и за време, указано от стандарта EN12897 и според декларираното от производителя на водосъдържателя [1, 5].

На базата на извършени проучвания са изведени недостатъците на досега съществуващите методи за изпитания и е предложен иновативен подход с използване на въздушно-воден цилиндър, който да може да изпълнява огромен брой цикли комбиниран с лесно, интуитивно управление. Този стенд е проектиран и разработен на базата на предложения подход за нуждите на Фирма “КИОСК БЪЛГАРИЯ” ООД.

ЛИТЕРАТУРА

[1] БДС EN 12897:2016, Български институт за стандартизация, https://bds-bg.org/bg/project/show/bds:proj:95025.

[2] Цанков Ц., Александрова А., Спасова М. Полезен модел на ремарке за мотоблок. Научна конференция с международно участие MATTEX 2018, гр. Шумен, 2018, ISSN 1314-3921, с. 203-209.

[3] Цанков Ц., Тончева Й., Спасов С. Безотпадна технология за изработване на кош за малко ремарке. Научна конференция с международно участие MATTEX 2018, гр. Шумен, 2018, ISSN 1314-3921, с. 210-216.

[4] Steingress, Frederick M.; Frost, Harold J.; Walker, Darryl R. (2003). High Pressure Boilers (3rd ed.). American Technical Publishers.

[5] Hadzhiivanov, H., Human machine interface siemens in industrial automation. Annual of Konstantin Preslavski University of Shumen, Vol T. XI E Technical Sciences, ISSN 1311-834X, pp.329-337

[6] Hadzhiivanov H., 2021, SIEMENS SIMATIC CONTROLLERS IN INDUSTRIAL AUTOMATION, Annual of Konstantin Preslavski University of Shumen, Vol T. XI E Technical Sciences, ISSN 1311-834X, pp. 99-105

[7] Tsankov Ts. Acquiring a patent in Republic of Bulgaria. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 73, September 2020, ISSN 2367-5721, pp. 168-182.

ИМПЛЕМЕНТАЦИЯ НА BEAGLEBONE BLACK ЗА УПРАВЛЕНИЕ НА СЕРВОМОТОР С ЕНКОДЕР

Милен К. Петков

A BEAGLEBONE BLACK IMPLEMENTATION OF SERVO MOTOR CONTROL WITH AN ENCODER*

Milen K. Petkov

ABSTRACT: *In this article, methods for measuring various analog, physical quantities are considered. Two types of sensors and the control of the power part of a servomotor are analyzed. A BeagleBone Black implementation for controlling a servo motor with an encoder is shown.*

KEYWORDS: *BeagleBone Black, encoders, MOC3063S, TMP36.*

Най-сериозното предизвикателство пред внедряването на BeagleBone Black в различни приложения за автоматизация в индустрията и бита е използването на периферни и крайни устройства (сензори и актуатори).

В индустрията основното напрежение за автоматизация е 24 VDC. Това е напрежението с което работят най-голямата част от PLC-тата. Съответно голяма част от предлаганите на пазара сензори, релета и всякакъв вид –мери са възприели това напрежение за захранващо и работно.

Силовите захранвания на мощните уреди (двигатели, нагреватели) в индустрията и бита са възприели монофазно напрежение 240 VAC и трифазно напрежение 400 или 680 VAC.

За една част от енкодери за двигатели, генератори на импулси на измервателни уреди и мултивибратори за управление са възприели напрежение 5 VDC. За същото напрежение има разработени PLC-та, базирани на Raspberry Pie или на Arduino [1, 4, 5].

В по-редки случаи се използва напрежение 12VDC.

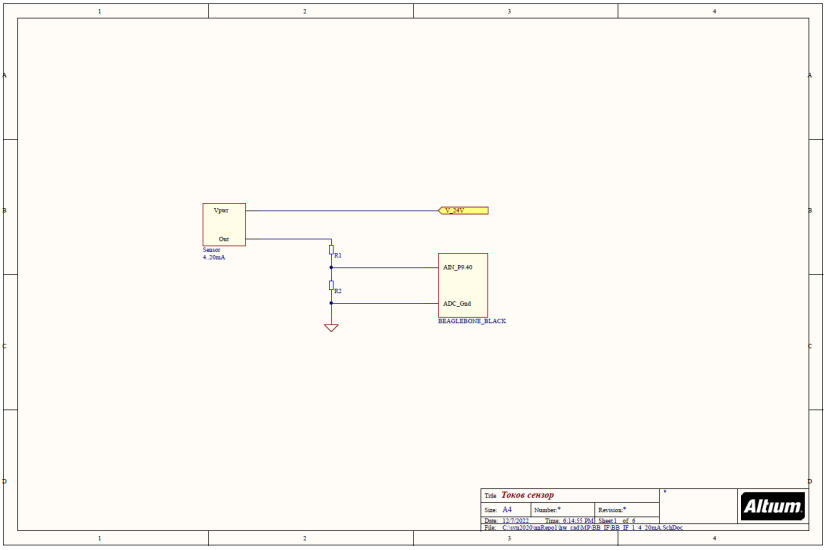
BeagleBone Black използва 5VDC за захранване, 3,3 VDC за оперативно напрежение и 1,8 V за аналоговите входове и изходи. Това не позволява директно използване на повечето от горе-посочените елементи.

В тази статия ще бъде показано начините с които стандартни сензори, актуатори и силови елементи могат да се адаптират за използване към BeagleBone Black.

Най-разпространения в индустрията метод за измерване на различни аналогови, физични величини е токовия сензор 4-20 mA (Фиг. 1). Предимствата му са че използва двупроводна линия и има самодиагностика. При нулева

* Този труд се издава с частичната финансова подкрепа на проект РД-08-130/04.02.2021 от фонд „Научни изследвания“ на Шуменския университет „Епископ Константин Преславски“

стойност на измерваната физическа величина през контура продължава да тече ток от 4 mA. В токовия кръг на сензора се включва съпротивление R2, с такава стойност че падът на напрежение върху него да не превишава 1,8 V при 20 mA ток в токовия кръг (максимална стойност на физическата величина. В този случай аналоговия вход на BeagleBone Black се включва паралелно на съпротивлението R2. Измервайки пада на напрежението върху съпротивлението можем да установим стойността на тока в токовия кръг и от там стойността на измерваната физическа величина.

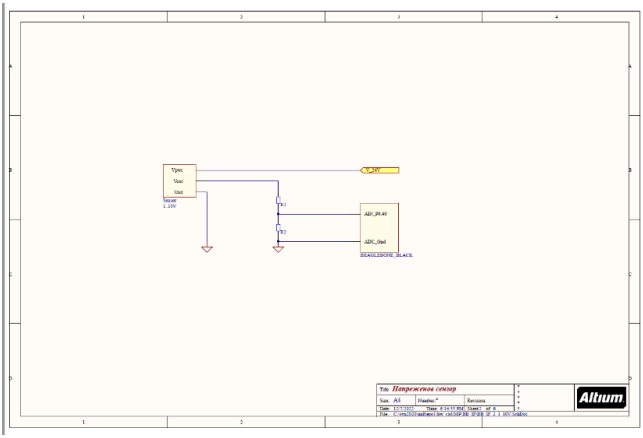


Фиг 1. *Токов сензор 4-20 mA*

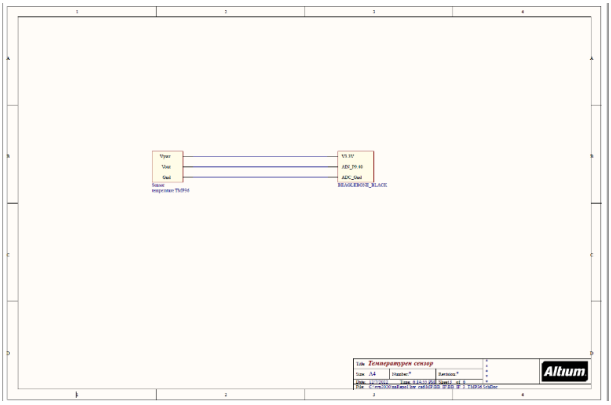
Най-обикновения и базов метод за измерване на аналогови, физични величини е сензора за напрежение 0-10 V (Фиг. 2). Предимствата му са че е много лесен за работа и диагностика и е универсален за всички видове индустриални контролери. Недостатъци са че е податлив на електромагнитни смущения, линията му е трипроводна и при голямо разстояние между контролера и реалното място на измерване може да се получи пад на напрежение, което да доведе до намалена точност на измерването. И най-големия недостатък е че не може да се направи разлика между нулева стойност на измерваната величина и повреда – напрежението и при двата случая е 0 V. Понеже изходящото напрежение може да достигне 10 V не може директно да се подаде към някой от DI на BeagleBone Black. Затова трябва да се направи делител на напрежение с използването на съпротивления R1 и R2, като стойностите им се избират така че при максимална стойност на измерваната физическа величина (изходящо напрежение 10 V) напрежението върху съпротивлението R2 да не надвишава 3 V [2, 3, 10].

Една много важна и често използвана в различни процеси физическа величина е температурата. За измерването ѝ има разработени безброй различни термометри, трансдусери и преобразуватели. Тук ще бъде разгледан един много

прост метод за измерване на температура с помощта на полупроводников елемент TMP36 (Фиг. 3). Това е малка интегрална схема със захранващо напрежение от 2.7V до 5.5V (т.е. директно може да се включи към оперативното напрежение на BeagleBone Black) и само 0.05 mA консумация на ток. Предимствата му са че изходящото напрежение (измерването) е линейно и пропорционално на температурата в градуси по Целзий. Не се нуждае от калибриране, работи добре при различни условия на околната среда и не се нуждае от допълнителна поддържка.



Фиг 2. *Сензор за напрежение 0-10 V*

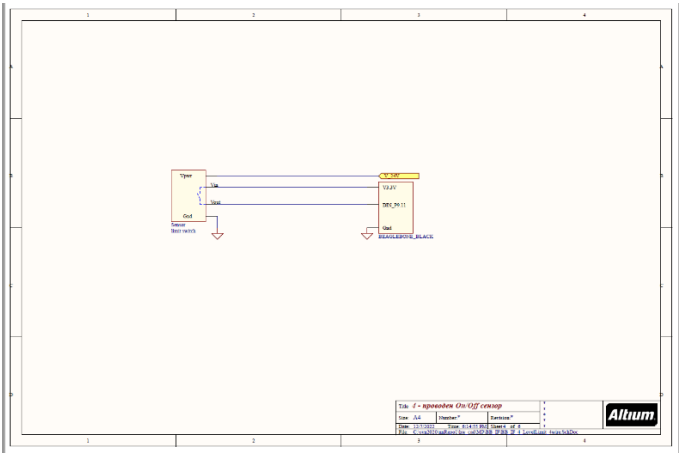


Фиг 3. *Температурен сензор*

Много често в индустрията не е необходимо непрекъснато измерване на дадена физическа величина, а само дали е премината някаква гранична стойност. Например дали даден котел е достигнал работни (или критични) налягане и температура, дали даден съд е празен за да включим помпата и дали е пълен за да я изключим, дали дадена машина е достигнала крайна точка на хода си и т.н. В тези случаи се използват така наречените ON/OFF сензори (ключове).

Тези сензори са два вида:

Четирипроводни (Фиг. 4). Това са сензори, които имат контактна система (нормално отворени или нормално затворени контакти) независима от захранващото напрежение. Тук приложението към BeagleBone Black е много лесно, защото контактната система на сензора се свързва директно към оперативното напрежение на BeagleBone Black (3,3 VDD) и към някой от GPIO-тата(general purpose input/output), конфигуриран като DI (дигитален вход).



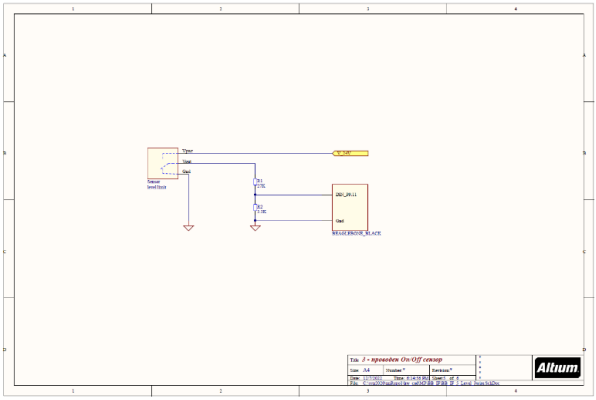
Фиг 4. *Четирипроводен ON/OFF сензор*

Трипроводни (Фиг. 5). Както личи от името им те имат само три проводника. Двата са захранващото напрежение, а третия е за обратната връзка на състоянието. При тях контактната система е от един нормално затворен и един нормално отворен контакт с общ край. Контролера получава две стойности в зависимост от стойността на физическата величина: или 0 V или захранващото напрежение. Когато захранващото напрежение е различно от 3,3 V не може директно да се подаде към някой от DI на BeagleBone Black. Затова трябва да се направи делител на напрежение с използването на съпротивления R1 и R2, като стойностите им се избират в зависимост от захранващото напрежение [6, 8, 9].

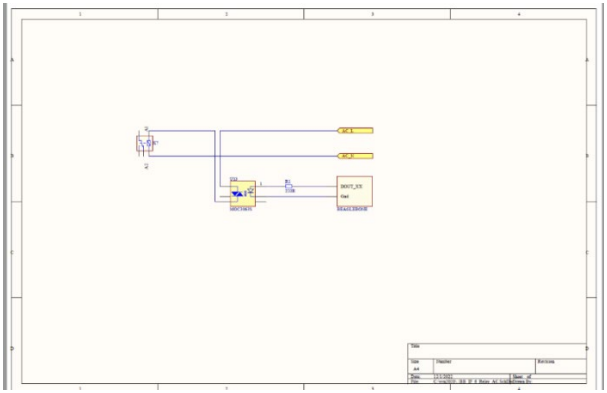
Когато става дума за управление на силова част (двигатели, нагреватели и други) BeagleBone Black не може да се включи директно в управляващата верига, а трябва да се направи така наречената вторична (или управляваща) комутация. Тук отново има два варианта:

Релета и актуатори с номинално, комутационно напрежение 3 V или Solid state relays с ниво на комутационно напрежение 3-32 V. Подобно на четирипроводния ON/OFF сензор и тук свързването е много лесно, защото комутационното и силовото напрежение са независими едно от друго.

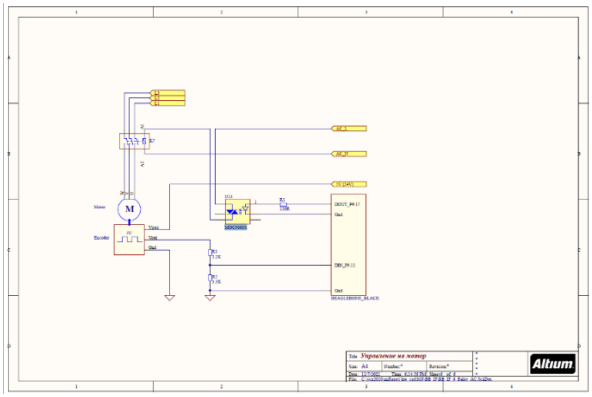
Релета и актуатори с номинално, комутационно напрежение различно то 3 V. При този вариант задължително трябва да се използва галванично разделяне на веригите. Това се постига с използването на optocoupler (оптична двойка). В този конкретния случай е използван MOC3063S (Фиг. 6).



Фиг 5. *Трипроводен ON/OFF сензор*



Фиг 6. *Свързване на актуатор*



Фиг 7. *Управление на мотор*

Следващата схема (Фиг. 7) е като обобщение на всичко казано по-горе. Показано е управление на сервомотор с енкодер. При команда (пуск бутон, софтуерна апликация и т.н.) се задейства дигиталния изход на BeagleBone Black, който посредством оптоизолатор-триак MOC3063S задейства контактора на силовата част на мотора. След стартирането на мотора импулсите от енкодера се подават на дигиталния вход на BeagleBone Black за да се ползват за обратна връзка за работата на мотора [7, 8].

ЛИТЕРАТУРА

[1] Лалев Х., Желев С., Цанков Ц. Анализ и мониторинг на честотните характеристики на RLC вериги. Научна сесия на факултет „Артилерия, ПВО и КИС“, Шумен, 2009, ISSN 1314-1953.

[2] Лалев Х. Л., Цанков Ц. С. Синтез на компютърни системи за работа в реално време. Международна научна конференция, посветена на 105-годишнината от рождението на Джон Атанасов и Джон фон Нойман, Шумен, 2008, ISBN 978-954-577-540-6.Steingress, Frederick M.; Frost, Harold J.; Walker, Darryl R. (2003). High Pressure Boilers (3rd ed.). American Technical Publishers.

[3] Denev D. Z-wave communication for home automation. Scientific Conference with international participation MATTEH 2020, Conference proceedings, Vol. 2, Shumen, 2020, ISSN 1314-3921, pp. 96-103.

[4] Denev D., Yankova-Yordanova Y., Konstantinova E. Program for managing an automated conveyor for packaged food products and 3D simulation of its work. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 68, April 2020, ISSN 2367-5721, pp. 1-7.

[5] Hadzhiivanov, H., Human machine interface siemens in industrial automation. Annual of Konstantin Preslavski University of Shumen, Vol T. XI E Technical Sciences, ISSN 1311-834X, pp.329-337

[6] Hadzhiivanov, H., Problem with start direction in servo system at Homing procedure MATTEH 2022, Conference proceedings, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 40-46.

[7] Stoyanov S., Stoyanova T. Process automation using microcontrollers and cloud databases. Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 23-28.

[8] Vasilev D. Automated monitoring and control system for photovoltaic hybrid power supply system for 10 kW server unit. Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of technical sciences, 2020, ISSN 1311-834X, pp. 294-298.

[9] https://cdn.bluecommerce.shop/media/1/c0d113702_solid-state-relais-3-32v-40a-24-380vac_1000x.webp

[10] https://www.pollin.de/images/600x600x90/I340633.1-Solid-State-Relais-SSR-D32A380-5-3-32-V-5-A-380-V.jpg

ПРИСВОЯВАНЕ НА ДЪЛЖИНА НА ВЪЛНАТА ЗА WDM МРЕЖИ

Цветослав С. Цанков, Екатерина М. Христова

WAVELENGTH ASSIGNMENT FOR WDM NETWORKS

Tsvetoslav S. Tsankov, Ekaterina M. Hristova

ABSTRACT: *One of the most fundamental problems in wavelength-routed WDM networks is addressed: the routing and assignment of wavelengths. The light stream is used to maintain a connection in a wavelength-routed WDM network and can span multiple fiber links. In the absence of wavelength converters, the flux must occupy the same wavelength on all fibers through which it passes. This property is known as the wavelength continuity limit.*

KEYWORDS: *Multiplexing, optical fiber, packet switching, signal-to-noise ratio, wavelength, WDM.*

Статичната RWA е известна още като проблем със Статично Създаване на Светлинни Потоци. При нея заявките за установяване на връзка със светлинен сигнал са известни предварително и операциите по маршрутизиране и присвояване на дължина на вълната са изпълнявани офлайн. Основната цел е намаляване броя на дължините на вълните, необходими за установяване на определен набор от светлинни потоци за дадена топология. Като алтернатива на намаляването на броя на вълните в мрежата, двойната задача е увеличаването на максималния брой на връзките, които могат да бъдат създадени (ограничаване на блокирането) за даден брой от дължини на вълните и дадено множество от връзки. Този двоен SLE проблем повдига въпроса на справедливост, като решаването на този проблем ще създаде повече къси връзки, които преминават по оптичните влакна, отколкото дълги връзки, които преминават през по-голям брой възли.

SLE с ограничение за непрекъснатост на дължината на вълната може да бъде формулирана като ILP – Целочислена Линейна Програма (ЦЛП), в която целевата функция е да се намалява потока във всяка връзка, което от своя страна съответства на намаляването на броя на преминаващите фотонни потоци през конкретна връзка.

Нека λ_{dw} означава трафика (брой заявки за връзка) от всеки източник s до всяко местоназначение d на всяка дължина на вълната w. При нужда могат да бъдат настроени две или повече оптични пътеки между една и съща двойка източник-предназначение, но всеки от тях трябва да използва различна дължина на вълната, т.е. $\lambda_{dw} < 1$. Нека F_{ij}^{sdw} обозначава трафика (брой заявки за връзка) от източник s до местоназначението d на връзка ij и дължина на вълната w.

$F_{ij}^{sdw} < 1$, тъй като дължина на вълната на връзката може да бъде присвоена само от един оптичен поток. Като се има предвид физическата топология на мрежата, множеството от дължини на вълните и матрицата на трафика Λ, в която $\Lambda\, sd$ обозначава брой връзки, необходими между s и d, проблемът може да се формулира както следва (което се оказва Целочислена Програма):

Търсене на минимален брой дължини: $F_{\max}$

така че

$$F_{\max} \geq \sum_{s,d,w} F_{ij}^{sdw} \ \forall ij \ (1)$$

$$\sum_{i} F_{ij}^{sdw} - \sum_{k} F_{jk}^{sdw} = \begin{cases} -\lambda_{sdw} & \text{ако } s = j \\ \lambda_{sdw} & \text{ако } d = j \\ 0, & \text{в останалите случаи} \end{cases}$$

$$\sum_{w} \lambda_{sdw} = \Lambda_{sd} \ (2)$$

$$F_{ij}^{sdw} = 0{,}1 \ (3)$$

$$\sum_{s,d} F_{ij}^{sdw} \leq 1 \ (4)$$

Този подход може също да се използва за получаване на минималния брой дължини на вълните, необходими за даден набор от заявки за свързване чрез търсене на минималния брой дължини на вълните в мрежата. При зададен брой дължини на вълната може да се приложи търси решение чрез ILP. Ако такова не се намери, се използват по-голям набор от дължини, докато се намери достатъчния минимален брой дължини на вълната [1, 2, 6].

Формулираната задача е NP-пълна. Разглежда се как една по-проста форма на проблема може да бъде решена чрез намаляване на размера му и облекчаването на ограниченията му за интегралност и цялостност.

Другата подзадача за намиране на максималния брой установени връзки за фиксиран брой дължини на вълните и даден набор от заявки за връзка може също да бъде формулиран като ILP.

Дефинирани са следните параметри:

N_{sd}: Брой двойки източник-местоназначение.

L: Брой връзки.

W: Брой дължини на вълните на връзка.

m = $\{m_{\text{i}}\}$, $i = 1, 2, \ldots, N_{sd}$: Брой връзки, установени за двойката източник-местоназначение i.

ϱ : Предлагано натоварване (общ брой заявки за маршрутизиране).

q = $\{q_i\}$, $i = 1, 2, \ldots, N_{sd}$: Част от товара, който пристига за двойката източник-местоназнчение i (по този начин q_i ϱ = брой връзки, които трябва да се настроят за двойката източник-местоназначение i). (Това е дефиницията на за натоварване за статичния случай. Дефиницията на натоварване динамичния случай е различна)

P: Набор от пътища за маршрутизиране на връзка.

$A = (a_{ij})$: $P \times N_{sd}$ матрица, в която $a_{ij} = 1$, ако път i е между двойката източник-местоназначение j и $a_{ij} = 0$ в противен случай.

$B = (b_{ij})$: $P \times L$ матрица, в която $b_{ij} = 1$, ако връзка j е по пътя i и $b_{ij} = 0$ в противен случай.

$C = (c_{ij})$: $P \times W$ матрица за маршрут и дължина на вълната, така че $c_{ij} = 1$, ако дължината на вълната j е присвоена на пътя i, и $c_{ij} = 0$ в противен случай.

Целта на задачата с Маршрутизирането и Присвояването на Дължината на Вълната е да се увеличи максимално броят на установените връзки, $C_0\,(\varrho, q)$. Формулата на ILP е както следва:

Търсене на максималния брой дължини: $C_0(\varrho, q) = \sum_{i=1}^{Nsd} \mathrm{m}_i$ (5)

$\mathrm{m}_i \geq 0$, цяло число, $i = 1, 2, \ldots N_{sd}$ (6)

$c_{ij} \in \{0, 1\}\, i = 1, 2, \ldots, \mathrm{P}, j = 1, 2, \ldots, \mathrm{W}$ (7)

$C^T B \leq 1_{W\,x\,L}$ (8)

$\mathbf{m} \leq 1_W C^T A$ (9)

$\mathrm{m}_i \leq q_i \varrho, i = 1, 2, \ldots, N_{sd}$ (10)

Уравнение (5) изчислява общия брой създадни връзки в мрежата. Уравнение (8) уточнява, че една дължина на вълната може да се използва най-много веднъж в дадена връзка, където $1_{W\,x\,L}$ е матрицата $W\,x\,L$, чиито елементи са единица. Уравнения (9) и (10) гарантират, че броят на установените връзки е по-малък от броя на заявените връзки, където 1_W е матрицата $1\,x\,W$, чиито елементи са единица.

В маршрутизирана по дължина на вълната WDM мрежа, ограничението за непрекъснатост може да бъде премахнато, а в междинако се използва преобразувател на дължина на вълната, за преобразуване на данните, пристигащи от една връзка в друга дължина на вълнов възел, преди да бъдат препратени по следващата връзка. Такава техника е осъществима и се нарича преобразуване на дължина на вълната. Маршрутизираните по дължина на вълната мрежи с тази способност се наричат мрежи с конвертируема дължина на вълната [3, 4]. Ако преобразувателят предоставя възможност за преобразуване от всяка дължина към всяка друга дължина (за такива преобразуватели на дължина на вълната се казва, че имат капацитет за пълен обхват) и ако има един преобразувател на дължина на вълната за всяка оптична връзка във всеки възел на мрежата, тогава се твърди, че мрежата има пълни възможности за преобразуване на дължина на вълната.

Единичен светлинен поток в такава конвертируема по дължина на вълната мрежа може да използва различна дължина на вълната по всяка от връзките по своя път. По този начин преобразуването на вълната може да подобри ефективността на мрежата чрез разрешаване на конфликтите между светлинните пътища. Обикновено, за дадена схема за маршрутизиране, преобразуването на дължина на вълната осигурява долна граница на постижимата вероятност за блокиране на дадена схема при определяне на дължина на вълната.

Нека λ_{sd} обозначава трафика (броя заявки за свързване) от всеки източник s до всяко местоназначение d. Нека F_{ij}^{sd} обозначава трафика (броя заявки за връзка) от s до d на връзката ij. Формулировката на RWA задачата без ограничението за непрекъснатост на дължината на вълната е както следва:

Търсене на минимален брой дължини : $F_{\max}$

$$\mathrm{F}_{\max} \geq \sum_{s,d} F_{ij}^{sd} \ \forall\, ij \quad (11)$$

$$\sum_{i} F_{ij}^{sd} - \sum_{k} F_{jk}^{sd} = \begin{cases} -\lambda_{sd} & \text{ако } s = j \\ \lambda_{sd} & \text{ако } d = j \\ 0 & \text{в останалите случаи} \end{cases} \quad (12)$$

В много случаи преобразуването на цялата дължина на вълната в мрежата може да не е предпочитано и дори да не е необходимо поради високите разходи и ограничението в производителността. Единият вариант е подгрупа от възли да позволява преобразуване на дължина на вълната, като преобразувателят на дължина на вълната се споделя от повече от една оптична връзка. А другият – възел да използва преобразуватели, които могат да преобразуват само в ограничен диапазон от дължини на вълната. Проблемите, свързани с проектирането на маршрутизирана по дължина на вълната WDM мрежа с ограничено преобразуване на дължина на вълната, могат да бъдат:

1. Рядко разположение на преобразувателите на дължина на вълната в мрежата: докато преобразувателите остават скъпи, може да не е икономически изгодно да се оборудват всички възли в една WDM мрежа с тези устройства. Ефектите от разреденото преобразуване (т.е. наличието само на няколко преобразуващи комутатора в мрежата) върху блокирането на връзката също са изследвани. Интересен въпрос е къде оптимално да се поставят тези трансформатори в произволна мрежа и какъв е вероятният път за надграждане към пълноценна конвертируемост. Представена е евристична техника за поставяне на тези редки преобразуватели.
2. Споделяне на преобразуватели: дори сред комутаторите, способни да преобразуват вълната, може да не е рентабилно да се оборудват всички изходни портове на комутатора. Предложени са дизайни на архитектури на комутатори, които позволяват споделяне на преобразуватели между различните сигнали в един комутатор. Показано е, че производителността на такава мрежа се насища, когато броят на преобразувателите на комутатора се увеличи над определен праг. Интересен проблем е да се определи количествено зависимостта на този праг от използвания алгоритъм за маршрутизиране и желаната вероятност за блокиране.
3. Преобразуване на дължина на вълната с ограничен обхват: изцяло оптичните комутатори, работещи чрез смесване на четири вълни, осигуряват възможност за преобразуване само на ограничен обхват. Ако обхватът е ограничен до k, тогава една входна дължина на вълната λ_i може да бъде преобразувана само в $\lambda_{\max(i-k,l)}$ до $\lambda_{\max(i+k,w)}$, където w е броят на дължините на вълната в системата (индексиран l чрез w). Преобразуването на дължината на вълната с ограничен обхват може също да бъде осигурено във възли, като се използват техники за оптоелектронно преобразуване.

В комуникациите с оптични влакна, WDM е технология, която мултиплексира няколко оптични носещи сигнали върху едно оптично влакно чрез

използване на различни дължини на вълните (т.е. цветове) на лазерна светлина [1, 5, 7]. Тази техника позволява двупосочни комуникации през една нишка от влакно, наричано още дуплексиране с разделяне на дължината на вълната, както и умножаване на капацитета.

Терминът WDM обикновено се прилага за оптичен носител, който се описва чрез неговата дължина на вълната, докато мултиплексирането с разделяне на честотата и се прилага за радио носител, който по-често се описва чрез честота. Това е чисто конвенционално, защото дължината на вълната и честотата предават една и съща информация. По-конкретно, честотата (в херцове, което е цикли в секунда), умножена по дължината на вълната (физическата дължина на един цикъл), е равна на скоростта на носещата вълна. При стъклените влакна той е значително по-бавен, обикновено около 0,7 пъти. Скоростта на предаване на данни в практически системи е част от носещата честота.

ЛИТЕРАТУРА

[1] Daniel Denev, Analysis of the requirements for optical cables for construction of underwater transmission systems, Journal scientific and applied research, vol. 21, 2021 International Journal, 2021, ISSN 1314-6289

[2] B. Mukherjee, Optical Communication Networks. New York, NY: McGraw-Hill, 1997.

[3] I. Chlamtac, A. Farago, and T. Zhang, "Lightpath (wavelength) routing in large WDM networks," IEEE Journal on Selected Areas in Communications, vol. 14, pp. 909-913, June 1996.

[4] B. Mukherjee, D. Banerjee, S. Ramamurthy, and A. Mukherjee, "Some principles for designing a wide-area WDM optical network," IEEE/ACM Transactions on Networking, vol. 4, pp. 684-696, Oct. 1996.

[5] K. Zhu and B. Mukherjee, "Traffic grooming in a WDM mesh network?' IEEE Journal on Selected Areas in Communications, pp. 122-133, Jan. 2002.

[6] K. Chan and T. P. Yum, "Analysis of least congested path routing in WDM lightwave networks," in Proc. IEEE INFOCOM '94, vol. 2, (Toronto, Canada), pp. 962-969, Apr. 1994.

[7] S. Ramamurthy, Optimized Design of WDM Network Architectures. PhD thesis, University of California, Davis, Dept. of Computer Science, 1998.

ОТНОСНО ПРОГНОЗИРАНЕТО НА ПОЯВАТА НА ГРЕШКИ В ПРОГРАМНИЯ КОД НА СОФТУЕРНИТЕ СИСТЕМИТЕ ЗА УПРАВЛЕНИЕ

Атанас Начев

PREDICTING THE OCCURRENCE OF ERRORS IN SOFTWARE CONTROL SYSTEMS

Atanas Nachev

ABSTRACT: *Achieving a high degree of efficiency in software development is one of the important tasks in the creation of information systems. This necessitates the development and application of mathematical models to predict the possible errors in the program code that may occur in the design and programming of computer programs. The object of the present exhibition are precisely such models.*

KEYWORDS: *Software control systems.*

Ефективността на информационните системи, използвани за управление на обекти и процеси в значима степен се определя от надеждността и ефективността на програмното им осигуряване. Предвид на сложността на процесите на проектиране и програмиране на софтуера възниква естествената необходимост от прогнозиране допускането грешки, при алгоритмизацията на процесите подлежащи на автоматизация и на при създаването на програмния код. В тази връзка един от възможните подходи се основава на използване на адекватни за целта математически модели [1]. В достъпната литература [1, 2, 3, 7 и др.] са изложени основни подходи за това.

В [4] е представен подход за математическо моделиране на процеса на прогнозиране на допуснати грешки в програмния код в условия на постоянна интензивност на тяхното откриване. Основава се на следната постановка: появата на откази на програмното осигуряване има случаен характер с постоянна интензивност; интензивността на възникване на откази зависи от бързодействието на компютърната система и не зависи от разпределението на типовите команди в програмния код; отказите, които настъпват в резултат на допуснати грешки в програмите се фиксират и отстраняват.

Нека в началото на тестването на програмното осигуряване ($\tau = 0$) в програмния код се съдържат N_0 допуснати грешки. В хода на тестването, което заема времето τ, са открити n_0 от съдържащите се грешки и са отстранени n броя от тях: $N_0 = n + n_0$. Времевият интервал τ съответства на продължителността на изпълняване на програмата от компютърната система и не

отчита времето на нейния престой за анализ на резултатите и извършване на съответните корекции в програмния код. В тези условия може да се приеме, че интензивността на възникване на откази поради допуснати грешки е пропорционална на количеството на тези грешки. Това определя корелационна връзка между n_0 и $\frac{dn}{d\tau}$.

Тогава

$$\frac{dn}{d\tau} = K^{'1}\lambda = Kn_0 = K\left(N_0 - n\right), \quad (1)$$

където $K^{'1}$ и $K^{'}$ са коефициенти на пропорционалност, отчитащи мащаба на изменение на времето за описване на процеса на откриване на грешките в програмния код, бързодействието на компютърната система, разпределението на тестовите значения на входа на проверяваната програма и пр.

Коефициентът $K^{'1}$ отразява изменението на интензивността на възникване на откази с увеличаване на времето за тестване и отстраняване на откритите грешки. Тази интензивност намалява и може да се приеме, че с прекратяване на тестовите процедури над софтуера става постоянна, равна на λ. В края на тестването е справедливо $K^{'1} = 1$. В такъв случай интензивността на откриване на грешки в програмата и абсолютното количество на отстранените грешки в нея са свързани количествено чрез уравнението:

$$\frac{dn}{d\tau} + Kn_0 = KN_0 \quad . \quad (2)$$

Като се предположи, че към началото на тестването ($\tau = 0$) на софтуера отсъстват открити грешки, решението на уравнение (2) ще добие вида:

$$n = N_0(1 - e^{-K\tau}) \quad . \quad (3)$$

Броя останали неоткрити грешки в тестваната програма се определя съгласно израза:

$$n_0 = N_0 e^{-K\tau} \quad . \quad (4)$$

Това количество е пропорционално на интензивността на откриване на грешките $\frac{dn}{d\tau}$ с точност до K.

Това, че времето до времето до възникване на два съседни отказа е равно на реципрочната стойност на интензивността на откриване на програмните грешки дава основание да се запише:

$$T = \frac{1}{\frac{dn}{dt}} = \frac{1}{KN_0} e^{K\tau} \quad . \quad (5)$$

Към началото на тестването на програмното осигуряване в програмният му код има N_0 грешки. Това определя наработка до отказ T_0. Тогава зависимостта на функционалната наработка до отказ от продължителността τ на извършеното тестване може да се изрази чрез съотношението

$$T = T_0 e^{\frac{\tau}{N_0 T_0}}. \tag{6}$$

Ако са известни моментите t_i на откриване на програмните грешки, при условие, че винаги при откриване на всяка една от тях тя се отстранява, като при това не се внасят нови, с използване на метода на максималното правдоподобие е получено [4] следното съотношение за определяне на N_0:

$$\sum_{i=1}^{n} \frac{1}{N_0 - (i-1)} = \frac{n \sum_{i=1}^{n} t_i}{N_0 \sum_{i=1}^{n} t_i - \sum_{i=1}^{n} (i-1) t_i}, \tag{7}$$

С използване на същия метода е получен [4] и израз за определяне на коефициента K на пропорционалност:

$$K = \frac{n}{N_0 \sum_{i=1}^{n} t_i - \sum_{i=1}^{n} (i-1) t_i}. \tag{8}$$

В такъв случай броя n_0 останали неоткрити грешки в програмния код и средната наработка до възникване на отказ, която представлява времето до откриване наличието на следващата програмна грешка, могат да се определят съответно с използване на израза (4) и съотношението $T = \frac{1}{\lambda}$.

За повишаване на времето до възникване на отказ от T_1 до T_2 е необходимо да се открият и отстранят Δn грешки Като се постави 5 в 3 се получава:

$$\Delta n = N_0 T_0 \left(\frac{1}{T_1} - \frac{1}{T_2} \right). \tag{9}$$

Времето $\Delta\tau$, необходимо за отстраняване на Δn грешки с оглед повишаване на времето между възникване на отказ от T_1 до T_2 се определя съгласно израза [4]:

$$\Delta\tau = \frac{N_0 T_0}{K} \ln \frac{T_2}{T_1} . \tag{10}$$

В [4] е представен, а в [1] е развърнат математически модел на надеждността на програмното осигуряване при линейно изменение на броя на възникналите откази поради грешки в програмния код за времето на изпитване на софтуера.Той се основава на хипотезата, че честотата на възникване на грешки в програмното осигуряване линейно зависи от времето t_i между моментите на проява на последователните $i-$ та и $i-1$ грешки. В тези условия

$$\lambda(t_i) = K\left[N_0 - (i-1)\right]t_i , \tag{11}$$

където N_0 е началния броя на допуснатите грешки в кода на програмното осигуряване; K -коефициент на пропорционалност, осигуряващ равенство на единица на площта на фигурата под кривата на вероятността за откриване на допуснатите грешки. За определяне на времето между възникването на откази е получен следния израз [4], който съответства на разпределението на Релей:

$$T(t_i) = \exp\left\{ - K\left[N_0 - (i-1)\right]\frac{t_i^2}{2} \right\} . \tag{12}$$

С използване на функцията на максимално правдоподобие са получени [4] следните изрази за определяне на общото количество N_0 на грешките в програмния код на софтуера и на коефициента на пропорционалност K:

$$N_0 = \left[\frac{2n}{K} + \sum_{i=1}^{n} (i-1) t_i^2 \right] \frac{1}{\sum_{i=1}^{n} t_i^2} ; \tag{13}$$

$$K = \left[\sum_{i=1}^{n} \frac{2}{N_0 - (i-1)} \right] \frac{1}{\sum_{i=1}^{n} t_i^2} . \tag{14}$$

Ще разгледаме математически модел на надеждността на програмното осигуряване, при който е налице намаляване на честотата на проява на допуснатите грешки в кода му в процеса на неговото тестване.

За апроксимиране на изменението на интензивността на възникване на откази във времето ще използваме функцията от вида $\lambda(t) = \lambda\alpha\, t^{\alpha-1}$.

Ако $0 < \alpha < 1$ интензивността на отказите при работата на софтуера намалява в процеса на тестване. При такъв вид на функцията $\lambda(t)$ плътността на разпределение на наработката до отказ ще се опише чрез разпределението на Вейбул-Гнеденко [6]

$$f(t) = \lambda\alpha t^{\alpha-1} \exp\left(-\lambda t^{\alpha}\right).$$

Времето до възникване на отказ в случая ще се определи като

$$T_0 = \frac{\Gamma\left(\frac{1}{\alpha}+1\right)}{\lambda^{\frac{1}{\alpha}}},$$

където $\Gamma\left(\frac{1}{\alpha}+1\right) = \int_0^{\infty} x^{\frac{1}{\alpha}} e^{-x}\, dx -$ Гама функция с дисперсия $D[T_0] = \frac{\Gamma\left(\frac{2}{\alpha}+1\right) - \Gamma^2\left(\frac{1}{\alpha}+1\right)}{\lambda^{\frac{2}{\alpha}}}$.

Разпределението на Вейбул-Гнеденко с достатъчна степен на адекватност описва реалната надеждност на програмното осигуряване с отчитане на процеса на отстраняване на допуснати грешки в софтуера след всеки възникнал отказ в процеса на тестването му.

ЛИТЕРАТУРА

[1] Начев А. И., Надеждност на програмното осигуряване, Университетско издателство „Епископ Константин Преславски“, Шумен, 2017.

[2] Начев А. И., Информационни процеси в компютърните мрежи в условия на реална надеждност, Военно издателство, София, 2001.

[3] Начев А. И. Общосистемно проектиране на автоматизирани системи за управление, За буквите, О‘писменех, София, 2014.

[4] Липаев В. В., Надежность программного обеспечения АСУ, Москва, Энергоатомиздат, 1981.

[5] Липаев В. В., Программная инженерия, Методические основы, Москва, ТЕИС, 2006.

[6] Гнеденко Б. В., Ю. К Беляев., А. Д., Соловьев, Математические методы в теории надежности, „Наука“, Москва, 1969.

[7] Reliability: “Theory&Aplications”, No1, Vol. 2, March 2007.

ОСНОВНИ ИЗИСКВАНИЯ КЪМ ЕКРАНИРАНЕТО, КАТО ПОДХОД ЗА ЗАЩИТАТА НА ИНФОРМАЦИЯТА ЧРЕЗ ОГРАНИЧАВАНЕ НА ВЛИЯНИЕТО НА ПАРАЗИТНИТЕ ЕЛЕКТРОМАГНИТНИ ИЗЛЪЧВАНИЯ

Атанас Начев

BASIC REQUIREMENTS FOR SHIELDING AS AN APPROACH TO PROTECTING INFORMATION BY LIMITING THE IMPACT OF PARASITIC ELECTROMAGNETIC RADIATION

Atanas Nachev

ABSTRACT: *One of the ways of unauthorized access to processed and exchanged information in the conditions of modern information means and technologies are based on acceptance and analyzes of parasitic electromagnetic radiations and induced electromotive voltages arising during the operation of electronic means. Various technical solutions are used to prevent this. One of them is the use for protective shielding. The subject of this presentation are basic requirements for the construction of effective protective screens.*

KEYWORDS: *Protecting information, shielding.*

Съществена опасност, от гледна точка на защитата на информацията, представляват възникващите в процеса на работа на електронните средства паразитни електромагнитни излъчвания. Същите се разпространяват в пространството под формата на електромагнитна вълна от радио честотния диапазон (радиовълни). Източници на такъв тип излъчвания се явяват електрически вериги от електронна апаратура, обхванати от паразитни капацитивни и индуктивни връзки; проводници по които протичат електрически токове, явяващи се носители на информация; паралелно разположени спрямо кабели и проводници на силови или слаботокови инсталации информационно носещи електрически проводници и пр. Опасни в това отношение са и участъци на електрическите вериги, разположени извън защитни екрани, които са подложени на въздействието на паразитни електромагнитни въздействия.

При въздействие на високочестотни информационно носещи сигнали върху нелинейни и параметрични вериги по които протичат високочестотни електрически токове, може да възникне модулация на същите. По такъв начин високочестотните токове се оказват носители на информация и създават канал за неоторизиран достъп до данни.

Канали за изтичане на информация могат да възникнат вследствие на излъчване на информационно носещи сигнали и индуциране на високочестотни електродвижещи напрежения в резултат на въздействието на тези сигнали върху

захранващата мрежа, веригите на слаботоковите инсталации, веригите за заземяване. Тези сигнали, разпространяващи се във вид на електромагнитни излъчвания и високочестотни токове, породени от възникналите високочестотни електродвижещи напрежения в съответни електрически вериги, могат да бъдат приети и анализирани по съответния начин, така че да бъде възстановена информацията която носят, скрито и от разстояние [1].

За предотвратяване на това се предлагат два основни подхода [1]:

1. Екраниране на съответните технически средства и помещенията, където е разположена компютърна и комуникационна техника.

2. Използване на обемно и линейно електромагнитно зашумяване.

Обект на настоящото изложение са препоръки относно екраниране на помещения, в които е разположена компютърна техника или комуникационна апаратура.

При проектиране и изграждане на екранирани помещения следва да се имат предвид следните особености на възникването и разпространяването на електромагнитните излъчвания:

Апаратура, в която протичат не големи токове, но е налично високо напрежение, в процеса на функционирането й се генерират в близката зона електромагнитно излъчване с преобладаваща електрическа съставляваща.

В апаратура, за която е характерно протичане на големи токове, които създават малки падове на напрежение генерира в близката зона електромагнитни вълни с преобладаваща магнитна съставляваща.

С оглед на защитата на информацията в съответните помещения, където е разположена електронна апаратура, в това число компютърни системи и мрежи, се предявяват следните основни изисквания към екранирането им [1,2]:

Належащо е прилагане на решения за ефективно екраниране, както на електрическата и така и на магнитна съставляваща на паразитното електромагнитно електромагнитното поле.

Необходимо е реализиране на технически решения, чрез които се предотвратява възникването на излъчване на електромагнитни вълни в радиочестотния диапазон в резултат на протичане на високочестотни токове в среда на водопроводната, отоплителната и електрозахранващата инсталации.

Прилагане на конструктивни решения, които изключват възникване на електромагнитни вълни от екранираните помещения през врати, прозорци, вентилационни шахти и др.

Предотвратяване появата на резонансни явления в определени честотни диапазони, които се явяват условия за интензивни електромагнити излъчвания.

В помещенията в които са разположени компютърни системи и комуникационно оборудване е необходимо да се осигури екраниране по отношение на възникващи електромагнитни излъчвания в диапазона от 50 kHz до 2 GHz, като ефективността на екраниране да не е по–малка от 80 dB.

Екранирането трябва да обхване вратата/вратите, като напълно се изолират прозорците. Местата където те са били разположени да са обхванат от екрана.

Изходът след вратата трябва да е изпълнен като обемен електромагнитен филтър.

Проводници на електрозахранващата мрежа трябва да излизат от помещението през отвори, защитени чрез обемни филтри.

Силовата електрическа инсталация на помещението да се свързва с проводниците на силовата електрическа инсталация на сградата чрез защитни филтри.

Екранирането трябва да се извърши чрез изграждане на екрани както за електрическата, така и за магнитната съставляващи на паразитното електромагнитното поле.

Задача на електрическото екраниране е да се изключи електрическата съставляваща на електромагнитното поле до повърхността на металния екран, като електрическите заряди върху него се отведат в земята. Всички технически решения, които са свързани с намаляване на паразитните капацитивни връзки, в самата електронна апаратура, така и извън нея водят до повишаване на ефективността от екраниране.

Екранът на електрическата съставляваща на паразитното електромагнитно поле се разполага от вътрешната страна, по отношение на екранираното помещение. Изпълнява се с медни листове, които се запояват, като преди това се застъпват минимум на 15 mm, като се разполагат така, че силовите линии на електрическата съставляваща на електромагнитното поле да се затварят на стените на екрана и да не излизат извън него. При ниски честоти, за които дълбочината на проникване на електрическата съставляваща на полето е по–голяма от дебелината на екрана, качеството на екраниране малко зависи от дебелината на екраниращите плоскости, но съществено зависи от качеството на заземяването им.

В областта на високите честоти, при които дебелината на металните листове е по–голяма от дълбочината на проникване, ефективността на екранирането зависи от дебелината на листовете, а така и от електрическата и магнитна проницаемост на материала от които те са изработени. С увеличаването на честотата ефективността на електрическото екраниране спада. Малки процепи и отверстия, които са с размери по–малки от дължината на вълната влошават качеството на екраниране на електрическата съставляваща на електромагнитното поле.

Магнитният екран се разполага от външната страна. Изпълнява се с метални листове от магнитно мек материал. Листовете се заваряват с аргона заварка, така, че да няма процепи в екрана. Такива процепи изпълняват ролята на процепн антени, които активно излъчват електромагнитни вълни в радиодиапазона. Магнитният екран осигурява ефективно потискане на ниските честоти, от 0–3 до 10 kHz.

За осигуряване на ефективно екраниране на магнитната съставляваща на полето е необходимо:

-Магнитната проницаемост на материала, от който е изработен екрана да е възможно по-голяма, например като тази на пермалоя.

- Увеличаването на дебелината на екраниращите повърхности води до увеличаване на ефективност на екранирането.

- Връзките между отделните метални листове, шевовете, разрезите трябва да са разполагат перпендикулярно на магнитните силови линии. Техният брой по възможност следва да е минимален.

- Заземяването на екрана не влияе на ефективността на екраниране на магнитната съставляваща на полето.

- Ефективността на екраниране се повишава с използване на многослойни екрани.

-Благодарение на вихровите токове напрегнатостта на първичното магнитно поле спада с дебелината на магнитния екран по експоненциален закон.

Екраниращата конструкция се заземява от вътрешната и външна страна, като съпротивлението на заземяване трябва да е в пределите 1–4 Ом. Системата за заземяване включва общ заземител и заземителен кабел. При заземяване на отделни устройства, всяко едно от тях се подключи към заземителя или към заземителния кабел чрез самостоятелен заземяващ проводник. Последователно включване на заземяващите проводници не се допуска. Контактните съединения не трябва да образуват окисни слоеве върху контактуващите повърхности.

Необходимо е да се отбележи, че чрез екраниране с метални мрежи на помещения, в които е разположена компютърна и комуникационна техника не се постига ограничаване на на възвиващите паразитни, информационно носещи електромагнитни излъчвания.

Когато говорим за екраниране на помещения с оглед на ограничаването на възникващите паразитни електромагнитни излъчвания следва да споменем за апаратурата, която конструктивно така е изпълнена, че практически не излъчва около себе си паразитно електромагнитно поле. Това е апаратурата, отговаряща на TEMPEST изискванията [3, 4]. В САЩ е въведена следната класификации на електронните устройства със система за защита на информацията по отношение на паразитните електромагнитни излъчвания:

TEMPEST Level 1 (аналог на стандарта NATO AMSG–720B)- оборудването от дадения клас се отнася към категорията за висша степен на секретност. Това оборудване се утвърждава от Агенцията за национална безопасност и е предназначено само за използване за нуждите на правителствени учреждения.

TEMPEST Level 2 (аналог на стандарта NATO AMSG–788A)- оборудването, което отговаря на това изискване е предназначено за обработване на информация с по–ниска степен на секретност, но също „критична“. Използването му изисква одобрение от Агенцията за национална безопасност на САЩ.

TEMPEST Level 3–оборудването от този клас е предназначено за защита несекретна, но „критична“ или комерческа информация. Оборудването се регистрира в NIST (National Institute of Standards and Technology).

За нуждите на бизнеса се използва класификацията ZONE, на която отговарят устройства със съществено по-ниска цена.

ЛИТЕРАТУРА

[1] Начев А. И., Технически средства и системи за защита на информацията, София, За буквите, О‘писменех, 2014.

[2] Atanas Nachev, Elektromagnetic Radiation and the Computer Data Securitry Problem, Information & Sequrity, Volume 4, 2000, pp. 105-113.

[3] Systems for protecting digital equipment against remote access, USA Patent № W090/00840.

[4] Computer security device, Europen Patent № 0240328.

ОТНОСНО УНИВЕРСАЛНОСТТА НА ВЕРОЯТНОСТНАТА ИНТЕРПРЕТАЦИЯ НА ИНФОРМАЦИЯТА

Анита Димитрова, Атанас Начев

THE UNIVERSALITY OF THE PROBABILITY INTERPRETATION OF INFORMATION

Anita Dimitrova, Atanas Nachev

ABSTRACT: *A characteristic feature of the term "information" is the difficulties associated with attempts to give it a strict definition accompanied by a universal metric for quantifying information. One of the approaches in this regard is its probabilistic interpretation. This paper shows the degree of universality of Shannon's approach not only in the technological sphere, but also indicates the accompanying limitations regarding its applicability.*

KEYWORDS: *Interpretation of information, Shannon's approach.*

Терминът „информация“, един от най-често употребяваните в повсеместния ни живот, в науката и пр. не ни освобождава от затруднения свързан със затруднение, когато трябва да му дадем ясна дефиниция [4]. Това в немалка степен се отнася и до научната общност, нещо което си личи и от следното определение за информация, дадено в авторитетно издание: „информацията е понятие, свързано с обективното свойство на материалните обекти и явления (процеси) да пораждат многообразие от състояния, които могат да се предават на други обекти чрез взаимодействия и да се запечатват в тяхната структура“ [1]. С недостатъчна яснота, но доста по-близо до действителната същност на нещата се характеризира и едно друго определение за информация: „Информацията представлява налично, използваемо знание“ [2]. А определението „В по-тесния технически смисъл информацията е подредена редица от символи данни“ се отнася повече за един от начините за представяне на информацията, отколкото до реалния смисъл на това понятие. Ето защо твърдението [3], че „не съществува единна дефиниция (за информация), а има сравнително широк кръг от значения в различните области на знанието“, не е лишено от смисъл.

Във всекидневието ни се използва и с такива термини като съобщение и данни, доста често възприемани като синоними, особено в обхвата на техническата им интерпретация. Ако трябва да следваме строгостта на изложението, под информация следва да се разбират тези съобщения или техни части, които попълват наши незнания [4]. Следователно дали дадено получено от нас съобщение ни носи информация зависи от текущото ни субективно състояние по отношение на съответната ни осведоменост.

В съответствие с трите форми на адекватност на информацията-синтактична, семантична и прагматична, може да говорим за синтактично,

семантично и прагматично количество на информацията. В конкретния случай ни интересува количеството на информацията на синтактическо ниво. Ще разгледаме това, придържайки се към статистическия подход на Шенън, но без да повтаряме метода му на изложение и без да се спираме на доказването на вероятностния характер на получаването на информация. Просто ще проследим нещата как изглеждат в количествено отношение на частен пример от технологичната област. За целта нека имаме, например, 32 разрядна двоична дума. Количеството двоични числа, които могат да се запишат в тази двоична дума е 2^{32}. При двоична дума от 64 разряда броя на двоичните числа, които могат да се запишат в нея е 2^{64}. Нека се опитаме да приемем за количество J на информацията мощността N на изходното множество от възможни състояния, т.е. $J = N$. За нашия пример това количеството ще е за първия случай $J = 2^{32}$, за втория $J = 2^{64}$. За да бъде тази метрика подходяща за изразяване на количеството на информацията трябва да се изпълнява условието за адетивност, т.е. два пъти по-голямото следва да съдържа два пъти повече. Думата от 64 разряда е два пъти по-голяма от 32 разрядната дума. Изпълнението на условието за адетивност в случая изисква $2^{64} = 2.2^{32}$. Но $2^{64} \neq 2.2^{32}$, което прави такъв подход неподходящ за количествено изразяване на информацията.

Нещата ще приемат други очертания, в случай че изразим количеството на информацията посредством $J = \log_2 N$. В случая условието за адетивност се изпълни, $\log_2 64 = 2.\log_2 32$.

От приведения пример се вижда, че N не може да бъде мярка за количество на информацията, тъй като не притежава свойството адитивност. За такава мярка е приет логаритъма от количеството на състоянията, т.е. на броят на възможните съобщения, които могат да се получат:

$$J = \log_2 N. \tag{1}$$

Тази мярка за количество на информацията е предложена от Ралф Хартли през 1928 г. за случай на равно вероятни съобщения.

При N равно вероятни съобщения вероятността на получаване на всяко едно от тях е $p = \frac{1}{N}$. Тогава $N = \frac{1}{p}$ и (1) ще запишем във вида:

$$J = \log_2 N = \log_2 \left(\frac{1}{p}\right) = \log_2 p^{-1} = -\log_2 p. \tag{2}$$

За да се определи мерната единица за количество на информацията ще разгледаме случай на множество от два елемента, т.е. множество с възможно най-малко елементи, което предоставя възможност за избор. Очевидно в случая $|J| = \log_2 2 = 1$ bit.

През 1948 г. Клод Шанън (Claude Shannon) дава решение за количеството на информацията за случай на не равно вероятни съобщения. Ще разгледаме нещата в това отношение по-подробно, но не по методологията на Шанън [6], а придържайки се към подхода в [4].

Нека обект на предаване са m вида съобщения, като от първи вид са получени n_1 броя от тях, всяко едно сот тях съдържа количество информация J_1. От втори тип са получени n_2 броя съобщения, всяко едно от които съдържа количество информация J_2. От трети тип- n_3 броя съобщения, всяко едно от които съдържащо информация в количество J_3. И така нататък, от $m-$ ти тип са получени n_m съобщения, всяко едно от които съдържа информация в количество J_m. В тези условия е необходимо да се определи средното количество J информация, което се съдържа в едно получено съобщение.

За условията на разглеждания случай ще имаме

$$J = \frac{n_1 J_1 + n_2 J_2 + n_3 J_3 + ... + n_m J_m}{n_1 + n_2 + n_3 + ... + n_m} \quad .$$

(3)

Ще въведем обозначението $M = n_1 + n_2 + n_3 + ... + n_m$ и ще запишем (3) във вида

$$J = \sum_{i=1}^{m} \frac{n_i}{M} J_i \quad . \qquad (4)$$

Отношението $p_i = \frac{n_i}{M}$, $i = 1,2,3,...,M$, представлява вероятността, че ако е получено съобщение, то с ще е от $i-$ ти тип. В такъв случай за (4) ще имаме:

$$J = \sum_{i=1}^{m} p_i J_i$$.

Съгласно (2) $J_1 = \log_2 p_i$, предвид на което окончателно ще получим следната формула за количеството на информацията:

$$J = -\sum_{i=1}^{m} p_i \log_2 p_i, \tag{5}$$

където $i = 1, 2, 3, ..., m$.

Изразът (5) е известен като формула на Шанън за средното количество на информацията, съдържаща се в съобщения, постъпващи с различна вероятност.

Формулата на Хартли може да се разглежда като частен случай на формулата на Шанън, когато всички съобщения са равно вероятни:

$$J = -\sum_{i=1}^{N} p_i \log_2 p_i = -\frac{1}{N}\sum_{i=1}^{N} \log_2 \left(\frac{1}{N}\right) = -\frac{1}{N} N \log_2 \left(N^{-1}\right) = \log_2 N$$

. (6)

Ние разгледахме метриките на Хартли и на Шанън не за демонстрираме един различен от описаните в литературата [6] подход за определяне на количествените характеристики на информацията, предложен по отношение на технологичната сфера на нейното предаване и обработване. Правим го за да обосновем универсалния характер на приложимостта му, в т. ч. и за случаи на притичващи социални процеси. По-нататък ще се предържаме към методологията, представена в [4]. За целта нека се спрем на два основни подхода за дефиниране на понятието вероятност-класически и статистически [5].

Вероятността като понятие отразява определени признаци на обективно протичащи процеси в природата, в техническите изделия, в обществото, в условията на нашето битие и пр. Класическото й определяне се основава на наличието на m благоприятстващи изходи при притичане на даден случаен процес, при който са възможни общо n изхода. В този случай вероятността, като характеристика на степента на възможност за настъпване на дадено събитие се дава чрез съотношението

$$p = \frac{m}{n}$$. (7)

Изразът (1) е справедлив, ако всички събития, които могат да настъпят в хода на статистическия експеримент са с еднаква степен на възможност.

В резултат на реално проведен статистически експеримент честотата на появата на дадено събитие ще се представи като:

$$p^* = \frac{m^*}{n^*}.$$

При достатъчно голямо n ($n \to \infty$) стойностите на честотата ще се групират около определено значение, което задава статистическата вероятност на събитието, т.е. $p \approx p^*$. Очевидно $1 \leq p \geq 0$.

При условия на случайни събития, т.е. на такова, които могат да настъпят или да не се случат вероятността представлява не само количествена мярка за възможността за поява на дадено събитие, но и количествена мярка за степен на случайност. Ако вероятността е равна на единица, то налице е достоверно събитие. Събитие, характеризиращо се с вероятност за поява равна на нула е недостоверно.

Ще се спрем на понятието неопределеност. То характеризира, че в даден начален момент не може да се каже дали ще настъпи ли дадено събитие или няма да настъпи. Неопределеността се намира в отношения с термини, като случайност и вероятност.

Степента на неопределеност на избора зависи от броя на избраните елементи, отнесени към общия брой на елементите в съвкупността. При множество от един елемент степента на неопределеност е равна на нула. Вероятността за избор в случая е равна на единица.

При множество, състоящо се от два елемента изборът на един елемент снема неопределеността по отношение на другия елемент. С увеличаване на броя на елементите в множеството расте степента на неопределеност и намаляване на вероятността за избор на един конкретен елемент. Множество с безкраен брой елементи се характеризира с безкрайна неопределеност и нулева вероятност за избор.

От изложеното се вижда, че между неопределеността и вероятността съществува ясно изразена взаимна връзка. Колкото по-голяма е вероятността p, толкова по малка е неопределеността H. Ако предположим, че тази зависимост е от вида $H = \frac{1}{p}$, налице е справедливост за всички случаи, за изключение когато $p = 1$. Така е защото не е вярно, че когато вероятност за избор е равна на единица налице е неопределеност със стойност единица. В този случай неопределеността е равна нула. Но ако приемем

$$H = \log\frac{1}{p} = -\log p \quad . \qquad (8)$$

се удовлетворяват всички условия за свързаност на неопределеността с вероятността. При $p = 0$ ще имаме неопределеност $H = \infty$, а при $p = 1$ тя ще е $H = 0$.За да се снема определена степен на неопределеност следва да получи информация, количествено равна на количеството снета неопределеност, т.е.

$$J = H = \log \frac{1}{p} = -\log p \quad , \tag{9}$$

Следователно получихме израза на Хартли по начин, който доказва неговата универсалност и приложимост не само в частните случаи на технологичната сфера.

Ако сме в ситуация, при която настъпват n събития, всяко едно от които носи определена информация, средното количество снета неопределеност от настъпването на едно събитие ще е равно на средното количество информация, получавана в резултат на това събитие. В такъв случай, извършвайки разсъждения, аналогични на разсъжденията за условията на (5) ще стигнем до същото количествено съотношение:

$$J = H = -\sum_{i=1}^{n} p_i \log p_i \quad . \tag{10}$$

От изложеното се вижда, че статистическия подход за дефиниране на информацията и определянето на нейното количество е справедлив не само по отношение на информационните средства и системи, но носи универсален характер. Що се отнася до приложимостта му в специфичните условия на социалната сфера, налице е определена непълнота, характеризираща се с не отчитане на семантичното съдържание на информацията и игнориране на полезността й. Това поставя въпроса за разширяване на понятието информация [7]. Статистическата теория не се ангажира с изискването за осмисляне на информацията, а от там от възможността за използване от човека в неговата дейност и битие. Информацията се възприема като снемане на неопределеност, свързана единствено със случайни процеси, а така също превръщането на възможността в действителност за тези случаи, при които има място наличието на случайни процеси. Само формулата на Шанън представя превръщането на случайни величини $\log \frac{1}{p} = -\log p$ в неслучайната величина средно количество информация. А това говори и за връзка на информационните процеси не само с чисто случайни, но и с необходими, неслучайни процеси [7]. Т.е. налице е и превръщане на случайността в необходимост. Заедно с това от статическата теория на информацията не следва, че информацията може да бъде присъща на

необходими процеси, например на процесите, които са обект на класическата електродинамика.

Статистическата интерпретация на информацията се характеризира със своята висока степен на универсалност и приложимост не само в техническата област. Но следва да се отбележи, че извън тази сфера на приложение й е присъща и значителни ограниченост. Например не отчитането на семантичната й същност в много области на приложение е една от тези ограниченост.

ЛИТЕРАТУРА

[1] Беджев Б., Технически средства в системите за национална сигурност, Университетско издателство „Епископ Константин Преславски“, Шумен, 2006.

[2] Белов, Л. А., В. М. Богачев, М. В. Благовещенский и др. Устройства генерирования и формирования радиосигналов. Москва, Радио и связь, 1994.

[3] Начев А. И., Общосистемно проектиране на автоматизирани системи за управление, За буквите, О‘писмененех, София, 2014.

[4] Гнеденко Б. В., Курс теории вероятностей, Физматгиз, Москва, 1961.

[5] Shannon, C.E., Comunications Theory of Secrecy Systems, Bell System Tehnicol.

[6] Виды информации е ее свойства, http//www. Ru.wikibook.org/wiki.

СТРАТЕГИЯ ЗА СИГУРНОСТ НА ОБЩИНА ШУМЕН 2022-2028 г.
Усъвършенстване и ефективно поддържане на системата за сигурност на Община Шумен

Илиана К. Симеонова

SECURITY STRATEGY OF THE MUNICIPALITY OF SHUMEN 2022-2028
Improvement and effective maintenance of the security system of the Municipality of Shumen

Iliana K. Simeonova

ABSTRACT: *The Security Strategy of the Municipality of Shumen outlines the most important perspectives that will establish the Municipality of Shumen as a safe place to live, where every citizen and guest can feel at ease. In order to realize it, it is necessary to improve the activities for the protection of public order, the protection of the population in the event of disasters, epidemics and emergency situations in the event of a declaration of war, in a military or other emergency situation, by developing the elements of security, and ensuring their passage at a qualitatively higher stage by finding innovative solutions to achieve horizontal and vertical security.*

KEYWORDS: *security strategy, Municipality of Shumen.*

Въведение

Стратегията за сигурност на Община Шумен, изписвана по-нататък за краткост „Стратегията“, е важен акт за деклариране на обществен консенсус при определяне на основните насоки за действие на Община Шумен за изграждане и поддържане на структура за сигурност на общината.

Стратегията очертава най-важните перспективи, които да утвърдят община Шумен като сигурно място за живеене, в което всеки гражданин и гост да се чувства спокоен, в устойчива среда и защитен от всички възможни рискове, застрашаващи живота и здравето му, като резултат да се постигне сигурност за всеки, което е и мотото на самата Стратегия.

В стратегията се използва понятието „Сигурност" със следното значение: съвкупност от динамично променящи се параметри, определящи състоянието на обществения ред на гражданското общество в мирно и във военно време, при нормално функциониране на обществото и в случай на природни и други бедствия, и като резултат от целенасочени действия да се повиши степента на защитеност на отделния човек както в публичната, така и в неговата лична среда.[2]

Настоящата Стратегия е синхронизирана със Стратегията за национална

сигурност на Р. България и показва пътищата за практическото реализиране на нейните основни принципи на територията на общината.

За реализирането й е необходимо да се усъвършенстват дейностите по опазване на обществения ред, защитата на населението при бедствия, епидемии и извънредни ситуации при обявяване на война, във военно или при друго извънредно положение, като се развият елементите на сигурност и се осигури преминаването им на качествено по-висок етап чрез намиране на иновативни решения за постигане на хоризонтална и вертикална сигурност.

Стратегията няма за цел да дублира политики и дейности на държавни органи, отговарящи за сигурността в Република България, а да допълни проблемните сектори, касаещи Община Шумен и нейните граждани, както и да набележи мерки за подобряване на взаимодействието с тези органи – МВР, ДАНС, МО, и др.

Един от основните елементи за разработването на Стратегията за сигурност е анализът на средата за сигурност. Основните фактори, които влияят на тази среда, са външни и вътрешни:

1. Външни фактори са съседните на България държави и развиващите се в тях процеси, Балканите, Европа и в света. Светът като цяло е засегнат от пандемия, което е основният външен фактор. В по-малка степен са външните заплахи от терористични актове на радикални елементи. В още по-малка степен е рискът от военни действия в нашия регион. В световен мащаб такива не са изключени, но те не могат да окажат съществено влияние.[2]

1.1. Външните фактори за сигурност не влияят в голяма степен на сигурността на общината, поради нейното географско разположение в страната.

2. Вътрешни фактори - отново на първо място е епидемията, която поставя на изпитание здравната система на общината. На второ място са намиращите се на територията на общината стратегически обекти, за които обаче основна отговорност носят държавните органи за сигурност. На трето място е криминалната престъпност, корупцията, нарушаването на обществения ред и други.

2.1. Вътрешните фактори за сигурност на територията на общината се влияят от големия брой стратегически обекти от състава на критичната инфраструктура, наличието на много места, където се провеждат различни прояви със струпване на големи групи от хора, риска от разпространение на заразни болести, бедствени и аварийни ситуации, съществуването на зони с концентрация на престъпления, обособяването на компактни малцинствени общности, интензивния пътен трафик и високото ниво на пътнотранспортен травматизъм, както и състоянието на публичната инфраструктура.

Във връзка с всичко това, приемането на настоящата Стратегия ще гарантира устойчивото развитие на Община Шумен и ще осигури по-добра среда на сигурност за гражданите на град Шумен и неговите гости.

Анализ и тенденция

За подобряване на състоянието на обществения ред и сигурността на територията на Община Шумен и за изпълнение на заложените цели в настоящата Стратегия за периода 2022-2028 г., в Община Шумен е необходимо с решение на Общинския съвет на Община Шумен да се приеме нова дирекция

- ***Дирекция „Сигурност***".

Тази нова дирекция ще работи по следните задачи, заложени в Стратегията: подобряване на работата по опазване на обществения ред, подобряване на средата за сигурност в общинските училища и детски заведения, подобряване ефективността в работата на Оперативен дежурен център и видео наблюдение (ОДЦ и Вн.) и на работно място ЕЕН 112 в ОДЦ и Вн., развитие на системата за видео наблюдение в Община Шумен и внедряване на нови технологии, повишаване сигурността на обектите от критичната инфраструктура на Община Шумен, предприемане на необходимите мерки за намаляване на риска за населението на ОШ при извънредни ситуации, намаляване на вредните въздействия върху здравето на хората, поддържане на военновременните пунктове за управление (ВВПУ) на Община Шумен в готовност за работа при бедствия, извънредно положение, военно положение или положение на война и осигуряване на ефективно денонощно оперативно дежурство, както и на търговските дружества за оповестяване при привеждането в готовност за работа във военно време на икономическата инфраструктура и населението, както и подобряване дейността по изпълнение на разпоредителните документи на Община Шумен.[3]

За периода 2019 – 2022 г. включително, в Община Шумен са постъпили близо 50 броя уведомления и заявления за провеждане на масови мероприятия на територията на общината. В работата си по обработването им общинска администрация чрез отдел жалби се ръководи от принципа за спазване на основните конституционни права на гражданите, прокламирани в Конституцията на Република България и винаги се търси баланс при спазване правото на всеки човек да изрази себе си, и правото на всеки човек на сигурна среда за живот [3].

Във връзка с нарушаване на обществения ред ежедневно в дирекция „ Гражданска регистрация, информационно и правно обслужване“ се обработват сигнали, писма и жалби на граждани и юридически лица. Анализът показва, че най-често срещаните проблеми се изразяват в нарушаване на нощната тишина, шум от работа в строителни обекти, неправилно паркирани автомобили на пътното платно, велосипедни алеи, тротоари и нарушаване на Закона за движение по пътищата. Тенденция при обработването на сигнали и жалби е стриктното спазване на въведените нормативни срокове и процедури, като при разглеждането им се анализират в дълбочина поставените въпроси с цел предприемане на необходимите действия или изготвяне на отговор.

Дирекция „Сигурност" ще извършва постоянен контрол по изпълнение на сключените договори за охрана в обекти, публична и частна общинска собственост, като акцентира върху използването на физическата охрана за гарантиране сигурността на децата, учениците и населението. Безопасността на децата трябва да бъде приоритет в политиката на Община Шумен, като се осъществява постоянен контрол чрез извършване на проверки, в изпълнение на утвърдена от кмета на Община Шумен „Методика за извършване на външен хоризонтален контрол на охраната на общински обекти“ и утвърдени „Методики за определяне на средата за сигурност в общинските учебни и детски заведения“.

В изпълнение изискванията на Закона за противодействие на тероризма (ЗПТ) и на основание Националния план за противодействие на

тероризма за този период трябва ще се изготви План за противодействие на тероризма на територията на Община Шумен, съгласно изискванията на Наредба № 8121з-1225/27.09.2017 г. на МВР и ДАНС и разработена Методика за определяне на степента на сигурност и безопасност в общинските обекти (сгради), и Планове за сигурност на всички общински училища и детски заведения, общински здравни заведения и административни сгради. [1]

Основните цели на плана са осигуряване на постоянна и адекватна защита на лицата на територията на община Шумен срещу терористична заплаха.

С цел ефективна превенция и предотвратяване на нарушения на обществения ред и престъпления, повишаване ефективността на осъществяваното видео наблюдение на територията на Община Шумен до 2023 г. ще бъде необходимо изграждане на допълнително видео наблюдение, което да обхване всички училища, детски градини, детски ясли. Едновременно с това да продължи изграждането на видео наблюдение в социални домове, паркове, подлези, градини и детски площадки.

През периода на изпълнение на Стратегията ще се разработи План за привеждане на Община Шумен в готовност за работа във военно време, който ще се съгласува с Министерството на отбраната.

Подцели на стратегията

1... Опазване на живота и здравето на отделния човек и на населението на територията на Община Шумен чрез контрол за спазване на изискванията, свързани със сигурността, както и върху общинската администрация, общинските предприятия, детските градини, училищата и общинската собственост.

2.. Поддържане на устойчива среда за сигурност в Община Шумен чрез предприемане на мерки за подобряване на спазването на обществения ред и повишаване на ефективността на работата на Общинско Предприятие „Стопанска и охранителна дейност“/ОП-СОД/, с предмет на дейност: Охрана на общински обекти, охрана на имущество на физически и юридически лица, на сгради, помещения и стопански обекти, включително физическа защита на административни, производствени складове и други сгради и помещения, и други охранителни дейности.

3. Защита на стратегически обекти от критичната инфраструктура на Община Шумен.

4. Опазване на общинската собственост и тази на гражданите и юридическите лица.

5. Ефективно управление при бедствия, аварии, епидемии и извънредни ситуации за защита на гражданите, имуществото, критичната инфраструктура и околната среда чрез подобряване на дейността по анализа и оценка на риска, както и превенцията.

6. Повишаване на нивото на защита на класифицираната информация и превенция срещу нерегламентиран достъп, чрез внедряване на нови и иновативни информационни технологии, за повишаване на киберсигурността в Община Шумен и общинските предприятия.

7. Повишаване на ефективността на отбранително-мобилизационна подготовка във всичките и аспекти с цел осигуряване на гражданите при военно

положение или война.

8. Разширяване на мрежата за видео наблюдение като важен елемент от превенцията и намаляване на престъпните посегателства върху гражданите и общинската собственост.

9. Промени в действащите нормативни документи на Община Шумен с цел адаптирането им към реалните обществено-икономически отношения.

10. Създаване на благоприятна среда за обитаване на всеки жител на общината, гарантираща намаляване рисковете за здравето и живота, увеличаване качеството на живот и опазване на околната среда, при отчитане на промените на климата.

Подцелите на Стратегията се реализират чрез целенасочени политики за сигурност, които да създадат устойчива среда.

Политики за сигурност

Стратегията за сигурност на Община Шумен ще бъде основополагащ документ на Общинския съвет за формиране, планиране, осъществяване, координиране и контрол в областта на сигурността, която обхваща обществения ред в мирно и във военно време, защитата на населението при бедствия, аварии, извънредни ситуации и епидемии, застрашаващи живота и здравето на гражданите. Стратегията ще се реализира чрез политики за сигурност, формиращи се посредством решенията на Общинския съвет (ОС), които се реализират в постоянен диалог с граждани, неправителствени организации, държавни институции и други структури. По тази причина политиките за сигурност се явяват стратегически насоки за действие и обхващат широк кръг от дейности, както в хоризонтално, така и във вертикално направление.[2].

4. 1. Хоризонтални политики

Хоризонталните политики за сигурност според дейностите на общината се разделят на три основни групи:

- състояние на обществения ред и свързаните с него технически системи за сигурност;
- отбранително - мобилизационна подготовка и защита на населението при бедствия и аварии;
- извънредни ситуации и епидемии в мирно и във военно време.

4.1.1. Обществен ред

Поддържането на добър обществен ред ще бъде сред приоритетите в дейността на Община Шумен, като опазването и подобряването се осъществява основно от Областна дирекция на министерство на вътрешните работи (ОДМВР), а при необходимост чрез взаимодействие с ДАНС и други институции и организации.

За този вид дейност, в Община Шумен ще бъде натоварена да отговаря основно Дирекция „Сигурност", както и ОП „Стопанска и охранителна дейност".

Функциите, съставът и предметът на дейност на дирекцията и общинското предприятие са приети след Решение на ОС. Конкретните задачи, отговарящи на спецификата на Община Шумен и динамиката в нейното развитие, се определят чрез заповеди на кмета. Дейността на Дирекцията и ОП ще се отчита чрез месечни, шестмесечни и годишни доклади и анализи.

При провеждане на масови мероприятия Дирекция „Сигурност" ще

извършва дейности по защита на живота и здравето на гражданите от инциденти и активно ще взаимодейства с органите на МВР, ДАНС и др.

4.1.2. Отбранително-мобилизационна подготовка

В рамките на Стратегията, целта на отбранително-мобилизационната подготовка – (ОБМ) е постигане на максимална ефективност от дейността на кмета на Община Шумен, общинските предприятия и дружества и други общински структури за изграждането и развитието на основни отбранителни способности (граждански компонент) от Община Шумен под управлението на ОМП, защитата на личния състав, населението и обектите от критичната инфраструктура, поддържането, възстановяването и изграждането на инфраструктурата, осигуряването на основна гражданска продукция и услуги и опазването на културните ценности при положение на война, при военно и извънредно положение.[3].

Това се постига чрез разработване на административни актове, документи и планове, свързани с отбраната, планиране, изграждане и поддържане на военновременната система за управление на общината, подготовка на местната администрация, територията и инфраструктурата, населението и общинската икономика за действие във военно време, планиране и осигуряване на граждански ресурси за отбрана.

За периода на действие на Стратегията, едни от основните задачи в тази насока са да се подобри работата по поддържане на военновременните пунктове за управление (ВВПУ) на Община Шумен, на комуникационно-информационната система (КИС) и осигуряване на денонощно оперативно дежурство за оповестяване при привеждане на възложени военновременни задачи в различни степени на готовност за работа във военно време. Да се подобри взаимодействието на отделните структурни звена на общинската администрация с държавните органи и институции, разположени на нейна територия по отношение на координиране на съответните дейности и задачи по отбранително-мобилизационната подготовка, както и опазване на обществения ред и защитата на населението във военно време. Да продължи разработването и поддържането на военновременните плановете на Община Шумен, като експертният потенциал за този вид дейност е съсредоточен в дирекция „Сигурност".

4.1.3. Защита при бедствия и други инциденти, застрашаващи здравето и живота на гражданите

Стратегията разглежда защитата на населението при бедствия на територията на Община Шумен като една от основните задачи, свързани със сигурността на гражданите. Независимо, че основно тази дейност по закон е възложена на органите на МВР, то Община Шумен ще изгради своя структура в лицето на дирекция „Сигурност". Ето защо укрепването и развиването на това звено е от изключителна важност за решаването на тази основна задача.

Към момента Община Шумен има регистрирано Доброволно формирование за предотвратяване и овладяване на бедствия, пожари и извънредни ситуации и отстраняване на последиците от тях, съгласно „*Закон за защита при бедствия*“ (ЗЗБ). Формированието е на пряко подчинение на кмета на общината.

Дирекцията трябва да доразвие дейността си в следните направления:

- обединяване на усилията на общинско ниво за устойчиво развитие и нормален ритъм на живот и работа след възникване на бедствия, аварии или

извънредни ситуации;

- планиране на общинско ниво за действие при различните видове опасности;

- провеждане на ефективна превенция за намаляване на риска и последиците от бедствия;

- готовност за бърза намеса и реакция с цел спасяване на хора;

- прилагане на мерки за ограничаване на въздействието при възникване на епидемични обстановки;

- прилагане на мерки за намаляване на вредните последици за хората и околната среда;

- изграждане на култура в обществото за поведение при бедствия, аварии, епидемии и извънредни ситуации.[3]

4. 1.4. Информационна и киберсигурност

Дигитализацията на съвременното общество изисква и защита на съвременните системи за обмен на информация и съхраняваните в тях данни. Броят на кибератаките нараства, а икономиката и обществото, които са все по-свързани с интернет, са уязвими за киберзаплахи и кибератаки и имат нужда от засилени защитни механизми.

Реакцията на киберинциденти може да има много форми – от определяне на технически мерки, предполагащи съвместно разследване на техническите причини за инцидента от две или повече организации (напр.анализ на зловреден софтуер) или определяне на начините, по които организациите да установяват дали са били засегнати.

Светът ни се уповава на цифрови инфраструктури, технологии и онлайн системи. Всичко това благоприятства киберпрестъпността. Престъпниците бързо се адаптират към използването на новите технологии за свои собствени цели. Необходимо е да се изпълняват процедури за сигурност постоянно и в периодичен цикъл:

1. ИДЕНТИФИЦИРАНЕ – по-доброто организационно разбиране на ИТ инфраструктурата и готовността за управление на киберрисковете за лица, системи, активи, данни и възможности.

2. ЗАЩИТА – подходящи предпазни мерки за намаляване на повърхността на атаката и за осигуряване на наличността, целостта, поверителността на информация, ревизирането и изпълнението на критичните ИТ услуги.

3. ОТКРИВАНЕ – подходящи инструменти за идентифициране на естеството и обхвата на кибератаките, извършени върху обекта.

4. РЕАКЦИЯ - включва предприемане на подходящи действия по отношение на открит инцидент в информационните системи и инфраструктура на Община Шумен. При реакция се ограничава въздействието на потенциален инцидент върху засегнатите системи и ресурси.

5. ВЪЗСТАНОВЯВАНЕ – подходящи мерки за ефективно смекчаване на откритите инциденти в киберсигурността, както и възстановяване на засегнатите ресурси до работоспособно състояние [2].

4.2. Вертикални политики

Вертикалните политики за сигурност определят йерархичните взаимовръзки между държавните институции и ведомства, структурите на местната власт и разнотипни групи от хора с цел постигане на сигурност на

общността и отделния гражданин. Те включват основно Министерски съвет (МС), Национално сдружение на общините в България (НСОРБ), Областната администрация (ОА), Общините, различни общности, групи от хора и достига до отделния гражданин.

Община Шумен работи активно с държавните институции, основно чрез Областна администрация към министерствата и централните ведомства по отношение на сигурността на гражданите.

Експерти от общината участват в комисии и работни групи за определяне приоритетите на общинската администрация по въпросите на сигурността.

По въпроси за сигурността, Община Шумен поддържа преки контакти с (НСОРБ) чрез участия във форуми, изготвяне на конкретни предложения за промени в нормативната база, изготвяне на стратегически документи и др.

Към общинският съвет на Община Шумен е сформирана постоянна комисия „Правна и опазване на обществения ред“ (ПКПООР), която приема и обсъжда отчети на различните структури и звена за сигурност, плановете на ОШ за защита при природни бедствия, доклади по текущи въпроси и др.

Основни насоки на действие на структурата за сигурност

Структурата за сигурност ще бъде важна и неразделна част от дейността на Община Шумен. Тя е изградена с цел:

- осигуряване на защита на гражданите при природни бедствия, аварии, инциденти и епидемии, застрашаващи живота и здравето им;
- опазване на общинската собственост и тази на гражданите и юридическите лица;
- незабавно разпространение на информация по хоризонтала и вертикала без забавяне;
- незабавна реакция при необходимост с наличните сили и средства;
- подпомагане на МВР и други държавни структури;
- осигуряване защита на гражданите при военно положение или война;
- превенция на рисковете и заплахите;

Структурата за сигурност се състои от инструментариум и дейности.

5.1. Инструментариум

Инструментариумът е съвкупност от всички средства, методи и способи, свързани с практическото осъществяване на хоризонталните и вертикалните политики за сигурност. Инструментариумът за сигурност на Община Шумен се състои от системи, центрове, пунктове, учебни бази и други елементи, свързани с прилагане на превантивни мерки и предприемане на реални действия за гарантиране сигурността на гражданите.

5.2. Дейности на сигурността

Дейностите по сигурността са всички реални действия на Общинския съвет на Община Шумен и Администрацията на Община Шумен. Дейностите включват:

-анализи и оценки на рисковете;

-различни видове планове - краткосрочни и дългосрочни;

-превенция на всички нива и във всички сфери на сигурността;

-финансиране на проекти, свързани със сигурността;

-осигуряване на необходимите материално-технически средства и среда на структурите, занимаващи се със сигурността в Общината;

-контрол върху всички структури, имащи отношение към сигурността на Община Шумен.

5.3. Контрол върху дейността

Контролът е елемент, неразривно свързан с реализирането на всички изпълнени по настоящата Стратегия дейности. Той трябва да бъде осъществяван на всички нива, имащи отношение към нея като:

-Общинския съвет чрез Комисията по обществен ред и сигурност;

-Кметът на Община Шумен чрез Дирекции „Сигурност" и ОП „Стопанска и охранителна дейност“;

-Кметове на кметства;

-Ръководители на общински предприятия и дружества;

-Директори на училища, детски градини и др.

Заключение

Стратегията за сигурност на Община Шумен (2022-2028г.) е разработена на базата на направени анализи, като е отчетено реалното състояние на сигурността в Община Шумен и са набелязани нови приоритети.

Стратегията е документ, който дава насоките за развитието на сигурността в Община Шумен, а детайлите ще бъдат разработени в План за реализирането ѝ, като той може да бъде променян и допълван ежегодно от Общинския съвет, в зависимост от нуждите на Община Шумен и на нейните граждани.

ЛИТЕРАТУРА

[1] Наредба № 8121з-1225/27.09.2017 г. на МВР и ДАНС

[2] Стратегия за сигурност на Столична Община за 2021-2027г. < https://www.sofia.bg/web/mayor-of-sofia/strategies/-/asset_publisher/A6phRQPDMA97/content/strategia-za-sigurnost-na-stolicna-obsina-za-2014-2020g /20182?inheritRedirect=false > (06.12.2022 г.)

[3] Структура на Община Шумен <https://www.shumen.bg/administratsiya/struktura-na-obshtinata/> (06.12.2022 г.)

АВТОМАТИЗИРАНО УПРАВЛЕНИЕ НА МРЕЖОВА ИНФРАСТРУКТУРА ЧРЕЗ РАМКАТА ЗА МРЕЖОВА АВТОМАТИЗАЦИЯ ANSIBLE

Мустафа Б. Узун, Валентин Т. Атанасов

AUTOMATED NETWORK INFRASTRUCTURE MANAGEMENT THROUGH THE ANSIBLE NETWORK AUTOMATION FRAMEWORK

Mustafa B. Uzun, Valentin T. Atanasov

ABSTRACT: *Network programmability is a trend enhanced and enforced by SDN (Software Defined Networking), which is based on scripting methods and standard programming languages used to manage and monitor network processes and elements. This article presents some new methods for configuring network devices using network automation frameworks, and often called tools, each framework is implemented through a set of software packages and predefined rules that address the network infrastructure configuration management system. These methods represent the future of networking, allowing the management of a large number of devices in a unified manner.*

KEYWORDS: *Automated computer network management; network automation; Ansible; network automation through Ansible.*

1. Въведение

Програмируемостта и автоматизираното управление на компютърните мрежи имат основната цел да опростят задачите, свързани с конфигурирането, управлението и работата на мрежовото оборудване. Съгласно тези условия има редица технологии и подходи за автоматизиране на мрежи, които са насочени към въздействие върху различни части на мрежата и идват като решения на споменатите проблеми.

Мрежовата автоматизация, подобно на повечето видове автоматизация, се смята за средство за по-бързо „правене на нещата“, което означава, че не е ръчно, в контекста на мрежата, това е процес за автоматизиране на конфигурацията, управлението, тестването, внедряването и работата на физически и софтуерно базирани устройства в мрежа. Задачите, които обикновено се изпълняват от мрежовия или системния администратор, могат да бъдат автоматизирани с помощта на редица инструменти и технологии [1] [2]. Всеки тип мрежа може да използва мрежова автоматизация, включително центрове за данни, доставчици на услуги и кампуси, за подобряване на ефективността, избягване на повтарящи се задачи, спестяване на време, намаляване на човешки грешки и по-ниски оперативни разходи.

Мрежовата програмируемост може да има различни значения в зависимост от гледната точка. За мрежовия инженер възможността за програмиране означава взаимодействие с устройство или група устройства (конфигурации за управление, отстраняване на неизправности и т.н.) със софтуер, който стои логически над устройството [3].

Мрежовата автоматизация използва програмна логика за управление на мрежови ресурси и услуги [4] [5], при които наборът от инструменти за програмиране на мрежата е основата за усъвършенствана мрежова автоматизация от следващо поколение с добавяне на предварително изградена интелигентност. По този начин може да се подпомогнат мрежови внедрявания, операции или отстраняване на неизправности, мрежовата програмируемост прави автоматизацията по-проста и по-достъпна чрез стандартни инструменти. Скриптовите езици се използват широко от мрежови и системни администратори за автоматизиране на задачи. Сред инструментите за автоматизация Python и Ansible са най-популярните, използвани при софтуерно дефинирана мрежа (SDN) [1].

2. Рамки за мрежова автоматизация

Един от основополагащите механизми, които се разглеждат в този подход за обогатяване на изследването, са рамките за мрежова автоматизация. Налице са широк набор от тях, често наричани инструменти, като всяка рамка се изпълнява чрез набор от софтуерни пакети и предварително дефинирани правила, които адресират системата за управление на конфигурацията на мрежовата инфраструктура. Ansible, SaltStack, Puppet, Chef и редица други инструментите имат възможностите за бързо предоставяне на инфраструктура чрез избягване на последователни и ръчни взаимодействия. Използвайки CMS (Configuration Management System) и комбиниране на инструменти за автоматизация с параметрите на желаното състояние се извършва конфигурация в системна последователност за цялата система, обхващаща мрежови устройства (маршрутизатори, комутатори, сървъри) [8]. Използваните инструменти имат сходни характеристики, като архитектурните разлики между тях са изброени в две части по-долу.

Общи точки [8]:

- Цялостно автоматизиране и управление на конфигурацията.
- Проверка на текущото състояние преди промяната му (идемпотентност).
- Факти и събиране на информация.
- Работа с модули и библиотеки на заден план.
- Фондация с отворен код.

Разлики:

- Базирани на агент и без агент.
- Централизирано и децентрализирано.
- Персонализиран протокол и базиран на стандарти протокол.
- Възможност за разширение чрез програмни езици.
- Домейн-специфичен език (DSL) срещу базирани на стандарти формати на данни и езици с общо предназначение.
- Push срещу Pull срещу event-driven (управлявано от събития).

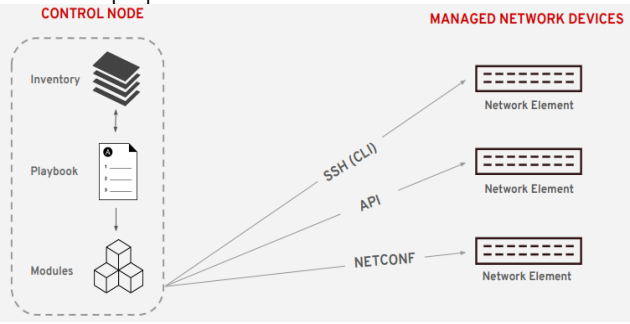
В следващия подраздел ще се разгледа Ansible като пример от тези рамки, който е обичаен инструмент при повечето случаи на употреба, тъй като е без агент, лесен за използване и популярен в бранша [8].

Ansible

Ansible е популярна рамка за мрежова автоматизация, написана на програмния език Python, която се използва за автоматизиране на мрежови операции и управление на конфигурации. Той опростява управлението на различни инфраструктурни възли и се явява посредник към бизнес логиката в добре известни процедури [10]. Това е безплатен софтуер с отворен код, придобит от корпорацията Red Hat [7]. Насочен към поддръжка за мрежови устройства, започвайки с Ansible 1.9, а с Ansible 2.9, текущата му поддръжка за мрежови устройства нараства значително. Той може да взаимодейства с мрежови устройства чрез SSH или чрез API, ако мрежовите доставчици поддържат API на своето оборудване [10]. Ansible се характеризира със следното [7]:

- *Лесен за използване:* Няма нужда от специално кодиране, за да се започне с всички инструкции или задачи, които трябва да бъдат автоматизирани. Те са документирани в стандартен, четим от хора формат на данни, който лесно може да разбере.
- *Без агент:* Няма нужда от инсталиране на агент или допълнителен софтуер в целевите мрежови устройства.
- *Разширяемост:* Тъй като е с отворен код и е написан на Python, той може да бъде разширен чрез добавяне на модули и интегриране на други, за да се активира даден набор от функционалности.

Ansible и други инструменти, предназначени за автоматизиране на сървърната инфраструктура, се изпълняват в разпределен начин, при който контролният възел/хост на Ansible се свързва към всеки автоматизиран сървър чрез SSH и последващо копиране на Python код на всеки сървър. Този код осъществява задачата за автоматизация, чрез разширяване способността за автоматизиране на мрежови устройства, като се установяване на лека промяна, с цел постигане на централизирано опериране. След осъществяване на комуникация чрез SSH (CLI), базиран API HTTP и NETCONF, кодовете на Python се изпълняват локално в контролния възел, без да се копират в целевите мрежови устройства [9]. На (фиг. 1) е илюстрирана общата идея на работния процес Ansible с мрежови елементи [14].



Фиг. 1. *Ansible работен процес с мрежови устройства*

От показаният подход на (фиг. 1) следва, че инструкциите и изпълнението на Playbook се основават на модули, които са набор от файлове на Python. За да бъде използвана Ansible за мрежова автоматизация, трябва да са известни някои терминологии и концепции. Тези термини и концепции са достъпни в документацията на Ansible [11], в комбинация с доклада на Edelman Ansible [7]. Информацията е допълнена с насочващи примери.

Контролен възел (Control Node)

Всяка машина (с изключение на Windows), с инсталиран Ansible, може да изпълнява команди и механизъм за сложни изпълними действия Playbook. Това се постига чрез извикване на /usr/bin/ansible или /usr/bin/ansible-Playbook. Може да се използва всяка компютърна система, на която е инсталиран Python, като контролен възел, в т.ч. мобилни устройства, споделени настолни компютърни станции или сървъри за изпълнение на Ansible.

Управлявани възли

Мрежовите устройства (и/или сървъри), които се управляват с Ansible, също се наричат хостове. Ansible не се инсталира на управляваните възли.

Инвентар (Inventory)

Управляваните възли са изброени в „инвентарен“ файл, който може да се нарича хост файл. При управлението на конфигурацията, използваният инструмент трябва да се знае на кои устройства трябва да работи. Това е известно като опис. Без инвентаризация би имало набор от Playbooks, които определят желаното състояние на системата, но не би било възможно да се определи на кои устройства трябва да се стартират.

С Puppet и Chef тази информация се съхранява на централен сървър. Тъй като в Ansible няма централен сървър, ще бъде необходим друг начин да се получи цялата тази информация в кода, който се изпълнява, за да се приложи желаното състояние. Това е мястото, където идва файлът с инвентара.

Описът може да посочи информация като IP адрес за всеки управляван възел. Инвентарът може също да организира управляваните възли чрез създаване и влагане на групи за по-лесно управление и мащабиране. Използвайки файл с инвентар, като предстоящия пример (фиг. 2) се дава възможност да се автоматизират задачи за конкретни хостове и групи от хостове, като се препращат към правилния хост/група, използвайки параметъра hosts, който съществува в горната секция на всеки „play“. Също така е възможно да се съхраняват променливи като потребителско име и парола в инвентарен файл. На (фиг. 2) е показан пример за инвентарен файл, включващ две групи Cisco устройства, IOS и NXOS, със специфициране на общи променливи [30].

Модули (Modules)

Модулите са единиците от кода, който Ansible изпълнява. Всеки от тях представлява конкретна употреба за изпълнение на дадена задача от администриране на потребители на конкретен тип база данни, до управление на VLAN интерфейси на конкретен тип мрежово устройство. Възможно е да се извика единичен модул със задача или да се извикат няколко различни модула в Playbook. Има четири общи мрежови модула, изброени в (табл. 1) [13].

```
[all:vars]
ansible_user=Administrator
ansible_password=1234

[ios]
R1 ansible_host=212.50.29.3
R2 ansible_host=212.50.29.6

[nxos]
SW1 ansible_host=213.169.52.2

[ios:vars]
ansible_network_os=ios
ansible_connection=network_cli

[nxos:vars]
ansible_network_os=nxos
ansible_connection=nxapi
```

Фиг. 2. *Пример за инвентарен файл на Ansible*

Таблица 1. *Модул с четири основни мрежови устройства*

Модули	Описание
command	Командните модули изпълняват произволни команди на мрежово устройство
config	Конфигурационните модули позволяват конфигурация на мрежовото устройство по начин със състояние (идемпотентен)
facts	Фактическите модули връщат структурирани текущи данни за мрежовото устройство
resource	Ресурсният модул може да чете и конфигурира конкретен ресурс на мрежово устройство (напр. VLAN)

Playbooks

Playbooks представлява обект от най-високо ниво, който се изпълнява при автоматизиране на процеси. Те представляват подреден списък със записани plays и задачи, така че да може да ги изпълнява многократно в този ред. Books могат да допълват променливи, както и задачи, написани на YAML (Yet Another Markup Language). Те са лесни за четене, писане, споделяне и разбиране. На (фиг.3) е показан пример за файл на Playbook, който включва един play и една задача за добавяне на VLAN към хост на мрежово устрой ство Cisco [12].

```
---
-     name: add VLANs
      hosts: cisco
      tasks:
            - name: add VLAN configuration
              ios_vlans:
                config:
               - name: desktops
                vlan_id: 20
               - name: servers
                vlan_id: 30
                        - name: printers
                          vlan_id: 40
```

Фиг. 3. *Пример за Ansible Playbook файл*

Съгласно документацията YAML е друг стандартен тип формат на структурирани данни, като JSON и XML, той започва с „---“ в горната част на файла и се основава на отстъп за разделяне и описание на списъци и информация за обекти.

Play

Една или повече play могат да съществуват в рамките на Ansible Playbook. В предишния пример на Playbook има една игра в рамките на Playbook, която започва със заглавна секция, където са дефинирани специфични за play параметри (име, хостове и може да включва тип връзка). Всяка игра се състои от една или повече задачи.

Задачи (Tasks)

Това са единиците за действие в Ansible. Допуска се изпълнение на една задача веднъж с ad-hoc команда. Задачите също могат да използват параметъра за име точно, както могат да се изпълнят с (play). Следващият ред след деклариране на името на задачата в примера показан на (фиг. 4), започва с ios_vlan като се цели изпълнение на модула Ansible, наречен ios_vlan.

Шаблони (Templating)

Ansible поддържа езика Jinja2, чрез който е възможно да бъдат създавани шаблони, които представляват конфигурацията на устройството, но с променливи, както е показано на (фиг. 4) [6].

В документацията се отбелязва, че целта за използването на шаблони е да се отделят входовете от основния собствен синтаксис на производителя на мрежово оборудване (CLI) на конфигурационния файл в отделни файлове, за да се избегне писането на повтарящи се редове, след което Ansible помага да се преодолее празнината между изобразяването на входовете и стойностите, поставени в YAML файл с конфигурационните шаблони [7].

```
hostname {{hostname}}
!
interface GigabitEthernet0/0
ip address {{address1}} {{mask1}}
ip ospf {{OSPF_PID}} area {{area}}
!
interface GigabitEthernet0/1/0
ip address {{address2}} {{mask2}}
ip ospf {{OSPF_PID}} area {{area}}
```

```
---
hostname: BR1
address1: 10.1.1.1
mask1: 255.255.255.0
address2: 10.1.2.1
mask2: 255.255.255.0
RID: 1.1.1.1
area: '11'
OSPF_PID: '1'
```

Фиг. 4. *Пример за шаблон на конфигурационен файл, използващ Jinja2 от ляво със свързаните стойности в YAML файл от дясно*

С изложеното по-горе, разглежданата Ansible предлага иновативен и надежден начин за автоматизиране на конфигурацията на мрежови устройства под формата на прости задачи в единични или множество Playbook. По този начин, не се налага използването от агенти или допълнителен софтуер, за да бъде инициализирано автоматизирането при мрежовото конфигуриране. В допълнение езикът Python може да бъде използван за разширяемост, основавайки се на поддържаните шаблони с помощта на езика за шаблони Jinja. Ansible използва определени интерфейси за програмиране, включително възможността за взаимодействие през CLI чрез SSH, изграждайки един автоматичен механизъм за мрежово конфигуриране.

Заключение

Програмната контролируемост на мрежата е концепция, която се прилага и в областта на мрежовите конфигурации, задвижвана от иновативните реализации на програмно дефинираните мрежи. Автоматизираното конфигуриране и наблюдение, независимо от производителя, е цел приложима не само на SDN устройства, но и при други мрежови решения. В тази статия се показва ефективността на програмната автоматизация в „наследените“ мрежи, които не могат да се конфигурират програмно с добре познатите SDN решения. Наследеното мрежово оборудване представлява важен набор от устройства, произведени от различни производители, които са по-трудни за управление използвайки добре познатите стандартни методи.

Използвайки Ansible, мрежовите инженери не трябва да конфигурират самостоятелно всяко отделно устройство, а да се прилагат програмнии модели на автоматизирано управление за постигане на ефективно управление на мрежовата инфраструктура, чрез внедряване на скриптове за автоматизация.

Организациите биха могли да се възползват от стратегия за автоматизирано управление с контрол на промените, архитектура, сигурност и оперативност. Основни предимства на този подход са ефективността на задачите, намалена уязвимост, непрекъснатост на процеса, ниското ниво на сложност,

стабилност на мрежовата топология, съкратеното време, за което програмно автоматизираните системи следят мрежата

ЛИТЕРАТУРА

[1] J. A. Alex, NETWORK AUTOMATION USING PYTHON 3, 2018.

[2] Cisco Inc, "What Is Network Automation?," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/solutions/automation/network-automation.html. [Accessed August 2020].

[3] T. Ryan and G. Jason, Programming and Automating Cisco Networks, USA: Cisco Press, 2016.

[4] A. W. Rheza and R. R. Nur, "PENGEMBANGAN APLIKASI OTOMATISASI ADMINISTRASI JARINGAN BERBASIS WEBSITE MENGGUNAKAN BAHASA PEMROGRAMAN PYTHON," Journal of Mechanical Engineering, Electrical and Computer Science, vol. 10, no. 2, pp. 741-752, 2019.

[5] A. Ratan, E. Chou, P. Kathiravelu and D. M. O. F. Sarker, Python Network Programming, UK: Packt Publishing, 2019.

[6] O. WENDELL, CCNA 200-301 Official Cert Guide, Volume 2, San Jose, CA: Cisco Press, 2020.

[7] E. Jason, "Network automation with Ansible," O'Reilly Media, Inc, USA, 2016.

[8] P. Hank, Writer, Configuration Management and the Network, A Network Programmability Basics Presentation. [Performance]. Cisco DevNet, 2017.

[9] E. Jason, S. L. Scott and O. Matt, Network Programmability and Automation, Skills for the Next-Generation Network Engineer, USA: O'Reilly Media, Inc, 2018.

[10] O. Karim, Network Automation Cookbook, UK: Packt Publishing Ltd., 2020.

[11] Red Hat, Inc, "Ansible for Network Automation, Documentation," Red Hat, Inc, 2019. [Online]. [Accessed August 2020].

[12] C. Sean and B. Andrius, Writers, What's new with Ansible Network. [Performance]. Red Hat, Inc.; Cisco DevNet, Inc.

[13] D. Gerald, Writer, Network Resource Modules. [Performance]. Red Hat, Inc.

[14] B. Kyle and D. Kevin, Writers, Ansible Network Automation. [Performance]. Red Hat, Inc., 2018.

WDM СПОСОБ ЗА УВЕЛИЧАВАНЕ ПРОПУСКАТЕЛНАТА СПОСОБНОСТ НА КАНАЛА

Екатерина М. Христова, Цветослав С. Цанков

WDM WAY TO INCREASE CHANNEL THROUGHPUT

Ekaterina M. Hristova, Tsvetoslav S. Tsankov

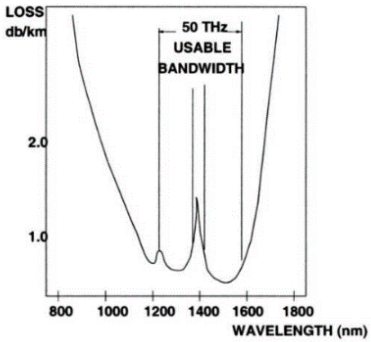
ABSTRACT: *WDM (Wavelength-division multiplexing) is the technology for combining several wavelengths on the same fiber at the same time. A powerful aspect of WDM is that any optical channel can carry any transmission format. WDM dramatically increases the capacity of a fiber optic network. In this way, it is recognized as a transport technology at all levels of the network.*

KEYWORDS: *Multiplexing, optical fiber, packet switching, signal-to-noise ratio, wavelength, WDM.*

Въведение във WDM

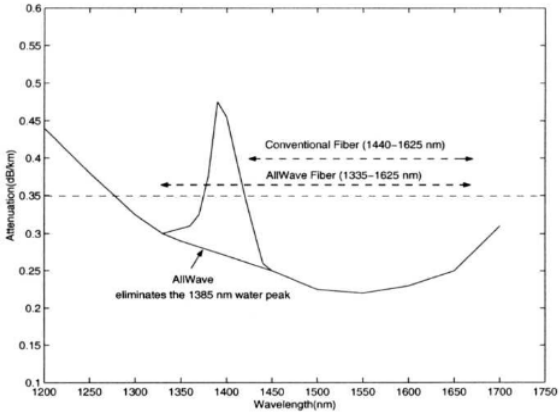
Поради бързия растеж на телекомуникационните връзки са необходими висок капацитет и по-високи скорости на предаване на данни на по-далечни разстояния. За да отговорят на тези изисквания, мрежовите мениджъри разчитат все повече на оптични влакна. Обикновено има три метода за разширяване на капацитета: инсталиране на повече кабели, увеличаване на системния битрейт за мултиплексиране на повече сигнали и мултиплексиране по дължина на вълната (WDM). Първият метод, инсталирането на повече кабели, ще бъде предпочитан в много случаи, особено в градските райони, тъй като влакното е евтино, а методите за инсталиране по-ефективни. Но когато не е налично място за изграждане на тръбопроводи или е необходима голяма конструктивна сила, този метод може да не е най-рентабилен.

Друг начин за разширяване на капацитета е да се увеличи битрейтът на системата, за да се мултиплексират повече сигнали. Но увеличаването на битрейта на системата също може да не се окаже рентабилно. Тъй като много системи вече работят при скорости на SONET OC-48 (2,5 GB/s) и надграждането до OC-192 (10 GB/s) е скъпо, изисква смяна на цялата електроника в мрежата за добавяне на сравнително малък капацитет (фиг. 1). Доказано е, че WDM е по-рентабилната технология. Тя не само поддържа текущата електроника и влакна, но също така може да споделя влакна чрез предаване на канали при различни дължини на вълната (цветове на светлината). Освен това системите вече използват усилватели с оптични влакна, тъй като повторителите също не изискват надстройка за повечето WDM мрежи.



Фиг. 1. *Регион на ниски загуби при едномодови оптични влакна*

Има много варианти на мултиплексиране с разделяне по дължини на вълните. Прост вариант може да бъде конструиран, ползвайки 1310 nm като една дължина на вълната, и 1550 nm като друга, или 850 nm и 1310 nm (фиг. 2). Този тип WDM-система може да бъде построена с относително прости и евтини компоненти, като някои приложения работят по този начин и на този принцип от много години.



Фиг. 2. *Регион на ниски загуби при едномодови оптични влакна*

От сравнението на трите метода за разширяване на капацитета лесно може да се направи заключение, че WDM е най-доброто решение за посрещане на търсенето на повече капацитет и по-бързи скорости на предаване на данни.

WDM Мрежова архитектура

При широкообхватните мрежи се използват комуртируеми връзки, като двете най-често срещани са с комутиране на пакети и комутиране на вериги. Тези подходи могат да се използват както в неоптични мрежи, така и в оптични мрежи.

В оптичните мрежи тези подходи се наричат съответно оптични мрежи с комутация на пакети и оптични мрежи с маршрутизиране по дължина на вълната.

В оптична мрежа с комутация на пакети, пакетът се предава на определена дължина на вълната и съдържа заглавно поле, което се предава на отделна или същата дължина на вълната. Заглавното поле се обработва от комутаторите в оптичния домейн и на самият пакет се задава маршрут. Пакетите се съхраняват изцяло в оптичната среда между източника и предназначението, поради което може да се постигне прозрачност на данните. Оптичните мрежи с комутация на пакети могат да бъдат както синхронни, така и асинхронни. В оптична мрежа с комутация на пакети всички пакети са с еднаква дължина и предаването на пакетите е синхронизирано към отделни времеви интервали. Асинхронните оптични мрежи с комутация на пакети страдат от повече конкуренция за пакети, докато синхронизацията въвежда допълнителни разходи за управление на хардуера и мрежата. И в двата типа мрежи разрешаването на конкуренцията има голямо влияние върху производителността на мрежата.

Маршрутизираните по дължина на вълната WDM мрежи [1, 2, 3, 4, 5, 6, 7], които използват оптични кръстосани връзки (Optical Cross-Connect – OXC), са способни да комутират данните оптично. С най-съвременната технология оптичната кръстосана връзка може да бъде един от двата вида:

— OXC с опто-електро-опто (OEO) преобразуване, които са оборудвани с предаватели и приемници и преобразуват данни от оптично поле в електронно поле, като комутират данни с електрическа комутираща нишка и преобразуват данните обратно в оптично поле. Този тип OXC често се наричат „OEO комутатори“.

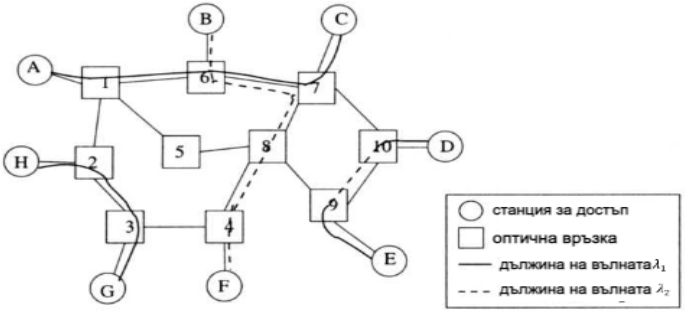
— Изцяло оптични OXC, които имат фотонни комутиращи нишки за комутиране и комутират данни изцяло в оптичен домейн. Изцяло оптичните OXC се наричат също „изцяло оптични комутатори“, „OOO OXC“ и „OOO комутатори“.

OEO комутаторите са способни на регенериране и преобразуване на дължина на вълната, които са две важни задачи в широкообхватните WDM мрежи [8]. Приема се, че всички OXC са изцяло оптични комутатори, които са способни на оптична регенерация. Оптичните преобразуватели на дължина на вълната не са задължителни в изцяло оптичен комутатор.

Оптичните кръстосани връзки са активни комутатори и могат да бъдат динамично конфигурирани. Поради тяхната функция в мрежи с маршрутизирана дължина на вълната, OXC се наричат също „маршрутизатори с дължина на вълната“ или „комутатор за маршрутизиране на дължина на вълната“ (WRS). Изцяло оптичните комутатори се наричат също фотонни кръстосани връзки (PXC).

В сравнение с традиционните мрежи, базирани на SONET [9], които обикновено са под формата на пръстени или взаимосвързани пръстени, базираните на OXC мрежи, маршрутизирани по дължина на вълната, могат да имат обща мрежеста топология. Маршрутизирана по дължина на вълната оптична WDM мрежа е показана на фиг. 3. Мрежата се състои от десет OXC, свързани с оптични връзки, за да образуват произволна мрежова топология. Всеки краен потребител е свързан към OXC чрез оптична връзка. Комбинацията от краен потребител и съответния му оптичен комутатор се нарича мрежов възел. Всеки възел (в своята станция за достъп) е оборудван с набор от предаватели и

приемници, като и двата могат да бъдат регулируеми по дължина на вълната. Предавател на възел изпраща данни в мрежата, а приемник получава данни от мрежата.



Фиг. 3. *Маршрутизирана по дължината на вълната WDM Mesh мрежа*

Основният механизъм на комуникация в мрежа с маршрутизирана дължина на вълната е светлинен път. Светлинният път е изцяло оптичен комуникационен канал между два възела в мрежата и може да обхваща повече от една оптична връзка. Междинните възли в пътя на влакното маршрутизират пътя на светлината в оптичната среда, като използват своите комутатори. Крайните възли на светлинния път имат достъп до него с предаватели и приемници. Ако предавателите/приемниците могат да се настройват, те трябва да бъдат настроени на дължината на вълната, на която работи светлинният път. Например на фиг. 3 светлинните потоци се установяват между възли A и C на канала за дължина на вълната λ_1, между B и F на канала за дължина на вълната λ_2 и между H и G на канала за дължина на вълната λ_1 . Светлинният път между възли A и C се маршрутизира чрез комутатори 1, 6 и 7.

При отсъствието на каквото и да е устройство за преобразуване на дължината на вълната, светлинният път трябва да бъде на един и същ канал с дължина на вълната по целия си път в мрежата; това изискване се нарича свойство за непрекъснатост на дължината на вълната на пътя на светлината. Това изискване може да не е необходимо, ако имаме и преобразуватели на дължина на вълната в мрежата. Например на фиг. 3 пътят на светлината между възли D и E пресича влакнеста връзка от възел D до комутатор 10 на дължина на вълната λ_1, преобразува се в дължина на вълната λ_2 при комутатор 10, преминава през влакнеста връзка между комутатор 10 и комутатор 9 на дължина на вълната λ_2, се преобразува обратно в дължина на вълната λ_1 при комутатор 9 и преминава през оптичната връзка от комутатор 9 до възел E при дължина на вълната λ_1.

Основно изискване в оптична мрежа с маршрутизирана дължина на вълната е, че две или повече светлинни пътеки, преминаващи през една и съща оптична връзка, трябва да бъдат на различни канали с дължина на вълната, така че да не си пречат [5, 6, 7, 8, 9, 10].

Маршрутизация и присвояване на дължина на вълната

Особено внимание се отделя на мрежи, работещи при ограничението за непрекъснатост на дължината на вълната, при което светлинните пътеки са настроени между двойки възли и един светлинен път заема една и съща дължина на вълната на всички връзки, които обхваща. При настройката на светлинен път се избира маршрут и му се присвоява дължина на вълната. Ако няма налична дължина на вълната за светлинния път по избрания маршрут, заявката за светлинен път се блокира. Разглежда се проблема с Маршрутизирането и Присвояването на Дължината на Вълната (RWA) и се изследват различни подходи за маршрутизиране и присвояване на дължина на вълната. Всички RWA подходи се симулират с разпределен контролен протокол и тяхната производителност се сравнява. Накратко се разглеждат характеристиките на мрежите с преобразуване на дължината на вълната (които нямат ограничение за непрекъснатост на дължината на вълната) и свързаните изследователски проблеми и предизвикателства.

Управление на връзката за WDM мрежи с маршрутизиране на дължина на вълната

В WDM мрежи с маршрутизиране на дължина на вълната е необходим контролен механизъм за създаване и премахване на изцяло оптични връзки. При пристигане на заявка за връзка, този механизъм трябва да може да избере маршрут, да присвои дължина на вълната на връзката и да конфигурира подходящите оптични комутатори в мрежата. Механизмът също трябва да може да предоставя актуализации, които да отразяват кои дължини на вълната се използват в момента във всяка връзка, така че възлите да могат да вземат информирани решения за маршрутизиране. Изследват се и се сравняват два различни разпределени механизма за управление за установяване на изцяло оптични връзки в WDM мрежа с насочена дължина на вълната: подход, базиран на маршрутизиране на състоянието на връзката и подход, базиран на маршрутизиране с вектор на разстояние.

Маршрутиране и присвояване на дължина на вълната за оцелели WDM мрежи с маршрутизиране на дължина на вълната

Светлинните пътеки са изцяло оптични канали с голям капацитет. Следователно, когато има повреда на връзката, напр. прерязване на оптичен кабел, загубата на данни може да бъде много голяма, ако трафикът не се пренасочва бързо. В мрежа могат да се прилагат различни защитни схеми, включително защита на посветения път, защита на споделен път и защита на споделена връзка и т.н. Предлагат се формулировки на Целочислена Линейна Програма (IPL), както и евристики за решаване на маршрута и дължината на вълната – проблем с присвояване (RWA) в такава мрежа. Целта е да се защити всяка връзка от откази на една връзка, както и да се сведе до минимум общото изискване за мрежови ресурси. Ресурсната ефективност на всяка схема за защита се оценява на примерни мрежи чрез ILP и евристични решения.

Управление на връзката за WDM мрежи с маршрутизиране по дължина на вълната

В мрежа с дължина на вълната с динамичен трафик, механизмът за онлайн управление на мрежата трябва не само да може да настрои светлинен път, но също така да може да защити светлинния път срещу откази и да пренасочва трафика в

случай на неуспехи. Разработва се онлайн механизъм за мрежов контрол за управление на връзките в такава мрежа, използвайки схеми за защита на пътя. Целта е да се защити всяка връзка от откази в, както и да се сведе до минимум общата вероятност за блокиране и закъснения от край до край. Сравнява се защитата чрез специализиран път и защитата чрез споделен път по няколко показателя за производителност. Резултатите от симулацията показват, че със защитата по споделен път може да се постигне ниска вероятност за блокиране на повиквания с бързо възстановяване при повреда.

Маршрутизация за защита на пътя и присвояване на дължина на вълната с ограничения на оптичните кабелни линии

В действителност снопчетата от влакна често се режат едновременно поради строителство или разрушителни природни събития, като земетресения. Влакната, положени в един и същи канал, имат голям шанс да се разрушат по едно и също време. Когато се използва защита на пътя, се изискват основният и резервният път да бъдат разделени на канали, така че мрежата да може да оцелява при повреди на един канал. Освен това два основни пътя не могат да споделят дължини на вълните на общи връзки. Офлайн алгоритмите за статичен трафик са разработени за борба с повредите на един канал. Целта е да се сведе до минимум общия брой дължини на вълните, използвани във всички връзки в мрежите. Представени са както ILP, така и евристични алгоритми и тяхната производителност се сравнява чрез числени примери.

Поставяне на преобразувател на дължина на вълната със споделени схеми за защита

В мрежови WDM мрежи, споделените защитни схеми, като защита на споделен път и защита на споделена връзка, се възползват от мрежовата свързаност и постигат по-добро използване на ресурсите в сравнение със защитата по специален път 1+1. Преобразуването на дължината на вълната улеснява споделянето между защитните ресурси и подобрява използването на ресурсите в мрежа със споделена защита. В мрежа с преобразуване дължина на вълната, където преобразувателите на дължина на вълната са поставени само на ограничен брой възли, изборът на места за преобразуване на дължината на вълната, за да се максимизират ползите от преобразуването на дължината на вълната, е NP-труден проблем.

Маршрутизиране на фотонни слотове

Маршрутизирането на фотонни слотове е подход за реализиране на изцяло оптична мрежа с комутиране на пакети по начин, който е мащабируем и не е прекалено сложен. При маршрутизирането на фотонен слот пакетите се предават в рамките на основна транспортна единица, наречена фотонен слот. Фотонния слот е фиксиран по дължина и обхваща множество дължини на вълната. Всеки фотонен слот се маршрутизира през мрежата като едно цяло; по този начин не е необходимо отделните дължини на вълните да бъдат мултиплексирани или определяни в междинни възли, през които преминава фотонният слот. Когато се реализира маршрутизиране на фотонни слотове в мрежова среда, трябва да бъдат разгледани редица съществени проблеми. Два такива въпроса са справедливостта и разрешаването на спорове. Разработен е аналитичен модел за оценка на производителността на такива мрежи и се валидира анализа чрез симулация. Показано е, че предложеният подход за разпределяне на капацитет може

значително да намали споровете в мрежата и да осигури справедливо разпределение на честотната лента за всяка двойка източник-назначение.

ЛИТЕРАТУРА

[1] Daniel Denev, Analysis of the requirements for optical cables for construction of underwater transmission systems, Journal scientific and applied research, vol. 21, 2021 International Journal, 2021, ISSN 1314-6289

[2] S. Yao, S. Dixit, and B. Mukherjee, "Advanced in photonic packet switching: an overview," IEEE Communications Magazine. pp. 84-94, Feb. 2000.

[3] T. E. Stem and K. Bala, Multiwavelength Optical Networks: A Layered Approach. Reading, MA: Addison-Wesley, 1999.

[4] I. Chlamtac, A. Farago, and T. Zhang, "Lightpath (wavelength) routing in large WDM networks," IEEE Journal on Selected Areas in Communications, vol. 14, pp. 909-913, June 1996.

[5] D. Banerjee, Design and Analysis of Wavelength-Routed Optical Networks. PhD thesis, University of California, Davis, Department of Computer Science, 1996.

[6] B. Mukherjee, D. Banerjee, S. Ramamurthy, and A. Mukherjee, "Some principles for designing a wide-area WDM optical network," IEEE/ACM Transactions on Networking, vol. 4, pp. 684-696, Oct. 1996.

[7] A. Mokhtar and M. Azizoglu, "Adaptive wavelength routing in all-optical networks," IEEE/ACM Transactions on Networking, vol. 6, pp. 197-206, Apr. 1998.

[8] K. Zhu and B. Mukherjee, "Traffic grooming in a WDM mesh network?' IEEE Journal on Selected Areas in Communications, pp. 122-133, Jan. 2002.

[9] W. J. Goralski, SONET. New York, NY: McGraw-Hill, 2 ed., 2000.

[10] O. Gerstel and S. Kutten, "Dynamic wavelength allocation in all-optical ring networks," in Proc. IEEE International Conference on Communications (ICC '97), vol. I. (Montreal, Quebec, Canada), pp. 432-436, June 1997.

ПРЕНОСИМИ СИСТЕМИ ЗА ИНДУСТРИАЛЕН КОНТРОЛ И УПРАВЛЕНИЕ

Христо Х. Хадживанов

PORTABLE SYSTEMS FOR INDUSTRIAL CONTROL

Hristo Hr. Hadzhiivanov

ABSTRACT: *This paper discusses portable systems for industrial control. They are necessary for training and development activities, as well as for partial or complete testing of the mechanics of production lines and replace old type PLC.*

KEYWORDS: *control system, training control system, portable control system, training automation system, portable automation system, automation device testing, automation trainer workstation and PLC experiment set.*

1. Въведение

В съвременното индустриално производство съществена оптимизация може да се осъществи чрез системите за технологичен контрол и управление.

Типична йерархична структура на тези системи е показана на Фиг.1. Първото, най-ниско ниво, е нивото на сензори и изпълнителни механизми, чрез които се получава информация и се въздейства върху производствения процес. Връзката между това и следващото, по-високо второ ниво - „управление и контрол“, се осъществява с цифрови входове и изходи, аналогови входове и изходи, и комуникация. Основните елементи на това ниво са програмируемите логически контролери (ПЛК) и човеко-машинните интерфейси (HMI). Програмата и параметрите на управляемия процес се намират в PLC контролера. С човеко-машинния интерфейс се извършва визуализация на производството като параметри, като текущо схематично състояние на продукцията и текущо техническо състояние на отделните секции. Преди стартиране на производствената линия, чрез HMI устройството се зареждат параметри, чрез рецепта. При необходимост се правят промени по време на производството. Връзката със следващото ниво „наблюдение и записи на данни“ се осъществява с комуникация. Това ниво има поглед върху целия производствен цех и при необходимост могат да се предприемат действия за синхронизиране между отделните производствени линии. От записаните данни може да се прави анализ за оптимизация на производството, за диагностика на повреди, за търсене на причини за проблем с качеството и др.

Фиг.1 Структурата на системите за технологичен контрол и управление.

На ниво „управление и контрол“ оптимизацията представлява корекция на съществуващите програми и алгоритми, както и подмяна на апаратура, за която производителят не предлага резервни части, предлага ги на значително по-висока цена или ги предлага с изключително дълъг срок на доставка.

В по-големите предприятия обикновено има специалисти, които разполагат с необходимите знания за извършване на тези дейности. При по-малките предприятия се използват външни фирми. И в двата случая е необходимо да се извършват тестове и обучения с преносими системи за технологичен контрол и управление.

2. Анализ на преносими системи за технологичен контрол и управление

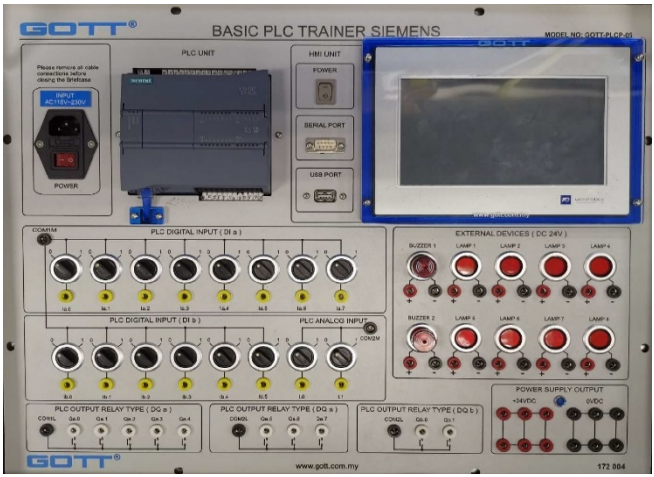
Това са специализирани системи с по-ограничено предлагане спрямо закупуването на програмируеми логически контролери и човеко-машинни интерфейси. Съществуват различни производители на преносими системи за технологичен контрол и управление, някои от които са световно известни, а други са по-известни в Азия.

2.1 Обучаващо куфарче модел GOTT-PLCP-05 на производителя GOTT SDN BHD – Малайзия

На Фиг.2 е показано обучаващо куфарче модел GOTT-PLCP-05 на производителя GOTT SDN BHD съставено от един модул.

Фиг.2 Обучаващо куфарче модел GOTT-PLCP-05.

Системата включва ПЛК SIEMENS с вградени входове и изходи и операторски панел със сензорен дисплей на Fuji Electric. Извеждането на входовете към буксите на панела е направено чрез последователно включване на селекторите във веригата. При свързване на външни бутони и селектори, те се поставят в позиция на затворена верига. Така се пести място и се опростява опроводяването и прегледността на схемата. Изходите са изведени със всички изводи на букси от контролера на панела и дават



Фиг.3 Панел н обучаващо куфарче модел GOTT-PLCP-05.

максимална гъвкавост. За товар и индикация могат да се използват вградените лампи или зумери. Има изведено захранване 24 V постоянен ток на букси за свързване към входовете, товарите (лампите) и др. Свързването към мрежово захранване 230 V се осъществява със стандартен кабел IEC C13/C14. За сензорния дисплей, в спецификацията на производителя GOTT SDN BHD, информацията е оскъдна. Системата няма вградени потенциометри и не е предвидено свързване на други устройства чрез клеморед или куплунг.

Постановката има минимални вградени устройства за входни сигнали и добри вградени устройства за изходните сигнали. Наличното вградено захранване 24 VDC улеснява свързването на външни устройства. Постановката е реализирана с висока гъвкавост и оптималност на вложени елементи.

Постановка съдържа следните хардуерни елементи:

1. Мрежово захранване за 24 V постоянен ток 2.1A.
2. Програмируем логически контролер SIEMENS от серията s7-1200, CPU1214AC/DC/RLY – захранване от 85 до 264 VAC, вградени входове и изходи, 14 бр. цифрови входове 24 VDC, 2 бр. аналогови входове 0-10 V, 10 бр. цифрови релейни изходи., 6 бр. високоскоростни броячи, 1бр. Етернет порт и поддръжка на SD карта памет.
3. Операторски панел: HMI MONOTOUCH на производителя Fuji Electric.
4. Селектори 14 бр.
5. Контролни лампи 8 бр.
6. Зумери 2 бр.
7. Букси за захранване с 24 VDC.
8. Тегло и размери на системата не са посочени.

2.2 Обучаващо куфарче модел TA 515 на производителя ABB

Фиг. 4 Обучаващо куфарче модел TA 515.

На Фиг.4 е показано обучаващо куфарче модел TA 515 на фирмата производител на апаратура за автоматизация ABB. Състои от два основни модула: а) сензорен дисплей и б) PLC система с операторски панел.

На Фиг.5 е показан модул б), състоящ се от операторски панел, CPU, разширителни модули за цифрови и аналогови входове и изходи и комуникационни модули. Операторският панел е много семпъл, на него има монтирани само селектори и потенциометри. Няма монтирани устройства за свързване към изходите, както и няма изведен електрически интерфейс или куплунг за свързване на други източници на сигнали и устройства. От друга страна, модулите на контролера са лесно достъпни за създаване на директни връзки, но честите опроводявания биха разбили вградените клемореди на картите.

Човеко-машинният интерфейс е тип CP6607 - представител на серията висок клас панели CP600-Pro на ABB. Тази серия предлага панели с четири размера на екрана 5” (CP6605), 7” (CP6607), 10.1” (CP6610), 15.6” (CP6615) и 21.5” (CP6621). Тези панелите могат да са част от системите за автоматизация на ABB: PLC-AC500, ABB Drives и ABB Motion. Серията CP600-Pro поддържат и web браузър. Производителят дава възможност тази серия да се интегрира и към

системи на други производители за компютърна автоматизация на производството.

Фиг. 5 PLC панел на куфарче модел TA 515 на производителя ABB.

Постановката се захранват с адаптер за 24 VDC. В комплекта е включена и SD карта с демо програми за ПЛК и операторския дисплей.

Модулите на системата имат значителни възможности, които не могат добре да се използват с вградените 8 бр. селектори. За да може възможностите на системата да се използват по-добре, е наложително използването на външни устройства с директно опроводяване към картите и допълнително захранване.

Постановка съдържа следните хардуерни елементи:

1. Програмируем логически контролер от системата AC500, CPU модул PM585-ETH – захранващо напрежение 24 VDC, няма вградени входове и изходи, може да се разширява до 10 бр. входно-изходни модула, 2 бр. Етернет портове, 2 бр. RS232/485, дисплей и поддръжка на SD карта памет.
2. TB521-ETH – Терминална основа за система AC500
3. CM579-PNIO – PROFINET комуникационен модул.
4. DA501 – входно-изходен модул съдържащ – 24 бр. цифрови входа, 4 бр. аналогови входа и 2 бр. аналогови изхода.
5. CI502-PNIO - PROFINET комуникационен модул с 8 бр. цифрови входове и 8 бр. цифрови изходи, 2 бр. висикоскоростни броячи (HSC)
6. Селектори – 2 бр.
7. Потенциометри за регулиране на аналогов сигнал – 2 бр.

8. 7” (CP6607) - операторски панел от серията - Control Panel CP600-Pro
9. Куфар
10. Захранващ адаптер
11. Размери на системата не са посочени
12. Тегло 7,2 кг.

2.3 Обучаващо куфарче SIMATIC S7 Training Case S7-1200 на производителя SIMENS

На Фиг.6 е показано обучаващо куфарче модел s7-1200 на фирмата производител на апаратура за автоматизация Siemens, съставено от един модул. Системата включва CPU модул с вградени входове и изходи, входно-изходни

Фиг. 6 Обучаващо куфарче модел 6ZB2310-0CG00 на производителя SIEMENS.

карти, мрежови комутатор, сензорен дисплей, операторски панел и куплунг за свързване на макетна конвейерна лента. На панела има изведени селектори, контролни лампи и потенциометър за регулиране на аналогов сигнал. Системата не е предвидена за свързване на външни бутони, селектори и др. устройства. Мрежовото захранване 230 V се осъществява със стандартен кабел IEC C13/C14 и ключ за „вкл“. и „изкл“.

Човеко-машинният интерфейс е тип KTP600. Представител на серията панели с основни функции (SIMATIC HMI Basic). Тази серия предлага панели с пет размера на екрана 3,6” (KP300), 3,8” (KTP), 5.7” (KTP600), 10.4” (KTP1000) и 15” (KTP). Тези панели могат да се свързват с по-голямата част от системите за автоматизация на SIEMENS. Производителят дава възможност тази серия да се интегрира към системи за компютърна автоматизация на производството и на други производители.

Постановката има минимални вградени устройства за входни сигнали и слаби вградени устройства за изходните сигнали. PLC и HMI хардуерът има значителни възможности, които не могат добре да се използват с вградените устройства. Много добро, дори отлично използване може да се получи, чрез свързване на външни макетни устройства с куплунг. Системата е по тясно специализирана за използване с външни макетни устройства.

В описанието на системата в сайта на SIMENS има връзка към курсове за обучения върху тази система.

Обучителната постановка съдържа следните хардуерни елементи:

1. Мрежово захранване от серията S7-1200.
2. Програмируем логически контролер SIEMENS от серията s7-1200, CPU1214DC/DC/DC – захранване 24 VDC, с вградени входове и изходи, 14бр. цифрови входове 24 VDC, 2 бр. аналогови входове 0-10V, 10 бр. цифрови транзисторни изходи., 6 бр. висококоростни броячи, 1бр. Етернет порт и поддръжка на SD карта памет.
3. Аналогов изходен модул – аналогов изход 1 бр.
4. Аналогов входно-изходен модул SM 1234 – входове 4 бр., изходи 2 бр.
5. Потенциометри за регулиране на аналогов сигнал – 1 бр.
6. Цифров входно-изходен модул SM 1223 – входове 8 бр. и изходи 8 бр.
7. Мрежови комутатор CSM 1277 – портове 4 бр. RJ45
8. Basic Panel KTP600 - 5.7” TFT display, 320 x 240 пиксела, 256 цвята
9. Интерфейс за свързване на макетна конвейерна лента
10. Размери (W × H × D) 390x 310x290 mm.
11. Тегло 11 кг.

2.4 Обучаващо куфарче FESTO със система на производителя на апаратура за автоматизация Rockwell Automation

На Фиг.7 е показано обучаващо куфарче модел Advanced PLC Training System 588969, съставено от един модул. Системата включва ПЛК с вградени входно-изходни карти, дисплей и операторски панел.

Панелът не само изглежда много професионално, но и разполага с най-много възможности от разгледаните до сега. Има изведени селектори, бутони, потенциометри, контролни лампи, цифрови и аналогови входове и изходи и куплунзи.

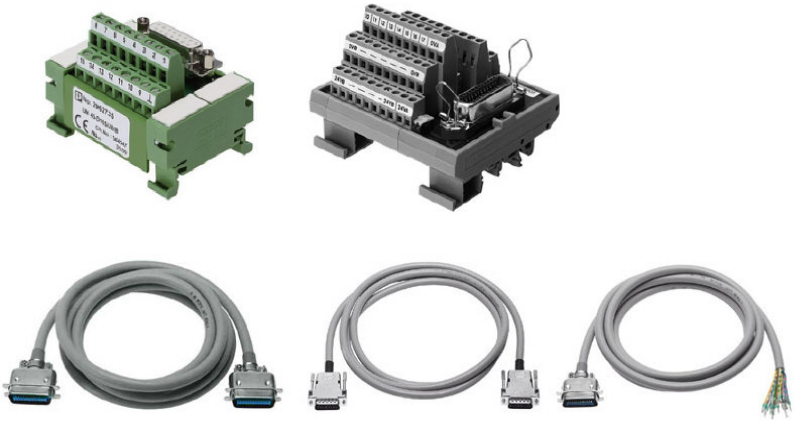
Всички входове, изходи, бутони, лампи и селектори са изведени на панела с букси тип „банана“ 2 mm. С помощта на тестови кабели, завършващи с „банана“ щекери, могат да се свързват различни тестови варианти. Това дава голяма свобода на реализираните тестови схеми и постановки. Чрез куплунзи тип „EasyPort“ и „SysLink“, могат да се свързват външни тестови макетни постановки и др. Системата няма интегриран електрически клеморед за директно свързване на проводници към външни бутони, селектори и други устройства. Но има възможност, чрез предлагани от производителя аксесоари - Фиг.8, да се присъединят клемореди за аналогови и цифрови сигнали. Друга възможност е, чрез направата на преходник от „банана“ букса 2 mm към клеморед. При този вариант се създава неудобство и объркване от струпването и оплитането на много едножилни проводници.

Фиг.7 Обучаващо куфарче FESTO със система на производителя Rockwell Automation.

Постановката има много добри вградени устройства за входни сигнали и добри вградени устройства за изходните сигнали. PLC и HMI хардуерът има значителни възможности, които могат сравнително добре да се използват с вградените устройства. Много добро, дори отлично използване може да се получи, чрез свързване на външни макетни устройства с куплунзи или с използване на преходниците, предлагани от производителя за свързване чрез клеморед на външни сигнали и устройства. Системата е гъвкаво направена за използване с вградените си устройства, с външни устройства или използване едновременно с външни и вътрешни устройства.

Свързване към мрежово захранване 230 V се осъществява със стандартен кабел IEC C13/C14 и ключ за „вкл.“ и „изкл.“.

В сайта на FESTO има посочени какви обучения се организират с тази система.



Фиг.8. Аксесоари за интегриране към обучаващата система.

Обучителната постановка съдържа следните хардуерни елементи:

1. Програмируем логически контролер CompactLogix 5370 controller (1769-L24ER-QBFC1B) – захранване 24 VDC, 16 бр. цифрови входове 24 VDC, 16 бр. цифрови транзисторни изходи., 4 бр. аналогови входове, 2 бр. аналогови изходи, 4 бр. висококоростни броячи, 1бр. Етернет порт и поддръжка на SD карта памет.
2. Селектори - 4 бр.
3. Бутони с контакти НЗ - 2 бр.
4. Бутони с контакти НО – 2 бр.
5. Контролни лампи – 8 бр.
6. Потенциометри за регулиране на аналогов сигнал– 2 бр.

7. Операторски дисплей - PanelView Plus 7
8. Мрежови комутатор Stratix 2000 – портове 5 бр. RJ45
9. Размери (W × H × D) 475x625x290 mm.
10. Тегло не е посочено.

Табл.1

СРАВНИТЕЛНА ТАБЛИЦА НА ПРЕНОСИМИ СИСТЕМИ ЗА ТЕХНОЛОГИЧЕН КОНТРОЛ И УПРАВЛЕНИЕ.					
Позиция	Параметър	GOTT SDN BHD – Малайзия „GOTT-PLCP-05“	ABB „TA 515“	SIEMENS „SIMATIC S7 Training Case S7-1200“	FESTO Rockwell Automation „Advanced PLC Training“
1	Сензорен дисплей 4.0”, 256 цвята, 320x240pix, USB порт и Етернет базирана комуникация.	Няма информация	ДА	ДА	ДА
2	Бутони – 2 бр.	НЕ	НЕ	НЕ	ДА
4	Селектори – 2 бр.	ДА	ДА	ДА	ДА
5	Контролни лампи – 2 бр.	ДА	НЕ	ДА	ДА
6	Потенциометър с контролен аналогов сигнал – 1бр.	НЕ	ДА	ДА	ДА
8	PLC контролер, цифрови входове 6 бр., цифрови изходи 4 бр., аналогови входове 1 бр., аналогови изходи 1 бр., добавяне/наличен порт RS232+RS485, слот за карта памет и етернет базирана комуникация.	ДА	ДА	ДА	ДА
9	Мрежови комутатор 100 Mbit/s, портове 4 бр.	НЕ	НЕ	ДА	ДА
10	Изведено захранване за свързване на външни устройства към 24 VDC.	ДА	НЕ	ДА	ДА
11	Възможност за добавяне / свързване на устройства към входовете и изходите с клеморед или букси.	ДА	НЕ	НЕ	ДА
16	Системата да е от един модул с размери макс. ДхШхВ (mm) 500x350x250	ДА	НЕ	ДА	ДА
17	Тегло до 12 кг с куфара.	Няма информация	ДА	ДА	Няма информация

3. Заключение

В Табл.1 са посочени минимални изисквания към една преносими система за извършване на тестове и обучения. От нея може да се направи извод, че

системата с най-добри параметри се предлага от фирмата FESTO с основни компоненти на производителя Rockwell Automation. Разгледаната постановка се предлага също във вариант с основни компоненти на производителя SIEMENS. По този начин, желаещите да се снабдят с преносима постановка имат възможност да избират от двата световни производителя на апаратура за автоматизация. FESTO предлагат и други обучаващи системи в областта на пневматиката, енергетиката, електрониката и др.

От направения анализ може да се почерпи информация кой предлага преносими системи за индустриален контрол и управление и какви възможности имат моделите на различните производители. Тъй като информация за тях е оскъдна, имат малка популярност.

С тази статия се цели да се предостави повече информация за преносимите системи за индустриален контрол и управление, която би била полезна за малки и средни предприятия, стартиращи фирми в областта на автоматизацията и университети.

ЛИТЕРАТУРА

[1] GOTT MECHATRONICS - PLC trainer Siemens s7 1200 with HMI touch screen, Model Number : GOTT-PLCP-05.

[2] SIEMENS S7-1200 Programmable controller, System Manual - Document ID: A5E02486680-AO, V4.5 05/2021.

[3] ABB Installation instruction TA515-CASE and TA5450-CASE, Document ID: 3ADR010438

[4] ABB System Settings for Training Cases TA515, TA5450 - Document ID: 3ADR010440

[5] ABB Processor module data sheet: PM572, PM573, PM582, PM583, PM585, PM590, PM591, PM592 - Document ID: 3ADR010064

[6] Siemens SITRAIN Training Cases · 03/2021

[7] SIEMENS HMI devices Basic Panels 2nd Generation 05/2021 - Document ID: A5E33293231-AD

[8] SIEMENS S7-1200 Easy Book 01/2015, Manual - Document ID: A5E02486774-AG

[9] Festo Didactic LabVolt Series, Advanced PLC Training System (Rockwell Automation) 588969 (3355-00)

[10] Festo Didactic: LabVolt Series Training Systems, A whole new range of possibilities

[11] Allen-Bradley CompactLogix 5370 Controllers, User Manual - Publication 1769-UM021I-EN-P - May 2018

[12] Allen-Bradley PanelView Plus 7 Operator Interfaces Publication 2711P-PP013I-EN-P - August 2019

ИСТОРИЧЕСКО РАЗВИТИЕ НА ФОТОГРАМЕТРИЯТА В БЪЛГАРИЯ

Найлян М. Салиева

THE HISTORICAL DEVELOPMENT OF PHOTOGRAMMETRY IN BULGARIA

Naylyan M. Salieva

ABSTRACT: *Bulgaria was the first country on the Balkan Peninsula to start applying photogrammetry. Photogrammetry has a wide application which allows not only optimization of time and financial costs, but also a unique approach in making decisions that otherwise would be difficult or impossible with any other means. This report will discuss the historical development of photogrammetry in Bulgaria. In the recent past, about 20 institutes, enterprises and professional services have developed and applied photogrammetry in various fields.*

KEYWORDS: *Photogrammetry, Development, Plan, Map*

1. Въведение.

България е първата страна на Балканския полуостров, която започва да прилага фотограметрията – научна дисциплина с широко приложение в редица сфери и позволяваща не само да се оптимизират времевите и финансови разходи, а и да се намери подход към задачи, решението на които с други средства е затруднено или невъзможно. В близкото минало около двадесет института, предприятия и служби са развивали и прилагали фотограметрията в различни области, като са изработвани различни по характер и предназначение обекти, включително задгранични [5].

2. Изложение.

2.1. Същност на фотограметрията.

Думата „фотограметрия“ произхожда от гръцките думи photos – светлина, gramma – запис и metreo – измерване, означаваща – измерване на записи, направени със светлина т.е. измерване на фотоснимки. С други думи възникването и развитието на фотограметрията е тясно свързано с развитието на фотографията, която е едновременно теория, техника и метод за получаване, съхранение и изучаване на изображения и за развитието на приборите за техните измервания. Фотограметрята е научна дисциплина, която се занимава с определяне на размерите, формата, положението и други количествени и качествени характеристики на различни обекти по техните фотографски изображения т.е. изградена е върху геометричните отношения между предметите в пространството и техните фотоснимки. Тя дава теоретичните закони и методи

за изучаване на различни обекти и явления, които са пълно и геометрически вярно изобразени на фотоснимки. Предмет на фотограметрията се явяват такива научни направления като теория на проекциите в частност централната проекция, разпознаване на образи т. н. дешифриране на аерофотоснимките, измерване на координати, теория на обработката на измерванията по фотоснимки и др. Тя намира широко приложение при: създаването на планове и карти в различни мащаби; строителството на метро, пътища, тяхната рехабилитация; архитектурата; археологията; селско, горско стопанство; медицина; криминалистика; космически проучвания, прогнози; астрономия; океанология; за сгъстяване на съществуващата опорна мрежа; за изследване на деформации на сгради и съоръжения и др. [1], [2].

2.2. История на възникването на фотограметрията.

За начало на фотограметрията се приема 1858 г., когато френският офицер Еме Лоседа конструирал въздушна камера и прави първите перспективни снимки на гр. Париж. Първоначално фотограметрията се развива като мензулна снимка чрез засечки и е наричана „метреофотография". През 1876 г. австрийският проф. Йордан дава названието „фотограметрия" [5]. Всъщност фотограметрията възниква едновременно с раждането на фотографията, когато на заседание на Парижката академия на науките и Академията на изящните изкуства е направено съобщение за изобретяването на способ от парижкия художник Луи Жак Манде Дагер за получаване на фиксирано изображение върху слой халогенно сребро, и преминава през няколко етапа на развитие:

- начален етап до края на 1900 г.;

През този период Еме Лоседа пръв изработва план от фотографски снимки, а парижкият фотограф Феликс Тураншон известен под псевдонима Надар първи в света предложил да се използва за тази цел въздушно фотографиране. Фотограметрията се развива бързо през XX век, когато са създадени методики и технически средства за обработка на фотографски снимки и получаването на топографски оригинали. Първият уред за измерване на снимки, наречен стереокомпаратор, е създаден през 1901 г. и дава силен тласък в развитието на стерофотограметрията и аналоговата фотограметрия.

- втори етап обхваща периода до 60-те години на XX век – характеризира се с развитието и масовото прилагане на методите на аерофототопографската снимка, като се използват специални фотограметрически прибори;
- трети етап от началото на 60-те до средата на 80-те години на XX век – характеризира се с развитието и масовото навлизане на аналитичните методи във фотограметрията;
- съвременно състояние[5].

В днешно време се извършва постепенен преход от методите на класическото аерофотографиране към методите на дигитално аерофотографиране, прилагат се цифрови методи за обработка на материалите от наземно, аеро и космическо фотографиране. В условията на невиждан досега в човешката история научно-технически прогрес, фотограметрията се развива, обогатява и усъвършенства непрестанно.

2.3. Историческо развитие на фотограметрията в България.

Фотограметрията се използва за първи път в България през 1908 г., когато край с. Студена, недалеч от гр. София, са направени земни фотограметрични

снимки, които са картирани във Виенския картографски институт от Едуард Фон Орел посредством създадения от него стереокартировъчен апарат Stereautograph. Част от резултатите от тези фотограметрични измервания със снимките на заснетите местности са публикувани през 1920 г. и 1923 г. [4].

През 1912 г. под ръководството на Едуард фон Орел от Виенския военно-картографски институт се извършват полски фотограметрични замервания на водосборния басейн на река Струма с площ от 100 km^2. Изработени са топографска карта в мащаб 1:20000 и топографски план в мащаб 1:2000.

До Балканската война у нас е направен още един опит за фотограметрично снимане, фотоматериалите от който са неизвестни [3].

По време на Балканската война се правят аерофотоснимки за разузнавателни цели, както и снимки от балон, в резултат на което се започва изработване на регулационни планове за настаняване на бежанците от Беломорска Тракия и Южна Македония.

През Първата световна война (в периода 1914 г. - 1918 г.) са извършени земни стереофотограметрични снимки по билото на Беласица планина за откриване укрепените позиции на противниковите войски от южния фронт и за проучване на бойните действия. По същото време е направено заснемане и между градовете Скопие и Битоля за построяване на железопътна линия. България е първата страна на Балканския полуостров, която прилага стереофотограметрията за топографски цели [3].

Непосредствено след Първата световна война в Географския институт (ГИ) се поставя въпросът за прилагане на земната и особено за въздушната фотограметрия, която се е наричала „Аерофотограметрия“ или „Аерогеодетика“ [4]. У нас по това време се извършват няколко земни фотограметрични снимки в Родопите и около гр. София, но резултатите не са известни. По-съществен опит за внедряване на земната фотограметрия за топографски цели е направен през септември, 1928 г. от Е. Бертхолд и проф. Асен Райков на един обект в района на гр. Банкя (до гр. София). С новоконструирания фототеодолит Wild се заснема площ от около 2,5 km^2, чието картиране в мащаб 1:10000 е осъществено във фабрика Wild Heerburg с новосъздадения стереокартировъчен апарат за земни снимки Autograph A-2. След установяване на безспорните предимства на фотограметрията като снимачен метод пред класическите методи за геодезична снимка, тя намира приложение при съставяне на картата на страната в мащаб 1:25000, извършено от ГИ при Министерството на войната [3].

През 1929 г. е създадено фотограметричното отделение към ГИ и за началник е назначен Гроздан Грозданов. Тогава започват задълбочени проучвания и изследвания за прилагането на фотограметричните методи в практиката. Към този момент ГИ разполага със стар модел фототеодолит „Цайс“ с фокусно разстояние 196 mm и формат 13x18 cm и са доставени още два стереоскопа и ръчна аерофотокамера Wild с фокусно разстояние 165 mm, работеща със стъклени плаки. През следващата година са осигурени още три фототеодолита Wild с по две фотокамери (фокусни разстояние 165 mm и 240 mm, формат 10x15 cm) и фототрансформатор Hugershoff-Heide, така че едновременно с приложението на земната фотограметрия започва и снимането на равнинните райони чрез въздушна фотограметрия. Извършват се пробни фотограметрически снимки, предназначени за създаване на топографска карта в мащаб 1:25000, както и пробно аерофотоснимане на площ от 50 km^2 около с. Божурище край (гр.

София). Аерофотоснимането с ръчната камера Wild е направено от височина над местността 1500 m и 2500 m, като за кадрите са използвани стъклени фотоплаки на различни фирми. Тогава всъщност е извършено първото аерофотозаснемане и започва внедряването на земно-фотограметричния и въздушно-фотограметричния метод [4].

През този период се организира първата у нас Топографска школа за подготовка на български фотограметристи и се започва подготовката на кадри за топографско и фотограметрично снимане и картографска обработка. Инженерите Васил Пеевски, Гроздан Грозданов и Асен Райков от Държавен географски институт (ГИ по това време е преименуван в Държавен географски институт) съставят първото българско ръководство „Курс по фотограметрия“ и изработват първата „Инструкцкия за земното фотограметрично снимане“, а Гроздан Грозданов е първият българин, участвал в мероприятие на Международното дружество по фотограметрия – ISP (сега ISPRS) – III Конгрес в гр. Цюрих [4].

През 1931 г. Държавния географски институт (ДГИ) извършва аерофотоснимане с ръчната аерокамера Wild от височина 3350 m - 3400 m (мащаб на фотоснимките 1:20000 – 1:21000) на район между гр. Пловдив, гр. Асеновград и с. Кричим с площ около 650 km^2. Използвани са не особено подходящи самолети двуплощници „Дар III” и “Фоке-Вулф“ при 30% надлъжно и напречно препокриване между съседните аероснимки. Тогава ДГИ разполага и със стереокартировъчен апарат Autograph A-2 (Wild) за картиране на земни стреореснимки и се пристъпва към осъществяване на една от основните цели – създаване на нова топографска карта на България.

Четири години по-късно столичната община възлага на ГИ (ДГИ се преименува отново в ГИ) изработването на топографски план в мащаб 1:10000 на гр. София и околностите. Приложена е аерофотограметрия с фототрансформиране, като впоследствие планът е увеличен в мащаб 1:5000 и е послужил за изработване на градоустройствен план на гр. София от германския професор Адолф Мусман [4]. През този начален период за 2471 дни от 2171 земни фотограметрични станции са заснети 13270 km или по 5,4 km на ден, а с ръчната аерофотокамера Wild с 3478 аерофотоснимки за 1577 дни от средна височина над местността 3300 m (среден мащаб на фотоснимките 1:20000) са заснети 7106 km или по 2 km на снимка.

След завършване на Втората световна война у нас се поставя начало на усилена строителна и стопанска дейност за изработване карта в мащаб 1:25000, като се започва редовната въздушна фотограметрична снимка (аерофотозаснемане) на страната. За изработване на топографската карта в мащаб 1:25000 се утвърждава аерофотограметрията. За целта за ГИ са доставени стереокартировъчните апарати Multiplex, Stereoplanigraph C-5, Autograph A-5 (Wild), фототрансформатор SEG-I и аерофотокамера RMK (Zeiss). Методите постоянно се усъвършенстват, като постепенно стереофотограметрията измества останалите методи. Картирането става с автографа Wild. Заснета е площ от 111000 km^2, от които 20% с мензулна снимка, 17% земно-фотограметрична, 37% - контурно-комбинирана и 26% стереофотограметрия. Едновременно с изработването на картните листи в мащаб 1:25000 на тяхна основа се извършва и съставяне на картите в мащаби 1:50000, 1:100000, 1:200000 и по-дребни. Тази задача се решава в срок, единствено като се използва високоефективният фотограметричен метод.

През 1942 г. е създадено първото Висше техническо училище в София, а през 1943 г. е основана катедра "Фотограметрия и топография", която по-късно е преименувана в катедра "Фотограметрия и картография". През 1945 г. Висшето техническо училище прераства в Държавна политехника, където е създадена катедра „Фотограметрия, топография и кадастър" (сега „Фотограметрия и картография" към УАСГ) с ръководител проф. инж. Асен Райков – професор по фотограметрия от основаването на Висшето техническо училище и публикува първия у нас учебник „Фотограметрия" [4].

Периодът 1919 г. - 1944 г. се характеризира с прилагането на фотограметрията за изработване на топографски карти на страната в М 1:25000 и снимки на населените места в едри мащаби.

Първото внедряване на еднообразната фотограметрия у нас започва при създаване на планове на населени места и план в мащаб 1:2000 на напоителното поле на изграждащия се по това време язовир „Ал. Стамболийски". Последват поредица от обекти, извършени по фотограметричен начин, както и организационнотехнически промени за широкото внедряване на фотограметрията в практиката. На първо място по подобие на СССР, през 1951 г. политбюро на Централен комитет на Българската комунистическа партия взема Решение № 176 за създаване на Главно управление по геодезия и картография (ГУГК) при Министерския съвет по приложен доклад от подпредседателя на Министерския съвет генерал-полковник Иван Михайлов. Управлението работи в състав от 75 души, с основно предназначение формиране и осъществяване на държавната политика в областта на геодезията, фотограметрията и картографията, извън приложението им за военни нужди. Правят се първи опити за пространствена фототриангулация във Военно-топографската служба (създава се през 1950 г. като наследник на ДГИ) [4].

През 1953 г. Министерският съвет приема Постановление П-653 за преустройство на ГУГК: „… да се създадат към Главно управление по геодезия и картография от 1 януари 1954 г. проектантски организации „Геопланпроект" в гр. София с клонове в провинцията, броят на които да се определя ежегодишно с бюджета и проектантска организация „Картпроект" в гр. София…". Създадената организация „Геопланпроект" започва работа по подготовка за изработването на Едромащабна топографска карта на страната (ЕТК) в М 1:5000 и М 1:10000. ГУГК насочва проектантската организация към прилагане на стереофотограметрията. Към „Геопланпроект" е създаден отдел „Фотограметрия" с основно предназначение изработване на ЕТК и кадастрални планове на населени места, както и друга фотограметрична продукция. Процесът е трудоемък и дълъг, изисква подходящите консумативи и техника, усвояване на технологичните пътища и производството на междинни материали. Отделът постепенно е снабден с необходимата апаратура (стереокартировъчни апарати, фототрансформатор, ортофотосистеми, стереокомпаратори, маркиращи апарати, плотер, фотолабораторна апаратура и др. спомагателни прибори). Така започва действителната работа по ЕТК. Тъй като в началото няма достатъчно аерофотозаснемания, използват се наличните геодезически снимки и планове, прилагат се тахиметричен, мензулен и контурно-комбиниран метод (ситуацията с еднообразна фотограметрия, релефа с мензулна снимка). Първите аерофотофилми се предоставят от Военно-топографската служба (ВТС) – десет на брой. С всяка следваща година броят на аерофотофилмите, обработвани от

„Геопланпроект“, отдел „Фотограметрия“, се увеличава и постепенно фотограметричният метод за създаване на ЕТК става основен. Едромащабната топографска карта се състои от около 16717 картни листове, от които 88% са в мащаб 1:5000 и 12% за планинските райони в М 1:10000. Завършени са оригиналите на топографската карта в мащаб 1:25000 от около 1400 картни листове [4].

През 1954 г. за „Геопланпроект“ е доставен универсален стереокартировъчен апарат Stereoplanigraph C-8 (Zeiss-Oberkochen), с което се създават условия за прилагане на въздушната стереофотограметрия за граждански цели.

Изработването на ЕТК чрез способите на фотограметрията става основна цел и тази дейност се развива все повече с всяка следваща година, заедно с развитието на стопанските дейности в държавата, като през 1955 г. за създаването ѝ е въведена въздушната стереофотограметрия [4]. Малко по-късно „Геопланпроект“ доставя от СССР шест топографски и един прецизен стереометър „Дробышев“, с което започва прилагане на диференцирания стереофотограметричен метод, но същият се ползва до 1961 г., поради неговата неефективност за едромащабно картиране на планински и полупланински райони. При обновяване на топографски карти в мащаб 1:25000 и 1:10000 започва да се прилага аеротриангулация.

През 1973 г. е основан Национален комитет за изследване и използване на космическото пространство. През същата година към Националния институт за паметниците на културата е създаден отдел „Фотограметрия“ с ръководител инж. Георги Хаджиев. Отделът е снабден с необходимата снимачна и обработваща фотограметрична апаратура и прилага близкообхватна земна фотограметрия за заснемане на археологически и архитектурни обекти с цел тяхното консервиране и реставриране. Първите приложения у нас на фотограметрия за архитектурни цели са през 1956 г., когато Милан Миланов, дипломант на катедра „Фотограметрия и картография“ към сегашния УАСГ, извършва земна фотограметрична снимка на южната фасада на храм-паметника „Св. Александър Невски“ с фототеодолит Wild и изработва едромащабен план на фасадата и детайлите с Autograph A-6 (Wild).

Към Научноизследователския и проектоконструкторски „Нипроруда“ (сега „Нипроруда“ АД) през 1975 г. също е създадена лаборатория по фотограметрия и дистанционни изследвания, като предназначението ѝ е да извършва земни и въздушни заснемания. Обзаведена е със снимачна и измерителна апаратура за земна фотограметрия, както и за обработка на многозонални и мултиспектрални земни, въздушни и космически снимки. Тогава е създадена технология за извършване на многозонални земни стереоснимки. В продължение на 12 години пролет и есен посредством земна, в комбинация с въздушна, фотограметрия се заснема 10% от Черноморската крайбрежна ивица за количествено и качествено определяне на видовете скали, клифа, абразия, ерозия, свлачищни процеси. С многозонални снимки е определено плитководието до 10 m дълбочина. Също така се създава технология за обработване на многозонални снимки, с която са разпознати видовете руда в открити рудници. През същия период Научноизследователски институт по геодезия и фотограметрия доставя ортофотосистема Topocart-Orthophot (Zeiss Jena) и се започва изработването на ортофотопланове, а малко по-късно ВТС

разработва и внедрява пространствена аналитична фототриангулация от космически снимки [4].

През 1991 г. във Фирмата за научни изследвания и технологии „Геодезия и фотограметрия“ е завършена „Технология и програмно осигуряване за аерофотограметрично заснемане на рудниците в СО „Марица изток“ с ръководител ст.н.с. д-р инж. Иван Кацарски, а седем години по-късно и задачата за специализиран дигитален кадастър на свлачищата Кабакум и Панорама в курортните комплекси „Чайка“ и „Златни пясъци“ с прилагане на геодезически и фотограметрични измервания. При численото стереокартиране са регистрирани триизмерни изображения на обектите. От фотограметричните дигитални модели на терена са изработени карти на векторите и изолиниите, както и триизмерни изображения на хоризонталните и вертикалните свличания на земните маси. Малко по-късно е приключена и темата „Експериментално изработване на кадастрални планове на населени места в цифров вид въз основа на геодезически и фотограметрични измервания. Сравнение на резултатите“, като е доказано предимството на фотограметрията. През този период е доставена и дигиталната фотограметрична работна станция ERDAS IMAGINE на ERDAS Inc за Централната военнокартографска база на Министерство на отбраната. Това е първата подобна система в страната, предназначена за производство [4].

Общинската фирма „Географска информационна система (ГИС) – София“ ЕООД започва проучване за внедряване на дигиталната фотограметрия за кадастър на населени места през 2001 г., като осъществява едногодишно теоретично и практическо обучение по фотограметрия на нейни специалисти, създава два експериментални обекта на територията на гр. София, изпраща специалисти в чужбина за обучение и участие в международни мероприятия, получава временни лицензи за работа с няколко дигитални фотограметрични работни станции на различни фирми. Също така организира едногодишен теоретичен и практически курс „Основи на фотограметрията“, обхващащ 15 раздела, за специалистите в новосъздадения отдел „Фотограметрия“ с лектор консултанта по фотограметрия ст.н.с. д-р инж. Иван Кацарски. През същата година португалската фирма Estereofoto предоставя на „Геопланпроект“ за ползване дигиталната фотограметрична работна станция DiAP NT на ISM International System Corp., с която започва изпълнение на обекти от чуждестранни инвеститори, а Институтът за космически изследвания към Българска академия на науките (БАН) доставя дигиталната фотограметрична работна станция Geomatica OrthoEngine на PCI Geomatics. Малко по-късно „ГИС – София“ ЕООД доставя дигиталната фотограметрична работна станция PHOTOMOD (Racurs Co.) – първата подобна система, собственост на българско стопанско производствено предприятие, и закупува от Eurimage S. p. A. (Италия), дистрибутор на DigitalGlobe за Европа, спътникова снимка на гр. София, която покрива площ 272 km^2. В резултат на това крайните продукти са дигитален ортофотоплан на централната част на гр. София и обновени 9 листа от ЕТК (1:5000) с обща площ 56,25 km^2 [4].

През 2004 г. орторектифицирана е цялата спътникова снимка на гр. София. ESRI България ООД закупува от SPACE IMAGING спътниковата снимка, която е направена на 18.10.2002 г. и покрива площ 100 km^2. Избран е продуктът GEO (PAN 1m + MSI 4m) от архива на спътника IKONOS. Снимката е орторектифицирана с програмата ERDAS IMAGINE 8.6. Използвани са 9 опорни

точки, определени с GPS от Централната лаборатория по висша геодезия – БАН, както и дигитален модел на релефа с размер на клетките 5 m, създаден въз основа на ЕТК в мащаб 1:5000. Получена е ситуационна точност по-добра от ±0,6 m. Чрез обединяване на панхроматичното с мултиспектралното изображение е изработено цветно (RGB) изображение с размер на пиксела върху терена 1 m. Ортофоректифицираната спътникова снимка в мащаб 1:5000 е оформена по картни листове с размери 50x50 cm. Точността на дигиталния оротофотоплан отговаря на продукта IKONOS PRE+, т.е. средната квадратна грешка е ±1 m. По същото време „ГИС – София“ ЕООД закупува от Space Imaging серия от снимки (3 панхроматични и 3 цветни), покриващи част от Природен парк „Витоша“. Снимките са направени по различно време, като крайните продукти са 2 мозайки (панхроматична и цветна) от ортоизображения с площ 220 km^2 и дигитализирани всички сгради в района на Витоша [4].

През 2005 г. – 2006 г. „ЕВРОСЕНС“ ЕООД – България изработва цветна ортофотокарта в мащаб 1:5000 на гр. Пазарджик от спътникови снимки Ikonos от 2004 г., както и в мащаб 1:1000 на централната градска част от аерофотоснимки в мащаб 1:4500. „ЕВРОСЕНС“ ЕООД – България е учредено през 2003 г. от белгийската корпоративна група ЕВРОСЕНС, която повече от 45 години развива успешна дейност в областта на дистанционните изследвания на Земята, картографията, фотограметрията, ГИС, въздушното лазерно сканиране и батиметрията в редица европейски страни – Белгия, Франция, Холандия, Германия, Полша, Чехия. Словакия, Унгария, Румъния и България. Малко по-късно Министерство на земеделието и горите възлага на „ЕВРОСЕНС“ ЕООД – България изработването на цветна дигитална оротофотокарта в мащаб 1:5000 от ареофотоснимки в мащаб 1:25000 с разделителна способност 50 cm на територията на страната за идентифициране на земеделските парцели. До началото на 2006 г. са аерозаснети 80% от земеделските земи. През същия период „ГИС – София“ ЕООД възлага на Hans Luftbild GmbH извършване на аерофотоснимане в мащаб 1:4500 на два обекта на територията на София – Витошка яка и Балкан с площ 57,6 и 11,4 km^2. Заснемането е извършено с аерофотокамера RMK TOP 30/23 (Z/I Imaging) и предназначено е за изработване на ортофотоплан в мащаб 1:1000 [4].

През 2011 г. е обнародвана и влиза в сила Наредба № РД-02-20-16 за планирането, изпълнението, контролирането и приемането на аерозаснемане и на резултатите от различни дистанционни методи за сканиране и интерпретиране на земната повърхност.

През 2017 г. се подписва договор № ГД-1-1 между сдружение Български антарктически институт и Агенцията по геодезия, картография и кадастър (АГКК) за геодезически и картографски дейности и научни изследвания за района на Българската антарктическа база (БАБ) на остров Ливингстън. АГКК е един от спонсорите на 25-та антарктическата експедиция. Едни от основните цели на експедицията са: разширяване на картографираните територии и разпространение и поддържане на Международната земна координатна система (ITRS) на територията на о-в Ливингстън. В изпълнение на договора и в съответствие с основните цели на експедицията е извършено полево обследване на стабилизираните по време на 24-та експедиция геодезически знаци; проведени са геодезически ГННС измервания на основната геодезическа точка KOH2. В обработката на измерванията са включени перманентни станции, работещи в

Антарктида и Южна Америка. Преизчислени са координатите на точките от съществуващата в района на БАБ геодезическа мрежа. Извършено е геодезическо и въздушно фотограметрично заснемане. Крайният резултат е качествена и подробна цифрова едромащабна карта, в мащаб 1:2000, с наименование „Българска антарктическа база“ – първата българска от най-студения континент. В отчетния доклад четем: „Предвид успешното прилагане на метода за аерозаснемане с леки безпилотни летателни апарати за нуждите на едромащабно картографиране на ограничени територии и все още некартографираните зони на интереси за българските научни проекти е целесъобразно бъдещо развитие на проекта“ [4].

За развитието на въздушната фотограметрия спомага и множеството научни, научноизследователски и популярни статии на ентусиазираните фотограметристи в нашата страна. За 20 години броят на публикациите в областта на фотограметрията е над 600, много от които са отпечатани извън страната и намират място в теоретичното и практическото развитие на фотограметрията. У нас се разработват редица методи и технологии по едромащабното фотограметрично картиране, които добиват известност и в други страни. Земната фотограметрия също намира приложение в много области на народното стопанство. Непрекъснато нараства броят на фотограметристите — носители на техническия прогрес в геодезическите и специалните измервателни дейности [5].

3. Заключение

Фотограметрията и дистанционните методи винаги са били най-прогресивната част от нашата високо-технологична професия, която търпи все по-бързо развитие, особено в последните години с масовото навлизане в геодезическото производство на безпилотните летателни средства и дигиталните фотограметрични технологии. Те са вече необходимост при решаване на сложни пространствени задачи за картиране и изследване на различни територии от нашата планета. С поглед от голяма височина се добиват реални представи за действителното състояние на нещата върху цели континенти. Далечното снимане стана основа на множество нови науки. Фотограметрията намира място главно при съставяне на планове и карти, но се прилага с успех и за изследване на различни обекти и явления в областта на селското и горското стопанство, строителството, архитектурата, транспорта, хидравликата, металургията, геологията, медицината и др.

ЛИТЕРАТУРА

[1] Михайлов, Пл. & Петров, Д., 2014. *Съвременни технически средства и технологии за събиране на геопространствени данни за местността*, Шумен: Университетско издателство „Епископ Константин Преславски“. ISBN 978954577933

[2] Петров, Д., 2013. *Пособие по цифрова фотограметрия*, Шумен: Университетско издателство „Епископ Константин Преславски“. ISBN 978-954-577-677-9.

[3] Малджански, Пл., 2012. *Развитие на методите за заснемане и обработка на данни в архитектурната фотограметрия,* София: „ТЕС Дизайн“. ISBN 978-954-2994-02-2
[4] Пенкова-Барутчийска, П., 2020. *Геодезията, картографията и кадастърът в България*, София: Алианс Принт
[5] Кацарски, Ив., 2015. Фотограметрията – от корените до короната, *Геомедия*

МОДЕЛИРАНА СИГУРНОСТ В КОДИРАНЕТО НА КОМУНИКАЦИОННА МРЕЖА

Даниел Р. Денев

MODELED SECURITY IN COMMUNICATION NETWORK CODING

Daniel R. Denev

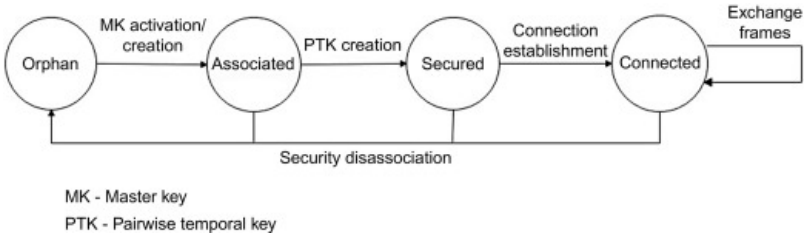
ABSTRACT: *When a network has relay nodes, there is a risk that some information will lead to an untrusted relay. Secure Network Coding (Secure NC) is known as a method to solve this problem, which allows message secrecy when the message is transmitted over a silent network and some of the edges or some of the intermediate (untrusted) nodes are eavesdropped. If the channels in the network are noisy, the error correction is applied to the noisy channels before applying the upper layer secure NC. In contrast, Secure Physical Layer Network Coding (secure PLNC) is a method for secure message transmission through a combination of node coding operations when the network is composed of a set of noisy channels. Since secure NC is an upper-layer protocol, secure PLNC can be considered an interlayer protocol. In this paper, we compare secure PLNC with a simple combination of secure NC and error correction in several typical network models.*

KEYWORDS: *Privacy Analysis, Secure communication, Unreliable relay, Network coding, Interlayer Protocol.*

Увод

Безжичните комуникационни мрежи с релейни възли крият риск от изтичане на информация към ненадеждни релета. За да разрешат този проблем, няколко проучвания [1] считат релейните терминали за ненадеждни въз основа на резултата от тестове за защитено изчисление, което е основната тема на защитеното мрежово кодиране на физически слой (PLNC). Въпреки това, този тип сигурност може да бъде реализиран чрез защитеното разширение на мрежовото кодиране (NC), накратко защитен NC е протокол от горен слой за сигурно предаване на съобщение чрез безшумна мрежа, когато част от междинните (недоверени) възли са подслушвани [2]. Тъй като безжичният канал е нарушен от шум, трябва да се приложи корекция на грешка към канала. След това защитеното NC се прилага към безшумни канали, виртуално реализирани чрез корекция на грешки. С други думи, корекцията на грешки и защитеното NC се извършват отделно в различните слоеве при горния сценарий. За разлика от това, тъй като защитеният PLNC съчетава и двете части, той може да се разглежда като междуслоен протокол. За да се изясни предимството на този междуслоен протокол, е необходимо да се сравни защитен PLNC с проста комбинация от

защитен NC и корекция на грешки през безжични канали, а това сравнение все още не е проучено. Тоест този тип сравнение е силно необходимо от гледна точка на безжичните комуникационни мрежи. Сигурният PLNC е базиран на PLNC [6], който ефективно предава модулната сума на съобщенията на два предавателя чрез канал на Гаус. За да се гарантира сигурността, предходните проучвания [7] изобретиха защитено разширение на PLNC, т.е. защитен PLNC, което е схема за сигурно предаване на съобщение чрез комбинация от кодиращи операции на възли, когато мрежата е дадена като набор от шумни канали. Сигурният PLNC може да бъде класифициран в два типа. В първия случай защитеният NC се прилага към безшумния CAF процес, реализиран от PLNC. Този метод може да се разглежда като проста комбинация от защитени NC и PLNC. Другият тип е директен метод за реализиране на сигурност в PLNC. Типичният пример е сигурният CAF. Кодът от последния тип не може да бъде направен чрез такава проста комбинация. Всички съществуващи проучвания [5] принадлежат към последния случай се отнасят само до релейна схема с два подскока или нейното просто разширение, схемата за много подскоци се основава на защитен CAF за сигурно предаване на модулната сума от две входни съобщения, когато каналът е шумен канал с множествен достъп (MAC). Наистина, сигурното NC може да гарантира секретността за подслушвателя, който подслушва каналите. Няколко типични сигурни NC не могат да гарантират секретността, когато един от междинните (ненадеждни) възли е подслушван. По този начин защитеният PLNC има предимство при атаки срещу междинни (ненадеждни) възли. Въпреки това мрежовите модели, изследвани в защитен NC, са по-напреднали и по-сложни и нито едно проучване не обсъжда защитен PLNC спрямо такива типични мрежови модели в защитен NC. Тоест мрежовите модели, изследвани в защитен PLNC, са твърде ограничени и твърде примитивни в сравнение с типичните мрежови модели в защитен NC. С други думи, нито едно предишно проучване не е изследвало приложението на защитен PLNC към такива типични мрежови модели. За да може защитеният PLNC да преодолее защитения NC, трябва да демонстрираме, че защитеният PLNC може да се използва в по-усъвършенствани мрежови модели. Най-малкото е необходимо да се изучава защитен PLNC върху типични мрежови модели в защитен NC. Тъй като нито един съществуващ документ не е направил сравнение между защитен PLNC и простата комбинация от защитен NC с корекция на грешки, този документ има за цел да направи този тип сравнение при типични мрежови модели в защитен NC. Това означава, че този документ е първото проучване за защитен PLNC върху типични мрежови модели в защитен NC, мрежовия модел на пеперудата и мрежовия модел, съставен от три изходни възела при определени предположения за атаката. За съжаление защитеният PLNC има напълно различна математическа структура от простата комбинация от защитен NC с корекция на грешки. Следователно е доста трудно да се изгради обща теория за тяхното сравняване. Поради тази причина разглеждаме два типични мрежови модела в областта на защитения NC, мрежата тип пеперуда [9] и мрежа с три изходни възела, която е специален мрежов модел, изследван в [4]. След това правим горното сравнение числено върху тези две мрежи. Наистина, много съществуващи проучвания [8] за сигурни PLNC използват решетъчни кодове.

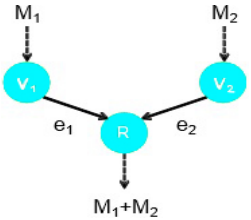


Фиг 1. *Сигурност в комуникационната мрежа*

CAF и защитен CAF

- *CAF*

Като първа стъпка преглеждаме съществуващите резултати за защитен CAF. За тази цел подготвяме важна бележка. Символът $\bigoplus$ изразява аритметичната сума върху крайно поле, а символът $\bigoplus$ означава сумата върху реалните числа. Типична настройка за защитен CAF има два предавателя, V_1 и V_2, и един приемник, R. Да предположим, че предавателят V_i има съобщение M_i 2 F_q, а приемникът R е свързан с (шумен) MAC, който има две входни променливи от двата предавателя V_1 и V_2. В тази схема се изисква приемникът R да получи модулната сума $M_1 \bigoplus M_2$ чрез (шумен) MAC, както е показано на фигура 2.



Фиг 2. *CAF (Изчисление напред)*

Много статии предлагат протокол CAF да преминава с Gaussian MAC. Да предположим, че предавателят Vi изпраща променливата с комплексна стойност X_i за $i = 1, 2$. Когато коефициентите на затихване на канала са дадени като h_1, h_2, приемникът R получава променливата с комплексна стойност Y като:

$$Y = h_1X_1 + h_2X_2 + N \quad (1)$$

където N е комплексна гаусова случайна променлива с нулева средна стойност и дисперсия от единица. Останалата част от този раздел предполага многократни употреби на горния MAC на Гаус. Референциите дават постижима скорост при енергийно ограничение чрез използване на решетъчни кодове. Тази скорост се нарича скорост на изчисление. Тук, за да търсим практическа схема, ние разглеждаме схемата BPSK, в която X_i е кодиран до $(-1)^{A_i}$ с $Ai \epsilon \phi_2$. Следователно (1) може да се пренапише като:

$$Y = h_1(-1)^{A_1} + h_2(-1)^{A_2} + N \quad (2)$$

- *ЗАЩИТЕН CAF*

След това разглеждаме условието за секретност за всяко съобщение до приемник R в допълнение към правилното декодиране. Тази настройка на

проблема се нарича защитен CAF. Тук се изисква получателят R да получи модулната сума $M_1 \oplus M_2$ докато променливата Y в ръката на получателя R трябва да бъде независима от M_1 и M_2. Референциите предлагат подход, използващ решетъчни кодове. Използвайки ефективно приложима алгебра за CAF, се предлага ефективно приложим код за защитен CAF. (Тук един код се нарича алгебричен код, когато картата на кодиране запазва алгебрична операция. Например кодовете на Рийд Соломон и LDPC кодовете са алгебрични кодове.) Той също така показа, че скоростта $2I(Y;\ A_1 \oplus A_2)Equation(1) - I(Y;\ A_1, A_2)Equation(2)$ Уравнение(2) е постижимо в схемата BPSK, където взаимната информация се дава с независими и еднакви произволни числа A_1 и A_2. Тоест, когато каналът (2) е подготвен и приемникът R влиза в тайно споразумение без предавател, защитеният CAF гарантира липса на изтичане на информация за всяко съобщение към приемник R, докато приемникът R може да възстанови сумата $M_1 \oplus M_2$. В кода $I(Y;\ A_1 \oplus A_2)Equation(2)$ е скоростта на CAF, а $I(Y;\ A_1, A_2)Equation(2) - I(Y;\ A_1 \oplus A_2)Equation(2)$ е скорост на жертвени битове за усилване на поверителността. Следователно, постижимата степен на защитен CAF е разликата между тези две скорости. Всъщност защитеният CAF се адресира само когато случаят е два за броя на предавателите. Адресирайте защитен CAF само когато броят на предавателите е по-голям от два. За съжаление, тези съществуващи проучвания не предлагат приложение за защитен CAF, освен за защитен двупосочен релеен канал с ненадеждни релета. Останалата част от този документ обсъжда по-нататъшното му приложение..

Конкретни изрази за взаимна информация

В този статия се използва взаимна информация $I(Y;\ A_1, A_2)Equation(2) - I(Y;\ A_1, A_2)Equation(2)$ когато $h_1 = h_2 = h$. Въпреки че конкретните им описания бяха представени в [10], ние даваме тези конкретни описания тук. Да приемем, че φ е разпределението на Гаус със средно α и α дисперсия от единица. Чрез използване на диференциалната ентропия H, взаимната информация $I(Y;\ A_1 \oplus\ A_2)Equation(2)$ се изчислява като::

$$H\left(\frac{\phi_0+2_{\phi_h}+\phi_{2_h}}{4}\right) - \frac{1}{2}H\left(\frac{\phi_0+\phi_{2_h}}{2}\right) - \frac{1}{2}H(\phi_h) \qquad (3)$$

когато $N \to \infty$, тази стойност отива на $\log 2$. В допълнение, взаимната информация I $I(Y;\ A_1 \oplus\ A_2)Equation(2)$ се изчислява като:

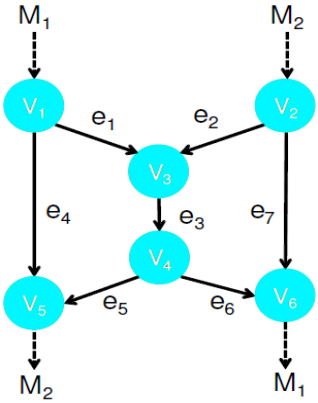
$$H\left(\frac{\phi_0+2_{\phi_h}+\phi_{2_h}}{4}\right) - H(\phi_h) \qquad (4)$$

когато $N \to \infty$, тази стойност отива до $\frac{2}{3}\log 2$

Мрежа пеперуда с конвенционален протокол

Типичен метод за NC е мрежата тип пеперудата, която ефективно предава информация по пътя на пресичане, както е обяснено на Фигура 3. Целта на тази настройка на проблема се състои от следните две изисквания: Едното е надеждното предаване на съобщение M1 от V_1 към V_6, а другият е надеждното предаване на съобщението M_2 от V_2 към V_5. Когато всеки канал предава само един елемент от F_q тясното място на тази мрежа ще е каналът E_3 от V_3 към V_4. Тук не се предава сигнал между прекъснати възли. Следователно не възниква кръстосано

обсъждане между несвързани възли. Въпреки това между E_5 и E_6 ако сигнала E_5 е различен от този на E_6. Следователно, ако те са различни, предаването на E_5 трябва да се извърши в различно време от предаването на E_6. Когато обаче са еднакви, тези предавания могат да се извършват едновременно. В този мрежов модел само възелът V_3 има свободата да избира предадената информация, тъй като другите възли получават само една информация, така че нямат друг избор за предадената информация, освен за предаване на получената информация. За да разреши затруднението в E_3, възелът V_3 предава модулната сума към възела V_4 чрез канал E_3. След това и двата целеви възела могат да възстановят съответните си предвидени съобщения, докато предаването на информация през E_3 се извършва само веднъж. Тоест целевият възел V_5 декодира съобщението M_2 от получената информация M_1 and $M_1 \oplus M_2$. По подобен начин другият целеви възел V_6 декодира съобщението M_1 от получената информация M_2 и $M_1 \oplus M_2$.



Фиг. 3. *NC тип Пеперуда*

Защитено NC

Възел V_3 получава и двете съобщения M_1 и M_2. Целевият възел V_5 възстановява нежеланото съобщение M_1, както и предвиденото съобщение M_2,, а другият целеви възел V_6 нежеланото съобщение M_2, както и предвиденото съобщение M_1. След това налагаме секретността срещу атака към един от междинните (ненадеждни) възли. С други думи, информацията на всички междинни (ненадеждни) възли трябва да бъде независима от M_1 и M_2., а информацията на целевия възел V_5 (V_6) трябва да бъде независима от нежеланото съобщение M_1 (M_2.). Този вид секретност може да бъде реализирана при следното предположение. Когато съобщенията M_1 и M_2 са елементи на F_q а q не е на степен 2 и е показана по следния начин (Фигура 3): Два изходни възела V_1 и V_2 споделят таен номер L, когато информацията Z_i t е предадена на ръба E_i и е дадена като:

$$Z_1 = 2M_1 \oplus L,\ Z_4 = -(M_1 \oplus L) \quad (5)$$

$$Z_2 = 2M_2 \oplus L,\ Z_7 = -(M_2 \oplus L) \quad (6)$$

$$Z_3 = Z_1 \oplus Z_2 = 2M_1 \oplus 2M_2 \oplus 2L) \quad (7)$$

$$Z_5 = Z_6 = Z_3/2 \quad (8)$$

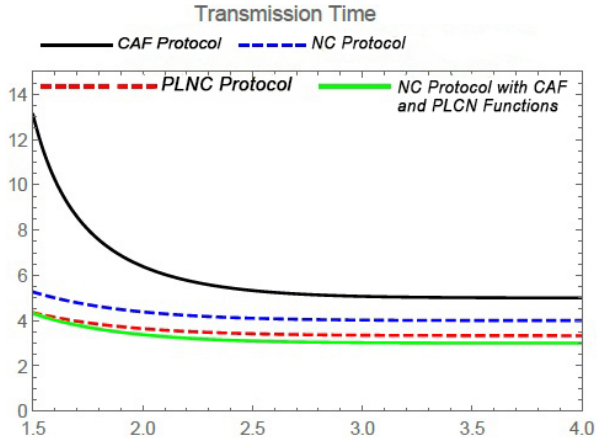
$$M_2 = Z_5 \oplus Z_4 \cong M_2,\ M_1 = Z_6 \oplus Z_7 \cong M_1 \quad (9)$$

Таблица 1 ще опише протоколите за сигурност и портовете.

Таблица 1. Описание на TLS/SSL на името на услугата и нейния мрежов порт

Service Name	smtp	https	nntps	ldaps	ftps- data	ftps	telnets	imaps	tftps
TCP Port	25	433	563	636	989	990	992	993	3713

Сигурният NC протокол за мрежова сигурност изисква по-кратко време за прехвърляне и за предаване от защитения PLNC протокол. Тъй като разликата не е толкова обширна, защитеният PLNC протокол е полезен, когато не е лесно да се подготви сигурна споделена произволност между два изходни възела. Всъщност, когато директната комуникация между два различни изходни възела не е налична, ние често използваме мрежата тип пеперуда. В този случай такава сигурна споделена произволност изисква допълнителни разходи. Сигурният PLNC обаче няма предимство пред защитения NC протокол с MAC канала. Тоест простата комбинация от защитени NC и PLNC не е полезна.



Фиг. 4. *Тест за време на предаване 1*

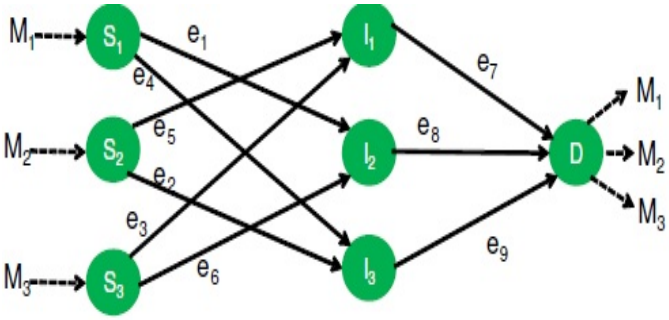
Графиката показва четири сигнала, всеки от които отговаря за защитен протокол. Този със зелен цвят е протоколът NC, който показва постоянна защита за целия период от време.

Мрежи с три изходни възела

В тази точка се изучава топологията на мрежата, показана на фигура 5, която е съставена от три изходни възела, S_1, S_2, и S_3; три междинни възела, I_1, I_2, и I_3; както и един дестинационен възел, D. Целта на този мрежов модел е сигурното предаване от трите изходни възела до целевия възел D, когато от изходния възел Si се изисква да изпрати елемент M_i и F_q до целевия възел D. Като първа стъпка нека се проучи мрежата с три източника в рамката на защитения NC.

На фигура 5 всеки ръб изразява безшумен канал за предаване на един елемент от F_q. Тук се разглеждат следните две изисквания за сигурност:

Когато се подслушва само един ръб сред три ръба (канала) между междинните възли и целевия възел, потребителя не получава информация за всяко съобщение. Когато се подслушва само един междинен (недоверен) възел измежду три междинни (недоверени) възела, потребителя не получава информация за всяко съобщение. Тук нито един възел не влиза в тайно споразумение с друг възел.



Фиг. 5. *Мрежа с три източника*

Следният код отговаря на изискванията за сигурност (първа подточка), когато q не е степен на 2. Този код използва 1/2, което не може да бъде разрешено в крайно поле F_q на степен 2 на q. Забележете, че матрицата $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ е обратима, защото

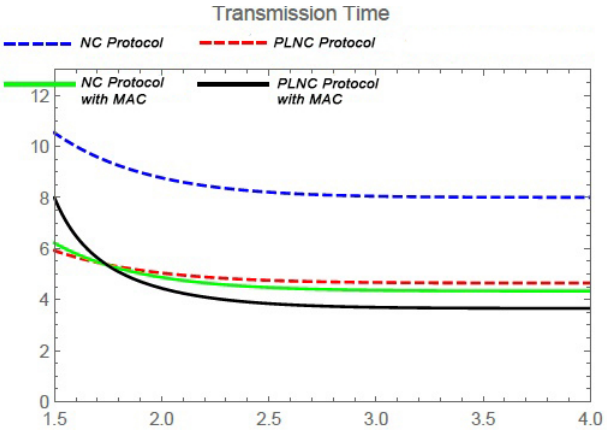
$\begin{pmatrix} -1/2 & 1/2 & 1/2 \\ 1/2 & -1/2 & 1/2 \\ 1/2 & 1/2 & -1/2 \end{pmatrix}$ е обратната матрица. Възлов източник S_i изпраща M_i във всеки ръб. Всеки междинен възел изпраща сумата от получения вектор. И накрая, се извършва прилагане на обратната матрица $\begin{pmatrix} -1/2 & 1/2 & 1/2 \\ 1/2 & -1/2 & 1/2 \\ 1/2 & 1/2 & -1/2 \end{pmatrix}$

Към получения вектор възелът D възстановява всички съобщения. В този код всяко от съобщенията $M_1 \oplus M_2$, $M_2 \oplus M_3$, и $M_3 \oplus M_1$ са независими от никоя стойност измежду M_1, M_2, и M_3. Следователно сигурността (първа подточка) е изпълнена. Този протокол постига оптимална скорост на предаване дори когато не е наложено условие за секретност.

Като следваща стъпка нека преминем към случая, когато q >4 и е на степен 2. Избрания елемент е $2F_q$ така че $e_3 \oplus e_1$ да е в сила и да предполага, че това $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & e \\ e & e & 0 \end{pmatrix}$ е обратимо, тъй като неговата детерминанта е $e_3 \oplus e_1$.

Кодовете за защитения PLNC протокол изискват по-кратко време за трансфер за предаване от защитения NC протокол. За сравнение, когато коефициентът h е по-голям от около 1,7, то тогава се показва по-сигурният. Това сравнение показва, че защитеният PLNC протокол има предимство пред

защитения NC протокол, когато мощността на сигнала е достатъчно голяма. В допълнение, това сравнение показва предимството на простата комбинация от защитен NC и PLNC пред защитения NC протокол, даден с MAC канала. С други думи, ако мощността на сигнала не е толкова голяма, защитеният NC протокол с MAC канала е по-добър от защитените PLNC протоколи



Фиг. 6. *Тест за време на предаване 2*

Заключение

Проучиха се предимствата на защитен PLNC пред защитен NC. За да се проучи този тип предимство, необходимо беше да се фокусира върху два типични мрежови модела. В разделите беше обсъден мрежовият модел на пеперуда, даден на фигура 3. Описаха се конкретни протоколи, които ефективно реализират необходимата секретност и работят върху тези мрежови модели. В тези примери защитеният PLNC може да реализира секретността дори с ненадеждни междинни възли. По-специално и по-общо мрежата тип пеперуда в сравнение с протоколите, използващи защитени мрежови кодове, изисква защитена споделена случайност, за тази цел, защитеният PLNC не се нуждае от нея. Сравнявайки времето за трансфер на предложените кодове, те показаха, че защитеният PLNC има по-кратко време за трансфер от простата комбинация от защитен NC и мрежа на физически слой. Като една от основните причини за тези предимства може да се посочи факта, че защитеният PLNC е многослоен мрежов протокол. Това означава, че може да се реализира чрез съвместно прилагане на корекцията на грешки и защитения NC чрез използване на механизма на физически слой, докато конвенционалният сценарий може да се разглежда като отделно приложение за коригирането на грешки и защитения NC. По-специално, шумът в каналите се използва за запазване на секретността в защитения PLNC. Следователно може да се заключи, че защитеният PLNC е полезен за реализиране на секретността срещу изтичане на информация в междинни (ненадеждни) възли

ЛИТЕРАТУРА

[1] Кульгин, М.С. Компьютерные сети. Практика построения, СПб, Санкт Петербург, 2007, pp.14-26.

[2] Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М. Технологии защиты информации в компьютерных сетях. Национальный Открытый Университет «ИНТУИТ», 2016

[3] Стоянова, Т., Милев, Ал., Обзор върху подобрените версии на LEACH. MATTEX 2016, Сборник научни трудове, том 1, Университетско издателство “Епископ Константин Преславски“, 2016, стр. 170-177, ISSN: 1314-3921.

[4] Стоянова, Т., Милев, Ал., Сравнителен анализ на алгоритми за рутиране в безжични сензорни мрежи. MATTEX 2012, Сборник научни трудове, том 2, Университетско издателство “Епископ Константин Преславски“, 2012, стр. 36-41, ISSN: 1314-3921.

[5] Стоянова, Т., Милев, Ал., Сигурност в безжичните сензорни мрежи. Международна научна конференция УНИТЕХ 2016 – Габрово, том II, Университетско издателство „Васил Априлов“ – Габрово, 2016, стр. 70-74, ISSN: 1313-230X.

[6] P. Baran et al., "On distributed communications, vols. I-XI. " RAND Corporation Research Documents. Aug. 1964.

[7] Boateng K., Asubamand B., Laar D., Improving the Effectiveness of the industrial networks, Kwame Nkrumah University of Science and Technology, Ghana.

[8] Krum R, Cool Infographics: Effective Communication for rapid responce with Data Visualization and Design; John Wiley & Sons: Hoboken, NJ, USA, 2013.

[9] R. A. Scantlebury, "A model for the local area of a data communication network -Objectives and hardware organization," ACM Symp. Data Communication, Pine Mountain, Oct. 1969.

[10] L. G. Roberts and B. D. Wessler, "Computer network development to achieve resource sharing," Proc. SJCC 1970. pp. 543-549.

[11] Fitigau I, Toderean G., Network performance evaluation for RIP, OSPF and EIGRP routing protocols, Proceedings of the International Conference on electronics, computers and artificial intelligence, ECAI-2013

ПРОУЧВАНЕ НА КАЧЕСТВОТО НА ДАННИТЕ ПРИ ЦИФРОВА ОБРАБОТКА НА АКУСТИЧНИ СИГНАЛИ

Даниел Р. Денев, Цветослав С. Цанков

A SURVEY OF DATA QUALITY IN DIGITAL* PROCESSING OF ACOUSTIC SIGNALS

Daniel R. Denev, Tsvetoslav S. Tsankov

ABSTRACT: *With development over time the features and quality of modern PC sound cards are increasing. New sound cards offer 24-bit quantization and higher sampling frequencies, which in some cases go up to 196 kHz. Every new sound card is compatible with professional DAW software which finds application for creating music, editing signals and it can be used as a measuring device. In music noise is one of the biggest problems which affects the dynamic range of a sound card, especially those in computer cases. It's shown that sound cards that are connected via a USB port rather than directly in the slot in a PC are slightly less affected by noise. The present scientific article is analysing and comparing two sound cards which are measured by the professional DAW software Studio One.*

KEYWORDS: *Digital processing, dynamic range, PreSonus.*

Въведение

Стандартите за аудио обработка и измерване на звуци и музикални сигнали се свеждат до основния въпрос: Кой DAW софтуер измерва звуковите карти по-правилно? Ако измерваме плейър с 16-битово квантуване, то DAW софтуера за измерване трябва да използва по-високо квантуване, например 24-битово или повече. Честотните диапазони на устройството, извършващо измерването, трябва винаги да са по-големи от тези на измерената стойност.

Настоящото изследване акцентира върху модерния и иновативен начин за измерване на звукови и музикални сигнали с помощта на DAW. Съвременният DAW софтуер и звукови карти отговарят на основните изисквания и следователно могат да се използват и като устройства и като измервателен инструмент. Например, по-голям проблем има при вградените звукови карти за компютър, където има много шум. Въпреки че се полагат големи усилия за намаляване на шума в корпусите на компютри, това все още е голям проблем. За да намалим шума в компютъра, трябва да намалим скоростта на голям брой вентилатори и

* Превод на статия, която е финансирана по Национална програма „Млади учени и постдокторанти – 2“, публикувана в IEEE Xplore, от участие в 2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES 2022), 24 – 26 November, 2022, Veliko Tarnovo, Bulgaria

множество движещи се части, използвани за охлаждане. Друг генератор на шум в компютрите могат да бъдат захранванията и техните високи честоти. В сравнение с всички аудио карти, тези, които са базирани на USB, имат по-малко проблеми с шума, но са ограничени по други начини, поради по-малката честотна лента на USB интерфейса. Както всички знаем, по-малката честотна лента за пренос на данни ограничава най-високата честота на семплиране и броя на едновременните аудио канали [1, 2].

Сравнихме 2 звукови карти със софтуер за измерване Studio One. Тази програма се счита за DAW софтуер и се използва за измерване на различни аудио карти, както и за създаване на музикални и звукови проекти. Първата звукова карта е външна, евтин модел с 16-битово квантуване и максимална честота на семплиране от 48 kHz. Втората също е външен клас от среден до висок диапазон с 24-битово квантуване и максимална честота на семплиране от 192 kHz. Освен това е хубаво да се отбележи, че първата карта е базирана на стандарта USB 2.0. По-важното което е необходимо да се опомене е, че втората аудио карта е многоканална звукова карта с балансирани входове и изходи и е свързана към компютър с FireWire.

Свързани изследвания и дейности

С развитието на технологиите във времето се създават много нови устройства. Те са подобрени версии на своите предшественици. Един тип от тези нови устройства са звуковите карти. Преди години се използваха само за правене на музика, но с времето започнаха да намират по-широко приложение. Сега те са запазили основната си роля в създаването на музика, но се използват и от ентусиазирани и среден клас потребители. Ентусиазираните потребители ги използват за манипулиране и измерване на сигнали, докато средният потребител ги използва за слушане на висококачествена музика. В това изследване се обръща внимание на предишна работа на други изследователи. Крейг Андертън, авторът на книгата на PreSonus „Работа със Studio One" казва кой е най-добрият и най-ефикасен начин за използване на DAW. Той споделя опита си как да се подготви DAW софтуера, така че изследователят или стандартният потребител да може да извлече максимума от всяко измерване или музика. Друг изследовател, Слави Андреев, описва начините да се извлече максимума от всяко музикално оборудване в своя учебник „Звукови карти и файлови формати". Михайло Рабасови от Института по физика в Белград също пише по подобна тема и показва как да вземем солидна проба от аудио. Проучване след проучване доведе до изследването на Ричард Кабот, където той говори за основите на съвременното аудио измерване.

DAW софтуер Studio One

PreSonus е производител на хардуер и софтуер за цифрова аудио обработка. Компанията е разработчик на най-иновативните аудио приложения и VST инструменти и ефекти. Нашата софтуерна програма използва иновативна технология, която й позволява да бъде използвана като VST инструмент в други програми за аудио обработка. Тя е проектирана специално за редактиране и е подходяща главно за създаване на повтарящи се фрагменти от аудио сигнали. Всеки модел може да се състои от неограничен брой инструменти или VST

инструменти. Инструментите в модела могат да бъдат пренасочени и свързани към прозореца Mixer за обработка и добавяне на ефекти [3].

Studio One е програма за обработка на цифрово аудио от PreSonus [4]. Програмата се разпространява в няколко различни издания: Studio One Express, Producer Edition, Signature Bundle, All Plugin's Bundle и Mobile Edition; Програмата изисква поне 32-битова версия на Windows 7. 2,0 GHz процесор от Intel или AMD с поддръжка на SSE2 инструкции, 1 GB RAM (препоръчително). Най-малко 2 GB безплатно хранилище. Видеокарта с поддръжка на минимална резолюция - 800 × 600 (Super VGA или по-добра). Самата звукова карта трябва да има инсталиран DirectSound драйвер и да е съвместима с ASIO / ASIO2 за аудио запис. Визуализацията на програмата е показана на фиг.1.

Фиг. 1. *Основен прозорец на Studio One*

Звуковите карти в настоящото изследване

Аудио картите са едни от най-необходимите устройства в съвременната аудио техника и са неразделна част от оборудването на музикалния композитор. Следните две аудио карти бяха използвани в настоящото изследване:

PreSonus Audio Box 96

Zen Go Synergy Core

PreSonus Audio Box 96 е аудио звукова карта с два комбинирани входа за микрофон и инструмент на предния панел. Това я прави идеален за певци/автори на песни, подкасти. Просто се свързват няколко микрофона и всеки потребител притежава лесна за използване система за стерео запис [5, 6, 7]. Микс контрола позволява на потребителите да контролират нивото между входния сигнал и компютърното възпроизвеждане, без да чуват досадни забавяния. Той използва балансирани изходи на ниво линия и осигурява кристално чист звук през високоговорители или слушалки.

Zen Go Synergy Core е първата звукова карта, захранвана с шинна технология, пълна е с множество технически характеристики и е от среден към висок клас. Подходяща е както за професионални студиа, така и за домашна употреба и дава незабавен достъп до първокласно качество на звука, където и да

е всеки потребител. Една от най-добрите му характеристики е наблюдението в реално време с незабележима латентност.

Zen Go Synergy Core е оптимизирана за запис с изключително ниска латентност, възпроизвеждане с висока разделителна способност, създаване на креативен ритъм и подкастинг без проблеми. С удобни за пътуване функции и дизайн, интерфейсът може да придружава потребителите при обиколки и записващи сесии на място, без да се жертва скоростта и ефективността. Звуковите карти в това изследване са показани на Фиг. 2 и Фиг. 3, а техните параметри в Таблица 1.

Таблица 1: *Параметри на звуковите карти*

PreSonus Audio Box 9	Zen Go Synergy Core
ADC Динамичен обхват (A-wtd, 48 kHz Честота на семплиране) - 104 dB	ADC Динамичен обхват (A-wtd, 192 kHz Честота на семплиране) - 127 dB
DAC Динамичен обхват (A-wtd, 48 kHz Честота на семплиране) - 104 dB	ADC Динамичен обхват (A-wtd, 192 kHz Честота на семплиране) - 127 dB
Битова Дълбочина - 16-bit	Битова Дълбочина - 24-bit
Поддържащи Честоти на семплиране (kHz) - 44.1, 48	Максимална Честота на семплиране (kHz) - 192 kHz

Фиг. 2. *PreSonus Audio Box 96*

Фиг. 3. *Zen Go Synergy Core*

Теория за звуковите вълни

Преди да започне да се манипулира звук или да се измерва е необходимо да се проучи характерът на звука и неговият процес на цифровизация. В тази част от настоящото изследване е необходима малко информация за аудио основите и тяхното цифрово представяне. Трите основни характеристики на звуковите вълни са:

Амплитуда: Мярка за степента на промяна в атмосферното налягане, причинена от звукови вълни. Тази амплитуда е пряко свързана с силата на звука.

Честота (f): Честотата на звука е скоростта на цикъла, образуван за секунда, и се представя с единица херц Hz. Честотата е право пропорционална на височината на звука.

Дължина на вълната: Дължината на вълната (λ) е разстоянието между два съседни върха на билото или падината. Зависи от скоростта на звука (v), представена чрез единица (m/s) и неговата честота (f). Следователно можем да дефинираме в уравнение (1) дължината на вълната като:

$$\lambda = \frac{v}{f} \quad (1)$$

Основният проблем в аудио оборудването е наличието на шум. Има различни техники за вземане на проби в аудиокартите и те се извършват чрез използване на съотношението сигнал към шум (SNR). SNR е съотношението на мощностите на сигнала към шума (изкривяването). Това е мярка за качеството на изходния сигнал след процеса на вграждане. Измерва се в децибели (dB). Колкото по-висока е стойността на SNR, толкова по-чисти са изходните сигнали с по-малко добавен фонов шум съответно.

$$SNR = 10\ log_{10} \frac{\sum_n A_n^2}{\sum_n (A_n - A'_n)^2} \quad (2)$$

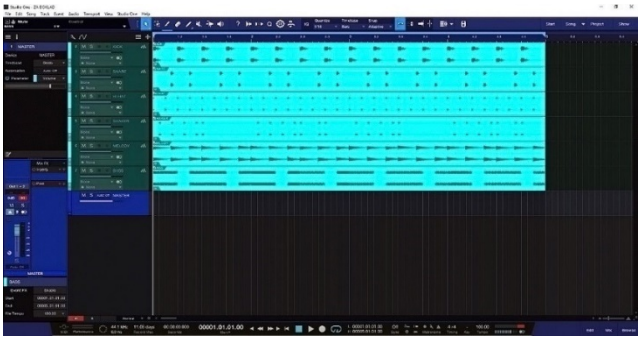
Където A_n е оригиналният аудио сигнал а A'_n е изкривеният аудио сигнал.

Експериментално изследване

В настоящото проучване се изследват две звукови карти, които са по-известни на професионалистите, като PreSonus Audio box 96 и Antelope Audio Zen Go Synergy Core. Между тях ще има процес, при който шест аудио wav файла ще бъдат сумирани (смесени) в един общ канал (шина).

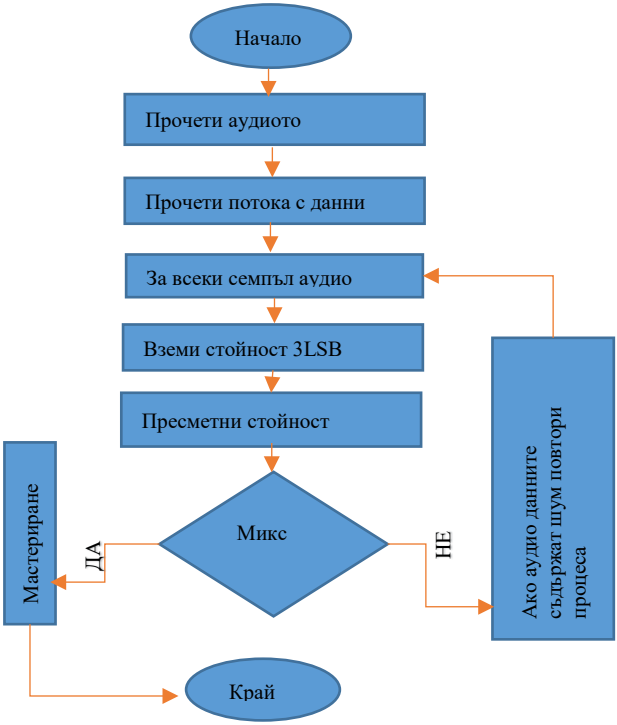
Основната цел на изследването е да се изследват две различни звукови карти. След това може да се заключи дали всеки аудио интерфейс е различен сам по себе си или всеки може да достави един и същ звук. Фиг. 4 показва шест музикални аудио записи. Всеки от тях има формат на аудио файл 16-бита, както и 24-бита. Те са предварително създадени и вмъкнати (импортирани) в сесията в цифровата аудио работна станция Studio One.

На фиг. 5 е показан първият етап от изследването, където се създава шинен канал, в който се изпращат звуковите сигнали от шестте аудиозаписи. Техните изходи са свързани към входа на този шинен канал. Този канал ще се използва за записване и сумиране на тези аудиозаписи чрез звуковата карта PreSonus audio box 96. Следователно изходът на този канал е свързан към нов и празен аудиозапис, който ще записва готовия общ аудио сигнал. Фиг. 6 показва блок-схемата на изпълнение с процеса на сумиране на сигналите.



Фиг. 4. *Създаване на шестте аудиозаписа*

Фиг. 5. *Създаване на шинен канал за шестте аудиозаписа – PreSonus audio box*



Фиг. 6. *Блок-схема на изпълнение*

Приставката софтуерен анализатор се използва за анализиране на работните процеси на аудио картата Presonus, при сумиране на звуци в DAW софтуера се открива следният математически алгоритъм:

$$\frac{\varepsilon+(S)}{\varepsilon-(S)} = \left[\rho\frac{\sigma_1}{\sigma_1-S} + (1-\rho)\frac{\sigma_2}{\sigma_2-S}\right]\frac{\mu}{\mu+2} = \phi_k(\vec{r}) = (2\pi)^{2/3}\exp\left(i\vec{k}\cdot\vec{r}\right) =$$

$$= \frac{[\rho\sigma_1(\sigma_2-S)+(1-\rho)\sigma_2(\sigma_1-S)].\mu(\sigma_1-S)(\sigma_2-S)(\mu+S)}{(\sigma_1-S)(\sigma_2-S)(\mu+S)} = \frac{\mu(a_0-a_1S)-(\sigma_1-S)(\sigma_2-S)(\mu+S)}{(\sigma_1-S)(\sigma_2-S)(\mu+S)} \quad (3)$$

Той е спомагателен и допринася за PreSonus Audio Box 96 за по-бърза обработка и смесване.

Фиг. 7 показва същата процедура, но за звуковата карта Zen Go Synergy Core. Отново, тук същите шест аудио записи са свързани и изпращат своя сигнал към нов канал шина, от който сигналът се изпраща към празна аудио писта, в която се записва сумираният сигнал [8]. Тук, когато приставката софтуерен анализатор се използва за анализиране на работните процеси на Zen Go Synergy Core при сумиране на песни, се открива следният математически алгоритъм:

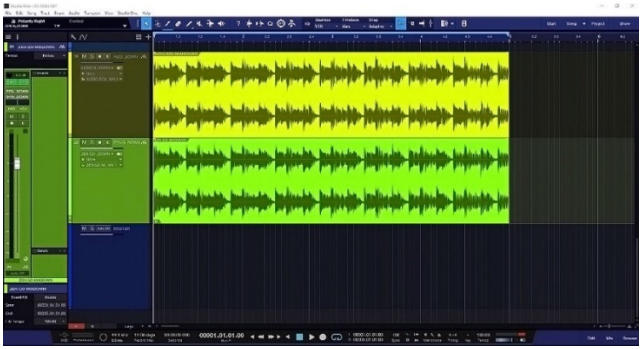
$$\frac{\varepsilon+(D^2)}{\varepsilon-(D^2)} = \left[\rho\frac{\sigma_1}{\sigma_1-D} + (1-\rho)\frac{\sigma_2}{\sigma_2-D}\right]\frac{\mu}{\mu+2} =$$

$$\frac{[\rho\sigma_1(\sigma_2-D^2)+(1-\rho)\sigma_2(\sigma_1-D^2)].\mu(\sigma_1-D^2)(\sigma_2-D^2)(\mu+D^2)}{(\sigma_1-D)(\sigma_2-D)(\mu+D)} = \frac{\mu(a_0-a_1D^2)-(\sigma_1-D^2)(\sigma_2-D^2)(\mu+D^2)}{(\sigma_1-D)(\sigma_2-D)(\mu+D)} \quad (4)$$

Фиг. 7. *Създаване на шинен канал за шестте аудио записи – Zen Go*

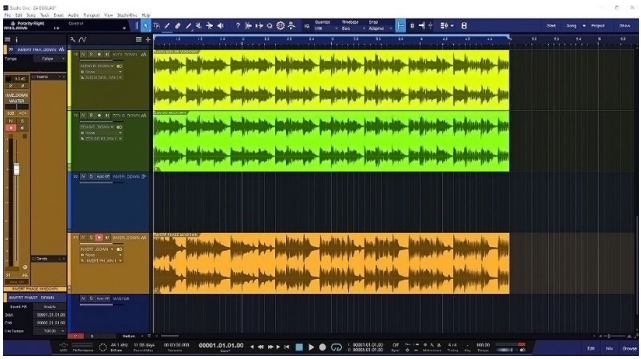
Буквата D в уравнението означава DDP (цифрова динамична обработка). Както е известно, това е една от търговските марки на Antelope Audio. Те прилагат тази технология във всичките си звукови карти от среден към висок клас. Следващата стъпка след записване на сумираните сигнали за съответните две звукови карти е завъртането на фазата на 180 градуса на една от тях, или създаване на обратна поляризация на нейните звукови вълни. В този случай обратната фаза се прилага върху аудиозаписа Zen Go Mixdown. Тъй като това е стерео канал, фазите както на левия, така и на десния канал в миксера на дадения аудио запис са обърнати, както е показано на снимката на фиг. 8. Обръщането на фазата е необходимо и в двете части на аудио файловете и трябва да са напълно еквивалентни по съдържание, тоест техните вълни трябва да са еднакви. При

възпроизвеждането им не трябва да има звуково съдържание поради факта, че вълните на двете аудио-та се неутрализират едно в друго.



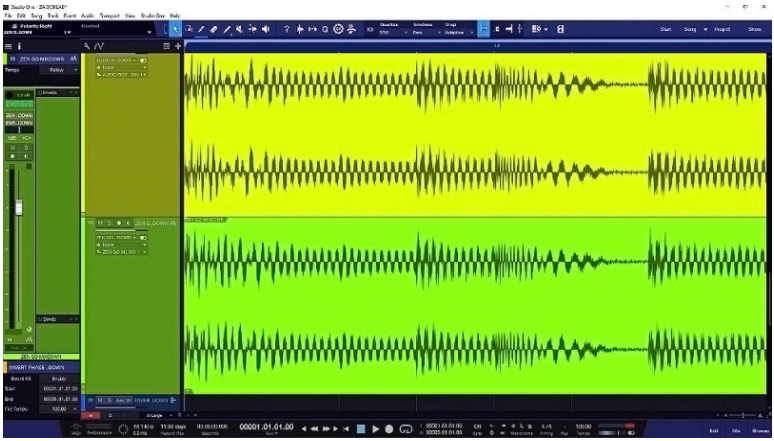
Фиг. 8. *Zen Go Mixdown Фазово завъртане*

Продължавайки напред в изследването, двете песни за миксиране от двете звукови карти са свързани към нов шинен канал и, съответно, неговият изход е свързан към нов празен аудио запис. В новия аудио запис се записва нов аудио файл, който е комбинация от двата микса. В конкретния случай се вижда, че комбинацията няма звуково съдържание и това означава, че ще бъде без звукови вълни, но в този случай, както се вижда на фиг. 9, има звукови вълни и аудио съдържание.



Фиг. 9. *Zen Go Сумиране след завъртане на фазата*

Фигура 10 показва малка извадка от вълните на двете песни за миксиране, която ясно показва как се различават, дори ако са комбинация от тези шест аудио записи. Разликите се дължат на това, че при сумиране на сигналите двете звукови карти преобразуват от цифров сигнал в аналогов и обратно в цифров. Ключовият момент е в преобразуването, защото няма суми от нули и единици както в дигиталния свят и стойностите винаги са абсолютно еднакви и правилни.



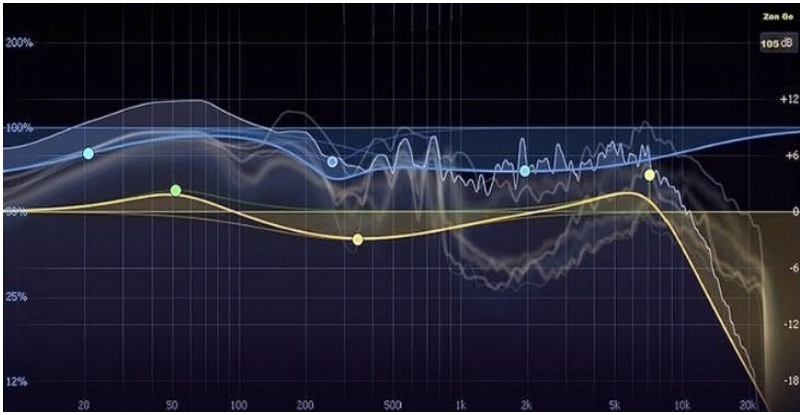
Фиг. 10. *Сравнение между двата сигнала от двете звукови карти*

В аналоговия свят токът играе роля, така че вече преобразуваният цифров сигнал първо се изчислява от алгоритъма и след това се превръща във формата на ток и всеки от тези шест звукови трака има текущ сигнал, който се сумира с останалите в съответната звукова карта, преди да бъде преобразуван обратно в цифров сигнал.

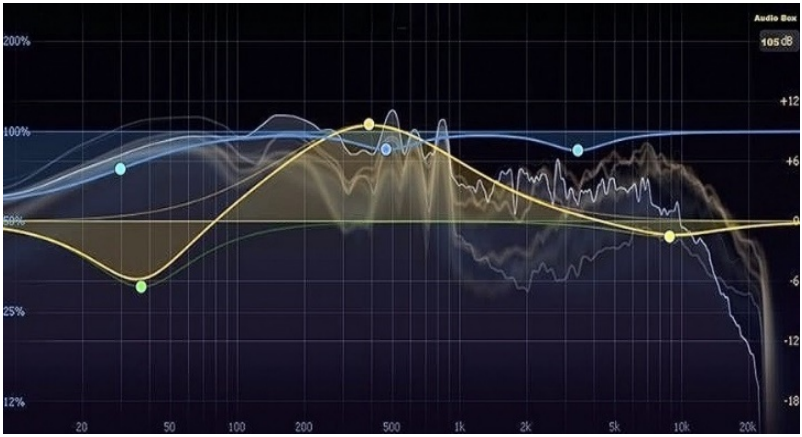
Всяка звукова карта има способността минимално да надвишава възможностите си спрямо описаните от производителя характеристики. В процеса на сумиране на сигналите беше решено да се зададат средни параметри между двете устройства. Това позволяваше да се следи обработката им, по-ниският клас звукова карта работеше с максимална мощност, а средният клас с минимална. Целта на тази проверка е да се види дали при осреднени параметри сигналът от картата от среден клас ще има шум и дали картата от по-нисък клас ще има щракане и пукане. Експортирането беше зададено на:

- ADC Динамичен обхват - 105dB,
- DAC Динамичен обхват - 105dB,
- Честота на семплиране - 96 kHz
- Битова Дълбочина - 16-bit and 24-bit.

Фиг. 11 и Фиг. 12 показват експортирането на сигнали чрез звукови карти Zen Go и Audio box 96. В спектъра се наблюдават два детерминистични сигнала. Първият е жълт и е основният сигнал на звуковата карта. Създаден е на базата на дискретизиран алгоритъм за обработка. Вторият е оцветен в синьо и отговаря за сумирането на всяка писта. Освен това в спектъра се наблюдава рекурсивен филтър с прорези, който взема проби при сумиране. Всяка проба, която е извън филтъра, показва, че има минимално количество шум в сигнала. Звукова карта с детерминистични сигнали, която избледнява плавно с течение на времето, показва, че създава предпоставки за щраквания и пукания при експортиране.



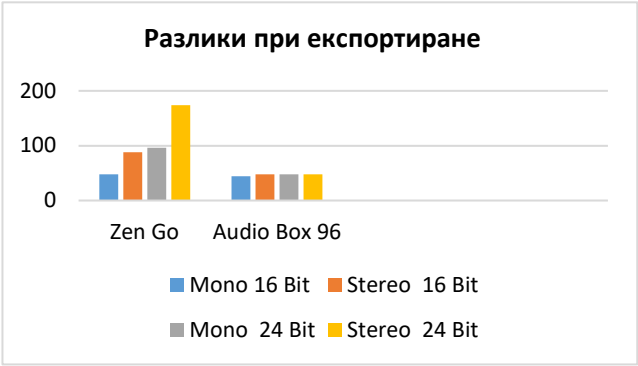
Фиг. 11. *Zen Go експортиращ спектър*



Фиг. 12. *Audio Box 96 експортиращ спектър*

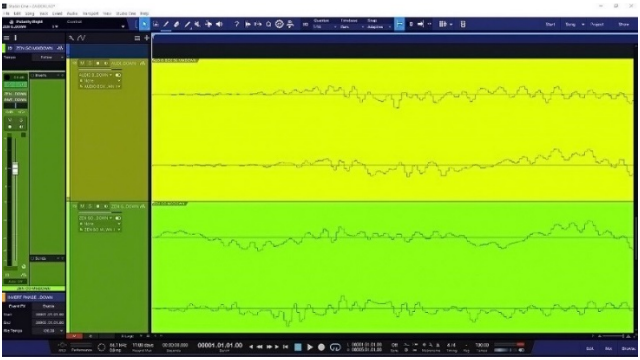
Фиг. 13 показва статистическо сравнение след експортиране на четири определени сигнала от всяка звукова карта. Може да се види, че сигналите от крайния експорт от Zen Go са с по-високо качество от тези от Audio Box 96. Тези от PreSonus Audio Box 96 съдържат щраквания и пукания, както и малко количество изкривяване.

В нашия пример разликата между PreSonus Audio box 96 и Zen Go се основава на хардуер и различни специфични характеристики. Всеки от тях има различни преобразувателни чипове и компоненти. С тях те обобщават аудио сигналите под формата на токове по свой отличителен начин. При преобразуването на звука от двете звукови карти, те дават променливи стойности от тези, подадени от цифрово-аналоговия преобразувател, съответно аналогово-цифровия преобразувател запечатва тези промени в нули и единици.



Фиг. 13. *Разлики при експортиране*

На Фиг. 14 се забелязва разминаване в началото на файловете във времеви интервали като този от Audio box 96, който работи с по-бавен математически алгоритъм и започва да сумира плавно, докато този на Zen Go започва да сумира динамично без забавяне. Допълнителен фактор, който помага на Zen Go за по-добра обработка, е по-ниската латентност [9, 10].



Фиг. 14. *Сравнение между двата сигнала от двете звукови карти*

Дискусия

Настоящата статия въвежда еволюционна тема за измерване на сигнали и звукови карти от ново поколение. Като цяло иновативните теми и новите техники не са получили достатъчно внимание в литературата. Измерването на звукови сигнали и аудио чрез DAW софтуер като потенциална тема е изследвана още по-малко. Повечето предишни теми или техники бяха базирани на модели от старо поколение. Второ, проучването потвърждава предишни качествени резултати, установени от други изследователи. Трето, някои предишни проучвания показват пропуски в измерванията, както и стари методи, които не са най-компактни.

С развитието си с течение на времето всяка нова звукова карта позволява на всеки потребител не само да чува по-добър звук, но също така им дава страхотна съвместимост с професионалния DAW софтуер. Този софтуер е иновативен и намира приложение не само при създаване на музика, но също така работи като измервателен инструмент за други цели. Настоящото проучване показва, че има значителни разлики между всяка звукова карта и тяхното качество. По-старите звукови карти, дори и да имат сходни параметри с настоящите, не могат да се сравняват, тъй като новите имат много нови функции, които правят работния процес много по-бърз.

Заключение

Предимствата на Zen Go пред Audio box 96 като аудио интерфейс от висок калибър се дължат на факта, че той има по-динамичен обхват от 127 dB в сравнение с Audio box 96, който има 104 dB, което позволява на Zen Go да има повече пространство за смесване песни, без да прави грешки при изчисляване и сумиране. Това дава на звука по-голяма разделителна способност на всеки звуков елемент, дълбочина, прецизност, яснота и престижен звук. Също така 64-битовият акустичен световен часовник помага за по-добро синхронизиране на сигналите, когато става въпрос за честота на дискретизация и особено когато става въпрос за преобразуване от една честота на дискретизация в друга честота на дискретизация, тогава ролята на световния часовник е много важна.

Настоящото проучване е предмет на бъдещи изследвания, разработки и намиране на още повече нови иновативни начини за измерване на сигнали и звукови карти. Има за цел да помогне на хората в областта на музикалната и аудио обработка, като им предостави практическа и теоретична информация за звуковите карти.

Една от следващите ни цели е да анализираме аудио карта от най-висок клас и след това да я сравним с карти от всеки друг клас. Това бъдещо проучване ще има за цел да покаже колко голяма е практическата разлика между всички карти и дали звуковата карта от висок клас е подходяща за нуждите на стандартния потребител.

Благодарности

Тази статия и изследването зад него не биха били възможни без изключителната подкрепа на аудиоинженер Таркан Исмаилов. Неговият ентусиазъм, познания и прецизно внимание към детайла бяха вдъхновение и поддържаха работата ни в правилния път. Благодарим и на декана на нашия факултет проф. Христо Христов, който подпомогна изследването чрез закупуването на лицензирана аудио техника.

ЛИТЕРАТУРА

[1] D. Howard, Acoustics and Psychoacoustics, CRC Press USA, 2017.

[2] N. Cvejic and T. Seppanen, Reduced distortion bit-modification for LSB audio steganography, Proc. 7-th Int. Conf. Signal Process. 3, pp. 2318-2321, 2004.

[3] C. Anderton, Working with Studio One, PreSonus Official Guide, 2018.

[4] C. Anderton, Audio Cards from new generation, PreSonus Official Magazine, 2019.

[5] N. Cvejic and T. Seppanen, Increasing the capacity of LSB-based audio steganography, Proceedings of the 5-th IEEE Workshop on Multimedia Signal Processing, St. Thomas VI, pp. 336-338, 2002.

[6] Yu. Guoshen, Audio classification from time-frequency texture, International Conference on Acoustics, Speech and Signal Processing, ACM Digital Library, 2008.

[7] Y. Lin and W. Abdulla, Perceptual evaluation of audio watermarking using objective quality measures, Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing, pp. 1745-1748, 2008.

[8] R. Cabot, Fundamentals of modern audio measurement, Audio Precision, Beaverton, USA, 2017.

ПОДДЪРЖАНЕ НА РАБОТНАТА ГЕОДЕЗИЧЕСКА ОСНОВА (РГО) В АКТУАЛНО СЪСТОЯНИЕ

Стефан Д. Добрев

KEEPING LOCAL GEODEDIC NETWORK TO ACTUAL STATUS

Stefan D. Dobrev

ABSTRACT: *Some neighborhoods or big areas in cities with cadastral map, have geodetic networks that significantly differ from GNSS measurements.*

KEYWORDS: *Cadastre, GNSS measurements, Geodetic networks.*

Увод

Поддържането на кадастралната карта в актуално състояние е предизвикателство за геодезическата гилдия. Според Агенцията по Геодезия, Картография и кадастър (АГКК): „Кадастралната карта и кадастралните регистри се поддържат в актуално състояние въз основа на задължително постъпващата в Агенцията по геодезия, картография и кадастър информация – при промяна на собственост или учредяване на вещни права, при създаване на нови обекти или при промяна на техни характеристики - за нови сгради, пристроени или надстроени сгради, при разделяне или обединяване на имоти и т.н.

Поддържането на кадастралната карта и кадастралните регистри се извършва за сметка на собствениците, т.е. след създаването на кадастралната карта държавата няма да осигурява финансови средства за поддържането й. Финансови средства ще се влагат само за осигуряване информационната система за обслужване на гражданите.

Подобряването на точността на кадастралната карта ще се извършва в процеса на поддържането й. Когато при създаването на кадастралната карта данните за обектите са получени от графичен план или карта, границите на поземлените имоти и очертанията на сградите се заснемат и координират с геодезически измервания.“

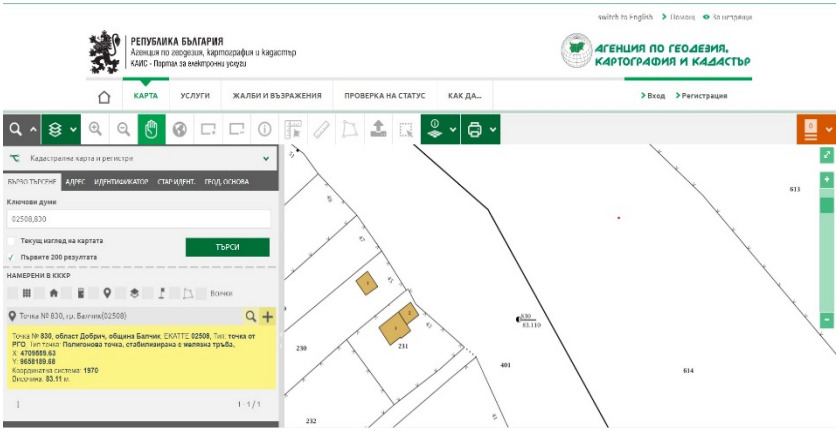
Проблемът при поддържането на кадастралната карта (КК) в актуално състояние е, че много често работната геодезическа основа (РГО) от която е създадена КК е унищожена или при измерването и чрез ГНСС метод, отклоненията в координатите са недопустими.

Координати на точки от РГО в информационната система на кадастъра - КАИС

Като пример от практиката във в.з. Кулака, гр. Балчик се наложи да се нанесе новопостроена сграда в кадастралната карта. Контура на сградата бе заснет и координиран чрез преки геодезически измервания чрез ГННС методи [2]. Като

изискване на някой служби по кадастър е при нанасянето на такава информация в системата им е да се измерят и точки от РГО в близост до обекта.

От системата КАИС на АГКК са взети координатите на 3 близки до обекта точки.



Фиг. 1. *Координатите на т. 830*

Координатите на точките от ГММП и РГО в тази информационан система са в координатна система 1970 год. – обикновено системата в която е предадена кадастралната карта. А всички останали елемнти от картата са в координатна система БГС 2005 (фиг. 1). Т.е. за изготвяне на проект за кадастъра си закупуваме имот с контура му в БГС 2005, а точките от РГО, който ползваме са в координатна система 1970 г. (табл. 1). От АГКК са помислили за този казус, като предлагат безплатен софтуер за геодезически трансформации на координати – BGStrans.

Таблица 1. *Координати на точките от РГО от информационната система на АГКК*

Номер на точка	*X (север) m*	*Y (изток) m*	*H (Надморска височина) m*
828	*4709320.38*	*9658308.23*	*77.208*
829	*4709447.31*	*9658244.24*	*81.172*
830	*4709559.63*	*9658189.68*	*83.11*

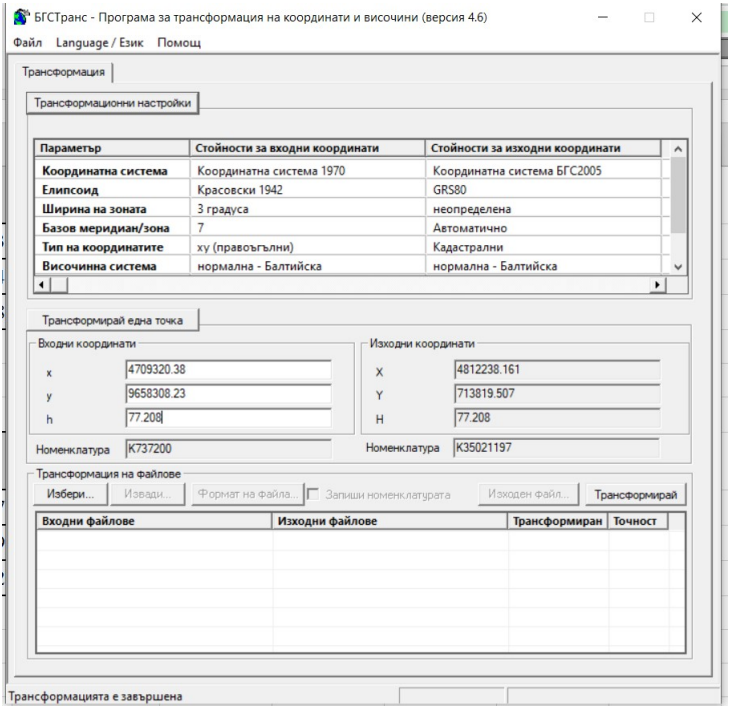
Координатите на точки 828, 829 и 830 са траснформирани със софтуера на АГКК – фиг. 2.

Резултатите от трансформацията са дадени в таблица 2.

Таблица 2. *Координати на точките от РГО трансформирани с БГС транс*

Номер на точка	X (север) m	Y (изток) m	H (Надморска височина) m
828	4812238.161	713819.507	77.208
829	4812364.559	713754.469	81.172
830	4812476.425	713698.982	83.11

Тези точки са намерини и измерени с двучестотен ГНСС приемник Trimble R4, използвайки лицензираната от АГКК инфраструктурна мрежа на ГЕОНЕТ. Измерванията са в координатна система БГС 2005, а височинната система е Геодезическа [1]. Резултатите от измерванията и разликите от координатите взети от КАИС са дадени в таблица 3.



Фиг. 2. *Трансформация на координати с БГС транс*

Таблица 3. *Координати на измерените точки от РГО разликите с тези от кадастъра*

Точки от информационната система на КАИС			
Номер на точка	X (север) m	Y (изток) m	H (Надморска височина) m
828	4812238.161	713819.507	77.208
829	4812364.559	713754.469	81.172
830	4812476.425	713698.982	83.11
Точки от преки геодезически измервания с ГНСС			
Номер на точка	X (север) m	Y (изток) m	H (Надморска височина) m
828	4812237.688	713819.304	112.902
829	4812364.002	713754.213	116.877
830	4812475.612	713698.597	119.095
Разлики			
Номер на точка	dX (m)	dY (m)	DMS
828	0.473	0.203	0.515
829	0.557	0.256	0.613
830	0.813	0.385	0.900

Заключение

Като приоритет АГКК трябва да приоритизира възстановяването на РГО и поддържането му в актуално състояние, т.е. разликите между РГО и ГНСС измервания да са в допустимите стойности.

ЛИТЕРАТУРА

[1] Стойков, Евгени, 2019 г. „Methodology for surveying and tracing of objects by using GNSS“, Годишник: Технически науки. Том IX E, Шумен, Университетско издателство "Епископ Константин Преславски", 21 - 24 стр., ISSN: 1311-834X..

[2] Ivanov S. „Principles of GNSS“. Journal scientific and applied research. Volume 20. Шумен 2021. Университетско издателство „Еп. К. Преславски“. ISSN: 1314-6289. Стр. 27 - 32.

МАРШРУТИЗАЦИЯ ПРИ WDM МРЕЖИ

Екатерина М. Христова, Цветослав С. Цанков

ROUTING IN WDM NETWORKS

Ekaterina M. Hristova, Tsvetoslav S. Tsankov

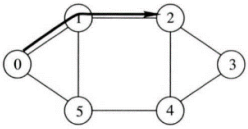
ABSTRACT: *The simplest approach to routing a link is to always choose the same fixed route for a given source-destination pair. In solving the wavelength assignment subproblem, a number of heuristics have been proposed: Random Wavelength Assignment, Least-Used/SPREAD, Most-Used/PACK, Min-Product, Least Loaded, MAX-SUM, Relative Capacity Loss, Wavelength Reservation and Protecting Threshold.*

KEYWORDS: *Multiplexing, optical fiber, packet switching, signal-to-noise ratio, wavelength, WDM.*

Макар комбинираното маршрутизиране с присвояване на дължина на вълната да е труден проблем, може да бъде опростен от разделяне на проблема на две отделни подпроблеми: подпроблемът с маршрутизирането и подпроблемът за определяне на дължина на вълната.

Фиксирано маршрутизиране

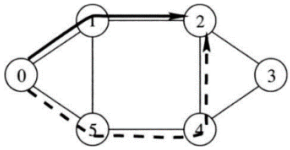
Най-простият подход за маршрутизиране на връзка е винаги да се избира един и същ фиксиран маршрут за дадена двойка източник-дестинация. Един пример за такъв подход е „фиксирано маршрутизиране с най-кратък път“. Най-краткият маршрут за всяка двойка източник-дестинация е изчислен офлайн с помощта на стандартен алгоритми за най-кратък път, като алгоритъма на Дейкстра или алгоритъмът на Белман-Форд. Всяка връзка между определената двойка възли се установява с помощта на предварително установен маршрут. На фиг. 1 е илюстриран фиксираният маршрут с най-кратък път от възел 0 до възел 2. Този подход за маршрутизиране на връзки е много прост, но недостатъкът му е, че ако ресурсите (дължини на вълните) по пътя са свързани, потенциално може да доведе до висока вероятност за блокиране в динамичния случай или може да водят до използване на голям брой дължини на вълните в статичния случай. Освен това фиксираното маршрутизиране може да не е в състояние за справяне със ситуации на повреда при провала на една или повече връзки в мрежата. При справяне с грешките при връзката, схемата на маршрутизация трябва или да обмисли алтернативни пътища към местонахождението, или да си намери маршрута динамично. Заявката за връзка от възел 0 към възел 2 ще бъде блокирана, ако общата дължина на вълната не е налична и за двете връзки във фиксирания маршрут, или ако някоя от връзките във фиксирания маршрутът е пресечен [1, 2, 3, 4].



Фиг. 1. *Фиксиран „най-кратък“ маршрут от Възел 0 до Възел 2*

Фиксирано-алтернативно маршрутизиране

Друг подход, който разглежда множество различни оптимални варианти за свързване е фиксирано-алтернативно маршрутизиране. При него всеки възел в мрежата трябва да поддържа маршрутизираща таблица, съдържаща подреден списък с определен брой фиксирани маршрути до всеки възел от местоназначението. Например, тези маршрути могат да включват най-краткият маршрут, вторият най-кратък път, третият най-кратък маршрут и т.н. Основен маршрут между изходен възел s и целеви възел d е определен като първия маршрут в списъка с маршрути към възела d в таблицата за маршрутизиране във възел s. Алтернативен маршрут между s и d е всеки маршрут, който не споделя всички връзки с първия маршрут в таблица за маршрутизиране на s. Терминът „алтернативни маршрути“ също е използван за описание на всички маршрути (включително основния маршрут) от изходен възел до възела на местонахождението. Фиг. 2 илюстрира основен маршрут (плътна линия) от възел 0 до възел 2 и алтернативен маршрут (пунктирана линия) от възел 0 до възел 2.



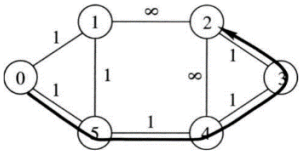
Фиг. 2. *Основен (плътна линия) и алтернативен (пунктирана линия) маршрут от Възел 0 до Възел 2*

Когато пристигне заявка за връзка, възелът-източник се опитва да установи връзката по всеки от маршрутите от таблицата за маршрутизиране последователно, докато бъде намерен маршрут с валидно присвояване на дължина на вълната. Ако не бъде намерен наличен маршрут от списъка с алтернативни маршрути, тогава заявката за връзка се блокира и губи. В повечето случаи таблиците за маршрутизиране във всеки възел са подредени по броя на сегментите на оптичната връзка (мрежови устройства) до местоназначението. Следователно, най-краткият път до дестинацията е първият маршрут в таблицата за маршрутизиране. Когато има равенство в разстоянието между различни маршрути, един маршрут може да бъде избран на случаен принцип. Фиксираното-алтернативно маршрутизиране осигурява простота на контрола за настройка и разрушаване на светлинни пътеки и може също да се използва за осигуряване на известна степен на толерантност към грешки при повреди на връзката. Друго негово предимство е, че то може значително да намали вероятността за блокиране на връзката в сравнение с фиксираното маршрутизиране. Доказано е също, че за определени мрежи наличието на само два алтернативни маршрута осигурява

значително по-ниски вероятности за блокиране, отколкото преобразуването на пълна дължина на вълната във всеки възел с фиксирано маршрутизиране.

Адаптивно маршрутизиране

При адаптивното маршрутизиране маршрутът от възел-източник до възел-местоназначение се избира динамично в зависимост от състоянието на мрежата. Състоянието на мрежата се определя от набора от всички връзки, които се изпълняват в момента. Една форма на адаптивно маршрутизиране е адаптивно маршрутизиране по най-кратък път, което е много подходящо за използване в мрежи с преобразувана дължина на вълната. При този подход всяка неизползвана връзка в мрежата има цена от 1 единица, всяка използвана връка е с цена ∞, всяка връзка с преобразувател на дължина на вълната има цена от c единици. Ако преобразуването на дължина на вълната не е налично, тогава с = ∞. Когато пристигне връзка, се определя най-евтиния път между изходния възел и целевия възел. Ако има няколко пътя с еднакво разстояние, един от тях се избира произволно. Чрез избор на маршрути за преобразуване на дължина на вълната с добра цена c, се подсигурява използването на преобразуването на дължината на вълната само когато не са налични пътища с непрекъсната дължина на вълната. При адаптивно маршрутизиране с най-кратки разходи, връзката се блокира само когато няма маршрут (или с непрекъсната дължина на вълната, или с преобразуване на дължина на вълната) от изходния възел до целевия възел в мрежата. Адаптивното маршрутизиране изисква широка поддръжка от протоколите за контрол и управление за непрекъснато актуализиране на таблиците за маршрутизиране в възлите. Предимство на адаптивното маршрутизиране е, че води до по-ниско блокиране на връзката в сравнение с фиксираното и фиксирано-редуващо се маршрутизиране. За мрежата на фиг. 3, ако връзките (1,2) и (4,2) в мрежата са заети, тогава алгоритъмът за адаптивно маршрутизиране все още може да установи връзка между възли 0 и 2, докато и двата фиксирани протокола за маршрутизиране и протоколите за фиксирано-редуващо се маршрутизиране с фиксирани и алтернативни пътища, както е показано на фиг. 2, биха блокирали връзката.



Фиг. 3. *Адаптивен маршрут от Възел 0 до Възел 2*

Друга форма на адаптивно маршрутизиране е маршрутизирането с Най-малко Претоварени Пътища (LCP). Подобно на алтернативното маршрутизиране, за всяка двойка източник-дестинация, предварително е избрана последователност от маршрути. При пристигането на заявка за връзка се избира най-малко натовареният път сред предварително определените маршрути. Претоварването на връзката се измерва с броя дължини на вълните, налични за връзката. Връзките, които имат по-малко налични дължини на вълната, се считат за по-претоварени. Задръстването на даден път се обозначава от задръстванията на най-натоварената

връзка в пътя. Ако има равенство, тогава може да се използва маршрутизиране по най-краткия път, за да се прекъсне равенството. Алтернативно изпълнение е винаги да се дава приоритет на най-кратките пътища и да се използва LCP само за прекъсване на равенството. И двете комбинации са изследвани чрез симулация и е показано, че използването първо на маршрутизиране по най-краткия път и второ на LCP работи по-добре, отколкото използването само на LCP [5, 8, 12, 13].

Недостатък на LCP е неговата изчислителна сложност. При избора на най-малко натоварения път трябва да се изследват всички връзки на всички кандидат-пътеки. Вариант на LCP е предложен в [2, 3, 8], който изследва само първите k връзки на всеки път, където k е параметър на алгоритъма. Доказано е, че когато $k = 2$, този алгоритъм може да постигне подобна производителност на фиксирано-редуващо се маршрутизиране, като LCP работи много по-добре от фиксираното-редуващо се маршрутизиране.

Формулировка на ILP за установяване на статичен светлинен път

Подобно на RWA задачата, маршрутизирането може също да бъде формулирано като ILP, в който намалява максималния брой светлинни потоци на дадена връзка. Основната разлика между тази формулировка и предишната е, че не налага ограничението за непрекъснатост на дължината на вълната. Вместо това се налага непрекъснатост на дължината на вълната, когато действително се присвояват дължини на вълните на светлинните пътища.

Този проблем е NP-пълен [1, 6, 7], но може да бъде изчислен успешно чрез ограничаване на пространството за търсене и чрез използване на произволно закръгляне [2]. Пространството за търсене може да бъде намалено чрез разглеждане само на ограничено подмножество от възможни връзки за маршрут между дадена двойка източник-местоназначение. Броят на ограничителните уравнения може да бъде допълнително намален чрез използване на произволно закръгляне. При това закръгляване задачата се представя като MFC (потока на множество суровини), при който всеки светлинен поток съответства на една суровина, която трябва да бъде насочена от източник към целевата връзка. Потокът на суровини във всяка връзка трябва да бъде 0 или 1. Сложността на задачата за намаляване на потока на всяка връзка е NP-пълен, но неинтегралната му версия, в която потоците на всяка суровина могат да приемат всякаква стойност между 0 и 1 може да се реши чрез подходящ метод чрез ЛП (Линейно Програмиране). След това частичните потоци, осигурени от ЛП решението, трябва да бъдат преобразувани в цели числа. Това преобразуване използва отстраняване на пътя, който представя набор от възможни алтернативни маршрути за всеки светлинен път и присвоява тегло на всеки възможен маршрут, а след това произволно се избира един от маршрутите според присвоеното тегло.

Този подход за маршрутизиране на връзките се комбинира с оцветяване на графите за решаване на задачата със SLE и съответните резултати са много близки до долната граница за броя на дължините на вълните, които са необходими за установяване на даден набор от светлинни пътища [6, 7, 11].

Устойчиво на грешки маршрутизиране

Когато се създават връзки в оптична WDM мрежа с маршрутизирана дължина на вълната, често е желателно да се осигури известна степен на защита срещу откази на връзка или възел в мрежата чрез запазване на известно

количество свободен капацитет. Често срещан подход за защитата е установяването на два несвързани светлинни потока (маршрутите за светлинните пътеки не споделят общи връзки) за всяка заявка за връзка. Единият светлинен път, наречен основен светлинен път, се използва за предаване на данни, докато другият светлинен път е като резервен в случай, че връзката в първичния път се повреди. Този подход може да се използва за защита срещу повреди на единична връзка в мрежата (при повреда на кое да е оптично влакно в мрежата). За допълнителна защита срещу повреди, първичният и алтернативният път може също да минават през различни възли.

Фиксираното-алтернативно маршрутизиране осигурява директен подход към защитата. Чрез избирането на редуващи се пътища така, че техните маршрути да са през връзки, различни от основния маршрут, се осигурява защита от евентуални повреди на една връзка, чрез разпределение на един от алтернативните пътища като резервен път.

При адаптивното маршрутизиране може да се приложи защитна схема, при която резервният път се настройва веднага след установяването на основния път. Същият протокол за маршрутизиране може да се използва за определяне на резервния път, с изключение на това, че стойността на връзката е ∞, ако тя се използва за основен път на която и да е дължина на вълната. След това полученият маршрут ще бъде разграничен от основния път. Алтернативата е да се приложи възстановяване, при което пътят на архивиране се определя динамично след възникване на повреда. Възстановяването ще бъде успешно само ако в мрежата има достатъчно ресурси. Трябва да се обърне внимание също, че когато възникне повреда, динамичното откриване и установяване на резервен път чрез този подход може да отнеме значително повече време, отколкото превключването към предварително установения резервен път с помощта на подхода за защита.

Статичната формулировка може също да бъде разширена, за да осигури защита от повреда в мрежата. Модифицираната формулировка ще включва допълнителни ограничителни уравнения, изискващи да бъдат настроени два светлинни потока за всяка връзка (единият е основен, а другият – резервен) и маршрутите за тези два светлинни потока не споделят никакви връзки.

Изучава се Задачата за статичното присвояване на дължината на вълната, т.е. при дадено множество от светлинни сигнали и техните маршрути, да се присвои подходяща дължина на вълната за всеки светлинен сигнал, така че да няма два пътя, които да споделят същата дължина на вълната на дадена оптична връзка. Един подход за решаването на този проблем е формулирането му като задача за оцветяване на графи [9, 10, 11].

Разглежда се и Задачата за динамично присвояване на дължината на вълната и обсъждането на евристики за определяне на дължина на вълната. Въвежда се също нов разпределителен алгоритъм за определяне на дължини на вълните наречен алгоритъм за Относително Разпредепяне на Капацитета на Загубата (ОРКЗ). Тези евристики също могат да бъдат приложени към SLE чрез подреждане на светлинните потоци и последователно присвояване на дължини на вълните към тях.

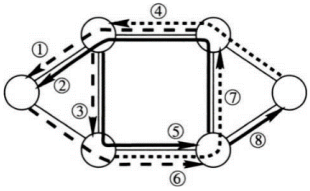
Статично Присвояване на Дължината на Вълната

След като бъде избран път за всяка връзка, броя на потоците, преминаващи през всяко оптично влакно определя претоварването на тази конкретна връзка. Дължините на вълните трябва да бъдат присвоени за всеки светлинен път така, че

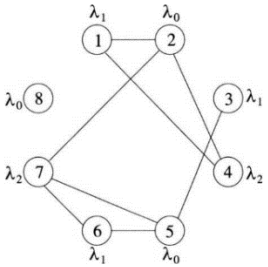
на всеки два сигнала, които споделят една и съща физическа връзка се присвоява различни дължини на вълната.

Присвояване на различни светлинни пътища по начин, който намалява броя на дължините на вълните използвани при ограничението за непрекъснатост се свежда до задача с оцветяването на граф, както е посочено долу.

1 Построява се спомагателен граф $G(V, E)$ такъв, че всеки светлинен път в системата е представен от възел в графа G. Съществува ненасочено ребро между два възела в графа G, ако съответните светлинни пътища минават през общо оптично влакно (фиг. 4 и 5).



Фиг. 4. *Мрежа с 8 маршрутизирани светлинни потоци*



Фиг. 5. *Спомагателен граф G(V, E) за светлинните пътища в мрежата показана на фиг. 4.*

2 Оцветяват се възлите на графа G така, че да два съседни възела да нямат същия цвят.

Доказано е, че този проблем е NP-пълен, и минималния брой цветове, необходими за оцветяване графът G (наречена хроматично число $\chi\ (G)$ на графа) е трудно определим. Има обаче ефективни алгоритми за последователно оцветяване на графи, които са оптимални в броя на използваните цветове. При подхода за последователно оцветяване на графи, върховете се добавят последователно към вече оцветената част и новите оцветявания включват всеки новоприсъединен връх. На всяка стъпка, общият брой на необходимите цветове се запазва до минимум. Лесно е да се забележи, че някои конкретни последователни оцветявания на върховете ще доведат до оцветяване на $\chi\ (G)$. За да се илюстрира това, нека T_i са върховете i на G, оцветени с $\chi\ (G)$. Тогава, за всяко подреждане на върхове $V\ (G)$, което има всички членове на T_i преди всеки член на T_j за $1 \leq i \leq j < \chi\ (G)$, съответното последователно оцветяване ще бъде $\chi\ (G)$ оцветяване.

Лесно е да се отбележи, че ако $\Delta(G)$ обозначава максимална степен на графа, тогава $\chi(G) \leq \Delta(G) + 1$. Въпреки това, интуитивно, ако един граф има само няколко възела от много висока степен, като ранното им оцветяване ще избегне необходимостта от използване на много голям набор от цветове в по-късен етап. Това води до следната теорема:

Теорема: Нека G е граф с $V(G) = v_1, v_2, \ldots, v_n$, където $deg(v_i) \geq deg(v_{i+1})$ за $i = 1, 2, \ldots, n-1$, а n е броят на възлите в G. Тогава $\chi(G) \leq max_{1 \leq i \leq n} \min\{i, 1 + \deg(v_i)\}$. Определянето на процедура за последователно оцветяване, съответстваща на такова подреждане, се нарича Най-Голям - Първи алгоритъм. Доказателството е просто и може да се намери в [9, 10].

По-внимателно разглеждане на процедурата за последователно оцветяване показва, че за дадено подреждане $v_1, v_2, \ldots, v_n$ на върховете на графа G, съответният алгоритъм за последователно оцветяване никога не може да изисква повече от k цветове, където

$k = \max\{1 + deg{<} v_1, v_2, \ldots, v_n{>}(v_i)\}$

и $deg{<} v_1, v_2, \ldots, v_n{>}(v_i)$ се отнася до степента на възела v_i в индуцирания от върха подграф, означен с $< v_1, v_2, \ldots, v_n >$. Определяне на подреждането на върховете, което намалява k е получено в [3, 8] и може да бъде намерено в следната процедура:

1 За $n = |V(G)|$ нека v_n бъде избран да има минимална степен по G.

2 За $i = n-1, n-2, \ldots, 2, 1$, да v_i бъде избран да има минимална степен в $< V(G) - v_n, v_{n-1}, \ldots, v_{i+1} >$

За всяко подреждане на върхове $v_1, v_2, \ldots, v_n$, определено по този начин, трябва да съществува $deg{<} v_1, v_2, \ldots, v_n{>}(v_i) = \min deg{<} v_1, v_2, \ldots, v_n{>}(v_j)$ за $1 \leq i \leq n$, така че такова подреждане ще се нарече подреждане на най-малките последни (SL) върхове. Фактът, че всяко подреждане на най-малкия последен връх намалява k възможните $n!$ подреждания. Прилагайки подреждане на върховете на SL към графа на фиг. 5 и използвайки индекса на възела за прекъсване на връзките, се получава следното подреждане: < 2, 5, 1, 6, 3, 4, 7, 8 >. Да се обърне внимание, че това подреждане дава 3 дължини на вълната, което е минималният брой дължини на вълните, необходими за набора от пътеки на светлината на фиг. 4.

Евристики за присвояване на дължина на вълната

За случая, в който светлинните сигнали пристигат един по един (или чрез инкрементален, или чрез динамичен трафик), трябва да се използват евристични методи за присвояване на дължини на вълните. При динамичния подход, вместо намаляване на броя на дължините на вълните, както в статичния случай, се приема, че броят им е фиксиран (това е практическата ситуация) като задачата е да се намали блокирането на връзката.

В литературата са предложени следните евристики: (1) Произволно присвояване на дължина на вълната (Random Wavelength Assignment), (2) First-Fit, (3) Най-малко използван/SPREAD (Least-Used/SPREAD), (4) Най-Използван/PACK (Most-Used/PACK), (5) Min-Product, (6) Least Loaded, (7) MAX-SUM, (8) Относителна Загуба на Капацитет (Relative Capacity Loss), (9) Wavelength Reservation и (10) Защитен Праг (Protecting Threshold). Всички тези евристики могат да бъдат реализирани като онлайн алгоритми и могат да се комбинират с различни схеми за маршрутизиране. Първите осем схеми се опитват

да намалят общата вероятност за блокиране при нови връзки, докато последните два подхода имат за цел да намалят вероятността за блокиране на сигнали, които преминават през повече от една връзка. Ще бъдат използвани следните обозначения и дефиниции:

L: Брой връзки.

M_l: Брой влакна на връзката l.

M: Брой влакна на връзка, ако всички връзки съдържат еднакъв брой влакна.

W: Брой дължини на вълните на дадено влакно.

$\pi(p)$: Набор от връзки, включващи път p.

S_p : Множество от налични дължини на вълните на избраните потоци p.

D: $L \times W$ матрица, където D_{lj} показва брой на назначените влакна на връзка l и дължина на вълната j. Стойността на варира между 0 и M_l.

За динамичен трафик времето на задържане е експоненциално разпределено с нормализирана средна стойност от една единица, а пристигащите сигнали са Поасонови; по този начин товарът се изразява в Ерланги.

Извършени са няколко експеримента върху проблема с оптимизацията (MAX-FLOW-w), за да се оцени и валидира ефективността на предложените решения. Инструментите GUROBI се използват за решаване на целочислената линейна програма (MAX-FLOW-w). Целта на експериментите тук е да се анализира ефективността на алгоритмите и да се сравнят предложените методи. Сравнението се извършва между базирания на ILP алгоритъм и модифицираният алгоритъм на Garg-Knemann след адаптирането му към гореописания случай на оптимизация. Сравнени са нейното оптимално решение, генерирано от алгоритъма, базиран на ILP, и приблизителното решение, извадено от модифицирания алгоритъм на Garg-Knemann.

ЛИТЕРАТУРА

[1] Daniel Denev, Analysis of the requirements for optical cables for construction of underwater transmission systems, Journal scientific and applied research, vol. 21, 2021 International Journal, 2021, ISSN 1314-6289

[2] I. Chlamtac, A. Farago, and T. Zhang, "Lightpath (wavelength) routing in large WDM networks," IEEE Journal on Selected Areas in Communications, vol. 14, pp. 909-913, June 1996.

[3] D. Banerjee, Design and Analysis of Wavelength-Routed Optical Networks. PhD thesis, University of California, Davis, Department of Computer Science, 1996.

[4] B. Mukherjee, D. Banerjee, S. Ramamurthy, and A. Mukherjee, "Some principles for designing a wide-area WDM optical network," IEEE/ACM Transactions on Networking, vol. 4, pp. 684-696, Oct. 1996.

[5] A. Mokhtar and M. Azizoglu, "Adaptive wavelength routing in all-optical networks," IEEE/ACM Transactions on Networking, vol. 6, pp. 197-206, Apr. 1998.

[6] K. Zhu and B. Mukherjee, "Traffic grooming in a WDM mesh network?' IEEE Journal on Selected Areas in Communications, pp. 122-133, Jan. 2002.

[7] R. Ramaswami and K. N. Sivaranjan, "Routing and wavelength assignment in all-optical networks," IEEE/ACM Transactions on Networking, vol. 3, pp. 489-500, Oct. 1995.

[8] D. Banerjee and B. Mukherjee, "A practical approach for routing and wavelength assignment in large wavelength-routed optical networks," IEEE Journal on Selected Areas in Communications, vol. 14, pp. 903-908, June 1996.

[9] K. Chan and T. P. Yum, "Analysis of least congested path routing in WDM lightwave networks," in Proc. IEEE INFOCOM '94, vol. 2, (Toronto, Canada), pp. 962-969, Apr. 1994.

[10] H. Harai, M. Murata, and H. Miyahara, "Performance of alternate routing methods in all-optical switching networks?' in Proc. IEEE INFOCOM '97, vol. 2, (Kobe, Japan), pp. 516-524, Apr. 1997.

[11] L. Li and A. K. Somani, "Dynamic wavelength routing using congestion and neighborhood information," 1EEE/ACM Transactions on Networking, vol. 7, pp. 779-786, Oct. 1999.

[12] S. Ramamurthy and B. Mukherjee, "Fixed-alternate routing and wavelength conversion in wavelength-routed optical networks," 1EEE/ACM Transactions on Networking, vol. 10, pp. 351 -367, June 2002.

[13] S. Ramamurthy, Optimized Design of WDM Network Architectures. PhD thesis, University of California, Davis, Dept. of Computer Science, 1998.

ОСНОВНИ ЕЛЕМЕНТИ НА ФИРМЕНАТА СИГУРНОСТ

Цветелина И. Методиева, Велимира К. Канчелова, Георги Жеков

BASIC ELEMENTS OF COMPANY SECURITY

Tsvetelina I. Metodieva, Velimira K. Kanchelova, Georgi Jekov

ABSTRACT: *The report examines internal and external threats to corporate security. The main elements of company security are reviewed. Enterprise security is defined.*

KEYWORDS: *Company security, threats to corporate security, internal and external threats to company security.*

Една корпорация може да стане успешна само в условията на гарантирана сигурност. Разширяването на пазарите, увеличаването на клиентите и стабилността и на пазара са възможни, ако компанията има добре оформена система за сигурност. Това до голяма степен определя не само професионалната жизнеспособност на компанията, но и нейният имидж.

Терминът "сигурност" има широко значение, например международна сигурност, национална сигурност, сигурност на корпорацията, сигурност на гражданите и т.н. Под този термин се разбира текуща и бъдеща сигурност срещу различни заплахи от имуществен и неимуществен характер. В допълнение, разглежданата концепция включва различни функционални области, например политическа, военна, екологична сигурност и др.

При дефинирането на сигурността в зависимост от причините за нейното нарушаване се открояват, както заплахи от външен характер - от чужди държави, промени в икономическата политика на собствената държава, неблагоприятна пазарна динамика и др., така и от вътрешни фактори, например ниска квалификация на собствения персонал или липса на финансови ресурси и др.

За нуждите на доклада ще разгледаме сигурността, като условие, при което въздействието на външни и вътрешни фактори не води до действия, които се считат за отрицателни по отношение на тази сложна система в сравнение с нуждите, знанията и идеите, които съществуват на този етап.

„Корпоративната сигурност на предприятието“ (бизнес организацията) е състояние на защитеност на стабилното функциониране и корпоративните интереси на предприятието от потенциални и реални заплахи, постигнати чрез хармонизиране и взаимно свързване на неговите интереси в съответствие с интересите на субектите от вътрешната и външна среда.*

* Методиева, Ц., Корпоративната сигурност и нейните компоненти, Годишник на Шуменски университет, стр 338-341, ISSN 1311-834X, 2020 (български)

С други думи, корпоративната сигурност е състоянието на корпорацията като система (нейните основни подсистеми), при което вероятността от актуализация на застрашаващи фактори за нейното съществуване е сведена до минимум.*

Корпоративната сигурност, също може да се нарече и комплекс от взаимно свързани мероприятия и дейности. Всичко трябва да е предварително обмислено и разработено като единна система – наречена „Концепция за сигурност на фирмата".†

Основната цел на този вид сигурност е да защити компанията от всякакъв вид заплахи и да осигури благоприятни условия за реализиране на нейните основни интереси.

Заплахите тук се делят на два вида – външни и вътрешни.

Външните заплахи са причинени от фактори на външната макро- и микросреда (природни бедствия, причинени от човека бедствия, икономически и политически кризи, нелоялна конкуренция и др.).

От проведени разговори с ръководители на фирми, става ясно, че от всички евентуални заплахи за компанията им, на първо място по опасност те поставят конкурентните фирми. Разбира се, конкуренцията е естествен и дори необходим процес в условията на пазарни отношения, но конкуренцията може да бъде различна:

- лоялна конкуренция, реализирана под формата на състезание в рамките на действащата нормативна уредба;

- съперничество, осъществявано с помощта на техники и методи, насочени към дискредитиране на конкурент, стоките, които произвежда или услугите, които предоставя;

- конфронтация, насочена към унищожаването на конкурент, когато се използват техники и методи, които противоречат на действащото законодателство.

Съперничеството и конфронтацията са нелоялни и пораждат два нови фактора на заплаха: индустриален шпионаж и нападение (враждебно поглъщане), които сами по себе си са пасивни и се активират само в момента на получаване на поръчка за техните услуги.

Що се отнася до престъпността, в момента този фактор на заплаха е по-малко значим и най-предвидим. Причинените от човека бедствия също представляват заплаха за корпоративната сигурност.

Външните рискове винаги са управляеми и предвидими, но трябва да се разбере, че има информация отстрани за условията на сигурност на компанията, тъй като без нея външните заплахи са непродуктивни. Следователно основната заплаха за корпоративната сигурност все още идва отвътре.

Вътрешните заплахи са свързани с проблемите на балансирането на интересите на участниците в корпоративните отношения, ефективността на корпоративното управление, общата ефективност и устойчивост на дейността на корпоративните структури.

Вътрешните заплахи за корпоративната сигурност се разбират като:

* https://moodle-kstu-ru.translate.goog/

† https://profisec.bg/50/firmena-sigurnost/

- заплахи от служители на компанията, както умишлени (измама, кражба, изкривяване или унищожаване на поверителна информация, индустриален шпионаж и др.), така и неумишлени (промяна или унищожаване на информация, ниска квалификация на служителите, невнимание и др.);

- заплахи, свързани с организационната несигурност на бизнеса;

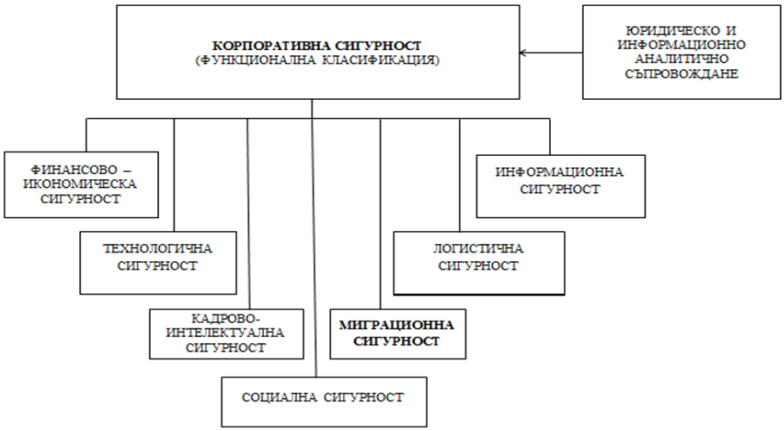
- заплахи, свързани с неефективно управление и организация на бизнес процесите;

- заплахи, свързани с работата на технически средства и средства за автоматизация.

Гарантирането на корпоративната сигурност е възможно само при изградена система за нейния контрол и управление.

Под системата за корпоративна сигурност в общи линии е обичайно да се разбира организиран набор от специални органи, методи, средства и мерки, чрез които корпорацията е защитена от външни и вътрешни заплахи. С други думи, може да се определи, като ограничен набор от взаимосвързани компоненти, които осигуряват сигурността на корпоративните структури и постигат стратегическите цели, пред които са изправени.

Основните елементи на системата за корпоративна сигурност са изобразени на фигура 1:



Фиг.1. *Класификацията на компонентите на корпоративната сигурност по ресурсно-функционален признак*[*]

Финансово-икономическият компонент на корпоративната сигурност на компанията оценява ефективното използване на корпоративните ресурси, осигуряващи финансова стабилност, ликвидност и рентабилност на дейността, както и постигане на максимален обем продажби на продукти на компанията в

[*] Методиева, Ц., автореферат на дисертационен труд „Миграционни процеси и влиянието им върху сигурността на корпорациите“, Шуменски университет „Еп. К. Преславски“, 2020г., стр. 9

резултат на ефективно насърчаване на продажбите и съобразяване с потребителските нужди.

Технологичната сигурност се определя от това, дали оборудването и технологиите, използвани в предприятието, отговарят на съвременните световни анализи и съответстват на приложимите екологични стандарти.

Кадрово-интелектуалният компонент на корпоративната сигурност е насочен към постигане на високо квалификационно ниво на персонала, развиване на креативно мислене и творчески подход на служителите.

Информационната сигурност осигурява ефективно информационно-аналитично подпомагане на икономическата дейност на предприятието, представлява предприятието сред партньори и конкуренти и защитава информационните ресурси.

На фигурата, като „юридическо и информационно-аналитично съпровождане“ е показан елементът, който осигурява правната подкрепа на организацията, както и възможността за адаптиране на компанията към промените на законодателството и публичната администрация.

В условия на нестабилност и несигурност в пазарната среда и несъвършенството на правния и организационно-икономическия механизъм за осъществяване на икономическите отношения, една от важните насоки за осигуряване на сигурността на предприятията е използването на принципите на логистичния мениджмънт, както на ниво отделно предприятие, така и на ниво между организационно взаимодействие. Това води до отделяне на логистичен компонент на корпоративната сигурност, свързан с вътрешното управление, обхващащ взаимоотношенията, възникващи на микро и макро ниво.

Корпоративната сигурност има политически и правни, информационни, екологични и властови компоненти. Силовият и социален компонент отчита всички аспекти на дейността на предприятието, които определят физическата сигурност на неговите служители, степента на защитеност на имуществото от отрицателни влияния и сигурността на информационните ресурси на предприятието.

Екологичният компонент отчита отрицателното въздействие на производствения процес върху околната среда и екологията на региона и държавата, степента на екологичен контрол и икономическата ефективност на екологичните мерки на предприятието.

Сигурността на корпорациите трябва да се базира на добре обоснована политика за сигурност, приета от ръководството на фирмата и ако е необходимо да се вземат организационни мерки за нейното постигане, в това число и създаването на собствена корпоративна система за сигурност, която да защитава организацията от външни и вътрешни заплахи.

Политика на сигурност е съвкупност от документирани правила, които определят как една организация управлява и защитава своите материални и финансови активи, търговските тайни и класифицирана информация. Комбинацията от всички защитни механизми (или целостта им) реализира

политиката за сигурност*. Политиката на сигурност се изгражда на база анализ на рисковете, които са реални за дадената организация†.

Корпоративната сигурност си остава най-големия резерв на укрепването на системата за национална сигурност. Това може да се осъществи ако добронамерено и компетентно се отстраняват възникващите противоречия и конфронтация между системите за осигуряване на националната и корпоративната сигурност.‡

ЛИТЕРАТУРА

[1] Слатински, Н. Същност, смисъл и съдържание на сигурността. Военно издателство ЕООД. 2011;

[2] Зайнуллин С.Б., Сорокин Н.Д. Особенности корпоративной безопасности российских предприятий // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №6 (2017) https://naukovedenie.ru/PDF/140EVN617.pdf

[3] Бахчеванов, Г., Система за национална сигурност, стр.346-359. В: Национална и международна сигурност.

[4] Сандев, Г. Сигурност на организациите.УИ "Епископ Константин Преславски". Шумен. 2012.

[5] Станев, С. и С. Железов. Комютърна и мрежова сигурност.УИ „Еп.К.Преславски", Шумен, 2005.

[6] Казаков, К. Управление на системата за защита на националната сигурност. Информация и сигурност. Първо издание. София. 2016.

[7] Асенов, Б. Теория на разузнаването и контраразузнаването. ВСУ „Черноризец Храбър", Варна. 2008.

* Станев, С. и С. Железов. Комютърна и мрежова сигурност.УИ „Еп.К.Преславски", Шумен, 2005.

† Тужаров, Х. http://www.tuj.asenevtsi.com/Sec2009/Sec23.htm

‡ Корпоративната сигурност, като елемент на системата за национална сигурност https://geopolitica.eu/ekip/1110

ТЕОРЕТИЧНИ АСПЕКТИ НА СИГУРНОСТТА

Цветелина И. Методиева, Велимира К. Канчелова

THEORETICAL ASPECTS OF SECURITY

Tsvetelina I. Metodieva, Velimira K. Kanchelova

ABSTRACT: *The paper examines the theoretical aspect of security. The definition of national security is con-sidered. The concept of security is considered together with the concept of system.*

KEYWORDS: *Security, national security, economic security.*

Свидетели сме на световна пандемия породена от Covid 19, война с неясни граници и край, носейки след себе си многобройни последици и незаличими белези, държави на ръба на оцеляването, политически колапс водещ до низ от кризи за страната ни. Всичките горе-изписани мрачни събития ги обединява необходимостта от само една дума „сигурност“. Сигурността се свързва с проблемите на оцеляване на нациите, а така също и на държавите, може да бъде свързвана едновременно с високите етажи на международните отношения и с всеки от аспектите на вътрешната политика.

Сигурността е степен на съпротива или предпазване от вреда. Сигурността се прилага към всичко, което е ценно и в същото време уязвимо, това може да е предмет, компютърна система, помещение, човек, група, общност, нация или организация.*

Сигурността е функционалното състояние на дадена система, което осигурява неутрализирането и противодействието ѝ на външни и вътрешни фактори, които оказват влияние или могат да въздействат деструктивно на системата (влошаване организационното състояние на системата или невъзможност за нейното функциониране и развитие). Обичайно организираните атаки срещу системата за сигурност са в резултат на заговор.

Като принцип, сигурността подсигурява живота и здравето на физическите лица, държавата, юридическите лица и дейността им, както и бизнеса от страна на потенциални и/или реални заплахи. Високата степен на сигурност на индивида, общността, страната, конкретна корпоративна или нестопанска организация, осигурява увеличаване на благосъстоянието. Сигурността подсигурява възможността за натрупване на блага за индивида, тъй като тя е втората стъпка след физиологичните нужди в Пирамидата на Маслоу.

---

* https://bg.wikipedia.org/wiki/%D0%A1%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81

Професор д-р Николай Слатински, подрежда в една опростена, но много добре разбираема „Схема Петте нива на сигурността“.

Фиг. 1. *„Схема Петте нива на сигурността“ подредена от професор д-р Николай Слатински*

Така той разглежда понятието, като го свежда до пет нива на сигурност: сигурност на индивида, сигурност на групата от индивиди, сигурност на държавата, сигурност на общността от държави, сигурност на света. Авторът подчертава, че подредбата от първо до пето място не прави нивата повече или по-малко важни, като всяко от тях има свое специфично значение.

Характерът на разглеждания проблем в доклада дава възможност да се ограничим само с нивото „сигурност на държавата“, за което обект на интереси е държавата, и с нивото „сигурност на групата от индивиди“, за което един от обектите на интереси е корпорацията.* За тези две нива понятията сигурност, безопасност и защитеност се определят като национална сигурност, национална безопасност, национална защитеност (защитеност на държавата) или корпоративна сигурност, корпоративна безопасност, корпоративна защитеност (защитеност на корпорацията).

Сигурността, като родово понятие се определя, като невъзможност да се нанесе вреда, защита на всеки човек и обкръжаващата го среда от опасности. Най-общо „сигурност“ в политически план се разбира „защитеност“, „състояние на безопасност“ и „състояние на гарантирана надеждност“ за развитието на хората, обществото и държавата.

Чуждестранните изследователи на проблемите на сигурността изтъкват, че за това понятие няма единна дефиниция†. И у нас то се разглежда в много научни трудове от различна гледна точка и в тях е трудно да се намери единно определение‡. В социологията, политологията и психологията определенията за сигурност корелират в областта на защита на важните необходими нужди на

* Методиева, Ц., Национална и корпоративна сигурност, Сборник научни трудове MATTEX 2018, стр. 286

† Бахчеванов, Г.Система за национална сигурност. стр.346-359. В: Национална и международна сигурност.

‡ Слатински, Н. Същност, смисъл и съдържание на сигурността. Военно издателство ЕООД. 2011;

обществото и човека. Философията и политологията разглеждат сигурността, като определено състояние на системата. Надеждността характеризира сигурността във философията, правото, политическите науки и математиката. Само социологията и политологията разглеждат сигурността от гледна точка на развитието на системата, тоест в динамика*.

Системата представлява множество от елементи, които се намират в отношения и връзки помежду си и образуват определена цялост†. Системата работи в определена среда с определена цел.

За решаването на проблемите на човешките организации през 80-те години на 20 век е поставено началото на системния подход при изследване и усъвършенстване на социалните системи. Системният подход е подход за изследване и управление на обекти, който ги разглежда като система, в която са определени елементите, вътрешните и външните връзки, влияещи на функционирането на системата, като целите на всеки елемент е да се формират в зависимост от общото предназначение на системата‡.

Понятието „сигурност“ трябва да бъде разгледано във връзка с понятието „система“, като интегрирана общност от взаимосвързани елементи§.

От такава гледна точка сигурността се определя като динамично състояние на защитеност на система, при което е гарантирано нейното съществуване и са защитени надеждно жизненоважните ѝ интереси. Затова за защита на жизненоважните интереси се отделят значителни ресурси, като само по този начин системата може да гарантира своето успешно съществуване и развитие**.

Формулирано по този начин, определението на понятието кореспондира и с определението за военна сигурност, дадено в съюзната доктрина на НАТО за разузнаване, контраразузнаване и сигурност: „Сигурността е постигането на такова състояние, при което обозначената информация, материал, личен състав, действия и съоръжения са защитени от шпионаж, саботаж, подривна дейност и тероризъм, както и от загуба или нерегламентиран достъп и разкриване“††. Сигурността включва мерките, предприети за защита от заплаха за сигурността, които могат да бъдат предизвикани както от външни, така и от вътрешни източници. Руски експерти също приемат определението, че сигурността в

---

* Зайнуллин С.Б., Сорокин Н.Д. Особенности корпоративной безопасности российских предприятий // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №6 (2017) https://naukovedenie.ru/PDF/140EVN617.pdf

† Бахчеванов, Г., Система за национална сигурност, стр.346-359. В: Национална и международна сигурност.

‡ Сандев, Г. Сигурност на организациите.УИ “Епископ Константин Преславски“. Шумен. 2012.

§ Казаков, К. Управление на системата за защита на националната сигурност. Информация и сигурност. Първо издание. София. 2016.

** Асенов, Б. Теория на разузнаването и контраразузнаването. ВСУ „Черноризец Храбър“, Варна. 2008.

†† Съюзна доктрина на НАТО за разузнаване, контраразузнаване и сигурност. AJP 2.0 (A). 2014

съвременното общество е състояние на защитеност на обектите на защита (организации, армия, физически лица и др.) от вътрешни и външни заплахи*.

Съществуват различни класификации на отделните аспекти на сигурността, т.е. на видовете сигурност†. Според различни критерии сигурността се определя като политическа, военна, икономическа, финансова, социална, демографска, информационна, етническа, религиозна, екологична, персонална и др.‡

Понятието „сигурност" е тясно свързано с категорията „национални интереси", нещо повече, първото е производно от второто.

Понятието „национална сигурност" се появява най-напред в американската политология в първите следвоенни години. В световната литература има над 200 определения за национална сигурност от различни гледни точки. Най-общо под „национална сигурност" се разбира динамично състояние, при което за държавата и обществото не съществува пряка опасност от въоръжено нападение, политически натиск или икономическа принуда, така че те могат свободно да осъществяват своето развитие§.

Според официално приетата у нас през 1998 г. Концепция за национална сигурност, „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"**.

Редица наши автори разглеждат проблемите, свързани с националната сигурност, като обхващат сферата на политиката, социално-икономическата сфера, засягат въпроса с етническите и демографски характеристики на сигурността, обръщат внимание на информационната сигурност, сигурността в нейните духовни измерения и гражданско-военните отношения свързани със сигурността. Тези автори дават и различни определения за националната сигурност. Интерес представлява определението, че „националната сигурност е устойчиво, но динамично състояние на държавата и обществото, при което са гарантирани: държавният суверенитет, териториалната цялост и защитата на националните граници; икономическият просперитет, социалната справедливост и националната духовност, култура и образование за всички хора, живущи на

---

* Землянов, В. Своя контрразведка. Практическое пособие. http://coollib.net/b/248996/read - прегледано 28 Март 2019.

† Слатински, Н. "Измерения на сигурността" София, Издателство "Парадигма", 2000 г. стр. 20-21

‡ Сигурност.https://bg.wikipedia.org/wiki/%D0%A1%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%

§ Бахчеванов, Г. Система за национална сигурност. стр. 346-359. В: Национална и международна сигурност.

** Концепция за националната сигурност на Република България, "Държавен вестник", брой 46/22.04.1998г.

територията на държавата; устойчивото състояние и възпроизводството на обществените отношения, природната среда, културно-историческото наследство, езикът, битът и традициите на населението; законите, отговорностите и задълженията, индивидуалните права и свободи на човека*.“

Националната сигурност на всяка една държава е следствие от нейното икономическо състояние. Над 90 % от икономиката у нас е в ръцете на частни компании. Големите и средни фирми имат под една или друга форма структури за сигурност, които пазят техните активи. Съответно тяхната работа (добра или лоша), оказва благоприятно или негативно влияние върху националната сигурност.† Следователно, финансово-икономическата сигурност е елемент на националната сигурност. Концепцията за национална сигурност е най-общата основа, върху която се реализира връзката между икономиката и потребностите на сигурността и отбраната. Понятието „икономическа сигурност“ е важен съставен компонент в комплексната сигурност и се употребява за пръв път през 1971 год. в Япония от Министерството на външната търговия и промишлеността. Все още липсва общоприето определение за понятието „Икономическа сигурност“‡.

Следва да се обобщи, че икономическата сигурност се откроява и реализира в действителността, посредством система от икономически субекти и обекти на различни равнища и в различни сфери.

ЛИТЕРАТУРА

[1] Слатински, Н. Същност, смисъл и съдържание на сигурността. Военно издателство ЕООД. 2011;

[2] Зайнуллин С.Б., Сорокин Н.Д. Особенности корпоративной безопасности российских предприятий // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №6 (2017) https://naukovedenie.ru/PDF/140EVN617.pdf

[3] Бахчеванов, Г., Система за национална сигурност, стр.346-359. В: Национална и международна сигурност.

[4] Сандев, Г. Сигурност на организациите.УИ “Епископ Константин Преславски“. Шумен. 2012.

[5] Казаков, К. Управление на системата за защита на националната сигурност. Информация и сигурност. Първо издание. София. 2016.

[6] Асенов, Б. Теория на разузнаването и контраразузнаването. ВСУ „Черноризец Храбър“, Варна. 2008.

* Иванов, Д. http://epicenter.bg/article/Prof--Dimitar-Ivanov--Natsionalnata-sigurnost-na-Balgariya--Ima-li

† Митев, Бойко, Корпоративната сигурност – защита на всички активи, CIO Media.2011 https://cio.bg/, 15 Юли 2020 г.

‡ Мичев, С., Вълкова. Л. Социално-икономически аспекти на сигурността. стр. 212-232. В: Национална и международна сигурност. Сборник, Военно издателство, София, 2005.520 стр.ISBN 954-509-306-4.

КОРПОРАТИВНА СИГУРНОСТ И ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД НЕЯ

Велимира К. Канчелова

CORPORATE SECURITY AND ITS CHALLENGES

Velimira K. Kanchelova

ABSTRACT: *The report examines security as a concept and how it relates to corporate security. The concept of corporate security is examined, as well as the structure of the Security department in an organization and what are the threats to security in an organization.*

KEYWORDS: *Corporate security, structure of the Security department, challenges, security of the organization.*

Има много определения за понятието „сигурност“. През различните етапи от развитието на човешкото общество и политико-икономически формации понятието „сигурност“ претърпява еволюция. В ранните стадии на развитието на обществата сигурността се свежда до защита от разрушителните въздействия на природните явления и изграждане на способности за оцеляване и съществуване на индивида. С развитието на обществените отношения се формира разбирането за защита от последствията на „злата воля на хората“.

Дефинирането на термина „сигурност“ в началото на XX в. е със значение на спокойно състояние на духа на човека, защитен от всякаква опасност, отразява принципно новите условия на развитие на човешката цивилизация. На преден план се очертава борбата за световно господство, за реализация на национални интереси и надмощие на социално-политически идеологии. Развитието на обществените отношения е придружено от разширяване на знанията за сигурността и усложняването на качествените характеристики на заплахите и опасностите, които поставят сигурността на държавата в центъра на разбирането на сигурността.

По времето на създаване на централизираните европейски държави понятието за сигурност не получава широко разбиране и приемане, т.к. на преден план е организацията на конкретната дейност на конкретен суверен, обезпечаващ сигурността на своите хора и територии.

В хода на общественото развитие се открояват определени закономерности, свързани с парадигмалните виждания за сигурността:

– понятието за сигурност се развива паралелно с развитието на обществото, за всяка обществено-политическа формация, за всяка страна и регион е присъщо собствено възприятие за сигурността;

– заинтересованите субекти обясняват понятието „сигурност“ от гледна точка на собствените си интереси;

– обществениият прогрес не отстранява опасностите за развитието на личността, обществото и държавата;

– вътрешните и външните заплахи не са неизменни и се трансформират заедно с измененията в обществото;

– нарастването на увереността на хората в тяхната мощ над природата увеличава мащаба на заплахите пред човечеството и неговите общества.[*]

Многообразието на употребата на понятието „сигурност" води до обособяването на редица области, където това понятие има всички отличителни черти на категория в съответния дискурс. Това са специализирани употреби на понятието „сигурност". Като илюстрация могат да бъдат посочени употребите на това понятие в различни сфери на обществените отношения.

В международните отношения сигурността е нещо, което гарантира защита, отсъствие на опасност от агресия или война. Изработена е собствена терминология като национална сигурност и колективна сигурност.

В полето на специализираните институции сигурността означава структури и дейности на полицаи, военнослужещи, служители или агенти насочени към защита на важни лица, инфраструктури и обекти, към пресичане на шпионаж, и на организирани от чужди сили враждебни действия. Отбранителна сигурност; Контраразузнавателна сигурност, Обществен ред и сигурност;

В сферата на финансите, както и на здравето сигурността се постига благодарение на инструменти, които гарантират защита или застраховане на парични средства, на ценности и стоки срещу възможни рискови събития, които могат да предизвикат тяхната частична или пълна загуба. Банкова сигурност; Подобни мерки по отношение на здравето на присъстващия и на неговите близки.

В областта на комуникациите сигурността е резултат от адекватното използване на физически и софтуерни системи за гарантиране на необходимата степен на защитеност на комуникациите и на инфраструктурните обекти със значение за стабилността на държавата и на корпорацията. Тук също е изработена собствена терминология като Киберсигурност, Защитна стена.

В инженерните и в техническите системи сигурността се схваща като безотказност и устойчивост на функциониране на техническите устройства и комплексите от тях. Възгледът е разработен в кибернетиката, където пораждането и поддържането на желаното равновесие на системата с нейната среда се обхваща от понятието хомеостазис.[†]

Сигурността на организациите изисква взаимодействие със средата и тогава, когато състоянието й е в норма, и тогава, когато състоянието й е в криза. Изхождайки от тези системни позиции, под сигурност на организацията ще разбираме такова комплексно състояние на средата – външна и вътрешна – при което възможностите да се актуализира силата на факторите, насочени срещу оцеляването на организацията, са минимизирани, като същевременно са взети необходимите мерки за компенсиране на вероятни загуби при настъпване на един или други рискове, заплахи или кризи.

Горното определение на понятието "сигурност на организацията" не противоречи, а развива дефиницията за "сигурност", дадена в един от най-

[*] Симеонов, С. В огледалото на сигурността: Гражданинът между обществото и държавата, стр. 351-354. ВСУ „Черноризец Храбър", Варна, 2022

[†] https://nbu-rechnik.nbu.bg/bg/obsht-spisyk-na-ponqtiq/sigurnost

важните нормативни документи в тази област – Концепцията за национална сигурност на Р Б. Включването на думата “организация” води до ново съставно понятие с частични промени в семантиката, даващи възможност то да бъде използвано в качеството на важен инструмент за конкретна организационна и управленска дейност в различни по характер компании и базови звена на обществото. Конкретното използване, естествено, предполага съчетаване на голямо количество цели и параметри, имащи отношение както към организацията като цяло, така и към нейните елементи.

Под корпорация трябва да се разбира сдружение, общност, съюз, група от лица. Следователно ние имаме право да считаме за корпорация всяка група от хора, ангажирани в съвместни дейности. В същото време всяка ортанизация или бизнес структура може да се разглежда като системно образувание.

Концепцията за националната сигурност се появява през 90-те години на миналия век. Основният акцент беше поставен върху защитата от страна на предприемачите и кооперациите на тяхното имущество и живот, което се дължи на високата криминализация на бизнеса и обществото. В този момент се появяват голям брой частни охранителни фирми и възниква институцията на бодигардовете.

Постепенно с развитието на пазарните отношения и на мерките за правно регулиране на пазара, акцентът започва да се измества към сферата на икономиката. Корупцията и данъчният натиск не позволиха на предприемачите да се развиват бързо. През този период практически нямаше предприятие, което да работи, без да нарушава действащото законодателство. В резултат на това се появяват много „черни“ и „сиви“ схеми за минимизиране на данъците. Естествено, при това състояние на нещата регулаторните и правоприлагащите органи се превърнаха в сериозна „ заплаха“ за бизнеса. Формално използването на такива схеми може да се припише на системата от мерки за осугоряване на икономическа сигурност.

Второто важно явление беше кризата на неплащанията и необходимостта от действия за връщане на дългове, обикновено принудително. За изпълнението им допринесоха и служителите на реда. За решаването на този набор от проблеми в предприятията и фирмите бяха създадени с ужби за сигурност, които бяха натоварени с отговорността да осигурят преди всичко икономическата и информационната сигурност организациите.

За ефективно противодействие на горните заплахи енеобходима подходяща система за корпоративна сигурност.

Под корпоративна сигурност, в широкия смисъл на понятието, съществува такова състояние на корпорацията като система, при която вероятността за реализиране на опасността, съдържаща се във факторите на заплаха е сведена до минимум.

Във всеки конкретен момент корпоративната сигурност може да бъде представена като числова стойност в диапазона 0-1. От своя страна тази стойност е прозиводна на текущото стъстояние на заплахата и ефективността на системата за корпоративна сигурност. Кумулативната заплаха, засягаща корпорацията, може да представлява реална опастност на нивото на икономическата, информационната или социалната сигурност.

Подходящи елементи на организационната структура, насочени към гарантиране на корпоративната сигурност, трябва ефективно да противодействат

на онези компоненти от общата заплаха, срещу които са насочени. В резултат на съвместната дейност на тези елементи се постига цялостна корпоративна сигурност като определено системно качество.

Кумулативният ефект се постига благодарение на това, че отделните елементи и подсистеми взаимно си помагат при решаването на своите специфични задачи. Всяка подсистема има обратна връзка, което дава възможност да се коригира нейната ефективност чрез използване на вътрешни ресурси в случаите, когато действителното ниво на сигурност е по-ниско от определеното. От своя страна всяка от подсистемите е минишстимо, състояща се от голям брой елементи.[*]

Фиг.1. *Принципна схема на системата за корпоративна сигурност*[†]

Осигуряването на сигурността при малките организации е органична част от общия проблем за обезпечаване на корпоративната сигурност. Често при малките организации, услугите, свързани с осигуряването на корпоративната сигурност, са обект на "аутсорсинг", т.е . на "външни услуги". Подобни услуги се оказват най-вече от частните охранителни и/или от частните детективски звена. В големите организации е необходимо и препоръчително създаването на Дирекция "Сигурност".

Дирекция „Сигурност" е най-важният елемент от интегрираната система за корпоративна сигурност на организацията. Проектирането на структура за сигурност се предшества от експертиза, която може да се извърши от назначен специалист (специалисти) или от частна консултантска агенция. Експертизата се реализира на базата на бизнес плана на фирмата. След експертизата избраният експерт (експерти), който ще консултира и контролира изграждането на дирекция „Сигурност", предлага на мениджъра проект за организационна структура, съобразен с особеностите на предприятието и бранша, както и с резултатите от експертизата. Различните варианти на този проект са задължителни и са

[*] Зайнуллин С.Б. Корпоративная безопасность, Макс Прес, Москва, 2016

[†] Бородин И.А. Основи на психологията на корпоративната сигурност. - М. Висше училище по психология, 2004

обвързани с разнообразните потенциални възможности за реализиране на заплахи и въздействия срещу предприятието. Алтернативните варианти са в зависимост от целите на фирмата за период от поне три години. Всяка от възможните структури на дирекцията се базира върху прогнози за бъдещото състояние на фирмената сигурност.

Дирекция „Сигурност" на фирмата е целесъобразно да се изгради от следните звена:

- Звено „Разузнаване и специализирани проучвания" - обезпечава параметрите на сигурността при взаимодействие със средата, партньорите и конкурентите.
- Звено „Управление на риска и противодействие" - обезпечава параметрите на сигурността при вътрешнофирмените процеси и отношения.
- Звено „Физическа и техническа защита" – обезпечава режима на безопасност на обектите на фирмата и на структурите за сигурност.

При изграждането на дирекция „Сигурност" на фирмата е целесъобразно да се използват следните основни критерии:

- изграждането да е съобразено с целите и направленията за реализиране на сигурността на фирмата;
- да е оптимална по състав;
- да се постига ефективно управление на относително самостоятелните елементи в структурата;
- да позволява взаимозаменяемост и съвместителство;
- да дава възможност за гъвкаво преструктуриране в зависимост от промените в средата, пазарните условия и конкуренцията;
- да осигурява възможност за координация с останалите структури на фирмата.[*]

Общият алгоритъм на действията, на които се основава работата на службата за сигурност, включва следната последователност от операции.

Системата от превантивни мерки се провежда редовно и непрекъснато. Тя осигурява защитата на корпоративна сигурност на базата на постоянна система от организационни мерки. В същото време трябва да се вземе предвид факта, че организирането на ефективна система от превантивни мерки ще струва много по-малко на организацията, от борбата с последствията от вече извършени престъпления и реализирани заплахи.

Какви са тенденциите в сигурността през 2023 г.? Очаква се световните разходи за ИТ сигурност и управление на риска да нараснат с 11%.

След изпитанието, на което бяха подложение всички държави по света и в частност всички организации, 2022 г. се очакваше да донесе светлина в тунела, но вместо това тя дойде с цяла плеяда неочаквани верижни ефекти. Има много неща, които компаниите биха искали да оставят зад себе си, но едно от тези, които няма как да попадне в тази категория, е корпоративната сигурност.

Заплахите и притесненията за сигурността продължават да преследват ИТ екипите в на практика всички предприятия. България не е изключение - в началото на октомври, по време на старта на Европейския месец на киберсигурността, Министерството на електронното управление излезе с данни, че 57% от организациите у нас са подложени на ежеседмични фишинг атаки.

[*] Сандев Г., Сигурност на ортанизациите, Шумен 2012

Фиг. 2. *Алгоритъм на действията на службата за сигурност*[*]

Организациите са изправени пред увеличаване на броя на атаките и пробивите в сигурността, като се очаква тенденцията да се запази следващите години. Атаките често водят до сериозни въздействия, които за някои фирми биха могли да бъдат фатални. Според IBM разходите за пробивите с изтичания на данни през 2021 г. възлизат средно на 4,24 млн. долара. За да избегнат такива големи разходи, предприятията трябва да разполагат с подходяща инфраструктура за предотвратяване поне на най-широко разпространените заплахи.

Кои са основните тенденции при киберсигурността?

1. Дистанционна работа

Въпреки че работата от вкъщи или просто извън офиса съществуваше много преди пандемията, възприемането на този модел нарасна главоломно през последните две години. Компаниите се стремяха да продължат с нормалните бизнес операции въпреки строгите ограничения. Според доклад на Owl Labs служителите на 69% от организациите са работили дистанционно по време и след пандемията.

"Новото нормално" обаче не дойде без нова порция трудности. Кибернападателите насочиха вниманието си към отдалечените работници, които, намирайки се извън пределите на офисните мрежи, в повечето случаи се оказват значително по-уязвими. Занапред дистанционната работа ще продължи да доминира, както и свързаните с нея заплахи. Сред тях са фишинг атаките, уязвимите пароли, незащитените домашни устройства и др.

2. Заплахи при веригите за доставки

Киберпрестъпниците продължават да използват по-модерни и усъвършенствани техники, за да се насочват към отдалечени работници, и част от вниманието им е насочено към веригите за доставки (supply chain).

Станалият вече знаменит пробив в сигурността на SolarWinds от 2020 г., когато хакери успяха да проникнат в мрежите на компанията и тайно да променят

[*] Зайнуллин С.Б. Корпоративная безопасность, Макс Прес, Москва, 2016

кода в един от пакетите за актуализация на нейния софтуер, излагайки на риск хиляди организации, използващи нейния продукт, продължава да е показателен пример.

3. Рансъмуер атаки

Рансъмуерът е преобладаващ през 2022 г. и тази тенденция вероятно ще продължи. Подобно на атаките срещу отдалечените работещи, кампаниите с криптовируси се възползваха от хаоса по време на пандемията и продължават да предизвикват значителни главоболия, особено в сектори като този на здравеопазването.

У нас нашумял случай в тази посока бе криптирането на данни на "Български пощи", за което на държавната структура бе наложена санкция в размер на 1 млн. лв. от Комисията за защита на личните данни (КЗЛД). Актът бе за това, че дружеството "не е приложило подходящи технически и организационни мерки" преди и по време на кибератаката.

Този тип атаки станаха толкова печеливши, че се появиха готови за ползване пакети и дори услуги. Тоест нападателите могат да си платят за използване на код за рансъмуер, който да използват за провеждане на кампании.

4. Интернет на нещата

Към Интернет на нещата (IoT) могат да се причислят свързани с интернет устройства, различни от традиционните компютри, сървъри и смартфони. Много организации вече са възприели IoT технология, създавайки повече възможности за киберпрестъпления. Според Business Insider до 2026 г. по света ще има повече от 64 млрд. такива устройства.

Колкото повече IoT устройства има в една организация, толкова по-широки са възможностите за атаки. Тъй като тези продукти разполагат с по-малко изчислителни възможности, не е лесно в тях да се внедрят механизми за сигурност като защитни стени и скенери за защита от зловреден софтуер.

Престъпници вече са се възползвали от такива възможности. Затова неслучайно сферата на Интернет на нещата се обсъжда като един от възникващите проблеми пред корпоративната сигурност.

5. Облаци и свързани с тях заплахи

Облачните изчисления са една от най-революционните технологии, на които сме свидетели напоследък. Според PandaSecurity 48% от глобалните предприятия съхраняват своите данни в облаци. Очаква се, че до 2025 г. повече от 200 зетабайта ще се съхраняват в такива инсталации. Данните са ключов актив за всяко предприятие и затова не е учудващ повишеният интерес на киберпрестъпниците към облачните хранилища и услуги.

Неправилно конфигурираната облачна изчислителна инфраструктура е една от основните причини за заплахи в тази посока. Други причини са проблемите с миграцията, вътрешните рискове, отвличането на акаунти и несигурните интерфейси. С увеличеното възприемане на частни, публични и смесени облачни модели и големите количества данни, съхранявани в тези инсталации, не е трудно да се предвиди, че заплахите в тази насока ще се увеличават през 2023 г. и занапред.

6. Социално инженерство

Фишинг атаките не са нещо ново. Нападателите, използващи т.нар. социално инженерство, обаче възприемат хитри методи и техники за внедряване и изпълнение на тези атаки. И те са насочили вниманието си към отдалечените

работници, тъй като те са по-лесни мишени в сравнение с колегите им в корпоративните мрежи в офисите.

Например т.нар. китоловни атаки (whailing attacks), насочени към изпълнителни директори и лидери на организации, са сравнително нова форма на социално инженерство. Друга новост в сферата е "смишинг" тактиката (Smishing - комбинация SMS и фишинг). При нея се използват SMS или приложения за обмяна на бързи съобщения за подмамване на потребители да изтеглят прикачен файл или да кликнат върху зловредна връзка.[*]

Глобализацията промени структурата и темпото на ковпоративния живот. Насищането на традиционните пазари, отвежда компаниите на по-рискови места. Нови безнис практики като офшоринг, предизвикват компаниите да управляват бизнеса си от разстояние.

Паралелно с тези промени и рисковете за сигурността на компаниите станаха по-сложни. Много от заплахите като тероризъм, организирана престъпност и информационна сигурност са все по-трудни за управление. В резултата на това корпоративната сигурност има много по-голямо значение в корпоративния свят днес, отколкото преди години.

Компаниите търсят нови ефективни методи за упрявление на съществуващите рискове и заплахи. От мениджърите по корпотаривна сигурност също се изисква да подобрят своите умения, за да управляват качествено този свят без граници в днешни дни.

ЛИТЕРАТУРА

[1] Слатински, Н. Същност, смисъл и съдържание на сигурността. Военно издателство ЕООД. 2011;

[2] Зайнуллин С.Б., Сорокин Н.Д. Особенности корпоративной безопасности российских предприятий // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №6 (2017) https://naukovedenie.ru/PDF/140EVN617.pdf

[3] Бахчеванов, Г., Система за национална сигурност, стр.346-359. В: Национална и международна сигурност.

[4] Сандев, Г. Сигурност на организациите.УИ “Епископ Константин Преславски“. Шумен. 2012.

[5] Казаков, К. Управление на системата за защита на националната сигурност. Информация и сигурност. Първо издание. София. 2016.

[6] Асенов, Б. Теория на разузнаването и контраразузнаването. ВСУ „Черноризец Храбър“, Варна. 2008.

[*] https://digitalk.bg/security/2022/10/17/4403862_tendenciite_v_sigurnostta_prez_2023_g_i_svurzanite_s/

МРЕЖОВА ЗАЩИТА

Димитър Р. Илиев

NETWORK PROTECTION

Dimitar R. Iliev

ABSTRACT: *Network security threats are frequent and serious these days, and the need for methods to prevent them is enormous. Cryptography plays a major role in Internet security. The coding and decoding of information, with the aim of preventing unauthorized access to it, is the basis of this science. There are two types of threats – external and internal – and their implications are examined, as well as the effectiveness of passwords and their requirements. Also, network administrators are tasked with always being prepared and aware of the latest technological innovations in the field of network security to protect the network from attacks and security breaches. The reason is that attacks are also evolving and becoming more sophisticated and difficult to prevent. Various companies and organizations actively care about the safety of confidential information.*

KEYWORDS: *Threats, security, attacks, passwords, cryptography.*

Увод

Мрежовата защита е от ключово значение за съвременните комуникации и бизнес. Често се случват проникването в мрежите на големи бизнес организации, атаки от вируси, и хакерски атаки. Интересът към сигурността, е валиден както от администратори на големи корпоративни мрежи, така и от обикновения потребител на интернет услуги. Ще бъдат разгледани случаите, когато трябва да се открият рискове за сигурността, и да бъдат приложени методи за справяне с тях. Благодарение на криптографията, се постига опазване на ценна информация от нарушители. Кодираните данни могат да бъдат декодирани само от получателя, като за очите на другите хора кодираната информация е неразбираема.

Криптография

Криптографията променя дадена информация във вид, в който не може да бъде разбрана от никой. В последствие, неразбираемата информация се преобразува в разбираем вид, така както е била в началото. Примери са банкови карти, пароли и имейли. Работи с шифър, който представлява код, който преобразува разбираемите данни в неразбираеми, с цел да опази информацията от неоторизирани индивиди. Използва се и ключ, който е известен единствено и само на изпращача и получателя. Криптирането кодира информацията, за да я защити когато се изпраща по Интернет или между устройства като мобилни телефони например. Кодирането и декодирането на информацията става с помощта на

ключа и шифъра. Назначени са дивизии, които използват криптографските методики за разгадаване целите на врага по време на война.

Видовете заплахи за сигурността са два вида-външни и вътрешни. При външните заплахи е характерно те да са свързани с хакерски атаки, които са или за забавление, или е платено на хакер да извърши атака.

Пробиви в сигурността са:

-непозволено използване на пароли и ключове;

Паролата е последователност от букви, цифри и/или символи, и е нужна за разпознаването на потребителя в системата.

Ключът е букви или шифър и се ползва за автентикация в системата.

Двата метода са ефективни в случай че само потребителят ги знае. В противен случай се открива риск за сигурността.

Хакерите имат множество методи за придобиване на пароли-чрез социален инженеринг(когато хакера се представя за техник, администратор и др.), чрез атака на грубата сила, където се използва софтуер за отгатване на пароли, който проверява всички възможни пароли, докато стигне до истинската.

-атаки Denial of Service(отказ на услуга-DOS);

DoS атаките спират достъпа на потребителя до мрежата, като пренасищат мрежата с ненужни пакети.

-вируси и червеи;

Компютърните вируси се разпространяват като копират кода си в други програми, неизвестни на потребителя. Едни извеждат на екрана съобщение, а други повреждат данни и файлове, което пречи на компютъра да стартира.

Червеят(Worm), се копира и премахва файлове от компютъра. Разпространява се чрез e-mail, като файлове или документи или HTML страници.

-Троянски кон;

Програмата се представя за друга, за да събере информация. Има Троянски кон, който изглежда като екран за влизане в системата и когато потребителя попълни данните, те отиват при първоизточника на програмата. В последствие, данните могат да се използват за неоторизирано влизане в системата.

Вътрешните заплахи, вторият вид заплахи, също са сериозни. Вътрешните рискове за сигурността, могат да доведат до множество проблеми. Причините за тях са няколко: шпионаж; недоволни служители; случайни пробиви.

Шпионаж

Корпоративният шпионаж е кражба на търговски тайни. Конкурентните фирми предлагат на служителите от целевата фирма възнаграждения за краденето на данни. Друг вариант е когато служител на една фирма бъде нает от друга такава с цел да споделя с първоначалната фирма тайните и информацията на новата организация. Трети вариант е когато шпионин на свободна практика открадне конфиденциалната информация, за да я продаде на търг, като може и да заплашва фирмата от която е откраднал данните, че срещу заплащане, няма да разкрие тайните. Добра идея за спирането на тези индивиди е наемането на професионалисти, които имат опит в предпазването на фирми от тях.

Недоволни служители

При този тип заплахи, настоящият или бивш служител, който е и технически грамотен, представлява проблем, защото може да си отмъсти за нещо, като изтрие хард дискове на фирмата или напълни мрежата на организацията с

вируси. За да бъде предотвратен този изход, се изтриват акаунтите на служителя и не му се позволява достъп до компютрите на фирмата.

Случайни пробиви

Те са дело на служители, с бегли технически познания или слаба подготовка.

Често биват изтривани важни файлове в опит да се реши даден проблем. Затова потребителите трябва да бъдат спирани, преди да изтрият или преместят системни файлове.

Пароли

Паролите трябва да са много силни, за да се предотврати отгатването им. Когато потребителите ги задават, трябва да спазват определени правила:

-паролите да не са лесни за отгатване думи или числа, които са тясно свързани с потребителски данни, фигуриращи в документи на потребителя;

-ако се използва методът на грубата сила за отгатване на пароли, е важно паролите да не съвпадат с думите от списъците на атакуващата програма. За да се избегне това е добре да се съчетаят думи с числа(good12);

-операционните системи разпознават големи и малки букви в паролите и е добре големите букви да са на случайни места, за да се избегне отгатването им (PaSsWOrd);

-когато паролата е лесна за запомняне от потребителя, не се налага тя да бъде записвана на листи;

-по-дългите пароли са по-трудни за отгатване и е добре да бъде постигнат баланс между дължината и умението на потребителя да запомни по-дългата парола, без да я записва на хартиен носител;

-честата промяна на паролата е необходима в дадени среди с по-голямо изискване за сигурност, като новата парола не трябва да напомня на старата. Например good25 и good29. Същевременно, трябва да има баланс, за да не се окаже паролата трудна за запомняне за потребителя и съответно да бъде написана на хартия-нещо, което се стремим да избегнем;

-администраторите поставят критерии за паролите, като минимална дължина, годност(водещо до периодична смяна на паролата) и история на паролите(за да не се повтарят паролите, които вече са използвани);

Заключение

Проблемът, свързан със заплахите за сигурността в днешни дни е актуален. Изброените атаки към мрежата и последиците от тях доказват, че е необходима адекватна методика за превенцията им.

ЛИТЕРАТУРА

[1] Компютърни мрежи – пълно ръководство по теория, изграждане и съвместна работа между мрежите-Дебра Литълджон Шиндър.

[2] Cryptographic Techniques от Университет Sun Yat-sen.

[3] Data Communications and Networking от Forouzan.

[4] Cryptographic communication and authentication от Paul Krzyzanowski.

ГЕОГРАФИЧЕСКИЕ АСПЕКТЫ РОССИЙСКО-УКРАИНСКОГО КОНФЛИКТА* (ДНЕПР)

Мирослав Н. Кацаров

GEOGRAPHICAL ASPECTS OF THE RUSSIAN-UKRAINIAN CONFLICT (DNIEPER RIVER)

Miroslav N. Katsarov

ABSTRACT: *The Russian-Ukrainian conflict is one of the most relevant events these days. In the article, it is considered from the point of view of the strategic characteristics of the geographical environment, which are extremely important in the conduct of hostilities. The geographical environment is formed by the natural geographical components - geographical position, relief, area, climate, waters, vegetation. The object of our attention is one of the largest rivers in Europe - the Dnieper, which has an extremely important and, in certain cases, decisive strategic importance in the conduct of hostilities by both parties involved in the conflict. The main characteristics of the river as a strategic geographical object are indicated and an analysis is made of the degree of its importance for the course of the conflict.*

KEYWORDS: *Russia, Ukraine, Dnieper River, conflict*

Введение

Любой отдельный военный конфликт можно рассматривать во многих аспектах. Учитывая тот факт, что любой вид боя ведется на определенной территории, географический аспект имеет первостепенное значение. Боевые действия в российско-украинском конфликте во многом зависят от стратегических характеристик географической среды, которая определяет стратегические свойства субъектов, действующих в этой среде.

Река Днепр является географическим объектом, имеющим стратегическое значение для хода боевых действий в конфликте. Его

* Российские власти определяют конфликт как «специальную военную операцию» и настаивают на использовании этого термина. Государственные СМИ говорят о событиях в основном как о «специальной военной операции». Китайские государственные СМИ используют термины «специальная военная операция» и «украинский кризис». Одни авторы говорят о вторжении как о «войне России против Украины», другие — используют термин «российско-украинская война» в более общем смысле для обозначения всего конфликта между странами с 2014 года. Также используется термин «российская агрессия против Украины» (в частности, в резолюциях ООН). В официальных документах Верховной рады говорится о «вооружённой агрессии Российской Федерации против государственного суверенитета Украины» (укр. збройна агресія Російської Федерації проти державного суверенітету України).

географические особенности делают его главным фактором, от которого во многом зависят стратегические действия сторон – России и Украины.

Географические характеристики реки Днепр

Днепр (белор. Дняпро, укр. Дніпро) - четвёртая по длине река Европы после Волги*, Дуная† и Урала‡, имеет самое длинное русло в границах Украины.[7][12]

Длина Днепра от истока до устья в естественном состоянии составляет 2201 км. - в пределах Украины - 1121 км., в пределах Белоруссии - 595 км. (115 км. находятся на пограничной территории Белоруссии и Украины), в пределах России - 485 км. Площадь водосборного бассейна - 504 000 км², из них в пределах Украины - 291 400 км². Средний расход воды в устье - 1670 м³/с. Уклон реки - 0,09 м/км. Днепр - равнинная река с медленным и спокойным течением. Имеет извилистое русло, образует рукава, перекаты, острова, протоки и отмели. Делится на три части: верхнее течение - от истока до Киева (1320 км.), среднее - от Киева до Запорожья (556 км.) и нижнее - от Запорожья до устья (325 км.).[1][7]

Направление течения несколько раз меняется: от истоков до Орши Днепр течёт на юго-запад, далее до Киева - прямо на юг, от Киева до Днепра - на юго-восток. В Запорожье идёт второй, более короткий (длиной 90 км.), направленный на юг отрезок реки. Далее, к своему лиману, она течёт в юго-западном направлении. Таким образом Днепр образует на территории Украины подобие большого лука, обращённого на восток, что вдвое увеличивает путь по Днепру из Центральной Украины к Чёрному морю: расстояние от Киева до устья Днепра по прямой линии - 450 км, по реке - 950 км. Ширина долины реки - до 18 км. Ширина поймы - до 12 км. Площадь дельты - 350 км².[6][10][12]

Верхнее и среднее течение

Днепр берёт начало в небольшом болоте Мшара на окраине болотистой местности, урочища Аксенинский мох, в лесном массиве Оковский лес на южном склоне Валдайской возвышенности, у села Бочарово Сычёвского района Смоленской области России. Со склонов Валдайской возвышенности стекают также Волга, Западная Двина, Ловать, Сясь и Молога. Впадает Днепр в Днепро-Бугский лиман Чёрного моря. В верхней части, в Дорогобуже, Днепр ещё маловоден и течёт среди лесистой равнины, его ширина - до 30 м. Питается в основном водами своего лесистого и болотистого правобережья. Ниже, от Дорогобужа к Орше, он течёт уже в западном направлении, расширяется до 40-120 м. и становится сплавным, а при высокой воде даже судоходным. Выше Орши Днепр пересекает девонские известняки, образуя небольшие Кобеляцкие пороги. От Орши до Киева река течёт прямо на юг и у Рогачёва выходит на Полесскую низменность, а от Лоева течёт уже по территории Украины. От Киева до города Днепра река Днепр проходит на пограничье Приднепровской возвышенности и Приднепровской низменности. Долина реки здесь отчётливо асимметричная: правые склоны крутые и высокие, левые - низкие и пологие. Правый берег возвышается на 100-150 м., он изрезан глубокими долинами и оврагами, образует живописный горный пейзаж. На таких Днепровских горах лежит Киев, а ниже, у Канева, на Чернечьей (Тарасовой) горе - расположена могила Тараса Шевченко. Левый берег низкий, песчаный, часто покрытый сосновым лесом, возвышается

* Волга – 3530 км.
† Дунай - 2850 км.
‡ Урал - 2428 км.

на восток широкими террасами. Долина реки широкая – 6-10 км., у Переяслава и Черкасс 15-18 км, ширина самой реки - 200-1200 м. Между городами Днепр и Запорожье река пересекает Украинский щит.[10][12]

Нижнее течение - устье

Ниже Запорожья Днепр входит в степную, сухую (300-400 мм осадков в год) равнину Причерноморской низменности и медленно течёт на юго-запад, к морю. Ниже сужения русла, у северного района Запорожья - Кичкаса, река делится на 2 ответвления, обтекающие большой и скалистый гранитный остров Хортица. Ширина долины Днепра в этом месте - 4 км., далее она расширяется до 20 км. Ниже правого притока - реки Базавлук - долина Днепра снова сужается, ширина поймы здесь 3-7 км., а при впадении в лиман - до 10 км. В городе Каховка оба берега реки высокие (около Никополя - 80 м.), от Каховки левый - низкий.

Ниже Каховки начинается устьевая часть Днепра. От Херсона река делится на рукава и образует большую дельту (350 км²) с множеством островцов и озёр. Около 2/3 дельты занимают плавни, 1/3 - вода.[10][12]

Днепр вливается в Днепровско-Бугский лиман несколькими мелкими устьями, важнейшие из них - Збуривское, Кизилмицкое и Бокач или Рвач. Углубление последнего позволяет морским теплоходам доходить до Херсона.

Водосборная площадь

Водный режим Днепра определяется хорошо выраженным весенним половодьем, низкой летней меженью с периодическими летними паводками, регулярным осенним повышением уровня воды и зимней меженью. Площадь бассейна Днепра - 504 000 км², из них в пределах Украины - 291 400 км². Доля площади водосбора реки на территории Украины - более 48 %. Верхняя часть бассейна Днепра расположена в районе чрезмерного и достаточного увлажнения (лесная зона), средняя — в районе неустойчивого (зона лесостепи на севере степи), а нижняя — в районе недостаточного увлажнения (зона степи). Питание Днепра смешанное. В верхней части бассейна преобладает снеговое питание (около 50 %), на дождевое и подземное приходится соответственно 20 и 30 %. Ниже, в пределах степной зоны, доля снегового питания возрастает до 85-90 %, подземного — уменьшается до 10-15 %, а дождевого почти нет. Около 80 % годового стока Днепра формируется в верхней части бассейна, где выпадает много осадков, а испарение маленькое. В частности, верхний Днепр с Березиной и Сожем даёт 35 % годовой массы воды, Припять - 26 % и Десна - 21 %. Средний годовой сток реки вблизи Киева — 43,4 млрд м³ (1370 м³/с), а в устье — 53,5 млрд м³ (1700 м³/с). Наибольший процент воды (55-57 % годового количества) стекает в Днепр в весенние месяцы (март-май), когда тают снега, наименьший - зимой (12 %); на лето (июнь-август) приходится 17-21 % годового стока, на осень (сентябрь-ноябрь) - 12-14 %. Отклонения от этих данных бывают довольно значительные, например, весенний сток воды в Киеве колеблется в разные годы от 46 до 78 %.[2]

Водный режим реки существенно изменяется после строительства каскада водохранилищ - Днепр превращается в ряд длинных искусственных озёр, отделённых плотинами и искусственными водопадами от природных отрезков реки; по обе стороны прорыты каналы с многочисленными шлюзами. Водохранилища выравнивают уровень воды в Днепре, а ниже плотин ледовый покров держится меньше. Их строительство нарушает экологическое равновесие, коренным образом изменяет условия водообмена. По сравнению с природными условиями, он замедляется в 14-30 раз.[1][2][4][8][10][12]

Притоки

Количество притоков Днепра невелико по сравнению с другими реками схожей величины. Их распределение по течению реки весьма неравномерно, больше всего притоков сосредоточено в части от истока до Киева. В бассейне Днепра протекает 15 380 малых рек или около 25 % от их общего количества на Украине. Суммарная их длина — 67 156 км. Из них рек протяжённостью менее 10 км. - 13 998 с суммарной протяжённостью 35 041 км.[2]

В верхней части, у города Дорогобуж, Днепр - это ещё небольшая речка. На территории Украины она становится уже значительно полноводнее, так как к этому моменту принимает свои наиболее крупные притоки. На белорусской территории: правостороннюю и многоводную Березину (длина - 613 км., величина стока - 24 530 км²) и левосторонний Сож (648 км. и 42 140 км²), на территории Украины - Припять (802 км. и 114 300 км²) и Десну (1187 км. и 88 840 км²) и небольшие притоки Тетерев и Ирпень. После впадения этих рек ширина Днепра доходит до 700 м., глубина - до 8 м. Расход воды (количество воды, которое протекает в реке за 1 секунду) возрастает с 45 м³, у Орши до 108 м³, у Рогачёва и 1380 м³ - возле Киева.[2]

Притоки, которые принимает Днепр в своём среднем течении, менее значительные, чем в верхнем, и существенно беднее водой. Правые притоки: Стугна, Рось и Тясмин - короткие, текут преимущественно узкими руслами, вырезанными в гранитном ложе. Левые, берущие начало в основном на Среднерусской возвышенности и пересекающие всю Приднепровскую низменность, длинные, широкие, с низкими берегами и террасами; это Трубеж, Супой, Сула (457 км., бассейн - 19 640 км²) с Удаем, Псёл (806 км. и 22 820 км²), Ворскла (421 км. и 21 400 км²) и Самара (391 км. и 23 180 км²). Но все они увеличивают количество воды в Днепре незначительно.[2]

Зимой Днепр замерзает обычно после 20-дневного периода, в течение которого удерживается температура ниже 0 °С. Замерзание начинается с севера, а вскрытие ледового покрова - с юга. Благодаря этому заторы льда и вызванные ими наводнения на Днепре случаются редко. Навигация на Днепре зависит от продолжительности весеннего ледохода и начала осеннего.

Политическая география

От истока до устья Днепр протекает по территории трёх государств: России, Белоруссии и Украины. Река и её притоки на отдельных участках служат естественной границей между странами. Они также орошают 12 густо заселённых областей, 1 - в России (Смоленская область), 3 - в Белоруссии (Витебская, Могилёвская, Гомельская область), 9 - на Украине (Черниговская, Киевская, Черкасская, Кировоградская, Полтавская, Днепропетровская, Запорожская, Херсонская и Николаевская область). На берегах реки расположены больших и малых городов, в том числе столица Украины - Киев.

Города России, стоящие на Днепре, от истока к устью: Верхнеднепровский, Дорогобуж, Смоленск.

Города Белоруссии, стоящие на Днепре, от истока к устью: Дубровно, Орша, Копысь, Шклов, Могилёв, Быхов, Рогачёв, Жлобин, Стрешин, Речица, Лоев, Комарин.

Города Украины, стоящие на Днепре, от истока к устью: Любеч, Вышгород, Киев, Козин, Украинка, Ржищев, Переяслав-Хмельницкий, Канев, Черкассы, Светловодск, Кременчуг, Горишние Плавни, Верхнеднепровск,

Каменское, Днепр, Запорожье, Васильевка, Днепрорудное, Энергодар, Никополь, Каменка-Днепровская, Нововоронцовка, Великая Лепетиха, Горностаевка, Берислав, Каховка, Таврийск, Новая Каховка, Днепряны, Алёшки, Херсон, Белозёрка, Голая Пристань.

Водохранилища, построенные вдоль реки Днепр, мосты через реку и построенные вдоль нее электростанции имеют непосредственное отношение к боевым действиям в российско-украинском конфликте и имеют стратегическое значение.

Потребности хозяйственного комплекса Украины определяет необходимость строительства большого количества водохранилищ и, соответственно, зарегулирования речного стока. Наибольшие водохранилища (Киевское, Каневское, Кременчугское, Каменское, Днепровское, Каховское) созданы на Днепре с 1930-е по 1970-е годы.[5]

Киевское водохранилище (объём 3,73 км³) - создано в 1964-1966 годах и является предпоследним из шести крупных водохранилищ на Днепре. Наибольшая его ширина составляет 12 км. Оно расположено по Днепру - от Вышгорода до с. Днепрово, по Припяти - от устья до г. Чернобыля и по Тетереву - от устья до с. Богданы. Площадь водохранилища превышает 922 км², протяжённость - около 110 км., наибольшая ширина - 12 км., в некоторых местах - до 3 км. Наибольшие глубины (до 15 м.) находятся у плотины. Разница в высоте используется Киевской ГЭС*.[1][3][9]

Каневское водохранилище (объём 2,63 км³) - покрывает площадь 675 км². Его длина составляет 123 км. при максимальной ширине 8 км. Наибольшая глубина составляет 21 м. У берегов Каневское водохранилище весьма мелкое. В него впадают реки Стугна и Трубеж. Наиболее крупными городами у Каневского водохранилища являются Киев (южные пригороды), Переяслав и Канев. Плотина водохранилища находится в 1 км. на северо-запад от центра Канева. При ней имеются гидроэлектростанция и шлюз. Плотина построена между 1972 и 1975 годами и является преимущественно крупной дамбой общей длиной в 16 км.[1][3][9]

Кременчугское водохранилище (объём 13,5 км³) - занимает площадь 2252 км². Его длина 149 км. при максимальной ширине 28 км. Наибольшая глубина водохранилища - 28 м. Средняя глубина 6 м. Это самое большое по площади водохранилище на Украине. Сооружённая между 1959 и 1961 годами плотина озера расположена 15 км. западнее Кременчуга, вблизи Светловодска, где находится крупная Кременчугская ГЭС. По верху плотины проходит автошоссе и железная дорога.[1][3][9]

Каменское водохранилище† (объём 2,45 км³) - занимает площадь размером в 567 км². Его длина составляет 114 км. при наибольшей ширине 8 км. В самом глубоком месте водоём насчитывает 16 м. Длина плотины составляет 7,2 км. Она расположена в западной части Каменского, на ней находится крупная Среднеднепровская ГЭС, построенная в 1964 году. В Каменское водохранилище впадают реки Ворскла, Псёл. Значимые города у Каменского водохранилища - Кременчуг, Каменское, Горишние Плавни и Верхнеднепровск.[1][3][9]

---

* Гидроэлектростаанция (ГЭС) — электростанция, использующая в качестве источника энергии движение водных масс в русловых водотоках и приливных движениях; вид гидротехнического сооружения. Гидроэлектростанции обычно строят на реках.

† До 2017 года – Днепродзержинское водохранилище

Днепровское водохранилище[*] (объём 3,3 км³) - площадь водохранилища при подпорном уровне составляет 410 км², объём 3,3 км³. Его длина составляет 129 км., максимальная ширина достигает 7 км., максимальная глубина - 53 м.). В него впадают реки: Самара, Орель, Мокрая Сура. После строительства Днепровской ГЭС и создания Днепровского водохранилища - удалось обеспечить условия судоходства на этом участке Днепра, так как гранитные пороги на протяжении десятков километров не давали возможности свободного судоходства вверх по течению Днепра от г. Запорожья. Создание водохранилища позволяет создать условия для сквозного судоходства по Днепру от его устья до Киева и выше.[1][3][9]

Каховское водохранилище (объём - 18,18 км³) - занимает площадь 2155 км². Длина водохранилища по оси составляет 230 км., максимальная ширина - до 25 км. Максимальная глубина водохранилища составляет 24 м. На Каховском водохранилище находится порт Никополь. Вдоль левого берега водохранилища проходит ветка железной дороги из Запорожья в Симферополь и Херсон. Расположено на территории Херсонской, Запорожской и Днепропетровской областей Украины. Введено в эксплуатацию в 1956 году. Гидроузел Каховской ГЭС. Водохранилище используется для сезонного и годового регулирования стока, а также для регулировки высоких и катастрофических наводнений при полном использовании рабочего и резервного объёмов. Каховское водохранилище — основной источник водоснабжения Юга Украины. Из него вода подается в Северо-Крымский, Каховский, канал Днепр - Кривой Рог, Верхнерогачинский канал, а также в системы водоснабжения рудников, предприятий, городов и посёлков Никополь-марганцевского промышленного комплекса, в ряд мелких орошающих систем прибрежных районов трёх областей. По времени создания Каховский гидроузел был вторым после ДнепроГЭС. Каховская ГЭС является последней - шестой ступенью в каскаде гидроэлектростанций на Днепре.[1][3][9][11]

Днепр очень важен для транспорта и экономики Украины: все водохранилища оборудованы большими шлюзами, позволяющими судам размерами до 270 х 18 метров иметь доступ к порту Киева и это создаёт транспортный коридор.

Северо-Крымский канал - в значительной мере снабжает водой полуостров Крым. В 2014 году перекрыт Украиной, в 2022 году разблокирован Россией.

Через Днепр наведено около пятидесяти переправ разного типа, в том числе более двадцати железнодорожных мостов. Транспортное сообщение осуществляется по плотинам Киевской, Каневской, Кременчугской, Среднеднепровской, Днепровской и Каховской гидроэлектростанций.

Стратегическое значение реки Днепр

Обе стороны конфликта стремятся сделать Днепр непреодолимой преградой для врага. При советской власти Днепр превращается из реки в цепь водохранилищ. Свои естественные очертания Днепр сохраняет только ниже Херсона.

[*] Другое имя – Запорожское водохранилище

Днепровские мосты

Разрушение мостов на реке сильно затрудняет действия воинских формирований. Возможная эвакуация солдат через реку становится затруднительной, а боевую технику вывести вообще не удастся. Речные теплоходы и лодки смогут перевозить через Днепр беженцев и войсковые подразделения с личным оружием. Для перевозки танков, самоходок, ракетных установок и т.д. требуются специальные танкодесантные корабли, которых нет ни на Днепре, ни в целом на Украине.

Каскад днепровских ГЭС и водохранилищ

На сегодняшний день Днепр пересекают 20 действующих мостов: 11 автомобильных (2 из них используются еще и для линий метро), 2 железнодорожных, 7 совмещенных автомобильно-железнодорожных мостов; 5 мостов проходят по плотинам ГЭС. В Киеве имеются в наличии 6 мостов. Московский (Северный) мост, мост Метро, мост Патона и Южный мост – автомобильные. При этом мосты Метро и Южный совмещены с путями соответственно красной и зеленой веток столичного метрополитена. Московский и Южный мосты – вантовые. То есть особо уязвимые. Дарницкий мост (мост Кирпы), построенный в 2011 году, - комбинированный. По нему проходят

железнодорожные пути от Киевского вокзала. Фактически это два отдельных моста, расположенные параллельно на небольшом расстоянии друг от друга. Чисто железнодорожный мост - Петровский. Используется для товарного сообщения и городской электрички. Это самый старый мост через Днепр, построенный в 1917 году. Подольско-Воскресенский мост - вечный киевский долгострой с 1993 года. Соединяет центральную часть города с Троещиной через Труханов остров. У моста отсутствует спряжение с постоянными дорогами, то есть по нему можно перебрасывать только отдельные машины.

Все мосты на Днепре построены на крутых холмах городов, на плотинах водохранилищ и многокилометровых грунтовых насыпях, вдающихся в водохранилища. *(Например, автомобильный и железнодорожный мост в Черкассах представляет собой грунтовую плотину длиной 10,5 км. на левом берегу, затем мост длиной 1174 м. и далее 900-метровую грунтовую плотину на правом берегу).*

В случае разрушения мостов через Днепр строительство понтонных переправ нереально. И Днепр станет непреодолимой преградой между Правобережьем и Левобережьем. Если рухнет Киевская дамба, то поток воды сначала уничтожит киевские городские мосты, а затем ринется вниз по течению Днепра и уничтожит все плотины и ГЭС.

Левобережье и правобережье - от границ Белоруссии до Черного моря река Днепр делит Украину примерно на две половины. Причем деление это не условное. Долгое время раздельно существовали два региона – Левобережье и Правобережье, мало связанные друг с другом.

Антоновский мост

Ключевым фактором успеха - прорыв российской армии из Крыма в Херсонскую область (штурмовые отряды вооруженных сил РФ уже в первые дни войны смогли продвинуться с полуострова на правый берег Днепра и захватить Херсон) - контроль над мостами, которые при наличии такого большого водного препятствия, как река Днепр, имеют стратегическое значение для скорости наступательных операций.

Через Днепр в Херсонской области есть всего три переправы: Антоновский автомобильный мост (или просто „Антоновский мост“) возле Херсона, Антоновский железнодорожный мост в 6 км. от него, а также дамба Каховского водохранилища в Новой Каховке - еще в 70 км.

Антоновский мост - стратегически важный мост, связывающий правый и левый берег Днепра в районе Херсона. Он самый большой и близкий к Херсону, поэтому считается ключевым. Этот мост был построен в 1985 году, имеет 31 опору, его ширина 25 м., а длина - 1366 м. Мост пересекает Днепр и его левый приток Конку.

Заключение

Река Днепр с ее географическими и гидрографическими характеристиками - шириной, глубиной, скоростью течения, характером дна и берегов прилегающей территории, наличием многочисленных гидросооружений, является ключевым природно-географическим фактором в ходе Российско-Украинского конфликта.

Река является крупной водной преградой и препятствием, в ряде случаев непреодолимым, для наступательных боевых действий, что определяется

главным образом ее шириной - нижнее течение Днепра представляет собой естественную преграду с шириной водного пути около 1000 м. Река при такой ширине замедляет темп наступления и смены огневых позиций. Различные гидротехнические сооружения – плотины, каналы, шлюзы, каскады и т. д. также могут серьезно затруднить переправу через реку.

Учитывая сложные форсирование реки, определяемый ее характеристиками, контроль над мостами через нее оказывается ключевым фактором исхода боевых действий в регионе.

ЛИТЕРАТУРА

[1] Водний фонд України: Штучні водойми — водосховища і ставки: Довідник (укр.) / Под ред. В. К. Хильчевского, В. В. Гребня. — К.: Интерпресс, 2014.

[2] Дегодюк Е. Г. Дегодюк С. Е. Малые реки бассейна Днепра. Эколого-техногенная безопасность Украины. М.: ЭКМО, 2006.

[3] Электроэнергетика. Строители России. XX век. М.: Мастер, 2003.

[4] Энциклопедия истории Украины. Днепр. М.: Высшая школа, Т2, 2004.

[5] Кравчук П. А. Рекорды природы. Любешов: Эрудит, 1993.

[6] Пазинич В. Г. Геоморфологічний літопис Великого Дніпра (укр.). — Прилуки: Гідромас, 2007.

[7] Поспелов Е. М. Днепр. Географические названия мира. Топонимический словарь. (отв. ред. Р. А. Агеева), 2-е изд. М.: Русские словари; Астрель, 2002.

[8] Ресурсы поверхностных вод СССР: Гидрологическая изученность. Т. 5. Белоруссия и Верхнее Поднепровье / под ред. Н. Д. Шек. — Л.: Гидрометеоиздат, 1963.

[9] Статистичний збірник «Україна 2019». 2020.

[10] Хильчевский В. К., Ромась Н. И., Ромась И. Н. и др. Гидролого-гидрохимическая характеристика минимального стока рек бассейна Днепра / Под. ред. В. К. Хильчевского. — К.: Ника-Центр, 2007.

[11] Яцык А. В. Экологические основы рационального водопользования. — К.: Генеза, 1997.

[12] Яцик А. В., Яковлєв Є. О., Осадчук В. О. Коротка історія освоєння Дніпра, К.: Оріяни, 2002.

ЕЛЕКТРОННИ РЕСУРСИ

[1] http://www.city.kherson.ua/ Официальный сайт города Херсона

[2] https://kyivcity.gov.ua/ Официальный сайт города Киева

[3] https://mev.gov.ua/ Министерство энергетики Украины

[4] http://bse.sci-lib.com/ Большая Советская Энциклопедия (БСЭ)

[5] https://textual.ru/gvr/ Государственный водный реестр России

[6] http://geoman.ru/books/ Короткая географическая энциклопедия

[7] http://vsereki.ru/atlanticheskij-okean/bassejn-chyornogo-morya/dnepr Все реки. Информационный сайт о реках России

[8] https://www.ukrstat.gov.ua./ Державная служба статистики Украины
[9] https://www.rada.gov.ua/ Верховная рада Украины
[10] https://rosstat.gov.ru/ Федеральная служба государственной статистики
[11] http://minenergo.gov.ru/ Министерство энергетики Российской Федерации
[12] https://uhistory.ru/

COUNTERMEASURES FOR PROTECTION OF INFORMATION IN THE COMPUTER SYSTEMS

Veselin Kr. Raynov, Ilko Sr. Marev, Svetlin E. Stefanov

ABSTRACT: *In this paper a comparative analysis of protection of information in the computer systems is presented.*

KEYWORDS: *Computer systems, Exploit, Information, Protection, Vulnerability.*

Introduction

The term information is definitely related to receiving information, but not information at all, but information that informs for new, until now unknown things. And in this line of thought, it quite intuitively uses the term information when it put into the meaning of acquiring new knowledge, and not simply of receiving some information through a given message.

In the context of the present scientific paper, by information it will understand information about facts, events, processes and phenomena, about states of objects with their properties and characteristics, distributed during direct communication between people, transmitted, processed and stored using relevant technical means. At the same time, the specific semantic content of this information will not be the subject of analysis or discussion in this paper.

There has always been, exists and will exist in the future information that is not for distribution and which is carefully guarded. Such information is subject to collateral interest and an existing desire for unregulated access to it with a view to unlawful and malicious use, or for its destruction, modification, etc. This also defines the basic essence of information protection as a set of methods, means and practices to prevent illegal, unregulated access to certain information with a view to ensuring the necessary level of information security [4],[5],[6],[7].

Information protection theory and practice

There are at least two things that relate to the importance of information protection theory and practice:

- Information without exaggeration can be referred to as one of the crucial resources for development and is among the main sources of economic power of the state.

- As a result of the scientific and technical revolution, a unique branch of the national economy arose and is developing - the information industry, and the development of all other branches of the economy and the social sphere depends on it to a greater extent in conditions of continuous provision of new technological opportunities for unauthorized access to certain information resources [3],[4,],[7],[8].

Nowadays, it is unthinkable that any sphere of human activity can exist and develop without the use of modern information technologies. Therefore, it is not surprising that in many areas the costs of storing, transmitting and processing

information exceed the costs associated with energy consumption. Today, the information processing industry plays for the development of countries the role that heavy industry played at the stage of industrialization. The efficiency of using active information resources increasingly determines the development of society as a whole.

In this scientific paper, the term information system is widely used [9],[10],[11],[12],[13]. In a narrow sense, such a system means a computer system or computer network through which information is processed and exchanged. There is also another, more general idea of the essence of the concept of an information system in the sense of an organized set of devices for receiving, transmitting, processing, storing and displaying information. In the paper, the understanding of an information system has been expanded even further, as under an information system it will understand, along with the above, the person - source and user of information. In this line of thinking, even just two people talking to each other and exchanging information would constitute an information system for it, the information of which can be accessed by unauthorized persons using appropriate technical devices.

The phrase information protection is directly related to information security. Information security, like any security, has, apart from everything else, its psychological dimension, which is related to the feeling of the absence of realizable threats. Along with that, information security is the result of certain actions that protect information in an information system. Information protection can be described by three main characteristics [3],[4],[5],[6],[7],[8]:

- Confidentiality (secrecy) - in general, these are the activities regarding the control over a person or group of persons who use certain information, in order to avoid its unregulated dissemination;

- Integrity, which means that the information and the system that processes and stores it is always maintained over time in a condition that allows their use. This requires that the information is valid, accurate, authentic, not altered or deleted in the process of storage [6], use or transmission.

- Availability - information is considered available if each of its users has real-time access to it, provided that they have the appropriate authorization.

The above-mentioned characteristics have different weights depending on the specifics of the information. It is obvious that when it comes to information related to national security, the defense of the country, etc., a particularly important characteristic of protection is its secrecy - confidentiality. When running a business, the most important thing is probably the availability.

The construction of the relevant information protection system is directly related to vulnerability and possible threats to information resources [10],[11],[12],[13].

Vulnerability means the points, i.e. the places in a given information system that are its weak points, as a result of which they are susceptible to cyber attacks [3],[4],[5],[6],[7].

A threat is the possible danger that a person, certain objects or possible events may pose to the security of information in a given computer system.

Countermeasures are techniques to protect information systems from any threats.

The following types of vulnerabilities exist:

- Physical vulnerability – it is meant that the elements of an information system, location objects, etc. are vulnerable to physical impact on them.

- Natural vulnerability – information systems are vulnerable to natural disasters and changes in working conditions.

- Hardware and software vulnerability – it is about damage to the technical devices of an information system and its software [3],[4],[5],[6],[7],[8].

- Media vulnerability – refers to information carriers, such as diskettes, flash drives, printouts, etc., which can be unintentionally acquired due to improper destruction, stolen, damaged by criminals or by natural disasters.

- Communication vulnerability – information is vulnerable when it is distributed over acoustic channels in the process of conducting conversations, when it is transmitted over different lines and channels for information exchange.

- Operational vulnerability – information that is processed, transmitted or stored with the help of technical devices during their operation can become accessible if relevant technical devices are built into these devices. Information can be retrieved during the operation of these devices, during their repair or after scrapping.

In general, threats form two main groups: accidental - unintentional and intentional - intended threats. Unintentional threats include threats that originate from incompetent or insufficiently qualified users of information systems. Losses of information due to incompetence or carelessness are many times more than losses caused by external influences.

Countermeasures combine methods to protect information systems and the information processed, transmitted and stored in them.

The development and use of modern information protection methods require continuous improvement of the forms and methods of preventing threats to information resources. This requires [3],[4],[5],[6],[7],[8]:

- Development and continuous improvement of the normative-legal basis related to the development, implementation and use of information protection devices.

- Development of methods for building a system for monitoring the relevant information protection systems [1],[2].

- Solving the problems related to the management of information protection systems and the automation of this management [1],[2].

- Continuous research and analysis of world achievements and existing trends in the field of means and technologies to ensure information protection and determination of prospective directions for development.

- Development of a system of indicators characterizing the efficiency of functioning of information protection systems, as well as development of methods for evaluating the effectiveness of these systems.

- Creation of a system of bodies responsible for the protection of information.

- Development of methodological foundations for ensuring the protection of information.

- Development of methods to increase the motivation, moral-psychological stability and social protection of people who work with confidential information [1],[2].

- Development of civilized democratic forms and methods of influence on mass media.

- Development of methods for researching information means and systems put into operation with a view to preventing their possible use for unauthorized information access [3],[4],[5],[6],[7],[8],[9].

- Improvement of methods of control of personnel working with protected information systems.

- Development of national scientific research related to information protection and deployment of national production of means for information protection.

- Organizing and conducting training of specialists on information protection issues.

- Creation of theoretical and methodological foundations for ensuring information security.

Conclusion

An important task for every system administrator is to implement security mechanisms in order to transmit information securely and without problems in the respective local computer networks. Thanks to the knowledge of the nature of terms and concepts in information security, it creates prerequisites for proper handling and storage of different types of information.

REFERENCES

[1] Atanasov V., Ivanova A. A Framework for Measurement of Interactivity of Digital Learning Resources, 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 649-654, 2019, ISSN: 2623-8764.

[2] Atanasov V. RFC in approach model paradigm, International Journal on Information Technologies & Security, Union of Scientists in Bulgaria, № 4 (vol. 13), 2021, pp. 15-24, ISSN 1313-8251.

[3] Boyanov P. Implementation of protection mechanisms of information resources in the local area networks, Annual of Konstantin Preslavsky University of Shumen, Shumen, Konstantin Preslavsky University Press, ISSN 1311-834X, Vol. IX E, 2019, pp. 115-121.

[4] Boyanov P. Educational exploiting the information resources and invading the security mechanisms of the operating system Windows 7 with the exploit Eternalblue and backdoor Doublepulsar, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 14, 2018, pp.34-41.

[5] Hristov H., Boyanov P, Trifonov T. Approaches to Identify vulnerabilities in the Security System of the local Organization and Computer Resources. Journal Scientific and Applied Research Vol. 5, 2014, ISSN 1314-6289.

[6] Iliev, R., K. Ignatova. Cloud technologies for building data center system for defense and security. T. Tagarev et al. (eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies, Studies in Big Data 84,, ISBN 978-3-030-65721-5, Springer 2020, pp. 13-24, https://doi.org/10.1007/978-3-030-65722-2.

[7] Kazakov S., Trifonov T., Tzonev I. Probabilistic-temporal characteristics in a three level centralized computer structure, Proceedings of the 10-th Baltic-Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7, 2014, Liepaya, Latvia, Riga.

[8] Konstantinova E., Tsankov Ts. Analyzing security threats in smart homes technology. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 373-378.

[9] Lilov V., Konstantinova E., Tsankov Ts. Cyber intelligence in protecting organizations from malicious activity. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 386-392.

[10] Pavlova. D., Gindev, P. Designing an intelligent system for knowledge and process management in a university information environment. INTED2020 Proceedings. 14th International Technology, Education and Development Conference, Valencia, Spain, 2nd-4th March 2020, pp. 2743-2747. ISBN: 978-84-09-17939-8 doi: 10.21125/inted.2020.0818.

[11] Pavlova, D., Dzhelepov, V., Gindev, P., Effectiveness of information security in computer systems for object and process management. 13th International traveling seminar, Modern dimensions in European education and research area. Bulgarian-Austrian cultural dialogue, 26-31 May 2019, Sofia, “ZA BUKVITE – O Pismeneh” Publishing House, vol. 7, 2019, pp. 241-249. ISSN 2367-7988.

[12] Pavlova, D., Gindev, P., System synthesis approach for intelligent knowledge management. 13th International traveling seminar, Modern dimensions in European education and research area. Bulgarian-Austrian cultural dialogue, 26-31 May 2019, Sofia, “ZA BUKVITE – O Pismeneh” Publishing House, vol. 7, 2019, pp. 250-257. ISSN 2367-7988.

[13] Pavlova, D., Gindev, P., A System for Intelligent Electronic Management of Knowledge and Business Processes in a University Information Environment. Proceedings of Seventh National Seminar with international participation - Intellectual property and digital people, 24 April 2019, Sofia, “ZA BUKVITE – O Pismeneh” Publishing House, vol. 7, 2019, pp. 221-234. ISBN 978-619-185-379-3.

TECHNICAL DEVICES AND PROTECTION SYSTEMS

Veselin Kr. Raynov, Ilko Sr. Marev, Svetlin E. Stefanov

ABSTRACT: *In this paper a comparative analysis of technical devices and protection systems is presented.*

KEYWORDS: *Authorization, Analysis, Devices, Exploit, Information, Protection, System, Vulnerability.*

Introduction

The technical protection of information is the use of technical devices to prevent unauthorized information access in information systems during the processing, transmission and storage of information in them. In essence, it is a set of organizational and technical measures, devices and legal norms, which aim to protect these systems from harm.

In the practice, unauthorized information access represents an uncontrolled dissemination of information from the carrier and through the physical medium through which the information is disseminated to the technical devices with the help of which this information is intercepted.

There are the following main technical channels, through the connection of which leakage of information can take place:

- Obtaining acoustic - speech information using various types of listening devices.
- Acquiring acoustic information using laser and directional microphones.
- Use of emergent parasitic electromagnetic radiations to access processed and transmitted data during the operation of electronic devices and computer systems.
- Reliance on discarded technical media due to inoperability or unfitness: flash drives, diskettes, HDD and SSD disks, optical data carriers, etc.
- Receiving information distributed in mobile communication systems.
- Receiving information distributed in satellite radio communication systems.

Technical channels for information leakage

When electronic devices work [1], alternating electric currents flow through them. This is accompanied by the emission of electromagnetic energy into the surrounding space, which propagates as electromagnetic waves. These waves are known as parasitic electromagnetic waves. A large part of the currents flowing in the circuits of electronic devices – computer systems, communication equipment, etc., and along the corresponding wires and cables of telecommunication and computer networks, carries information [3],[4],[5],[6]. Therefore, the electromagnetic waves they excite are also information-carrying. By intercepting these broadcasts and after analyzing them, information can be obtained about both the processed and transmitted data.

The parasitic electromagnetic emissions during the operation of computer systems occur when: writing and reading information in or from the operating memory, displaying information on a screen, entering data from a keyboard, recording

information on magnetic media, reading information from magnetic media, transmitting information within the scope of a local network and on communication systems, printing the information [2].

The voice recorders are a convenient device of unauthorized access and recording of acoustic information. A recorder can be located at one of the participants of a specific meeting or installed in a given room when an interested person has unrestricted access to it. In a number of cases, it is possible for the recorder to be camouflaged under various objects: a pack of cigarettes, a box of writing instruments, a book, etc. Modern voice recorders provide continuous recording of speech information from 50 minutes to several hours. They have an automatic switch-on system according to the level of the acoustic signal [1],[7],[8],[9],[10]. Most of them can be controlled remotely.

Radio telephones are an easy target for intercepting the conversations that take place with them. The reason is that the exchange of information takes place in the radio range, which is available to everyone. For this purpose, it is enough to set the receiver to the carrier frequency of the wave on which the radiotelephone works and to the corresponding modulation mode of the signals [7],[8],[9],[10].

The GSM digital network is the most widely used today. The GSM (Group Special Mobile) standard was developed by the European Telecommunications Standard Institute. Until recently, GSM was considered to have a sufficiently powerful system to protect against eavesdropping and cloning. But there are a number of reports of cell phone cloning being done. It should be borne in mind that without immediate access to a given telephone, in the last case at least for a few hours, its cloning is impossible. There are no guarantees that this will remain so in the future.

GSM uses two types of connection. The first is used to connect and exchange information over the air between the mobile phone and the base radio station and second is used to connect the base station with the ATC via a wired channel. A characteristic feature of GSM is that the information that is distributed over the wired part of the network is not encrypted [2]. Therefore, the wiretapping here can be carried out using the methods typical for the wiretapping of telephone lines [2]. The radio communication system has two levels of protection of the transmitted information. The first level guarantees some degree of anonymity and authentication of the subscriber, implemented by the network authentication center. The second level of protection ensures the confidentiality of the conversation to a certain extent by using information encryption methods. Algorithms for authentication and coding of information guarantee a fairly high level of protection. Given what has been said about call interception systems in GSM networks, it is relatively complex. At the moment, there are both active and passive devices of interception on the radio channel of transmitted calls in a GSM environment. Active means are a complex that works as an active base station. A large number of GSM telephones allow them to be used to eavesdrop on conversations taking place in a given room. For this purpose, the corresponding device is activated, without its owner knowing about it, to work in such a remote mode. In this case, the GSM phone works as a radio eavesdropping device that uses the radio communication environment of the GSM network. When a telephone set is turned on, it periodically sends out signals [7],[8],[9],[10] that identify itself to the network to be potentially serviced. This allows the location and movement of the owner of the device to be determined.

During the operation of electronic devices, currents flow through their electrical circuits. A large part of these currents is information-bearing. It is known that when an

electric current flows along a given wire, an electromagnetic field is excited around it, which spreads in the surrounding space in the form of an electromagnetic wave. This electromagnetic wave has a frequency and spectrum like the frequency and spectrum of the electric current that excited it. This effect is known as the antenna effect. When used in radio transmission antennas, it is a useful antenna effect through which information [3],[4],[5],[6] is transmitted in radio communication systems. However, for the considered case of operation of electronic means, the antenna effect has a parasitic nature and it accompanies the functioning of the electronic equipment, and is also present in the transmission of information over cable and wire lines. It follows from what has been written that by intercepting the parasitic electromagnetic radiation during the operation of communication equipment or computer systems, unauthorized remote information access to the processed and transmitted information can be realized. Such access can also be realized by intercepting the electromagnetic fields that are excited around the communication cables and wires. Parasitic electromagnetic radiation induces high-frequency currents in the power supply network and in the wires of the various low-current installations such as telephone lines, network cables, etc. That is why the power supply network and low-current installations turn out to be carriers of information about the processed or transmitted data in computer systems and networks and on communication cables and wires. During the operation of a number of information devices, such as printing devices, faxes, keyboards, etc., acoustic waves are generated, some of which carry information [3],[4],[5],[6] about printed documents, text typed using the keyboard, etc. The interception and transmission of this information is also possible.

Conclusion

Today, most of the information that is obtained without authorization in business environments through technical means is obtained from radio microphones. There is a great variety of such means, both in terms of their technical implementation and in terms of their functional characteristics. Their practical application implies the presence of a corresponding radio receiver.

REFERENCES

[1] Boyanov Kr. P. et al., Equipment for evaluation of the characteristics of electronic-optic converters, Comptes rendus de l'Academie bulgare des Sciences, ISSN 1310–1331 (Print), ISSN 2367–5535 (Online), Vol. 70, No. 11, 5 December 2017, pp. 1575-1578, Scopus, Web of Science (Q4) - IF: 0.270 (2017), SJR: 0.210 (2017), SNIP: 0.332 (2017), CiteScore: 0.29 (2017).

[2] Iliev, R., K. Ignatova. Cloud technologies for building data center system for defense and security. T. Tagarev et al. (eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies, Studies in Big Data 84,, ISBN 978-3-030-65721-5, Springer 2020, pp. 13-24, https://doi.org/10.1007/978-3-030-65722-2.

[3] Pavlova. D., Gindev, P. Designing an intelligent system for knowledge and process management in a university information environment. INTED2020 Proceedings. 14th International Technology, Education and Development

Conference, Valencia, Spain, 2nd-4th March 2020, pp. 2743-2747. ISBN: 978-84-09-17939-8 doi: 10.21125/inted.2020.0818.

[4] Pavlova, D., Dzhelepov, V., Gindev, P., Effectiveness of information security in computer systems for object and process management. 13th International traveling seminar, Modern dimensions in European education and research area. Bulgarian-Austrian cultural dialogue, 26-31 May 2019, Sofia, "ZA BUKVITE – O Pismeneh" Publishing House, vol. 7, 2019, pp. 241-249. ISSN 2367-7988.

[5] Pavlova, D., Gindev, P., System synthesis approach for intelligent knowledge management. 13th International traveling seminar, Modern dimensions in European education and research area. Bulgarian-Austrian cultural dialogue, 26-31 May 2019, Sofia, "ZA BUKVITE – O Pismeneh" Publishing House, vol. 7, 2019, pp. 250-257. ISSN 2367-7988.

[6] Pavlova, D., Gindev, P., A System for Intelligent Electronic Management of Knowledge and Business Processes in a University Information Environment. Proceedings of Seventh National Seminar with international participation - Intellectual property and digital people, 24 April 2019, Sofia, "ZA BUKVITE – O Pismeneh" Publishing House, vol. 7, 2019, pp. 221-234. ISBN 978-619-185-379-3.

[7] Trifonov T. 2019, Modeling and Calculation of Passive Audio Crossovers, Annual of Konstantin Preslavski University of Shumen, Vol IX E Technical Sciences, ISSN 1311-834X, pp. 182-189.

[8] Tsankov Ts., Staneva L., Trifonov T. An algorithm for synthesis of phase manipulated signals with high structural complexity, Journal "Scientific and applied research", vol. 4, pp. 80-87, Shumen, 2013, ISSN 1314-6289.

[9] Tsankov Ts., Staneva L., Trifonov T. A survey of phase manipulated signals with high structural complexity and small loses after processing with mismatched filters, Journal "Scientific and applied research", vol. 4, pp. 88-97, Shumen, 2013, ISSN 1314-6289.

[10] Zhekov Zh., Antonov A., Boyanov P., Chervenkov D., Trifonov T. Method for Identification of signals. Journal Scientific and Applied Research Vol. 5, 2014, ISSN 1314-6289.

ГОДИШНИК

НА ШУМЕНСКИЯ УНИВЕРСИТЕТ

„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Т. XII Е

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

Университетско издателство

„Епископ Константин Преславски“

Шумен, 2022

ISSN 1311-834X (print)
ISSN 2815-4703 (online)