ГОДИШНИК

НА ШУМЕНСКИЯ УНИВЕРСИТЕТ

„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Т. XIII Е

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

ANNUAL

OF KONSTANTIN PRESLAVSKI

UNIVERSITY OF SHUMEN

Vol. XIII E

FACULTY OF TECHNICAL SCIENCES

Университетско издателство

„Епископ Константин Преславски“

Шумен, 2023

ISSN 1314-8818 (print)
ISSN 2815-4703 (online)

ГОДИШНИК

НА ШУМЕНСКИЯ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Т. XIII Е

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

ANNUAL

OF KONSTANTIN PRESLAVSKI
UNIVERSITY OF SHUMEN

Vol. XIII E

FACULTY OF TECHNICAL SCIENCES

Университетско издателство
„Епископ Константин Преславски“
Шумен, 2023

Настоящият годишник съдържа статии и студии за 2023 г. от Факултета по технически науки

РЕДАКЦИОННА КОЛЕГИЯ

ISSN 1314-8818 (print)
ISSN 2815-4703 (online)

СЪДЪРЖАНИЕ

ИЗГРАЖДАНЕ НА УСТОЙЧИВА И ЕФЕКТИВНА ВРЪЗКА МЕЖДУ ВИСШИТЕ УЧИЛИЩА И СЕКТОРА ЗА СИГУРНОСТ

Доника В. Диманова, Добринка П. Добрева

BUILDING A SUSTAINABLE AND EFFECTIVE RELATIONSHIP BETWEEN HIGHER SCHOOLS AND THE SECURITY SECTOR

Donika V. Dimanova, Dobrinka P. Dobreva

ABSTRACT: *In today's dynamic world, the importance of quality education has been recognized. Every country needs sufficient and well-trained human resources to enhance its national security. Therefore, it is of particular importance to build an effective connection between education - science - the labor market (business).*

KEYWORDS: *Education – science – the labor market, Security.*

Въведение

В днешния динамичен свят, е призната важността на качественото образование. Всяка държава се нуждае от добре обучени специалисти за повишаване на националната си сигурност. Поради това е от особено важно значение изграждането на ефективна връзка образование - наука - пазара на труда (бизнес).

На националната сигурност са присъщи специфични проблемни области: политически, икономически, социални, етнически, духовни, военни, информационни и екологични компоненти. Всеки от компонентите може да се окаже критичен за държавата, но всички те са зависими по един или друг начин от нивото на образование на човешките ресурси в тях [1]. Следователно, образованието трябва да дава подходящите компетенции във всеки аспект от националната сигурност.

Когато говорим за НС трябва да имаме предвид това, че сигурността не включва само отбраната, външната политика, охраната на обществения ред и защитата на законността. В нея се включва и сигурността и стабилността на гражданите, обществените и икономическите аспекти (като здравеопазване, образование, финансова и социална стабилност, екология и др.).

Националната сигурност е приоритетно направление, без осигуряване на което няма държавност. Целта е формиране на национална култура за сигурност, която да бъде естествена обществена основа за ефективно и пълноценно реализиране на политиките за сигурност.

В тази връзка, специалисти в тази област са необходими не само за отбраната и структурите на МВР, но и в държавната администрация, частните, гражданските и неправителствените организации, особено в мултиетнически и мултикултурни региони на страната.

За постигане и запазване на конкурентоспособна икономика и повишаване на жизнения стандарт на населението е необходимо да се насърчава заетостта на хората и да се повишава квалификацията им в приоритетните професионални направления и защитени специалности.

Основните моменти, които ще бъдат засегнати в доклада са:

1. Пазарът на труда и потребностите от специалисти с висше образование.

2. Стратегически значими професионални направления и реализация на пазара на труда.

3. Регионални измерения: недостиг на специалисти и значимост на висшите училища.

4. Сътрудничество между бизнеса и висшите училища.

Изложение

Пазарът на труда и потребности от специалисти с висше образование

През последните години се наблюдава трудно предвидима динамика на пазара на труда. Съществено се променят изискванията към необходимите за пазара на труда компетентности, продиктувани от технологичните промени и иновациите. Все по-често се наблюдава появата на нови професии и изчезването на традиционни такива. Наблюдава се търсене на професии, изискващи високи аналитични и социални умения, на нерутинни професии в сферата на обслужването и социалните грижи и др. [5].

Основните предизвикателства, свързани с ускоряващата се динамика на пазара на труда могат да се обобщят като [5]:

- Разминаване между потребностите на пазара на труда и получаваната във ВУ подготовка по отношение на знания, умения и компетентности.
- Необходимост от своевременно осъвременяване на учебните планове и програми с оглед на динамичния пазар на труда.
- Използване на гъвкави форми на обучение, включващи активното участие на представители на бизнеса.
- Осигуряване на висока квалификация на академичен състав.

От направено проучване през 2019 г. са установени секторите, в които се търсят на-много специалисти с висше образование. Топ 10 икономически дейности с най-голям брой на работни места за специалисти с висше образование (в хил. души) са показани в табл. 1 [2, 4].

Това определя повишаването на потребностите от специалисти с висше образование в секторите: Образование, Държавно управление, Хуманитарно здравеопазване, Строителство, Култура, спорт и развлечения.

В направление „Сигурност и отбрана“, обявения за учебните години (2018 и 2019) прием е запълнен на 100 %, като основен работодател е държавата. Това е направлението с най-висока реализация на завършилите висше образование и е желана от кандидат студентите.

Таблица 1. *Топ 10 икономически дейности за 2019 г.*

Сектор	Брой специалисти (хил. души)	Сектор	Брой специалисти (хил. души)
Държавно управление	145,2	Юридически, счетоводни, архитектурни и др.	43,5
Образование	120,4	Финансови и застрахователни дейности	42,9
Търговия	111,9	Информационни услуги и др.	38,5
Хуманно здравеопазване	59,4	Транспорт, складиране и съобщения	36,5
Строителство	45,6	Култура, спорт и развлечения	15,8

От табл. 2 е видно, че завършилите студенти в специалност „Национална сигурност“ в Шуменски университет имат 44,898 % регионална реализация и отрицателна безработица.

Данните се потвърждават и от Рейтинговата система на ВУ в България за 2023[1], представени на фиг. 1.

Като негативна тенденция, в търсенето на специалисти с висше образование в краткосрочен план, може да се посочи ефекта от COVID-19. По данни на МТСП, към 30.09.2020 г. е намаляло търсенето на специалисти с 20 хил. души.

В заключение може да се обобщи, че потребността от инвестиции във висше образование за изграждане на висококвалифицирани специалисти се увеличава. През последните години броят на завършилите висше образование по отделните професионални направления не отговаря напълно на потребностите на пазара на труда. Поради това са необходими целенасочени мерки, насочени към формирането на ключови умения и изграждането на висококвалифицирани специалисти в онези сфери, които са решаващи за социалноикономическото развитие на страната.

Стратегически значимите области на образованието

По данни от Рейтинговата система на Висшите училища в България[2] за 2023 г., най-висока степен на приложение на придобитото висше образование (над 90%) се наблюдава сред завършилите „Медицина“, „Стоматология“, „Фармация“ „Военно дело“ и „Теория и управление на образованието“, а най-ниска сред завършилите „Туризъм“ (26%).

Значителен дефицит на национално и регионално ниво се наблюдава в здравеопазването и образованието. Едни от причините за очакван недостиг от педагози на пазара на труда са застаряването на педагогическите кадри, по-малкия брой завършващи от нуждите на системата, завършилите не работят по специалността и др. Като причините за недостиг на медици на пазара на труда могат да се отбележат застаряването на медицинските кадри, по-малкия брой

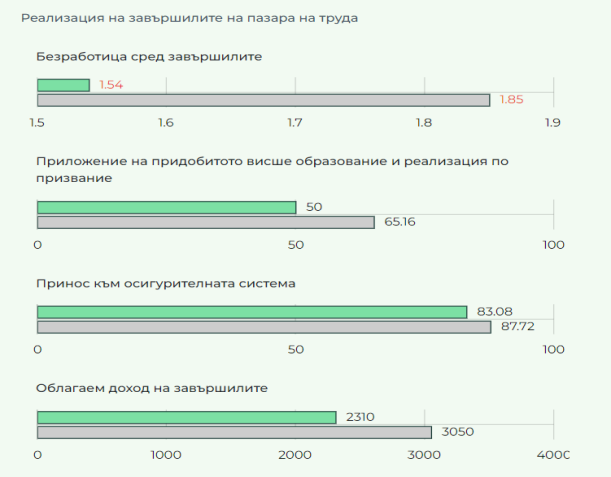
[1] https://rsvu.mon.bg/rsvu4/#/general-comparison

[2] https://rsvu.mon.bg/rsvu4/#/; https://rsvu.mon.bg/rsvu4/#/media-article/149

завършващи, трудова миграция на здравните специалисти към ЕС, ниски трудови възнаграждения и др.

Таблица 2. *Безработицата сред завършилите студенти в Шуменски университет и процента на регионална реализация*

Шуменски университет "Епископ Константин Преславски", 2019		
	Безработица сред завършилите	Регионална реализация
Администрация и управление	n/a	n/a
Архитектура, строителство и геодезия	-2,158	51,799
Биологически науки	-5,046	50,917
Икономика	-2,459	56,557
Информатика и компютърни науки	-3,52	52,174
История и археология	-4,167	47,222
Комуникационна и компютърна техника	-2,062	51,546
Математика	-2,326	55,814
Науки за земята	n/a	n/a
Национална сигурност	-2,041	44,898
Обществени комуникации и информационни науки	-4,327	52,404
Общо инженерство	-2,62	66,812
Педагогика	-3,191	65,525
Педагогика на обучението по ...	-3,325	45,719
Растителна защита	-4,53	48,084
Религия и теология	-2,041	32,653
Социални дейности	-1,559	52,561
Теория и управление на образованието	-3,409	57,955
Туризъм	-4,074	40,741
Физически науки	-4	49
Филология	-2,646	40,423
Химически науки	-4,762	48,98



Фиг. 1. *Реализация на пазара на труда на завършилите в ПН „Национална сигурност“ в ШУ спрямо средната стойност с страната*

Като стратегически значими се определят и специалистите, необходими за развитие на високотехнологични производства и интензивни на знания услуги. Това са „Природни науки, математика и информатика“, „Технически науки“ и „Изкуства“.

Като причини за очаквания недостиг от ИТ и технически специалисти може да се отчете развитието на високотехнологични производства, необходимостта от интензивни на знания услуги налагащи потребности от повече специалисти, малък процент завършили в посочените направления, част от завършилите в тези специалности работят на позиции не изискващи висше образование и др.

Относително популярни в България области на образованието, за които обаче е налице осезаема потребност от добре подготвени кадри в съответствие с установените международни стандарти са „Социални, стопански и правни науки“, „Хуманитарни науки“, „Аграрни науки и ветеринарна медицина“ и „Сигурност и отбрана“.

От изложеното до тук може да се направи извода, че политиката на държавата е насочена към подкрепа на направленията и специалностите, с цел преодоляване на дългосрочния дефицит на пазара на труда. В тази връзка е прието Постановление № 283/19 август 2021 г. на МС, в което е посочен Списък на професионални направления и защитени специалности по чл. 95, ал. 7, т. 8 от ЗВО.

Постановлението указва 8 ПН („Педагогика на обучението по…“, „Религия и теология“, „Математика“, „Физически науки“, „Химически науки“, „Химични технологии“, „Енергетика“, „Материали и материалознание“) и 18 защитени специалности, които са с най-висок бъдещ недостиг от специалисти на пазара на труда [3].

Регионални измерения: недостиг от специалисти и значимост на висшите училища

Все повече се повишава ролята на ВУ като активен фактор за регионално развитие. В тази връзка се активизира партньорството на ВУ с регионалните власти по отношение на интелигентната специализация и развитието на регионите. В това отношение ШУ отговаря за интегритета на обществото в изключително сложен мултиетнически и мултикултурен район.

Наличието на ВУ в региона и областта оказва влияние върху регионалната реализация на завършилите, привлича студенти, част от които остават в региона и задържа млади хора в региона. В резултат на това се преодолява недостига от специалисти с висше образование, повишава се конкурентоспособността, повишава се иновационната активност на местните предприятия на регионално ниво. Следователно може да се отчете положителното влияние на ШУ върху технологично развитие на региона и като социалноикономическия фактор.

Очакван недостиг от човешки ресурси с висше образование по райони за планиране (на база на фактическото и очакваното развитие на икономическите сектори) и на най-търсените професии в тях са посочени на фиг. 2 [2].

Фиг. 2. *Недостиг от човешки ресурси с висше образование по райони за планиране*

Сътрудничество между бизнеса и ВУ

През последните години бизнес организациите играят важна роля в процеса на обучение на студентите. Представителите на бизнеса участват в различни форми на сътрудничество с ВУ, като най-често това се изразява в провеждане на практики, стажове, изнесени обучения в реална работна среда и други форми на взаимодействие. Потребителите на кадри участват и при обсъждането на учебните планове и програми, практическата подготовка и кариерното ориентиране на студентите, изграждането и поддържането на научни инфраструктури и др.

Заключение

В заключение може да се обобщи, че за изграждането на ефективна връзка образование-наука-бизнес, както е заложено и в Стратегията за развитие на висшето образование в Република България за периода 2021-2030, е необходимо:

- Създаване на система за актуализиране на учебното съдържание в съответствие с новите постижения на науката и технологиите.
- Активизиране на партньорството на ВУ с работодателите и държавата в образователната дейност и продължаващото обучение.
- Активизиране на партньорството на ВУ с бизнеса и държавата в научните изследвания.

Преодоляването на дисбаланса между пазара на труда и висшето образование изисква промените в политиките в сферата на образованието да са съобразени с дългосрочните потребности и структурни проблеми на пазара на труда в България.

За ефективно справяне с основните социални предизвикателства и повишаване сигурността на гражданите може да се посочи Цифровата трансформация на България за периода 2020-2030. Цифровата трансформация, е предпоставка за цялостно преобразуване на процесите и моделите на функциониране на системите за защита на населението, на системите за защита на обекти от критичната инфраструктура на държавата, на системите за превенция на битовата престъпност, на системите за наблюдение на обекти за пребиваване на многобройна група от хора, на системите за пътна безопасност [6].

С развитието на цифровите технологии и тяхното влияние във всички сфери от нашия живот, се поражда необходимостта от подобряване на технологичните знания и цифровите умения на работната сила. Това се явява едно от най-важните предизвикателства пред системите за образование и обучение на всички нива [6]. Не случайно е заложено и като политика на страната ни за периода 2020-2030.

ЛИТЕРАТУРА

[1] Димитров П. Образованието като подсистема на системата за национална сигурност. https://postvai.com/publications/Doklad_EDU.pdf.

[2] Доклад „Изграждане на устойчива и ефективна връзка между ВУ и пазара на труда“ 2020. Прогнози за пазара на труда на МТСП; https://rsvu.mon.bg/rsvu4/#/documents.

[3] Постановление № 283 от 19 август 2021 г. за приемане на Списък на професионални направления и защитени специалности по чл. 95, ал. 7, т. 8 от ЗВО, МС, обн. ДВ. бр.70/24.08.2021 г.

[4] Рейтинговата система на Висшите училища в България, https://rsvu.mon.bg/rsvu4/#/.

[5] Стратегия за развитие на висшето образование в Република България за периода 2021 - 2030.

[6] Цифровата трансформация на България за периода 2020-2030, София 2020.

ЗЕЛЕН МАРКЕТИНГ – КРАТЪК РЕФЕРАТИВЕН ПРЕГЛЕД НА НЯКОИ ХАРАКТЕРИСТИКИ

Георги П. Георгиев, Светлозар П. Стоянов

GREEN MARKETING – A SHORT REVIEW OF CHARACTERISTICS

Georgi P. Georgiev, Svetlozar P. Stoyanov

ABSTRACT: *This article reviews the newest trends in green marketing and analyzes an example of statistical research regarding the willingness and acceptance of green products by customers.*

KEYWORDS: *Green marketing, Ecological products, Literature review, Trends in green marketing.*

Множество технологични и бизнес решения, използвани през XX в., причиняват вреда на глобалната екосистема и пораждат проблеми като замърсяване, намаляване на горите и зеленината, ерозия на почвата и изчезване на биоразнообразието [8, p. 64]. В съвремието нарастващата загриженост за околната среда, замърсяването ѝ и изменението на климата, представляват нови предизвикателства. Те подтикват бизнесите и организациите да търсят нови решения, и да разработват нови стратегии, като напр. зеления маркетинг, които биха помогнали за по-добро запазване на околната среда [17, p. 428]. За намаляване на отрицателното влияние върху околната среда са необходими нови екологични продукти и услуги. Последователното създаване на пазара за такива продукти и услуги включва използването на зеления маркетинг, повишаването на осведомеността на потребителите, относно екологичните предимства на тези нови продукти и услуги [5, p. 1265].

Независимо, че концепцията на зеления маркетинг се прилага все по-широко през последните десетилетия, все още има съществена необходимост от още повече академични научни изследвания в тази област [15, p. 300] и целенасочено приложение в практиката [27, p. 240]. Това подсказва, че съществува необходимост от още по-задълбочено анализиране на темата за зеления маркетинг, както на теоретично ниво, така и чрез изследване на практиката, допълвайки тази област с нови виждания и данни. Зеленият маркетинг не е само краткосрочна модна тенденция [5, p. 1279]. Твърди се, че зеленият маркетинг ще има значително влияние върху покупателните и консуматорски навици на потребителите в бъдеще [4, p. 40].

Целта на предложената тематика е да се проучат концептуалните рамки на зеления маркетинг; да се систематизират теоретични изследвания, относно

концепцията на зеления маркетинг; да се обобщят характеристиките на зеления маркетинг; да се анализира представеното, като пример, статистическо изследване.

В научната литература концепцията за зеления маркетинг се заражда още в края на 80-те и началото на 90-те години на XX в. [7, p. 58; 23, p. 20], но различните приложения на този подход започват да се развиват през първото десетилетие на XXI в. и в момента се считат за движеща сила на потреблението [32, p. 2]. Развитието на зеления маркетинг е анализирано от Бухари [2, p. 375], който твърди, че то се състои от три фази, всяка от които има относително отличителен ефект върху маркетинговата дисциплина и нейната роля в зелената перспектива. Този модел на развитие е изследван и от Пити [28, p. 132], когато анализира зеления маркетинг. Следователно зеленият маркетинг може да бъде разграничен в три основни фази:

• *Фаза 1: Екологичен зелен маркетинг* – Началото на екологичния зелен маркетинг е свързано със социални и екологични проблеми, възникващи през 60-те и началото на 70-те години. Формирал се е вследствие на осъзнаването, че ограничените природни ресурси, от които зависи цялото човечество, се използват нерационално в търговията и услугите. На тази фаза фокусът е върху екологичните проблеми, като замърсяване на въздуха, консумация на резервите от нефт, отпадъци от нефт и последствията от синтетични пестициди. Пити се аргументира, че във фазата на екологичния зелен маркетинг, публичните дейности се фокусират върху решаването на екологични проблеми. Според Катранджиев [18, p. 75], промените в потребителското поведение на тази фаза все още не са забележими, а маркетингът на екологично съдържание е насочен към намаляване на замърсяването, причинено от производствения процес на продуктите или услугите на компаниите. Независимо от това много производители не са склонни да инвестират в по-екологични решения за производство, тъй като това не е актуално за потребителите. Следователно може да се твърди, че екологичният маркетинг като подход към публикуване на екологично съдържание е ограничен, тъй като повечето внимание е отделено на компаниите и техните отговорности по отношение на екологичните проблеми;

• *Фаза 2: Зелен маркетинг* – Тази фаза на зеления маркетинг започва в края на 80-те години на XX в. В анализа на развитието на зеления маркетинг през 80-те и края на 90-те години на XX в., Гарг и Шарма [11, pp. 180 – 181] идентифицират фазата като съществена за еволюцията на зеления маркетинг. Големите природни бедствия, настъпили през този период имат отрицателни последици по света, подтикват потребителите да мислят за запазването на природата за бъдещите поколения. Бопалската катастрофа през 1984 г., идентифицирана като най-голямото химическо бедствие в световната история, Чернобилската катастрофа през 1986 г., разливането на петрол от танкера „Ексон Валдес“ през 1989 г. и дупката в озоновия слой, забелязана през 1995 г., са събитията, които предизвикват съществени промени в екологичните възприятия и поведението на потребителите. Изследването, проведено в Съединените американски щати (САЩ) през 1990 г. от Уйгур [37, p. 10], показва, че значителна част от потребителите (82%) са готови да платят 5% по-висока цена за по-екологосъобразни продукти. Следователно Пити [28, p. 135] идентифицира

фазата на зелен маркетинг като съществено значима за маркетинга, тъй като фокусът се пренася не само върху промишлените производства и вредите, причинени от тях, но и върху екологичното въздействие на продуктите, използвани у дома, като почистващи продукти, хартия, козметика. Така втората фаза на зеления маркетинг е изключително значима за основите на промените в потребителското поведение и за разширяването на пазара за екологосъобразни продукти;

• *Фаза 3: Устойчив зелен маркетинг* – През 1999 г. Фулър [10, p. 17] за пръв път дефинира термина „устойчив маркетинг“ като процес на планиране, изпълнение и контрол, ценообразуване и разпределение на продуктите съгласно три критерия: задоволяване на потребителските нужди, постигане на целите на организацията и развитие на целия процес със запазването на околната среда. Към края на XX в. Организацията на обединените нации (ООН) инициира няколко международни договора, вкл. Монреалският протокол от 1987 г., регулиращ използването на вещества, които разрушават озоновия слой. В тази посока държавите по света започват да приемат закони, които биха помогнали за защитата на околната среда и намаляване на замърсяването. Забелязват се промени в законодателството за защита на околната среда в Република Литва. Пити [28, p. 133] твърди, че по време на фазата на устойчивия зелен маркетинг започват да се разработват екологосъобразни продукти, а компаниите широко прилагат стратегии за зелен маркетинг, позиционирайки продуктите си като екологични и спомагащи за запазването на околната среда. Трандафилович [36, p. 265] отбелязва, че тези промени в маркетинга подтикват компаниите да се стремят да представят своите продукти като екологични, независимо дали техният продукт отговаря на изискванията. В контекста на нарастващото недоверие на хората към компаниите, през 2016 г. е въведен т.нар. Greenwashing Index, който определя дали компаниите манипулират потребителите, за да продават своите продукти като екологични. Следователно вероятно третата фаза на зеления маркетинг, т.е. устойчивият зелен маркетинг, продължава и до ден днешен, като държавите се опитват да контролират причинителите на проблемите с околната среда, а интересът на потребителите към екологичните продукти стимулира компаниите да създават такива продукти, както и да разпространяват неточна информация в стремеж към печалба.

Предвид широкия обхват от дейности, свързани със зеления маркетинг, е трудно да се даде еднозначна дефиниция за него. Тук са представени само три от дефинициите, възприети в научната литература:

• *Зеленият маркетинг* е усилие, полагано от компании, за да проектират, рекламират, определят цени и разпространяват продукти по начин, който насърчава защитата на околната среда [30, p. 1312];

• *Зеленият маркетинг* е нов фокус в бизнеса, стратегически маркетингов подход за сигурно постигане на възможността да се достигне до пазар, който се интересува от околната среда и здравето [16, p. 1609];

• *Зеленият маркетинг* е участие на организацията в стратегически, тактически и оперативни маркетингови дейности и процеси, насочени към създаване на продукти, които оставят минимален отпечатък върху околната среда [38, p. 4].

Според анализа на научна литература зеленият маркетинг е широко понятие, което съдържа разнообразни дейности, включително модификация на продукта и неговата опаковка, промени в производствения процес, както и приспособяване на рекламата към екологичните тенденции. На основата на производната концепция на зеления маркетинг може да се твърди, че той е цялостна стратегия, чието приложение се фокусира върху печеливша, но екологично безопасна дейност, насочена не само към удовлетворяване на потребителските желания, но и към повишаване на осведомеността на клиентите по отношение на околната среда и отговорното потребление, като целта е да се включат екологичните проблеми в традиционния маркетинг.

Независимо, че зеленият маркетинг включва различни дейности, първата от тях е модификацията на дизайна и опаковката на продукта [26, p. 5]. Дизайнерският процес предполага разработка на продукта така, че той да е екологосъобразен, производството му да не използва токсични съставки или други вредни вещества, които могат да влияят неблагоприятно върху околната среда. Следва да се използват по-здравословни материали, съдържащи естествени съставки и биоразградими и нетоксични химикали със съдържание, което може да се рециклира, а по време на производството на продукта и всички материали, и други ресурси трябва да се използват разумно, намалявайки екологичните вреди на продукта през целия му жизнен цикъл [19, p. 88].

Опаковката на продукта следва да съответства на концепцията 3R (reduce, reuse, recycle – намаляване, повторно използване, рециклиране) – да консумира колкото е възможно по-малко материали, да бъде с възможност за рециклиране и повторно използваема [13, p 27].

Поради проблемите с околната среда се налага разработването на нови продукти. Затова предприятията правят прегледи на съществуващите продукти, а в някои случаи, дори променят оценките, дизайна или производството на продуктите си [29, p. 10]. Целите на разработката на зелени продукти включват намаляване на консумацията на ресурси и намаляване на замърсяването, както и увеличаване на запазването на ограничените ресурси. Екологосъобразният продукт помага за поддържането и подобряването на природната среда, както и за запазването на енергия или ресурси, и намаляването на токсични вещества, които увеличават замърсяването. Практически пример е инициативата PlantBottle на Coca-Cola, която цели да ограничи последиците за околната среда, свързани с пластмасовите бутилки, чрез включването на материали, получени от растителни източници. PlantBottle съдържа до 30% материали от растителен произход, като захарна тръстика и меласа, които са възобновяеми ресурси и имат намален въглероден отпечатък в сравнение с конвенционалните пластмасови материали. Продуктът е в центъра на маркетинговия микс на зелените продукти и е съществения компонент на стратегията за зелен маркетинг. Независимо от това, трябва да се признае, че екологосъобразността не се ограничава само до създадения продукт, а включва всички негови елементи, като материалите, които се използват, производствения процес, опаковката на продукта и др. [24, p. 1044].

Зеленият маркетинг най-често се свързва с рекламни материали, насочени към потребностите на клиентите, които са запознати с проблемите на околната среда. Според Чанг зелената реклама включва информация за екологичните

ангажименти и усилията на компаниите да предадат тази информация на потребителите. Средствата за реклама включват уебсайтове, маркетингови материали, книги, връзки с обществеността, пряка маркетингова дейност, рекламни кампании, видеа и презентации, базирани на екологосъобразност [3, p. 22].

Съществено е рекламираният продукт да има реалистично въздействие. Напр. използването на създадения продукт да намали замърсяването на въздуха. След като такива ефекти се демонстрират и данните за предимствата на продукта са предоставени, като се посочат характеристиките на съответния продукт, следва да се обяснят техническите термини и да се докажат екологичните ползи. По този начин предоставената информация за продукта не нарушава материалните и моралните интереси на потребителите [14, p. 95].

За разлика от традиционните маркетингови практики, зеленият маркетинг взема предвид екологичното въздействие на стоките, услугите и методите за комуникация, използвани в маркетинговите кампании. Той активно съблюдава и намалява емисиите на въглерод и приема платформи, насочени към екологично съзнателното разпространение на съдържание. Зеленият маркетинг е ориентиран към развитието на устойчиво бъдеще. Той подчертава важността на признаването и приемането на значимите роли, които бизнесите и физическите лица играят в ефективната комуникация на стойността на екологичните продукти. Крайната цел е да се работи за бъдеще, в което и природните ресурси, и човешкото благосъстояние могат да просперират. В този контекст зеленият маркетинг приема холистичен подход, като разглежда бизнесите целокупно и изучава техните операции в цялостната верига на доставката, от разработката на продукта до разпространението (Табл. 1) [21, p. 361; 35, pp. 102 – 104].

Изследването на осведомеността и нагласите на потребителите, относно закупуването на зелени продукти е от значение, защото това помага за определяне на модела на поведение и вземане на решения при покупката на продукти [6, p. 402]. Увеличаването на знанието и осведомеността е от съществено значение за промяна в отношението, намеренията и поведението на потребителите към постигане на по-екологичен начин на живот. Предишни изследвания, относно намеренията за покупка на потребителите, са ги идентифицирали като ключови за прогнозиране на потребителското поведение [1, p. 117]. Статистическо проучване е проведено в Хашемитско кралство Йордания, чиято цел е определяне на влиянието на зеления маркетинг (екологична добавена стойност), зелените продукти (зелени сгради) и екологичните загриженост на йорданските потребители към покупката на зелени сгради [31, pp. 237 – 253]. Прочувването е избрано, тъй като може да бъде проведено и в Република България, за да се установят нагласите на потребителите тук.

За целта на изследването са били анкетирани потребители в столицата Аман, които може да се интересуват от закупуването на зелени сгради. Градът е избран поради високата плътност на населението и неговото разнообразие. Според Департамента за статистика (ДС), през 2021 г. в Аман живеят над 4 млн. души от общо 11-милионното население на Хашемитско кралство Йордания. За събиране на данни от жителите е използвана извадка, тъй като този метод може да се счита за евтин и удобен. Според Хеър и кол. [12, p. 20] обемът на извадката,

необходим за постигане на достоверност в статистическия анализ, е равен на 400 потребители. За намирането на тези потенциални лица за анкетиране, изследователите придобиват списък с електронни адреси на фирми за инженерингово изпълнение и техните съответни клиенти от различни професионални съсловни организации.

Таблица 1. *Особености на традиционния маркетинг и на зеления маркетинг*

Наименование	Традиционен маркетинг	Зелен маркетинг
Продукт	Продуктът и свойствата му се развиват според потребностите на клиентите	Продуктът и свойствата му се развиват така, че да се намали максимално вреда върху околната среда
Цена	Цените се базират върху стойността на продукта и възможностите на клиентите да я платят	Цените се базират върху стойността на продукта, включвайки цената за екологична разработка и възможностите на клиентите да я платят
Локация/ дистрибуция	Заводът производител трябва да има добра логистична система за дистрибуция до клиентите	Заводът производител и логистичната система трябва да създават възможно най-малко вредни емисии
Реклама	Комуникацията с клиентите е с цел те да се информират за продукта и да се изгради имидж на фирмата	Комуникацията с клиентите е с цел да ги информира за екологични продукти и да ги накара да имат предвид и екологичните фактори при покупка

На анкетираните участници са зададени въпроси, свързани с 3 основни критерия: добавена „зелена“ стойност, зелени продукти (в това изследване това са сгради) и загриженост за околната среда. Хипотезата на изследването е, че всеки от тези критерии влияе на избора на потребителите да купят екологични продукти:

• *добавена „зелена“ стойност:* добавената екологична стойност, която потребителят ще получи при покупка на зелен продукт. Тази променлива може да се измери като се изчислят положителните ефекти върху околната среда при покупка на екологичен продукт в сравнение с покупката на неекологичен продукт [22, p. 137];

• *зелени продукти (зелена сгради):* екологични сгради, които помагат на околната среда като намаляват отпадъка, консумират по-малко ресурси, използват рециклирани материали или такива, които могат да бъдат рециклирани в бъдеще и предоставят чист начин на живот, който е и здравословен и комфортен за потребителя. Тази променлива може да се изчисли като се пресметне до колко

тези продукти задоволяват потребността на клиенти за здравословен живот и намаляване на замърсяването [39, p. 185];

• *загриженост за околната среда:* убеждения и мисли на клиентите, които ги насочват към закупуването на екологични продукти и реалните причини за закупуването на зелени сгради. Тази променлива може да се измери като се изчисли доколко опазването на околната среда влияе на решението на потребителите [34, p. 51].

Извършва се експлораторен факторен анализ, за да се оцени валидността на променливите в изследването. Лахер [20, p. 4] посочва, че стойността на всеки фактор не трябва да е под 40%. Според Хеър и кол. [12, p. 23], при условие, че стойността на т.нар. критерий на *Кайзер – Майер – Олкин* е *0,5* или повече, използваните данни са подходящи и достатъчни, а т.нар. тест на *Бартлет* се използва, за да се установи дали корелационната матрица на променливите е нулева.

С цел да се определят границите на „ниски“, „умерени“ и „високи“ интервали е използвано следващото равенството [9, p. 127], за да се установят съответните класови интервали:

$$\text{Интервал на клас} = \frac{\text{Макс.клас} - \text{Мин.клас}}{\text{Брой нива}} = \frac{5-1}{3} = 1{,}33 \qquad (1)$$

Средната стойност за всяка подпроменлива на независимата променлива (зеленият маркетинг) е представена в Табл. 2. Тук най-високата стойност е за зелените продукти (зелени сгради), равна на *3,71*, докато най-ниската е за загрижеността за околната среда със стойност *3,45* [31, p. 244].

Таблица 2. *Нива на влияние на зеления маркетинг върху потребителите*

Наименование	Променливи	Средна стойност	Ниво
Независима променлива: зелен маркетинг		3,61	Средно
Подпроменливи	Добавена „зелена“ стойност	3,68	Високо
	„Зелени“ продукти (сгради)	3,71	Високо
	Загриженост за околната среда	3,45	Средно
Зависима променлива: отношение към зелени сгради в Хашемитско кралство Йордания		3,25	Средно
Модерираща променлива: осведоменост, относно зелени продукти		3,43	Средно

[Нивата се определят по следния начин: 1 – 2,33: ниско; 2,34 – 3,67: средно; 3,68 – 5: високо]

Според статистическия анализ общата относителна значимост на подпроменливите на зеления маркетинг е висока. Този резултат потвърждава тезата на Шукла [33, p. 7], в която се посочва, че зеленият маркетинг влияе на

отношението на потребителите към закупуването на зелени продукти. Поради това този резултат съответства на изказването на Маниатис [25, p. 228], който твърди, че зелените продукти могат да привлекат потребителите поради множество причини, като собствената съзнателност и загриженост за околната среда, икономическите ползи, които ще получат, надеждността и външния вид на продуктите.

Представената накратко и в най-общ план тематика предполага да се отбележи, че зеленият маркетинг възниква от необходимостта да се подчертаят екологичните проблеми в света (замърсяване на въздуха, отпадъци от нефт, излагане на синтетични пестициди). Чрез систематизирането на изследванията по концепцията на зеления маркетинг, той би могъл да се дефинира като цялостна бизнес стратегия, която се стреми да задоволява потребностите на клиентите по начин, който е печеливш и устойчив. Нейните дейности (производство на продукти, анализ на потребностите, реклама и др.) са насочени към намаляване на отрицателните екологични влияния и работа по устойчив начин, както и повишаване на осъзнаването на потребителите за значимостта на опазването на околната среда и отговорното потребление. Зеленият маркетинг подчертава екологично безопасни дейности, устойчивост, отговорно потребление.

Усилията на световни организации и държави да намалят вредните емисии, съчетани с нарастващото желание на потребители да закупуват екологични продукти ще даде възможност на предприемачи и фирми да интегрират значителен зелен маркетинг в развитието на продуктите и услугите си. Представеното статистическо проучване и подобни ще са в основата на разработването на бизнес стратегия при създаването на нов продукт или услуга.

ЛИТЕРАТУРА

[1] Al-Soluiman, R. K., Bataineh, A. Q., Al-Jabaly, S. M., Salhab, H. A. (2020). The impact of smartphone advergames characteristics on purchasing intentions: The mediating role of game involvement. Innovative Marketing, 16(3), 113 – 125.

[2] Bukhari, S. S. Green Marketing and its impact on consumer behavior. Eur. J. Bus. Manag. 2011, 3, 375 – 383.

[3] Chang, C. Feeling ambivalent about going green: Implications for green advertising processing. J. Advert. 2011, 40, 19 – 31.

[4] Chen, S., Chen, Y. An empirical analysis of green marketing—A case study of government's plastic reduction policy. Int. J. Bus. Manag. Econ. Rev. 2020, 3, 34 – 43.

[5] Dangelico, R. M., Vocalelli, D. "Green Marketing": An analysis of definitions, strategy steps, and tools through a systematic review of the literature. J. Clean. Prod. 2017, 165, 1263 – 1279.

[6] Dewindaru, D., Syukri, A., Maryono, R. A., Yunus, U. (2022). Millennial customer response on social-media marketing effort, brand image, and brand awareness of a conventional bank in Indonesia. Linguistics and Culture Review, 6(S1), 397 – 412.

[7] Domazet, I., Kovaˇcevi´c, M. The role of green marketing in achieving sustainable development. In Sustainable Growth and Development in Small Open Economies.

[8] Durmaz, Y., Yasar, H.V. Green Marketing and Benefits to Business. Bus. Manag. Stud. 2016, 2, 64 – 71.

[9] Fruned, J. E. (1982). Statistics: A first course. New Jersey: Prentice Hall Inc.

[10] Fuller, D Sustainable Marketing: Managerial-ecological Issues, 1999.

[11] Garg, S., Sharma, V. Green Marketing: An Emerging Approach to Sustainable Development. Int. J. Appl. Agric. Res. 2017, 12, 177 – 184.

[12] Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Tatham, R. L. (2010). Multivariate data analysis (7th ed.). New York: Pearson.

[13] Handayani, W., Prayogo, R. A. Green Consumerism: An Eco-Friendly Behaviour Form Through the Green Product Consumption and Green Marketing. Sinergi 2017, 7, 25 – 29.

[14] Hashem, T.N., Al-Rifai, N. A. The influence of applying green marketing mix by chemical industries companies in three Arab States in West Asia on consumer's mental image. Int. J. Bus. Soc. Sci. 2011, 2, 92 – 101.

[15] Hossain, A., Khan, M. Y. H. Green Marketing Mix Effect on Consumers Buying Decisions in Bangladesh. Mark. Manag. Innov. 2018, 4, 298 – 306.

[16] Jamal, F. N., Othman, N. A., Saleh, R. C., Chairunnisa, S. Green purchase intention: The power of success in green marketing promotion. Manag. Sci. Lett. 2021, 11, 1607 – 1620.

[17] Jamal, F. N., Othman, N. A., Saleh, R. C., Nurhanay, A. H., Rohmah, W. Evaluating Information Credibility Toward Green Marketing in Indonesia. J. Asian Financ. Econ. Bus. 2021б, 8, 427 – 438.

[18] Katrandjiev, H. Ecological marketing, green marketing, sustainable marketing: Synonyms or an evolution of ideas? Econ. Altern. 2016, 1, 71 – 82.

[19] Kotni, D. P. Problems & Prospects of Green Marketing. Int. J. Bus. Res. 2017, 4, 86 – 90.

[20] Laher, S. (2010). Using exploratory factor analysis in personality research: Best-practice recommendations. SA Journal of Industrial Psychology, 36(1), a873.

[21] Lahtinen, V., Dietrich, T., Rundle-Thiele, S. Long live the marketing mix. Testing the effectiveness of the commercial marketing mix in a social marketing context. J. Soc. Mark. 2020, 10, 357 – 375.

[22] Lin, J., Lobo, A., Leckie, C. (2017). The role of benefits and transparency in shaping consumers' green perceived value, self-brand connection and brand loyalty. Journal of Retailing and Consumer Services, 35, 133 – 141.

[23] Mahmoud, T. O. Green Marketing: A Marketing Mix concept. Int. J. Elect. Electron. Comput. 2019, 4, 20 – 26.

[24] Mahmoud, T. O., Ibrahim, S. B., Hasaballah, A. H. The Influence of Green Marketing Mix on Purchase Intention: The Mediation Role of Environmental Knowledge. Int. J. Sci. Eng. Res. 2017, 8, 1040 – 1048.

[25] Maniatis, P. (2016). Investigating factors influencing consumer decision-making while choosing green products. Journal of Cleaner Production, 132, 215 – 228. https://doi.org/10.1016/j. jclepro.2015.02.067.

[26] Nedumaran, G., Manida, M. Green Marketing on Customer Behaviour towards Usage of Green Products. Available online: https://ssrn.com/abstract=3551990.

[27] Papadas, K. K., Avlonitis, G. J., Carrigan, M. Green marketing orientation: Conceptualization, scale development and validation. J. Bus. Res. 2017, 80, 236 – 246.

[28] Peattie, K. Towards Sustainability: The Third Age of Green Marketing. Mark. Rev. 2001, 2, 129 – 146.

[29] Peattie, K., Belz, F. M. Sustainability marketing – An innovative conception of marketing. Mark. Rev. St. Gall. 2010, 27, 8 – 15.

[30] Polonsky, M. J. Transformative green marketing: Impediments and opportunities. J. Bus. Res. 2011, 64, 1311 – 1319.

[31] Sahioun A., Bataineh A., Abu-AlSondos I, Haddad H. (2023). The impact of green marketing on consumers' attitudes: A moderating role of green product awareness. Innovative Marketing, 19(3), 237 – 253.

[32] Shabbir, M. S., Sulaiman, M. B., Al-Kumaim, N. H., Mahmood, A., Abbas, M. Green Marketing Approaches and Their Impact on Consumer Behavior towards the Environment – A Study from the UAE. Sustainability 2020, 12, 8977.

[33] Shukla, S. (2021). Exploration of green marketing: A shift from traditional marketing to green marketing for sustainable environment. Proceeding of the Ancient Indian Wisdom Panacea for Sustainable Wellbeing Conference. https://www.researchgate. net/publication/354922140_ Exploration_of_Green_ Marketing_A_Shift_from_Traditional_Marketing_to_Green_Marketing_for_Su stainable_Environment_Introduction.

[34] Suki, N. M. (2013). Green awareness effects on consumers' purchasing decision: Some insights from Malaysia. International Journal of Asia Pacific Studies, 9(1), 49 – 63.

[35] Thabit, T. H., Raewf, M. B. The Evaluation of Marketing Mix Elements: A Case Study. Int. J. Soc. Sci. Educ. Stud. 2018, 4, 100 – 109.

[36] Trandafilovic, I., Mani´c, M., Blagojevi´c, A. History of Green Marketing: The Concept and Development. In Proceedings of the Sedmi Medunarodni Simpozijum o Upravljanju Prirodnim Resursima, Zaje˘car, Serbia, 31 May 2017, pp. 260 – 271.

[37] Uygur, E. M. Market – Driven Strategic Green Marketing within the New Sustainability Paradigm. In Proceedings of the Cambridge Business & Economics Conference, Cambridge, UK, 27 – 29 June 2011.

[38] Vilkaite-Vaitone, N., Skackauskiene, I., Díaz-Meneses, G. Measuring Green Marketing: Scale Development and Validation. Energies 2022, 15, 718.

[39] Wen, B., Musa, S., Onn, C., Ramesh, S., Liang, L., Wand, W., Ma, K. (2020). The role and contribution of green buildings on sustainable development goals. Building and Environment, 185, 107091.

ИНФОРМАЦИЯ ПОДЛЕЖАЩА НА ЗАЩИТА В БИЗНЕС ОРГАНИЗАЦИЯТА

Иван И. Кантарджиев

INFORMATION SUBJECT TO PROTECTION IN THE BUSINESS ORGANIZATION

Ivan I. Kantardzhiev

ABSTRACT: *The types of information in the business organization are considered - classified information, personal data, trade secret, confidential and public information. Guidelines for their protection are proposed.*

KEYWORDS: *Business information, Competitive Counterintelligence, Counterintelligence unit.*

Увод

Всяка бизнес организация от създаването и през цялото си съществуване създава и използва информация, която е основен актив за нейното съществуване, растеж и развитие. Всяко посегателство към бизнес организация (БО) започва с придобиване на информация. Поради това за всяка БО един от основните приоритети е защитата на собствената информация. За да се постигне високо ниво на защита е необходимо тя да бъде правилно организирана и управлявана.

Докато информационната дейност в държавните структури е регламентирана с необходимата нормативна база и е на високо ниво, то този проблем за БО не е достатъчно разглеждан. Това води до наличие на уязвимости в сигурността на БО и повишава риска от развитие на заплахите.

При проведено анкетно проучване на автора през 2022 г. в Североизточна България обхващащо 50 бизнес организации от Североизточна България от областите Шумен, Търговище, Разград, Силистра и Добрич на въпрос касаещ необходимостта от защита на активите на БО 28% от анкетираните ръководители посочват човешки ресурси, 47% материални активи и 25% нематериални активи. Това показва, че ръководителите на БО са в голямата част се насочват към защита на материалните активи, а само една четвърт към нематериалните, където попада и собствената информация на БО.

Целта на настоящата работа е да бъдат определени видовете информация в БО подлежащи на защита.

В работата се приемат следните ограничения:

— разглеждат се само бизнес организации извършващи производствена и търговска дейност;

— не се разглежда защитата на информация във финансови организации – банки, застрахователни компании и др. поради спецификата на тяхната дейност;

— не се разглежда детайлно класифицираната информация, т.к. дейностите свързани с нея са детайлно регламентирани в ЗЗКИ и подзаконовите нормативни актове.

1. Видове информация в БО и дейност на конкурентните структури по придобиването ѝ

В схемата по-долу е показано виждането на автора относно видовете информация в бизнес организацията и на какъв вид дейност от страна на конкурентни организации е обект тя.

Фиг. 1.1. *Класификация на дейността на разузнавателните структури по придобиване на информация*

Конкурентно разузнаване при извършване на своята дейност ползва общодостъпна информация за БО от публични източници. Шпионажът [1, 2] от друга страна е насочен към останалите видове информация. Той бива корпоративен и икономически. Обект на корпоративния шпионаж е конфиденциалната информация, търговската тайна и личните данни. В зависимост от вида на информацията, която се стреми да придобие той е отчасти неетична и отчасти противозаконна дейност извършвана от конкурентни стопански организации. Икономическият шпионаж е насочен към търговска тайна, личните данни и класифицирана информация.

Дейностите във връзка с осъществяване на конкурентно разузнаване, корпоративен и икономически шпионаж могат да бъдат извършвани както от разузнавателните структури на БО, така и от държавни разузнавателни структури.

Стремежът при осигуряването на необходимата информация за БО при извършване на тези дейности е да се извършва тайно, без знанието на ръководството на организацията и нейната служба за сигурност. Съществуват и изключения, като например ООН. От ООН са приети правила при извършване на

разузнаване с хора, според които използването на конспиративни подходи е недопустимо [3, 4].

Част от съществуващите видове информация в БО са обект на защита чрез законодателни актове от страна на държавата, като например Закон за защита на класифицираната информация (ЗЗКИ), Закон за защита на търговската тайна (ЗЗТТ), Закон за защита на конкуренцията (ЗЗК), Закон за защита на личните данни (ЗЗЛД). За частта от информацията, попадаща или не попадаща в обхвата на държавната регулация, която в същото време е обект на разузнавателните структури на конкурента, отговорен за опазването ѝ е самият собственик. Придобиването на същата дава реална възможност на конкурентите за реализиране на предимство или директно нанасяне на вреда на организацията. Като цяло възможните видове информация в БО могат да се разделят на следните видове: класифицирана информация, търговска тайна, лични данни, вътрешна информация за БО (конфиденциална) и публична информация.

Конфиденциалната информация не е търговска тайна, но не трябва да бъде общодостъпна. Свободния достъп до нея би могла да даде предимство на конкурентите и да доведе до нанасяне на щети на организацията.

Публичната информация е информация, която е общодостъпна и се разпространява свободно. Относно нея не се предприемат мерки за защита, но е необходимо същата да бъде прецизно разглеждана с цел недопускане попадането в нея на елементи от по-горе разгледаните други видове информация.

Противодействието на конкурентното разузнаване се осъществява от структурата за сигурност на бизнес организацията (ССБО), на корпоративния шпионаж от ССБО и компетентни държавни органи, а на икономическия шпионаж от държавните структури за контраразузнаване и компетентните държавни органи.

2. Видове информация в БО

Класифицираната информация е информация попадаща в обсега на Закон за защита на класифицираната информация и Правилник за прилагане на закона за защита на класифицираната информация (ППЗЗКИ).

Законът за защита на класифицираната информация съгласно чл. 1. (1) урежда обществените отношения, свързани със създаването, обработването и съхраняването на класифицирана информация, както и условията и реда за предоставяне на достъп до нея [5]. В ЗЗКИ и ППЗЗКИ ясно са регламентирани видовете класифицирана информация, как се извършва достъпа до нея, кой има право на достъп, длъжностните лица и органите осъществяващи контрол на дейността свързана с работата с класифицирана информация и т.н.

Личните данни са вид информация, чиято защита е определена чрез Закон за защита на личните данни и общ регламент относно защитата на данните: Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета на Европа от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО [6].

Понятието лични данни е дефинирано в чл. 4, т. 1 от Регламент (ЕС) 2016/679 [8], както следва: „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

Националните нормативни актове [7], третиращи проблема „защита на личните данни“ са:

— Закон за защита на личните данни – в сила от 01.01.2002 г.;

— Правилник за дейността на Комисията за защита на личните данни и нейната администрация – в сила от 10.02.2009 г.;

— Наредба № 1 от 7 февруари 2007 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. Издадена от Комисията за защита на личните данни. Обн., ДВ, бр. 25 от 23 март 2007 г.

Лични данни [9] е всяка информация, която се отнася до конкретен човек, ако с нея той може да бъде ясно идентифициран. Според практиката на Комисията за защита на личните данни, един човек например се идентифицира, когато са посочени трите му имена. Той обаче може да бъде идентифициран, дори ако е представен само с две имена, но тяхната уникалност позволява да се досетим за кого става въпрос. И в двата случая – както когато даден човек е ясно идентифициран, така и когато просто можем да се досетим кой е, т.е. е идентифицируем, е приложимо и законодателството за защита на личните данни.

Личните данни относно даден човек включват най-различна информация. Тя може да съдържа характеристики, свързани с физическата, физиологичната, генетичната, психическата, умствена, икономическа, културната или социална идентичност. Може да е снимка на лицето, поради което и видеонаблюдението попада в обхвата на защитата. Може да бъде дори данни за електронна поща или електронни съобщения, когато са свързани с конкретен човек или лесно може да се разкрие кой ги използва, респективно е участник в такава кореспонденция. Отнасящата се до даден човек информация се смята за лични данни и в случаите, в които са отразени публични аспекти от неговия живот. Така например лични данни са и записите от видеонаблюдение по улиците и площадите, разкрити подробности от личния живот в публикации в медиите, информацията в публичните регистри, съдържащи имена на упражняващите определени видове професии, управителите и собствениците на търговски дружества, собствениците на недвижими имоти и др. В тези случаи публичността на данните е поначало оправдана с основанията, предвидени в Регламента, но в случай на нарушения на изискванията при обработването на лични данни пак се носи отговорност. Лични данни представлява само информацията, която е записана и се съхранява на някакъв материален носител като хартия, магнитни носители и др. Не представляват лични данни възприетите от сетивата ни образи и знания, поради

което възприемането и предаването на информация от човек на човек не попада в обхвата на защитата на личните данни.

Тук е необходимо да се обърне особено внимание на това, че личните данни са такива само ако са записани на някакъв вид материален носител и че възприемането и предаването на информация от човек на човек не попада в обхвата на защитата на личните данни. Служителите на БО ежедневно възприемат и предават информация, особено в случаите, когато информацията е „интересна“ и ги представя като „много компетентни“ пред околните. При такъв вид обмен на информация, която нерядко съдържа лични данни, информация от личен характер и вътрешнофирмена информация, предоставя възможност същата да бъде придобита и използвана при подготвяне на посегателство срещу БО или придобиване на предимство от конкурентна БО.

Всеки бизнес притежава бази с данни, ноу-хау и друга важна информация за своите бизнес активности, градени и надграждани с години. Освен уникалния продукт или услуга, които компанията предлага, тази информация е “съкровищницата” на компанията, която е в основата и изгражда добрата търговска репутация и създава нейните конкурентни предимства. Най-общо казано, тази информация съставлява и е част от безценния актив, наречен “търговската тайна на компанията”[10].

Търговската тайна, за разлика от защитените обекти на интелектуалната собственост като търговските марки, патентите, промишлени образци не се ползва със същата специална закрила, поради което незаконното й разкриване или използване могат да причинят на компанията огромни щети. Затова всяка компания следва да създаде надеждни вътрешни механизми и да използва най-добрите практики, за да запази строго конфиденциални своята търговска, технологична информация и ноу-хау, които създават нейното конкурентно предимство.

Определения за търговска тайна се съдържат в два закона по българското право. Това са Закон за защита на търговската тайна (ЗЗТТ) [11] и Закон за защита на конкуренцията (ЗЗК) [12].

Според Директива (ЕС) 2016/943, въз основа на която е приет ЗЗТТ, определението за търговска тайна следва да бъде съставено така, че да обхваща ноу-хау, търговската информация и технологичната информация в случаите, когато са налице законен интерес те да бъдат запазени поверителни и основано на закона очакване за запазването на тази поверителност. Освен това такова ноу-хау или информация следва да се счита, че имат реална или потенциална търговска стойност, например когато тяхното незаконно придобиване, използване или разкриване може евентуално да навреди на интересите на законно контролиращото информацията лице, като уронва неговия научно-технически потенциал, стопански или финансови интереси, стратегически позиции или конкурентоспособност.

Определението за търговска тайна изключва несъществената информация и опита и уменията, придобити от служителите в нормалния процес на работата им, както и изключва информацията, която е общоизвестна или лесно достъпна за лица от средите, които обичайно се занимават с въпросния вид информация.

Според ЗЗТТ „търговска тайна“ е всяка търговска информация, ноу-хау и технологична информация, която отговаря едновременно на следните изисквания:

1. представлява тайна по такъв начин, че като цяло или в точната си конфигурация и съвкупност от елементи не е общоизвестна или леснодостъпна за лица от средите, които обичайно използват такъв вид информация;
2. има търговска стойност, поради тайния си характер;
3. по отношение на нея са предприети мерки за запазването ѝ в тайна, от лицето, което има контрол върху информацията.

Според пар. 1, т. 9 от Допълнителните разпоредби на ЗЗК „производствена или търговска тайна“ са факти, информация, решения и данни, свързани със стопанска дейност, чието запазване в тайна е в интерес на правоимащите, за което те са взели необходимите мерки.

От горните определения става видно, че те не си противоречат. Напротив, те се допълват. По-новото определение по ЗЗТТ възлага по-детайлни изисквания за това какво е търговската тайна, които трябва да бъдат съобразявани и при тълкуване на понятието по ЗЗК. Търговска тайна може да е всяка информация, която кумулативно отговаря на трите посочени изисквания по ЗЗТТ. Поради това във всеки случай трябва да се преценява дали информацията може да се квалифицира като търговска тайна и дали тя подлежи на защита съобразно ЗЗТТ и ЗЗК. Всъщност, смятам че това е въпрос, който търговецът трябва да поставя преди всичко превантивно още към момента на оценяване на дадена информация като ценна за бизнеса му и имаща важно икономическо значение. Ако информацията бъде оценена като такава, то търговецът трябва да предприеме незабавни юридически мерки за запазването ѝ в тайна. Ако такива мерки не са били предприети, то такава информация не може да бъде квалифицирана като търговска тайна, тъй като ще липсва един от трите елемента от определението по ЗЗТТ. Какви да бъдат тези юридически мерки е въпрос на правилна преценка във всяка конкретна ситуация, която трябва да се прецени съобразно спецификите на извършваната дейност от търговеца. В най-общ план обаче това може да са включване на клаузи в трудовите договори на работниците и служителите и в договорите за изработка (напр. на софтуерни продукти), сключване на допълнителни анекси към вече подписани договори, изричното издаване на заповедни или инструкции от работодателите и възложителите на работата, подписани и от изпълнителя на работата, с които се определя извършване на определени действия по повод на търговска тайна. Смисълът от тези документи е изричното определяне на това коя информация е търговска тайна и поемането на задължение за конфиденциалност от работника, служителя или изпълнителя на работата. Предприемането на тези мерки е условие за възможността за квалифициране на информацията като търговска тайна и осигуряване на бъдещата възможност тя да се ползва от защитата на ЗЗТТ и ЗЗК[13].

Информацията в БО представляваща търговска тайна е необходимо да бъде ясно, конкретно и точно определена от лицето имащо контрол върху нея, да бъде защитена посредством мерки и предварително зададени механизми и правила за нейната защита. В противен случай, клаузите в договорите със служителите на БО ще бъдат крайно недостатъчни, особено в случаите на

активни действия от страна на конкурентни организации при подготовка и извършване на посегателства срещу БО. Търговската тайна в БО е такава, тогава и само тогава, когато отговаря на трите изисквания съгласно ЗЗТТ.

Съществува и информация, която отнесена към конкретния момент не отговаря едновременно на трите изисквания на ЗЗТТ и не може да бъде квалифицирана като търговска тайна.

Конфиденциалната информация е информацията, която не е защитена от законите на страната, но по своята същност тя е достатъчно значима за БО. Придобиването ѝ от страна на конкурентни БО дава възможност за подготовка и реализация на посегателства, които да доведат до нанасяне на значими щети на организацията.

В тази категория попада информация основно информация, която на следващ етап предстои да бъде защитена като търговска тайна и информация, която не би могла да попадне по защитата на ЗЗТТ например, но е необходимо тя да бъде защитавана.

В първия случай това може да е информация за продукти на които предстои лицензиране, информация свързана с подготовка за иновативни разработки, т.е. на идеен етап, за която все още не са изпълнени трите изисквания на ЗЗТТ. Във втория случай това може да бъде информация относима към бъдещо взимане на управленски решения, която може да послужи за разкриване на предстоящи действия на ръководството на БО.

Публичната информация е общодостъпна и се разпространява свободно, поради това е необходимо тя да бъде контролирана. Това от една страна може да бъде информация разпространявана в различните видове медии, а от друга например да се съдържа в носители на информация определени като незначителни и към които контрола е занижен.

Ако публичната информация, която БО официално представя с цел реклама, изграждане на имидж и т.н. като ръководство, структура, услуги, продукти и други не бъде прецизно оценявана от гледна точка на защита на БО от посегателства, може да предостави възможности на конкурентното разузнаване на друга БО за получаване на значително предимство. Посредством анализ на такава информация разузнаването на конкурентна БО ще придобие представа относно текущото състояние на БО, посока и планове за бъдещо развитие, вероятните субекти с които БО ще влезе във финансови и търговски взаимоотношения. Това от своя страна ще даде възможност на конкурентна БО за подготовка и реализация на посегателства.

Предоставяната информация в медиите от структурите за връзки с обществеността на БО е необходимо да бъде прецизирана по съдържание и момент на представяне, т.к. наред с подобряване на авторитета може да подпомогне нанасянето на щети на БО.

Заключение

Задълбоченото познаване на всички аспекти свързани със защитата на информацията е задължително условие, което ще осигури съществуването и развитието на БО, както и изпълнението на поставените цели. [14]

За поддържането високо и устойчиво ниво на сигурност на БО е необходимо:

— детайлно познаване на нормите на законите защитаващи информацията в БО;

— задълбочено познаване на видовете информация от ръководителите на БО;

— изработване на механизми и процедури за работа с информация в БО;

— планиране и извършване на проактивни действия по защита на информацията в БО;

— извършване на постоянен мониторинг на действията по защита;

— периодично преразглеждане и усъвършенстване на механизмите и процедурите за работа, както и действията по защита на информацията в БО.

ЛИТЕРАТУРА

[1] Михайлов А. Наказателноправна уредба на шпионажа. Научен алманах, кн. 2 за 2002 г., стр. 96-103, ВСУ „Черноризец Храбър“.

[2] Михайлов А. Разследване на шпионство. Научен алманах, кн. 3 за 2003 г., стр. 75-89, ВСУ „Черноризец Храбър“.

[3] Михайлов, А. Разузнаване с хора в операции на ООН. София 2023 г., 172 стр., ISBN 978-619-7143-06-5.

[4] Михайлов А. Разузнаване с хора в операции за поддържане на мира на Организацията на обединените нации. 2023, Фондация „Институт за национална и международна сигурност“ (монография).

[5] Закон за защита на класифицираната информация (https://lex.bg/laws/ldoc/2135448577).

[6] http://bcnl.org/uploadfiles/documents/Naruchnik.pdf

[7] Великов И. Политиката по защита на личните данни в контекста на присъединяването на Република България към Шенген. В: Сборник научни трудове. Том първи. София, Фондация „Национална и международна сигурност“, 2012, с. 143 – 164.

[8] https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32016R0679#d1e1633-1-1

[9] http://bcnl.org/uploadfiles/documents/Naruchnik.pdf.

[10] https://www.tbmagazine.net/statia/kakvo-predstavlyava-trgovskata-taina-i-kak-mozhe-da-bde-zaschitena.html

[11] Закон за защита на търговската тайна, https://lex.bg/en/laws/ldoc/2137192307

[12] Закон за защита на конкуренцията, https://lex.bg/laws/ldoc/2135607845

[13] https://ivp.bg/news/targovskataina/

[14] Denev D., Konstantinova E. Main Issues in the Protection of Information in the system of National and Corporate Security. 2020, MATTEH 2020, Conference Proceedings, vol. 2, ISSN 1314-3921, pp. 110-115.

ПРИЛАГАНЕ НА СИСТЕМНИЯ ПОДХОД ПРИ УПРАВЛЕНИЕ НА МАТЕРИАЛНИ ПОТОЦИ В СИСТЕМАТА НА ПОЩЕНСКИТЕ УСЛУГИ

Анатоли Ж. Стоянов

APPLICATION OF THE SYSTEMS APPROACH IN THE MANAGEMENT OF MATERIAL FLOWS IN THE SYSTEM OF POSTAL SERVICES

Anatoli Zh. Stoyanov

ABSTRACT: *The purpose of the study is to systematize the main principles related to the implementation of the system approach in the management and control of material flows in the postal service system and to prove its advantage in the organization and management of production processes in this area.*

KEYWORDS: *System approach, Material flows, Postal services.*

Въведение

Организацията и управлението на материалните потоци е сложен и многообразен процес, съчетаващ в себе си икономически, технически, организационни и високоефективни решения. Съвременният оператор на пощенски услуги трябва да отговаря на съвременните равнища на техниката, технологиите и организацията на производство. В технологично управление на процесите се разработват концепции определящи логистичните цели, свързани със закупуването, производството, пласмента и отилизация на отпадъците. Принципно това формулира логистичните системи, които оказват непосредствено влияние на организаторските решения. Следователно поставените логистични цели трябва да решават проблеми свързани с организацията и управлението на производствени процеси в системата на пощенските услуги. Определяйки параметрите на материалните потоци, можем да определим тези характеристики, които са свързани с етапите на производствения процес и системата за складовото съхранение, гъвкавостта на доставките, използване на системите за планиране и др. [6]

Целта на изследването е да се систематизират основните принципни постановки, свързани с прилагане на системния подход при управление и контрол на материалните потоци в системата на пощенските услуги и да се докаже

неговото предимство при организация и управление на производствени процеси в тази сфера.

ОБЕКТЪТ на изследването е състоянието на система за контрол и управление на материалните потоци, като са дефинирани основните фактори влияещи на производствената програма в системата на пощенските услуги.

ПРЕДМЕТ на изследването са материалните потоци за организация и управление на технологичното производство, неговата организационна, технологична и икономическа характеристика гарантираща пощенските услуги, като гъвкава и последователна логистична система.

За изпълнение на поставената цел е необходимо да се решат следните **ОСНОВНИ ЗАДАЧИ**:

1. Да се проучи и анализира състоянието на проблема и възможностите за организация и управление на материалните потоци, като се дефинират правните и икономико-технологични показатели за локализация и намаляване на недостатъците при оценка на продукта.

2. Да се изследват и систематизират получените данни и сведения от прилагането на системния подход при организация и управление на материалните потоци да се дефинират основните показатели.

1. Организация и същност на системния подход към управлението на материалния поток:

Системният подход е методология за изучаване на обекти и процеси като системи, която включва изучаване на тяхната структура, връзки с технологичната среда, както и свойствата на елементите и техните взаимодействия.

При управлението на материалните потоци системният подход позволява да се организира ефективно управление на всички процеси и операции, свързани с движението на материални активи. Това обосновава и основните цели на системния подход към управлението на материалите съчетавайки оптимизиране на процесите, намаляване на разходите, подобряване на качеството на услугите и повишаване нивото на обслужване. Това налага прилагането на системният подход към управлението на материалния поток и включва разглеждане на всички процеси и операции в рамките на една система. Следователно прилагането на този подход включва няколко етапа:

1. Определяне на целите и задачите на системата.
2. Анализ на входните и изходните параметри на системата.
3. Определяне на структурата на системата и нейните компоненти.
4. Разработване на модели на функциониране на системата.
5. Оценка на ефективността на системата и нейното оптимизиране.
6. Внедряване на системата и наблюдение на нейната работа.
7. Оценка на резултатите и коригиране на системата, ако е необходимо.

Използването на системния подход позволява получаването на по-точни резултати и подобряване на ефективността на управлението на материалния поток. Този вид потоци са неразделна част от функционирането на всяка

организация и включват всички видове суровини, материали, готова продукция, оборудване, стоки, услуги и др. Това позволява адаптиране на управлението на материалните потоци и позволява да се оптимизират процесите на всички етапи от движението на материални активи, от закупуването на суровини до доставката на готови продукти на потребителя. За успешното му прилагане е необходимо да се вземат предвид много фактори, като производствени характеристики, характеристики на продукта, изисквания на клиентите, пазарни условия и тяхното съчетаване със съвремните технологични процеси.

2. Логистична система на пощенските услуги при управление на материални потоци.

Логистичната система при реализацията на пощенските услуги включва в себе си поредица от процеси, свързани с доставката на писма, колети и други пратки. Тя обхваща всички етапи от получаването на писмо от изпращача до доставката до получателя. Основните елементи на логистичната система са: прием и обработка на поща от пощенските служители проверката според изискванията, описването им и регистрацията. Сортировка и разпределение, включва следната последователност: пощата се сортира по пощенски кодове, направления и други параметри, след което се разпределя по съответните товарни отсечки. Опаковка и маркировка съдържа: отделните опаковки на продукта в пощенски пакети или кутии и се маркират според стандартите за поща. Транспортиране на материалния поток се определя от: пратките, които се превозват между пощенските отделения, между градовете и страните с помощта на различни видове транспорт – автомобилен, железопътен, въздушен и др. Съхранение на пратките се извършва в пощенските клонове до тези порции, докато те не бъдат потърсени от получателя или в определен срок. Доставка е процес обоснован от непосредственото изпълнение до адресата, или до неговия пощенски клон. Мониторинг и наблюдението на изпращачите и получателите могат да определят статуса на своите желания с помощта на специални услуги и приложения.

Основни материални потоци в сферата на пощенските услуги можем да обощим като пощенски поток включващ: писма, колети, и други пощенски пратки. Поток от оборудване и материали включва: всичко необходимо за работата на пощенските служби, като компютри, принтери, мебели и др. Под поток на персонала разбираме всички служители на пощата, от пощальони до мениджъри на структурите. Другият характерен елемент е информационният поток обединяващ цялата информация, необходима за функционирането на пощенските услуги, като клиентски данни, адреси, тарифи и др.

3. Методи за нормиране на разхода на материали и показатели за оценка

Теоритичната характеристика на показателите за оценка може да бъде нормативна, аналитична и статистическа. Нормативната оценка се основава на

използването на предварително определени стандарти за разход на материали, които са установени на базата на лабораторни изследвания или практически опит. Тя се извършва чрез сравняване на реалния разход на материали с установените норми. Аналитичната оценка включва анализ на производствените процеси и определяне на оптимални норми на разход на материали, като се вземат предвид характеристиките на производството и характеристиките на използваните материали. Оценката се извършва въз основа на сравнение на получените стандарти с реалния разход на материали. Статистическата оценка осигурява нормите на потребление на материали и се определят въз основа на исторически статистически данни за потреблението на материали. Оценката се извършва чрез анализ на отклоненията между действителния и нормативния разход на материали и определяне на причините за тези отклонения. Разглеждаме два вида модели, свързани с материалните потоци X(t) и дефинираме целевата функция на изследването. [7] Първият тип представлява от само себе си нестационарни случайни величини в точния смисъл на думата, плътност на разпределение p(x,t), която бавно се изменя във времето. Бавното изменение на плътността на разпределение се разбира като възможност за разделяне продължителността на технологичния процес, приемащ свойството квазистационарност (в точния смисъл на думата). Анализираме едномерен, стационарен случаен процес X(t), представен от отделна реализация x(t) във вид N със стъпка h, т.е. x(xn), n=0,1,2,…,N-1. Предполага се, че реализацията е вече центрирана, т.е.

$$\frac{1}{N}\sum_{n-1}^{N-1} x(nh) = 0 \quad (1)$$

Оценката на плътността на разпределение за X(t) може да се намери по формулата:

$$P(x) = \frac{N_x}{NW}, \quad (2)$$

където: N_x - число, попадащо под центрирана реализация x(t), представено N със значението на интервала $x \pm \frac{W}{2}$. Оценка за плътността на разпределение за средата на всеки i-ти интервал се изразява чрез:

$$p_i = \frac{N_i k}{N(b-a)}, \quad i = 1,2,\dots k \quad (3)$$

където: k – цяло число на равни интервали, на които е разбит целия диапазон на изменение; [b, a] - разгледания диапазон на изменение x(t). Оценката на плътността на разпределение p(x) се явява изместена. Изместените оценки са приблизително: b[p(x)] = E[p(x)-1]p(x) са приблизително:

$$b[p(x)] \approx \frac{W^2}{24} p(x) \quad \rightleftarrows \quad (4)$$

където: - втора производна за по p (x) по x.

Тогава дисперсията за оценка ще определим по формулата:

$$D[p(x)] \approx \frac{c^2 p(x)}{2BTW} \quad \rightleftarrows \quad (5)$$

където: c – постоянна величина, равна на единица.

Предполага се, че случайния процес X(t) има най- висока честота B (в херцове), а реализацията x(t) е зададена в крайния интервал от време T(c). За

решение на задачата за диагностиране или прогнозиране на състоянието на оборудването оценката на плътността на разпределение ще има вида:

$$P_{откл.} = P_E - P_T, \quad (6)$$

където: Роткл. – отклонение на параметрите; РЕ – експлоатационно измерено състояние; РТ – теоретично определеното състояние (технически паспорт).

Показатели за оценка на основните показатели са:

— процент на отклонение на действителния разход на материали от стандарта;

— ниво на спестявания/свръхконсумация на материали;

— коефициент на използване на материала, който показва дела на полезното използване на даден материал в общото потребление;

— индекс на производителността, който отразява ефективността на използването на материалите в производствения процес.

За оценка на материалните потоци в пощенските услуги могат да се използват следните методи:

— анализ на структурата на потока: изследване на състава на потока, определяне на неговите основни компоненти и техните характеристики;

— оценка на скоростта на потока: измерване на броя пратки, оборудване, персонал и информация, преминаващи през пощенската система за единица време;

— измерване на скоростта на потока: определяне на скоростта, с която пощата, оборудването и персоналът се движат между различни точки в пощенската система;

— определяне на оптималния размер на потока: анализ на връзката между размера на потока и разходите за обработката му, определяне на оптималния размер на потока за минимизиране на разходите.

— оценяване на ефективността на контрола на потока: анализиране на индикатори като време за обработка на поща, процент на загуби и грешки, нива на удовлетвореност на клиентите и т.н., и сравняването им с целевите индикатори.

За да се оценят материалните потоци в пощенските услуги, трябва да се вземат предвид следните принципи:

— обективност: оценката трябва да се базира на реални данни, а не да зависи от субективни мнения;

— точност да се извърши с висока степен на за да се осигурят надеждни резултати;

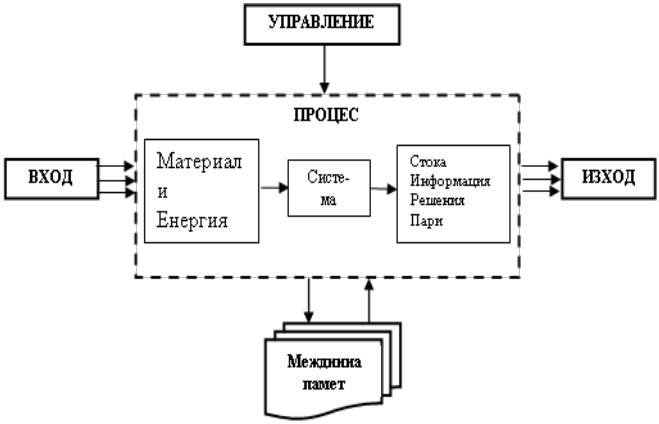
— уместност съчетаваща в себе си последните промени в пощенските услуги и технологии;

— ефективност на разходите трябва да се извърши с минимален ресурси и време.

— видимост на резултата трябва да бъдат представени в ясна и визуална форма.

Резултатът към потока от материали е важна консолидация на отговорността на ръководството за мениджмънта на материалните ресурси през

последните години. [8] Но по-важно е, че вниманието на висшето ръководство дава възможност на все повече и повече пощенски оператори да започнат решаването на въпросите на взаимодействието с инженеринга, маркетинга и производството за подобряване на ефективността на цялата организация според фиг. 1.



Фиг. 1. *Структура на системата за управление на материални потоци*

От фиг. 1 следва, че най-общо входовете и изходите на системата могат да принадлежат към една от следните обобщаващи категории: системите са съставени от подсистеми, които взаимодействат помежду си чрез своите входове и изходи; системите се изграждат на йерархичен принцип; декомпозирането на системите следва дървовидна структура; всяка подсистема удовлетворява изискванията за система, като притежава входове, изходи, цели и може би памет и управление. Разширеният обсег на отговорността позволи на мениджърите на материалните потоци да разширят перспективата за подобряване на производителността от един чисто функционален фокус върху транспортирането за експедиране и складирането на завършени стоки (PDM) или транспортирането за приемане и складиране на суровини (MM) към едно общо разглеждане на целия поток от материали. Анализ на резултатите от изчисленията и вземане на решения за оптимизиране на материалните потоци ни позволяват да се вземат обосновани управленски решения.

Заключение

Прилагането на системния подход за управление на материалните поток има редица предимства. [7]. То позволява да се оптимизират процесите на движение на материала, намалявайки времето и разходите за движение. Подобряване на качеството на работа, свързване с идентифицирани и коригирани

на ранен етап. Намаляват се рисковете от неправилно планиране и управление на материалните потоци и се повишава конкуренто-способността на предприятието, тъй като дава възможност за бързо реагиране на промените в нуждите на клиентите и пазара. Системният подход укрепва връзките между различните отдели, което подобрява координацията на тяхната работа.

Като основна препоръка и заключение може да се приеме, че комплексната методика за оптимизирането на структурата и елементите на логистичните вериги, канали или мрежи, реализираща интегралната система в логистиката, и моделите и подходите свързани с нейната реализация трябва да бъдат едни от основните инструменти за взимане на обективни стратегически и оперативни решения от логистичния мениджмънт на фирмите при управление на потока от заявки за снабдяване с материали и суровини.

1. Предложена е структура от три нива на логистичните системи, като са интегрирани в едно цяло: логистичната инфраструктура, логистичните дейности и структурата от фирми. Интеграцията се осъществява от материалния поток (ГП и МР), а логистичния мениджмънт се съобразява със стойностната му верига.

2. Интегралният подход в управлението на логистичните системи се основава на обективни решения взети на база оптимизация на структурата и елементите им. Направена е класификация на факторите, свързани с декомпозиция на логистичните мрежи. Предложен е подход за декомпозиция на логистичните вериги в зависимост от тези фактори. Това дава възможност за прилагане на подходящи оптимизационни модели.

ЛИТЕРАТУРА

[1] Гаторна Дж. Основи на логистиката и дистрибуцията. Бургас, 1996.

[2] Голиков Е. А. Маркетинг и логистика. Москва, 2001.

[3] Миротин Л. Б. Основы логистики. Москва, 2000.

[4] Чудакоов А. Д. Логистика, учебник. Москва, 2001.

[5] Джабраилов А. Э., Моргунов В. И. Маркетинг логистика. Дашков и К, Москва, 2010.

[6] Anderson D. R., Gattoni R. L. The management of logistics systems: a systemic approach to improving performance. John Wiley & Sons, 2013.

[7] Bowersox D. J., Closs D. J., Stank T. P. Logistical Management. The McGraw-Hill Companies, 1996.

[8] Christopher M. Logistics and supply chain management: strategies for reducing cost and improving service. Pearson Education, 2005.

[9] Coyle J. J., Bardi E. J., Langley C. J., Novack B. G. Fundamentals of Logistics: An Integrated Supply Chain Perspective. McGraw Hill, 2021.

УСЪВЪРШЕНСТВАНЕ НА МРЕЖОВАТА КОМУНИКАЦИЯ И ПОВИШАВАНЕ НА НАДЕЖДНОСТТА НА ПРОГРАМИРУЕМИТЕ УСТРОЙСТВА В ИНДУСТРИЯТА

Даниел Р. Денев, Екатерина М. Христова, Цветослав С. Цанков

IMPROVING NETWORK COMMUNICATION AND ENHANCING THE RELIABILITY OF PROGRAMMABLE DEVICES IN THE INDUSTRY

Daniel R. Denev, Ekaterina M. Hristova, Tsvetoslav S. Tsankov

ABSTRACT: *In this article, an experimental study related to the information level of an industrial network is carried out. It aims to increase the quality and speed of her workflow. Monitoring and data extraction of the communication of programmable devices is carried out as well. A method for improving data transmission in the same network is proposed. A statistical method is used to analyze the general reliability.*

KEYWORDS: *Industrial network, Programmable logic controllers, WireShark, Reliability.*

Въведение

Статистиката представлява математически методи за събиране, организиране и интерпретация на числени данни, особено анализа на характеристиките на популацията чрез извод от извадка. Статистическият анализ, от своя страна, е процес на събиране и анализиране на голям обем от данни, нужни за идентифициране на тенденциите и развиване на ценни прозрения. В професионалния свят статистиците вземат необработени данни и намират взаимоотношение между променливите, за да разкрият модели и тенденции за съответните заинтересовани страни. Работейки в широк спектър от различни области, статистическите анализатори са отговорни за нови научни открития, бизнес решения и много иновации.

Етапи на изследване

Всяко конкретно статистическо изследване има за обект някакво масово явление, проявяващо се в определени пространствени и времеви граници. То обхваща три взаимосвързани етапа: статистическо наблюдение, статистическа групировка и статистически анализ.

1. Целта на статистическото наблюдение като първи етап на цялостното изследване, се свежда до събирането на първична емпирична информация.

2. На втория етап чрез методите за групировка първичните сведения трябва да бъдат обобщени, систематизирани, така че към тях да могат да се приложат методите за статистически анализ.

3. Заключителният етап е самият статистически анализ, който трябва да отговори на целите и очакваните резултати, които са били причина за провеждането на цялостното статистическо изследване.

Голяма част от научните изследвания се отнасят до сравняване на разпределението на две или повече променливи величини. Особеното на тези сравнения е, че изводите, които се правят, трябва да се отнасят до целите съвкупности, а данните, с които разполага изследователят, обхващат само извадка от нея. Поради това първоначално се формулират предположения – хипотези, като впоследствие се прави проверка дали данните от извадката ги потвърждават или отхвърлят.

1. **Нулева (H0)** - твърди, че няма статистически достоверна разлика в сравняваните статистически показатели. Въпреки, че в извадките може да се наблюдава известна разлика, тя е случайна и не може да бъде обобщена за генералните съвкупностите.

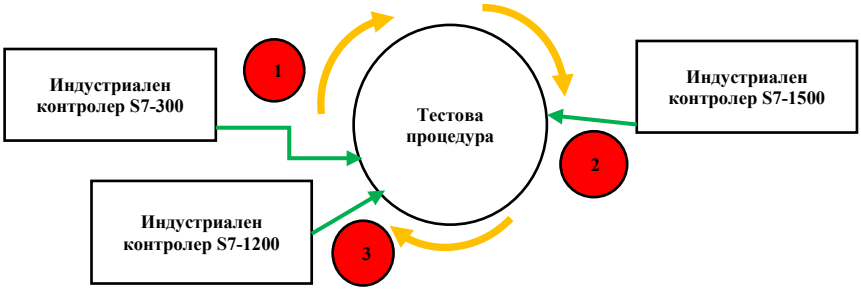
2. **Алтернативна (H1)** - твърди, че констатираната разлика в сравняваните статистически показатели в извадките е статистически достоверна и може да бъде обобщена за генералните съвкупности.

Степента на сигурност, с която се приема за вярна алтернативната хипотеза, се нарича **гаранционна вероятност (P).** Рискът да се допусне грешка, като се приеме за вярна алтернативната хипотеза, се нарича **ниво на значимост (α).** След формиране на хипотезите се избира подходяща статистика (критерий), която се изчислява според параметрите, подробно описани в хипотезите. Окончателно решение се взема като табличната (теоретичната) стойност на критерия се сравнява с емпиричната (изчислената по данни от извадката).

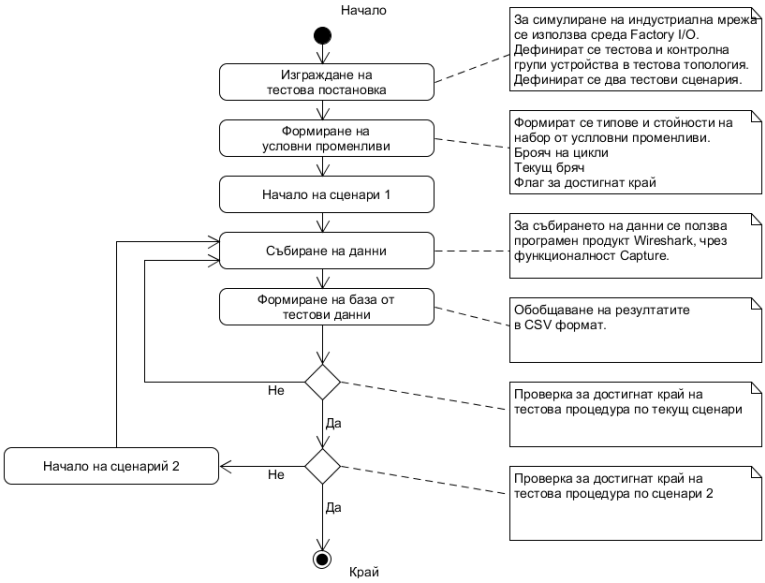
Тестова постановка и алгоритъм за проверка на хипотези

За провеждане на тестова процедура и за целите на изследването в три етапа се организира тестова постановка с контролна и тестова група от индустриални устройства и комутатор, играещ ролята на ключов тестов елемент. Тестовата постановка е показана, съответно на фиг. 3 и фиг. 4, включваща контролната и тестовата групи. На фиг. 1 е представен подходът за организиране на трите етапа на тестовата постановка. За целите на изследването са подбрани три типа индустриални контролери (S7-300, S7-1200, S7-1500). Всяка текуща тестова постановка включва пет броя индустриални контролери от дадения тип, която се прилага за съответния етап. А, за тестовата постановка се добавя интелигентен комутатор от тип Cisco Business 220. [1, 4]

С използване на диаграми на дейности на фиг. 2 е представен алгоритъм за провеждане на тест, валиден за всеки един етап.



Фиг. 1. *Подход за организиране на тестовата постановка*

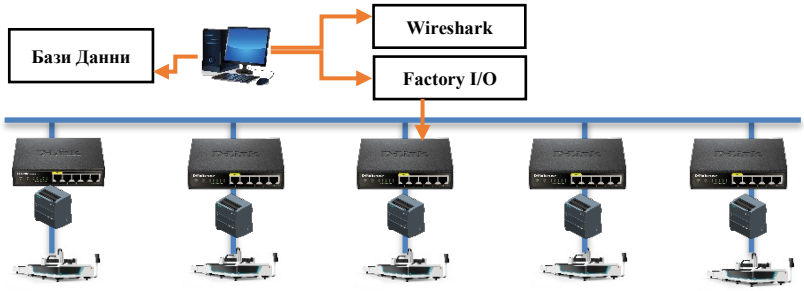


Фиг. 2. *Алгоритъм за провеждане на тест от даден етап*

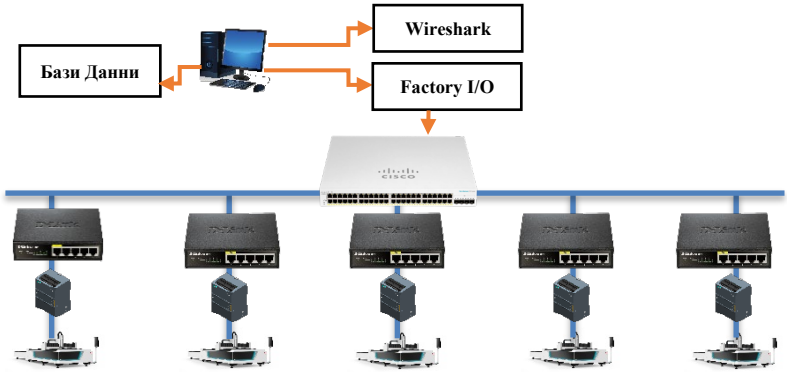
И в двата вида тестови постановки се използва работна станция със следното предназначение [3]:

1. Управление на тестовите приложения;
2. Съхранение на междинни данни;
3. Съхранение на тестовите резултати;
4. За целите на изследването са подбрани следните приложения;

5. Factory I/O – интегрирана среда за симулации на мрежи;
6. Wireshark – приложение за анализ на мрежови протоколи и мрежови данни;
7. Rstudio – интегрирана среда за синтез на скриптове, предназначени за анализиране на данни.



Фиг. 3. *Схема на индустриална мрежа с контролен набор от устройства*



Фиг. 4. *Схема на индустриална мрежа с тестови набор от устройства*

За формиране на емпиричен набор от резултати се установява следният набор от критерии:

1. Номер на порт;
2. Брой пакети;
3. Размер на пакетите в байтове;
4. Общ брой пакети;
5. Брой изпратени пакети;
6. Брой приети пакети.

По тези критерии са формирани набори от таблици 1, 2, 3 с емпиричните данни.

Таблица 1. *Profinet числови данни за контролер S7-300 след усъвършенстване*

Addresses	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Siemens S7-300	*50*	*9595*	*50*	*100.00%*	*0*	*0*	*50*	*9595*
Siemens S7-300	*585*	*36852*	*650*	*90.00%*	*400*	*16852*	*185*	*20000*
Siemens S7-300	*10*	*777*	*10*	*100.00%*	*0*	*0*	*10*	*777*
Siemens S7-300	*29*	*654*	*33*	*90.00%*	*0*	*0*	*29*	*654*
Siemens S7-300	*61*	*9000*	*61*	*100.00%*	*0*	*0*	*61*	*9000*
Siemens S7-300	*20*	*1365*	*22*	*93.00%*	*0*	*0*	*20*	*1365*
Siemens S7-300	*2*	*415*	*3*	*90.00%*	*2*	*415*	*0*	*0*
Siemens S7-300	*7*	*450*	*7*	*100.00%*	*0*	*0*	*7*	*450*
Siemens S7-300	*4*	*741*	*4*	*100.00%*	*0*	*0*	*4*	*741*
Siemens S7-300	*6*	*633*	*6*	*100.00%*	*0*	*0*	*6*	*633*

Таблица 2. *Profinet числови данни за контролер S7-1200 след усъвършенстване*

Addresses	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Siemens S7-1200	*60*	*7564*	*60*	*100.0%*	*60*	*7564*	*0*	*0*
Siemens S7-1200	*400*	*23563*	*400*	*100.0%*	*400*	*23563*	*0*	*0*
Siemens S7-1200	*91*	*500*	*100*	*91.0%*	*31*	*200*	*60*	*300*
Siemens S7-1200	*30*	*2356*	*30*	*100.0%*	*0*	*0*	*30*	*2356*
Siemens S7-1200	*50*	*8411*	*50*	*100.0%*	*50*	*8411*	*0*	*0*
Siemens S7-1200	*440*	*1515*	*500*	*88.0%*	*240*	*807*	*200*	*707*
Siemens S7-1200	*18*	*325*	*20*	*90.0%*	*0*	*0*	*18*	*325*
Siemens S7-1200	*5*	*508*	*6*	*88.0%*	*0*	*0*	*5*	*508*

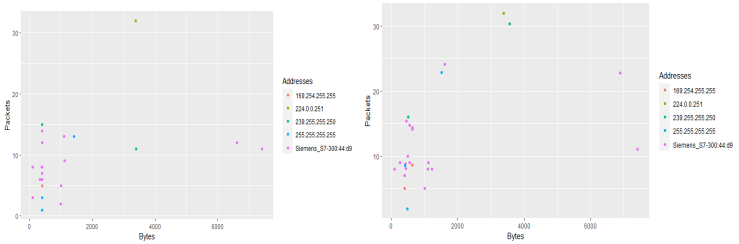
Таблица 3. *Profinet числови данни за контролер S7-1500 след усъвършенстване*

Addresses	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Siemens S7-1500	*100*	*8410*	*100*	*100.0%*	*100*	*8410*	*0*	*0*
Siemens S7-1500	*445*	*22886*	*500*	*89.0%*	*445*	*22886*	*0*	*0*
Siemens S7-1500	*186*	*714*	*200*	*93.0%*	*186*	*714*	*0*	*0*
Siemens S7-1500	*45*	*2285*	*50*	*91.0%*	*0*	*0*	*45*	*2285*
Siemens S7-1500	*25*	*8365*	*30*	*86.0%*	*25*	*8365*	*0*	*0*
Siemens S7-1500	*285*	*1410*	*300*	*95.0%*	*285*	*1410*	*0*	*0*
Siemens S7-1500	*36*	*366*	*40*	*92.0%*	*0*	*0*	*36*	*366*
Siemens S7-1500	*17*	*501*	*20*	*88.0%*	*0*	*0*	*17*	*501*

Визуализация и доказателство за достоверност на данни

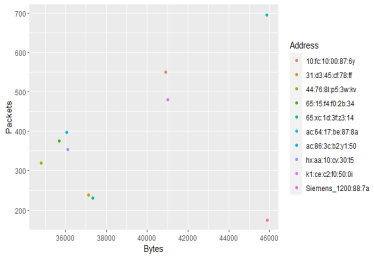
На основание теоретичната постановка е направено статистическото проучване за проверка на хипотези и доказване на резултатите от усъвършенстването на индустриалната мрежа. Графичното представяне на информация и данни, използвайки визуални елементи като диаграми, графики, карти и инструментите за визуализация, осигуряват достъпен начин за виждане и разбиране на тенденции, отклонения и модели в данните. То предоставя отличен начин за представяне на данни на нетехнически аудитории без объркване. За целите на изследването, данните от гореспоменатите контролери са представени в точкови диаграми. Такива наблюдения се наричат сдвоени или повторни, т.е. на всяко x_i съответства y_i. Изходният код е представен:

S7-300 - (Фиг. 5, Фиг. 6)

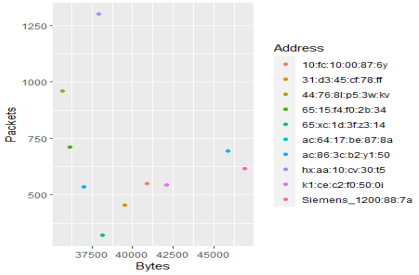


Фиг. 5. *Точкова диаграма на контролер S7-300*, **Фиг. 6.** *Точкова диаграма S7-300 на контролер S7-300 след усъвършенстване*

S7-1200 - (Фиг. 7, Фиг. 8)



Фиг. 7. *Точкова диаграма на контролер S7-1200*



Фиг. 8. *Точкова диаграма на контролер S7-1200 след усъвършенстване*

Извод: На фигурите се вижда отчетлива разлика на измерванията преди и след поставянето на допълнителното ниво на оптимизация. Но въпреки това, не може да се направи заключение за точната големина на ефекта на интелигентния комутатор Cisco Business 220 върху контролерите в мрежата.

Избиране на хипотеза и ниво на значимост

Въпреки невъзможността да се оцени точната големина на въздействието на комутатора по точковите графики, числовите стойности в извадките показват възможно подобрение в броя предадени пакети и байтове между контролерите в индустриалната мрежа.

1. $H_0: m_y - m_x = 0$, т.е. няма значителна разлика между данни свалени преди добавянето на комутатора;
2. $H_1: m_y > m_x$, т.е. има значително подобрение на надеждността на мрежата, предаването на пакетите и оптимизирането на работата на системата след свързване на допълнителни устройства [2, 5];

Използва се статистиката:

$$U_x = \sum_{i=1}^{n_x} \sum_{j=1}^{n_y} \delta_{ij} \quad \textbf{(1)}$$

където

$$\delta_{ij} = \begin{cases} 1, & x_i > y_j \\ \frac{1}{2}, & x_i = y_j \\ 0, & x_i < y_j \end{cases} \quad \textbf{(2)}$$

При проверка на H_0, доверителната област за проверка на хипотезата W придобива вида

$$W = \{U_{1-\alpha} \leq U_x\}, P(W) = \alpha \quad \textbf{(3)}$$

В практиката, най-често се работи с α = 0,05.

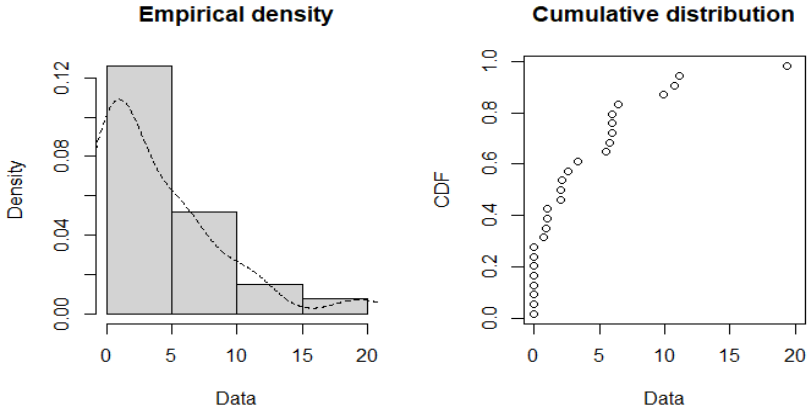
Избиране на статистически критерий за проверка на хипотези

Методи за измерване на плътност

При проверка на статистическата хипотеза за наличието на съществена разлика между „двойка“ измервания се разглеждат разликите на данните в извадките $d_i = y_i - x_i$. Важен фактор за определяне на нужната статистика е вида на разпределението на разглежданите извадки, в т.с. на получената разлика. Това се постига чрез хистограми, представляващи плътността на честотното разпределение и графики на кумулативните функции. Нужният код е представен:

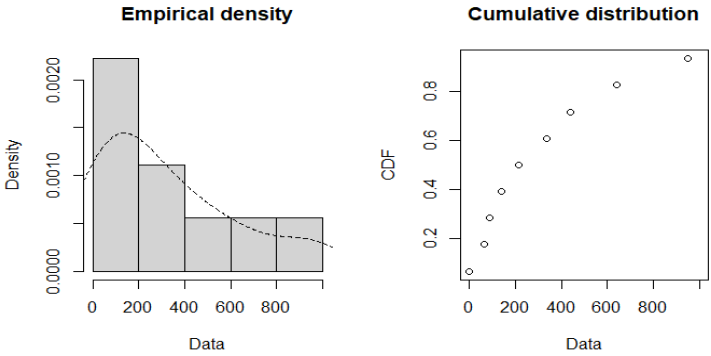
```
library(readxl)
library(fitdistrplus)

UDP_before_raw <- read_excel("Statistics/UDP_S7-300_before.xlsx",
range = "C2:C29")
UDP_after_raw <- read_excel("Statistics/UDP_S7-300_after.xlsx",
range = "C2:C29")

UDP_before = as.numeric(unlist(UDP_before_raw))
UDP_after = as.numeric(unlist(UDP_after_raw))
Diff = UDP_after - UDP_before
plotdist(Diff, histo = TRUE, demp = TRUE)
```

Графики за плътност на разликата d_i на контролер S7-300



Фиг. 9. *Емпирична плътност и графика на кумулативната честотна функция на контролер S7-300*

Графики за плътност на разликата d_i на контролер S7-1200



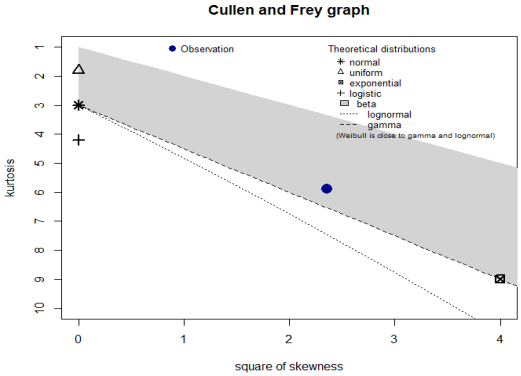
Фиг. 10. *Емпирична плътност и графика на кумулативната честотна функция на контролер S7-1200*

Извод: От представените графики на емпирична и кумулативна плътност, разпределенията не са нормални, а са с положителна асиметрия.

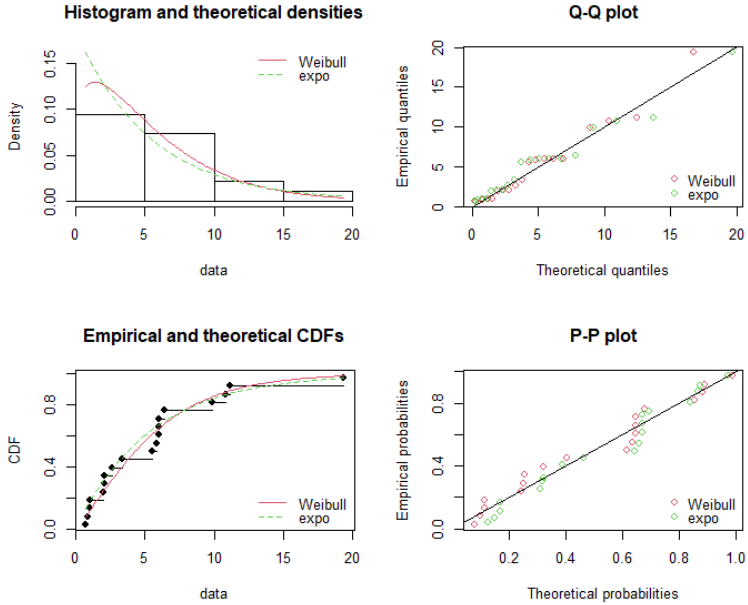
Методи за съответствие на разпределения

Някои от разпределенията, които имат подобни честотни графики и статистическите критерии, са експоненциални и за тях е в сила разпределението на Вейбул. Съществуват методи за точно определяне на разпределенията. Един такъв ефективен начин е чрез графиката на Калън и Фрей, която съпоставя стойностите на симетрия и ексцеса, а получените резултати могат да бъдат съпоставени чрез класическите параметри за измерване на разпределения: теоретична плътност, Q-Q (кванитил-квантил), кумулативни честоти и P-P (вероятностни). Нужният код е представен:

```
# Cullen and Fray kurtosis-skewness graph
descdist(data, discrete = FALSE)

#Comparison of the right-tailed distributions
fw <- fitdist(data, "weibull")
fe <- fitdist(data, "exp")
par(mfrow = c(2, 2))
plot.legend <- c("Weibull", "expo")
denscomp(list(fw, fe), legendtext = plot.legend)
qqcomp(list(fw, fe), legendtext = plot.legend)
cdfcomp(list(fw, fe), legendtext = plot.legend)
ppcomp(list(fw, fe), legendtext = plot.legend)
```

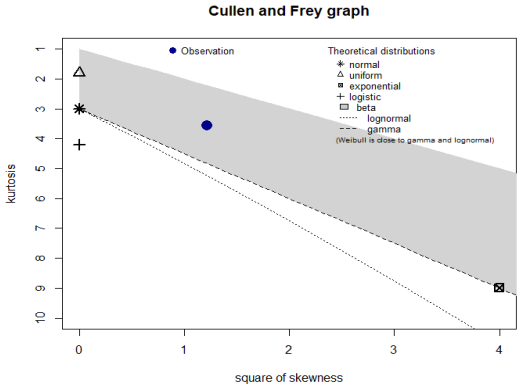


Фиг. 11. *Графика на Калън-Фрей на d_i на контролер S7-300*

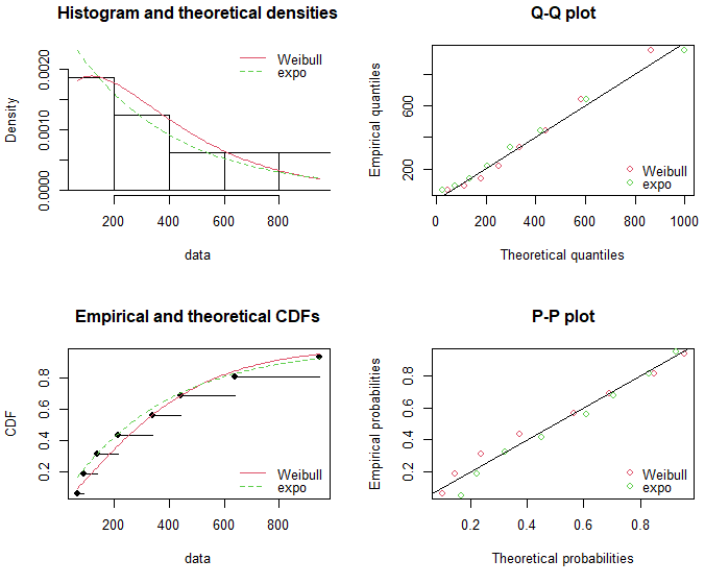


Фиг. 12. *Параметри за съответствие на разпределение на d_i на контролер S7-300*

Система за съответствие на разпределение на d_i на контролер S7-1200



Фиг. 13. *Графика на Калън-Фрей на d_i на контролер S7-1200*



Фиг. 14. *Параметри за съответствие на разпределение на d_i на контролер S7-*

Извод: Според представените данни се вижда, че изследването на дистрибуциите и на трите двойки данни са разпределения на Вейбул.

Разпределение на Вейбул

Това разпределение е едно от най-широко използваните разпределения в областта на изпитванията на здравината и надеждността в електрониката. Вейбуловото разпределение е често срещано при анализиране на надеждността на живота и полезността на различни компоненти и като модел за време до отказ. Той обобщава експоненциалния модел, за да включва функции с непостоянен процент на отказ. По-специално, той обхваща както функциите за нарастване, така и за намаляване на степента на повреда и е използван успешно за описване както на откази при първоначално изгаряне, така и на откази, дължащи се на износване. Вероятностната функция на плътността на случайна променлива се изразява в параметричното уравнение:

$$f(x;\lambda,k) = \begin{cases} \frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1} e^{-\left(\frac{x}{\lambda}\right)^{k}}, x \geq 0 \\ 0, x < 0 \end{cases} \quad \textbf{(5)}$$

където $k > 0$ е параметърът за форма, а $\lambda > 0$ е параметърът за мащабируемост. В областта на електрониката разпределението може да бъде преобразувано и разписано с различни: мащабен параметър (η), параметър на формата или Вейбулов наклон (β) и параметър на разположението или минимално време на живот (t_0). Функцията на разпределението на Вейбул най-лесно се запомня, когато е написана като функция на надеждност:

$$R(t) = 1 - F(t) = exp\left[-\left(\frac{t-t_0}{\eta-t_0}\right)^{\beta}\right] \quad \textbf{(6)}$$

Съответната функция на плътностите на вероятностите е:

$$f(t) = \frac{\beta}{\eta-t_0}\left(\frac{t-t_0}{\eta-t_0}\right)^{\beta-1} e^{-\left(\frac{t-t_0}{\eta-t_0}\right)^{\beta}} \quad \textbf{(7)}$$

А функцията на интензивността на отказите е:

$$\alpha(t) = \frac{\beta}{\eta-t_0}\left(\frac{t-t_0}{\eta-t_0}\right)^{\beta-1} \quad \textbf{(8)}$$

Експерименталната оценка съставлява съществена част от необходимите мероприятия по осигуряване на висока надеждност, като се позволява установяването на истински стойности на показателите. При провеждане на такива оценки се използват способите на математическата статистика. След провеждането на задълбочен анализ за вида и разпределението на двойките извадки беше установено, че:

1. извадките са съставени от непрекъснати случайни величини;
2. извадките са „зависими“;

3. разликите между тях не са нормално разпределени.

От тези заключения следва, че не могат да бъдат ползвани стандартните t-тестове, като по-подходящ е тестът на Уилкоксън за зависими извадки.

Изчисляване на избрания критерий в средата за програмиране RStudio, тест на Уилкоксън

Статистически метод се нарича непараметричен, ако не прави предположения за разпределението на генералната популация или размера на извадката. В контраст с повечето параметрични методи, които приемат, че данните са количествени, популацията има нормално разпределение и размерът на извадката е достатъчно голям. Като цяло заключенията, направени от непараметричните методи, не са толкова мощни, колкото параметричните. Въпреки това, тъй като непараметричните методи правят по-малко предположения, те са по-гъвкави, по-стабилни и приложими към неколичествени данни. Поради тези причини е препоръчително работа с медиани, а не със средни стойности.

Определяне емпиричните p-стойности и вземане на решение

Извършване на тест на Уилкоксън на двете извадки от данни за контролер S7-1500

```
median(Profinet_before)
median(Profinet_after)

wilcox.test(Profinet_before, Profinet_after, paired = TRUE,
exact=FALSE)
```

Wilcoxon signed rank test with continuity correction
alternative hypothesis: true location shift is not equal to 0
p-стойност (0,01415) < α (0,05)

Решение: поради съществуване на значима разлика между p и α, хипотезата H_0 се отхвърля, а H_1 се приема за истинна.

Изчисление на оценка на големината на корелационния коефициент като мярка за размера (силата) на ефекта

Размерът на ефекта е стойност, измерваща силата на връзката между две променливи в съвкупност, или базирана на извадка оценка на това количество. Може да се отнася до стойността на статистика, изчислена от извадка от данни. Примерите за размери на ефекта включват корелацията между две променливи, коефициента на регресия, средната разлика или риска от настъпване на конкретно събитие. Размерите на ефекта допълват тестването на статистическите хипотези и играят важна роля в анализите на мощността, планирането на размера на извадката и в мета-анализите. Коефициентът на Коен d се определя като разликата между две средни стойности, разделена на стандартно отклонение за данните.

$$\boldsymbol{d = \frac{\overline{x_1} - \overline{x_2}}{s}} \qquad \textbf{(9)}$$

```
test_3 <- wilcox.test(Profinet_before, Profinet_after,
paired = TRUE, exact=FALSE)
Zstat_3<-qnorm(test_3$p.value/2)

#Effect size using
abs(Zstat_3)/sqrt(10)
```

##[1] 0.7758644

$d = 0{,}78$ => голям ефект

Извод: Интелигентният комутатор Cisco Business 220 показва съществено влияние върху работата на контролерите в мрежата, като оптимизира работата им, подобрява надеждността на предаваната информация и на електронните изделия и подобрява скоростта на предаване на пакети между устройствата.

Заключение

От предложената статия може да се заключи, че чрез комбинирането на знания, умения и технически средства от няколко научни и приложни области, се постига целта, а именно – усъвършенстване на информационно ниво в индустриалната комуникация. Осигурява се по-добра надеждност както и защита на информацията с по-малки загуби. Интелигентните комутатори показват съществено влияние върху програмируемите устройства и дават широк спектър от възможности за подобряване на индустриалната комуникация. Предвидена е бъдеща разработка на софтуерна приставка за програмата Wireshark, чрез която ще се осъществява пряка връзка с програмата за симулация. Чрез нея, в процес на симулация, ще се извършва прослушване и анализиране на индустриални мрежи в реално време, което от своя страна ще улеснява и други бъдещи разработки и подобрения.

ЛИТЕРАТУРА

[1] Георгиева И. Интегрирани системи за автоматизация с програмируеми логически контролери. 2016, Благоевград, ISBN 954-8118-06-8

[2] Петров Н. Надеждността като технико-икономически проблем при кибернетизация на обществото. 2015, Дисертация за присъждане на НС „Доктор на икономическите науки“, ВСУ „Черноризец Храбър“, ISBN 978-954-92960-8-2,400с.

[3] Цанков Ц. Съвременни методи за достъп до ресурсите в комтюпърни индустриални мрежи. 2022, Шумен, ISBN 978-619-201-618-0.

[4] Стоянов, С., Стоянова, Т. Автоматизиране на процеси с помощта на микроконтролери и облачни бази данни. MATTEX 2022, Сборник научни трудове, Том 2, Университетско издателство „Епископ Константин Преславски“, 2022, стр. 23-28, ISSN: 1314-3921.

[5] Petrov N., Dimitrov V., Dimitrova V. Reliability of Technology Systems in Industrial Manufacturing. 2019, Monograph, „AkiNik Publications”, New Delhi, India, ISBN: 978-93-87072-59-6.

МОРСКИ ПРОСТРАНСТВА НА РЕПУБЛИКА БЪЛГАРИЯ – НАЦИОНАЛНО ПРАВНА УРЕДБА. ОСНОВНИ ПОНЯТИЯ

Галин П. Петков

MARITIME SPACES OF THE REPUBLIC OF BULGARIA – NATIONAL LEGAL FRAMEWORK. BASIC CONCEPTS

Galin P. Petkov

ABSTRACT: *This report examines the legal regulation of the maritime spaces of the Republic of Bulgaria in the adjacent Black Sea, as well as the basic concepts ratified by the Republic of Bulgaria through the UN Convention on the Law of the Sea from 1982 and their implementation in the Law on Maritime Spaces, internal internal waterways and ports of the Republic of Bulgaria.*

KEYWORDS: *Maritime spaces of the Republic of Bulgaria, UN Convention on the Law of the Sea, Internal sea waters, Territorial sea, Adjacent zone, Continental shelf, Exclusive economic zone.*

1. Въведение

Правната регламентация на морските територии е процес започнал още през 1927 г., когато Събранието на Обществото на народите свиква дипломатическа конференция за кодификация на три от пет готови теми, една от които е и тази за териториалните води. Тогава не се стига до изготвяне на конвенция, а само на доклади. По късно през годините темата за морските пространства по един или друг начин не е била обект на дискусия.

След създаването на ООН и приемането на резолюция 94/1 от 31 януари 1947 г. за учредяване на Комитет за прогресивно развитие на Международното право, и така до приемане на Конвенцията на ООН по морско право подписана в Монтегю Бей – Ямайка усилено се работи от страните за регулиране на световните морски пространства.

2. Национално правна уредба.

Като всички страни граничещи с морета или океани Република България е ратифицирала голяма част от международните споразумения, конвенции и договори регламентиращи морските пространства, използването и управлението на ресурсите, търсенето и спасяването, както и мирното преминаване през тях. Като суверенна държава право и задължение е издаването на нормативен акт

уреждащ разрешените и забранени дейности който могат да се извършват в морските и пространства.

За уреждане на правния режим на морските пространства и в пристанищата, в които Република България упражнява суверенитет, определени суверенни права, юрисдикция и контрол в съответствие с общопризнатите принципи и норми на международното право и международните договори, по които Република България е страна в момента действа "Закон за морските пространства, вътрешните водни пътища и пристанищата на Република България" (Обн. ДВ, бр. 12 от 11.02.2000 г, ... изм. ДВ. бр.102 от 23 Декември 2022 г.). [1]

Този закон има за цел да обезпечи използването на Черно море и на река Дунав в интерес на сътрудничеството с черноморските, крайдунавските и други страни, да улесни морските и речните връзки, да осигури безопасност на корабоплаването, опазване на морската и речната среда при корабоплаване и поддържане на екологичното равновесие. С него се урежда правния режим на морските пространства, вътрешните водни пътища и пристанищата в Република България.

Съгласно чл. 5, ал. 1, раздел I, глава втора на Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България морските пространства на Република България обхващат:

- вътрешните морски води;
- териториалното море;
- прилежащата зона;
- континенталния шелф и
- изключителната икономическа зона.

Съгласно чл. 5 ал. 2, вътрешните морски води и териториалното море, както и въздушното пространство над тях, тяхното дъно и неговите недра са част от територията на Република България, върху които тя осъществява своя суверенитет.

Съгласно чл. 5 ал. 3, в прилежащата зона, в континенталния шелф и в изключителната икономическа зона Република България осъществява суверенни права, юрисдикция и контрол.

3. Основни понятия

3.1. Вътрешни морски води

Вътрешните морски води са част от територията на крайбрежната държава, разположени между сушата и териториалното й море. Това утвърждава и чл. 8 от Конвенцията на ООН по морско право от 1982 г. [2] Към вътрешните морски води се отнасят:

- морета, напълно обкръжени от сушата на една и съща държава и морета цялото крайбрежие на които и двата бряга на съединението му с друго море (океан) принадлежат на една държава (Азовско и Бяло море);
- водите на морските пристанища и рейдовете;
- морските заливи и бухти, чиито брегове принадлежат на една и съща държава.

Съгласно чл. 5 от закона за морските пространства, вътрешните водни пътища и пристанища на Република България, във вътрешните й морски води се включват:

— водите между бреговата линия и изходните линии от които се измерва ширината на териториалното море;

— водите на пристанищата ограничени откъм морето и линията, съединяваща най-отдалечените точки в морето на котвените места и други съоръжения;

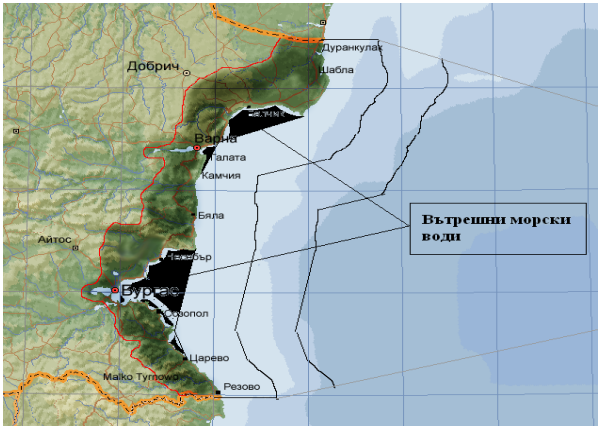
— водите на Варненския и Бургаския залив;

— водите между бреговата линия и правите изходни линии съединяващи нос Калиакра с нос Тузлата, нос Тузлата с нос Емине и Маслен нос с нос Рохи (фиг. 1).

Като част от територията на съответната крайбрежна държава върху вътрешните морски води се разпространява нейния суверенитет. Само крайбрежната държава има право да определя режима в своите води. Тя установява правилата на корабоплаване в тях, за риболов, за използване на радиотехнически средства, за полети на летателни апарати и други.

Режимът на морските пристанища като цяло е същият, като режимът на вътрешните морски води. Неговите норми се съдържат във вътрешното законодателство, правилата и обичаите на крайбрежната държава, в някои международни конвенции и други многостранни и двустранни споразумения между държавите. Съгласно международното право, крайбрежната държава сама решава въпроса в кои от своите пристанища да допуска чужди кораби и определя реда за тяхното пребиваване. Пристанищата и рейдовете също са част от страната. В настояще всяка крайбрежна държава има пристанища, които са открити за посещения от чужди търговски кораби. Тя периодически публикува списъкът на тези пристанища в “известия до мореплавателите” за всеобщо сведение. Достъпа на чужди кораби в пристанищата, не упоменати в този списък се счита за закрит. Според закона за морските пространства, вътрешните водни пътища и пристанища на Република България чуждестранен кораб, използван за търговска или хуманна цел, може свободно да влиза във вътрешните води и да посещава откритите пристанища и рейдове. Чуждите търговски кораби могат свободно да посещават откритите пристанища не само на онези държави, с които държавата на техния флаг има договор за търговия и мореплаване, но и на онези, с които няма дипломатически отношения. За своето посещение те не са длъжни да отправят предварително искане или да уведомят по дипломатически път. Съгласно морските обичаи чужд кораб, който са нуждае от убежище, трябва да бъде пуснат във всяко пристанище (включително и закрито). Достъпа на научноизследователски кораби в пристанища на други държави не е окончателно решен върху договорно правна основа. Допускайки чужди невоенни кораби в своите пристанища, крайбрежната държава определя режима за пребиваването им в тях, който най-често се обуславя от сключените договори за търговия и мореплаване. Този режим обикновено се съставлява по два основни принципа: принцип на националния режим или принципа за най-голямо облагоприятстване.

В случаите на националния режим чуждите кораби се ползват в пристанищата на пребиваване със същия режим, както и отечествените кораби на крайбрежната държава. Най- голямо разпространение са получили договорите, основани на режима на най-голямо облагодетелстване. Този режим означава, че на корабите на всяка една от договарящите се държави се предоставят в пристанищата на другите държави условия, не по-лоши от тези, от които се ползват корабите, на която и да е трета държава.



Фиг. 1. *Вътрешни морски води*

3.2. Териториално море

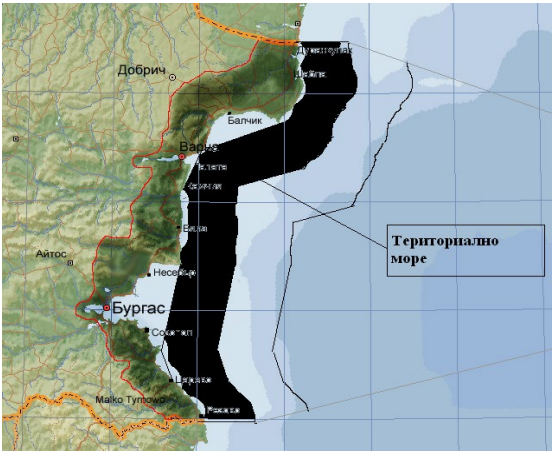
Съгласно чл. 3 от Конвенцията на ООН по морско право от 1982 г. [2], всяка държава има право да установи ширината на своето териториално море и границите, разстоянието до което не надхвърля 12 морски мили.

Под "териториално море" се разбира морският пояс около крайбрежието на съответната морска държава с определена широчина в границите на 12 морски мили, които заедно с въздушното пространство над него и морското дъно е част от нейната територия. Върху този пояс крайбрежната държава разпространява своя пълен суверенитет. Този суверенитет се разпростира отвъд сухоземната територия и вътрешните води на държавата и за архипелажните държави и архипелажните им води. Суверенитетът над териториално море се осъществява, като се спазват разпоредбите на Конвенцията на ООН по морско право от 1982 г. [2] и други норми на международното право.(Фигура 2)

Външната граница на териториалното море е линията, всяка точка, на която се намира от най-близката точка на изходната линия на разстояние, равно на ширината на териториалното море. Външните и страничните граници на териториалното море са държавни граници на Република България.

Вътрешната му граница се образува от така наречените прави изходни линии, прокарани през определени пунктове на материка, островите, рифовете,

скалите и изсъхващите при отлив възвишения. Международното право не установява максималната дължина на тези линии.



Фиг. 2. *Територално море*

Нормалната изходна линия за измерване на ширината на територалното море е линията на най-големия отлив покрай брега, обозначена на официално признатите от крайбрежната държава едромащабни карти. При прокарване на изходните линии, съгласно Конвенцията на ООН по морско право от 1982 г. [2] се спазват следните правила:

— в местата, където бреговата линия е дълбоко врязана и криволичеща, или където до брега има верига от острови за прокарване на изходната линия, от която се отмерва широчината на територалното море, може да се прилага методът на правите изходни линии, съединяващи съответните точки;

— там, където поради наличието на делти или др. природни условия, бреговата линия се явява крайно непостоянна, съответните точки могат да бъдат избрани по максимално навлизащата в морето линия на най-големия отлив и независимо от последващото преместване на линията на най-големия отлив;

— правите изходни линии се прокарват към изсъхващите при отлив възвишения и от тях само в случай, че върху тях са построени фарове и др. подобни съоръжения;

— системата от правите изходни линии не може да се прилага от държавата по такъв начин, щото територалното море на друга държава да се окаже откъснато от територалното море или изключителната икономическа зона.

Установяването от конвенцията на максималната широчина на територално море до 12 морски мили като всеобща юридическа, задължителна норма е едно от постиженията на третата конференция на ООН по морско право.

Конвенцията на ООН по морско право от 1982 г. [2] признава правото на чуждестранните кораби на т.н. „мирно преминаване" през териториално море при спазване на установените условия, гарантиращи уважение на интересите на крайбрежната държава. „*Мирно*" преминаване означава – безвредно преминаване, което не накърнява суверенните права, установения обществен и правен ред и законни интереси на крайбрежната държава. Има се предвид възможността преминаване през териториално море на чужди на своя флаг държави, без да искат разрешение за това.

„*Преминаване*" – означава плаването през териториално море с цел:

— да се пресече морето, без да се навлиза във вътрешни води;

— да се навлезе във вътрешни води или излезе от тях. Преминаването трябва да бъде непрекъснато и бързо. То включва спиране и заставане на котва, само доколкото са свързани с обичайното плаване или са поради непреодолима сила или бедствие.

На преминаващите кораби се забранява да извършват действия, които се характеризират като:

— заплаха със сила и приложението ѝ по отношение на крайбрежната държава;

— различни маневри или учения с оръжия;

— акт, насочен към събиране на информация във вреда на отбраната или безопасността на крайбрежната държава;

— акт на пропаганда, имаща за цел заплаха на отбраната или безопасността на крайбрежната държава;

— излитане във въздуха или кацане на военно устройство;

— товарене или разтоварване на стока или валута в противоречие с правилата на крайбрежната държава;

— акт на преднамерено и сериозно замърсяване;

— риболовна дейност;

— провеждане на изследователска дейност;

— всяка друга дейност, нямаща пряко отношение към преминаването.

В териториално море подводните лодки и други подводни транспортни средства са длъжни да се движат на повърхността и с издигнат флаг.

За преминаването си през териториално море чуждестранните кораби не плащат на крайбрежната държава никакви такси.

Суверенитетът на териториалното море се осъществява при спазване на конвенцията на ООН от 1982 г. [2] и други норми на международното право. Терминологичният юридически речник определя суверенитета като върховенство и независимост на държавната власт, нейно най-важно качество, характеризиращо политико-правната ѝ същност. Суверенитетът на крайбрежната държава над териториалното море служи, като основа за определяне на обема на нейните права по отношение на намиращите се в неговите пределите чуждестранни кораби и лица. Крайбрежната държава има право да издава нормативни актове за регламентиране режима на териториалното море. Тя установява правилен план на корабоплаване, за радиотехническите средства, за сигурността, за митническия и други надзор. Крайбрежната държава забранява на чужди кораби

да извършват както хидрографски работи и изследвания, така и морски риболов без специално разрешение. Така международното право разглежда териториалното море, като съставна част от държавната територия.

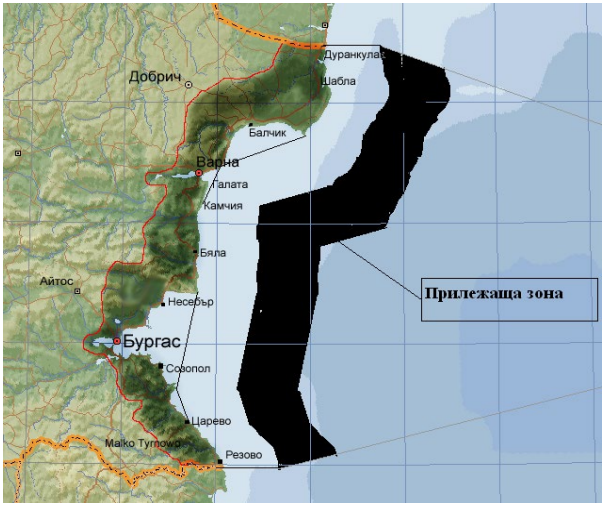
3.3. Прилежаща зона

В раздел IV, част II на Конвенцията на ООН на морско право от 1982 г. [2] озаглавен „прилежаща зона“ се подчертава, че:

В зоната принадлежаща към нейното териториално море наричана прилежаща зона, крайбрежната държава може да осъществява контрол необходим за предотвратяването на нарушенията на митническите, финансовите, граничните и здравните закони в пределите на нейната територия или териториално море, а така също и контрол необходим за наказание при нарушаване на закона и правилата.

Прилежащата зона не може да се разпростира извън пределите на 24 морски мили от изходните линии, от които се отмерва широчината на територията. На тази основа прилежащата зона може да се определи, като район прилежащ към териториалното море на крайбрежната държава, чиято външна граница не може да се сметне на повече от 24 морски мили от изходната линия от която се отмерва териториалното море.(Фигура 3)

Ако бреговете на две държави са разположени един срещу друг или са съседни нито едната от тях няма право ако не е постигнато споразумение да разпростират своята прилежаща зона зад средната линия, всяка точка на която стои на равно разстояние от най-близките точки на изходните линии, от които се измерва широчината на териториалното море.



Фиг. 3. *Прилежаща зона*

Правата, които се признават от международното право на крайбрежна държава в прилежащата зона се характеризират с:

— целевото си предназначение, тоест защитават определени интереси (митническите, финансовите, граничните и здравните);

— определено ограничение в техния обем или контролът може да има характер на инспекция с цел предотвратяване на определени нарушения.

За видовете прилежащи зони конвенцията има в предвид следните:

— митническите зони са най-стария вид прилежащи зони установени от държавата - в тях се осъществява контрол за опазване на постановленията на държавните органи регламентиращи външната търговия за да се предотврати внасяне и изнасяне през морските граници на стоки за които е наложена забрана;

— финансовите зони се създават с цел да се осигури контрол за опазване правилата и да не се допускат нарушения на финансовите закони на крайбрежната държава;

— в граничната зона крайбрежните държави осъществяват контрол за спазване на националната законодателност относно влизането и излизането в страната на чужденци;

— здравните зони се установяват с цел са осигурят изпълнението на международните санитарни правила за предотвратяване на разпространени на заразни болести по хора и животни.

Освен тези зони редица държави са установили и други специални зони, например: зона за наказателна и гражданска юрисдикция, риболовни зони, зони за морски контрол и други.

3.4. Континентален шелф

Континенталния шелф на крайбрежната държава включва повърхността на морското дъно и недрата на подводния район, който се разпростира отвъд нейното териториално море по цялото продължение на сухоземната територия до външния ръб на окрайнината на континента или на разстояние до 200 морски мили от изходните точки от които се измерват границите на териториалното море, там където външния ръб на окрайнината на континента не се разпростира до това разстояние.

Окрайнината на континента включва потопеното под водата продължение на земната маса на крайбрежната държава и са състои от повърхността на морското дъно и недрата на шелфа. Крайбрежната държава установява външния ръб на окрайнината на континента там, където тя се разпростира отвъд 200-те морски мили. Установените точки съставляващи външните граници на континенталния шелф на повърхността на морското дъно са разположени или на разстояние не по-голямо от 350 морски мили или на разстояние не по-голямо от 100 морски мили от 2500 метровата изобата.

Външната граница на континенталния шелф не надхвърля 350 морски мили от изходните линии от които се измерват границите на териториалното море, крайбрежната държава прокарва външни граници на нейния континентален шелф там където той се разпростира на разстояние по-голямо от 200 морски мили

от изходните линии, и предоставя информация на комисията за континенталния шелф и депозира при генералния секретар на ООН, карти и геодезически данни чрез които външните граници на континенталния шелф са описани трайно.

Крайбрежната държава упражнява в континенталния шелф суверенни права за промишлено проучване и експлоатация на природните ресурси. Ако не използва правата си никой не може да предприеме тези дейности без нейно съгласие. Правата на крайбрежната държава върху континенталния шелф не засягат правния статут на покриващите води или на въздушното пространство над тези води.

Всички държави имат право да полагат подводни кабели и тръбопроводи върху континенталния шелф съгласно установените разпоредби, със съгласието на крайбрежната държава, тя разрешава и контролира сондирането в континенталния шелф.

Делимитацията на континенталния шелф между държави със срещуположно положение или прилежащи брегове се извършва по споразумение въз основа на международното право, до постигане на крайно споразумение се полагат условия за постигане на временно договаряне.

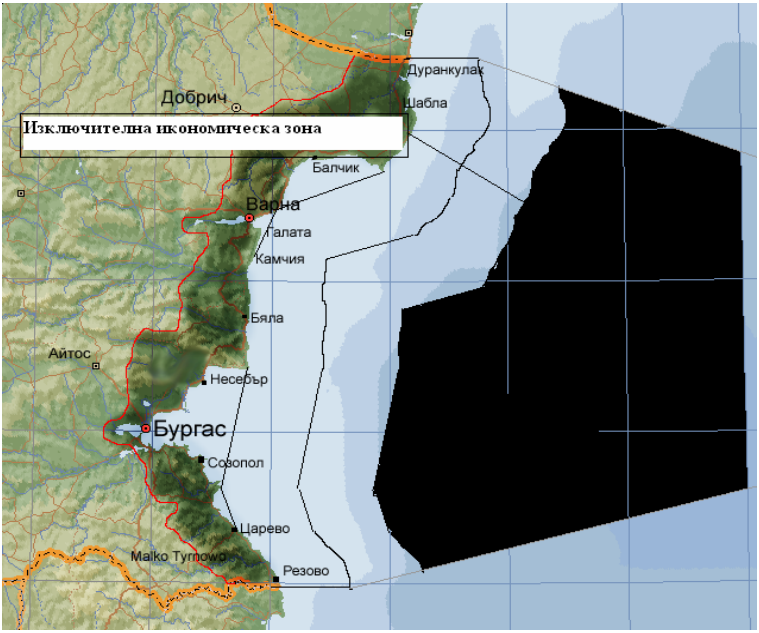
3.5. Изключителна икономическа зона

Изключителната икономическа зона е район, разположен отвъд пределите на териториалното море и прилежащ към него, намиращ се под особен правен режим, който урежда правата и юрисдикцията на крайбрежната държава и правата и свободите на другите държави.

Съгласно Конвенцията на ООН по морско право от 1982 г. [2] ширината на изключителната икономическа зона е до 200 морски мили от изходните линии, от които се измерва ширината на териториалното море. На крайбрежната държава се предоставят определени суверенни права и юрисдикция, които тя осъществява в точно изпълнение на разпоредбите на конвенцията (промишлено проучване и експлоатация, съхраняване и стопанисване на природните ресурси, намиращи се на морското дъно, в недрата и водите му). Има юрисдикция да създава и използва изкуствени острови, съоръжения и структури за морски научни изследвания, за защита и опазване на морската среда и други.(Фигура 4)

Всички държави се ползват в изключителна икономическа зона от свободите на корабоплаване и прелитане, полагане на кабели и тръбопроводи и от други международно правомерни начини за използване на морето, съвместими с разпоредбите на конвенцията. Другите държави са длъжни да зачитат правата и задълженията на крайбрежната държава и да спазват законите и правилата, приети от нея в съответствие с конвенцията.

Споровете се решават на основата на справедливостта, като се зачитат интересите на страните и на международната общност. Разграничаването на изключителната икономическа зона между държави със срещулежащи или прилежащи брегове става със сключване на международен договор. Повече от 80 държави имат изключителна икономическа или риболовна зони.



Фиг. 4. *Изключителна икономическа зона*

Изводи

1. Основен национален нормативен акт уреждащ правният режим в морските пространства е Закона на морските пространства, вътрешните водни пътища и пристанища на Република България. [1]

2. В морските пространства, вътрешните водни пътища и в пристанищата Република България упражнява суверенитет, определени суверенни права, юрисдикция и контрол в съответствие с общопризнатите принципи и норми на международното право и международните договори по който Република България е страна, както следва:

— във вътрешните морски води, се разпространява нейния суверенитет. Само крайбрежната държава има право да определя режима в своите води. Тя установява правилата на корабоплаване в тях, за риболов, за използване на радиотехнически средства, за полети на летателни апарати и други;

— в териториалното море, разпространява своя пълен суверенитет. Този суверенитет се разпростира отвъд сухоземната територия и вътрешните води на държавата. С границите на териториалното море се определят и държавните граници на крайбрежната държава;

— в прилежащата зона, осъществява контрол необходим за предотвратяването на нарушенията на митническите, финансовите, граничните и

здравните закони в пределите на нейната територия или териториално море и контрол необходим за наказание при нарушаване на закона и правилата;

— в континенталния шелф, упражнява суверенни права за промишлено проучване и експлоатация на природните ресурси;

— в изключителната икономическа зона, упражнява определени суверенни права и юрисдикция - промишлено проучване и експлоатация, съхраняване и стопанисване на природните ресурси, намиращи се на морското дъно, в недрата и водите му. Има юрисдикция да създава и използва изкуствени острови, съоръжения и структури за морски научни изследвания, за защита и опазване на морската среда и други.

ЛИТЕРАТУРА

[1] https://lex.bg/bg/laws/ldoc/2134907392, 22.11.2023 г.

[2] https://eur-lex.europa.eu/BG/legal-content/summary/united-nations-convention-on-the-law-of-the-sea.html, 22.11.2023 г.

МЕЖДУНАРОДНО МОРСКО ПРАВО – НАЧАЛО, РАЗВИТИЕ, ПРАВНИ ИНСТИТУТИ

Галин П. Петков

INTERNATIONAL MARITIME LAW - BEGINNING, DEVELOPMENT, LEGAL INSTITUTIONS

Galin P. Petkov

ABSTRACT: *This article is a kind of review of the emergence, development and confirmation in the legal framework of the legal institutes of the science of International Maritime Law, a constituent part of Public International Law. The connection between international customs and treaties - the main regulator in ancient times - with the current rules regulating international maritime law - treaties, agreements and conventions - is established. The conventions adopted by the UN General Assembly concerning the maritime spaces of the countries with access to the sea or ocean have been examined in detail.*

In conclusion, the author brings out the main legal institutions and their codification in UN conventions and EU directives.

KEYWORDS: *International Maritime Law, UN conventions on the Law of Sea, Geneva Conventions.*

1. Въведение

Както всяка отраслово правна наука, така и международното морско право има свои източници или онези правни форми, отразяващи волята на субектите на международното публично право.

Основни източници на Международното морско право се явяват международните договори и международните обичаи.

В продължение на много столетия Международното морско право се е развивало под въздействието на международни обичаи, които са били основен регулатор в древността. В един по-късен етап тези обичаи прерастват в правни норми посредством кодифицирането им в международноправни актове.

Международното морско право е съвкупност от юридически норми и правила, регулиращи отношенията между субектите на Международното публично право, възникващи във връзка с тяхната дейност по използване на морските пространства. По своята природа и същност Международното морско право е съставна част на Международното публично право. То също така е в корелативна връзка с останалите негови органични части - Правото на

международни договори, Международното въздушно право, Международното космическо право, Дипломатическото и консулско право.

Примерите в тази насока са следните нормативни документи:

— Договор за забрана разполагането на ядрени и други видове оръжия на морските и океанските дъна от 1971 г. [1];

— Чл. 3 от Спогодба за спасяване на космонавти, връщане на космонавти и връщане на обекти, изстреляни в космическото пространство (ратифицирана с указ № 250 ОТ 6.III.1969 г., ДВ, БР. 30 ОТ 1969 Г. влязла в сила на 16.IV.1969 г.) [2];

— Чл. 2 от Конвенцията на Организацията на обединените нации по морско право от 1958 г., която гласи за свободата да се лети над Открито море.

Правен статут на териториалното море и на въздушното пространство над териториалното море и неговото дъно и недра:

1. Суверенитетът на крайбрежната държава се разпростира отвъд нейната сухоземна територия и вътрешните й води, а за архипелажните държави и архипелажните им води - върху прилежаща морска ивица, наречена териториално море.

2. Този суверенитет се разпростира върху въздушното пространство над териториалното море, както и върху морското дъно и неговите недра.

3. Суверенитетът над териториалното море се осъществява, като се спазват разпоредбите на тази конвенция и другите норми на международното право. [3]

Виенската конвенция за консулски отношения от 1963 г. предвижда правото на консулите да оказват всякакво съдействие и помощ на кораб, плаващ под флага на държавата, представлявана в чуждата държава от консулските лица.

Тези актове са малка част от стотиците договори, споразумения и конвенции, подкрепящи тезите за взаимодействие на Международното морско право с останалите съставни части на Международното публично право.

2. Начало и развитие на Международното морско право. Правни институти

През 1927 г. Събранието на Обществото на народите свиква дипломатическа конференция за кодификация на три от пет готови теми, сред които е и тази за териториалните води. Интересно е, че не се съставят проекто-конвенции, а само доклади, обобщаващи различията и съвпаденията в излаганите мнения на интервюираните правителства. На конференцията, провела се в Хага 1930 г. са участвали 47 правителства, което никак не е малко за тогавашните измерения на световната общност. Въпреки това се приемат само 4 международни акта и то по проблемите на гражданството, като не се отделя внимание на Морското право. Може би за това от 1930 г. до края на своето съществуване Обществото на народите не се занимава с кодификационна дейност. Ето как е пропилян един опит за частично официално нормиране на Международното морско право.

Най-успешният и ползотворен период в развитието на съвременното Международното морско право започва след създаване на ООН. Общото събрание на ООН приема резолюция 94/1 от 31 януари 1947 г. за учредяване на Комитет за прогресивно развитие на Международното право и неговата кодификация, която включва представители на 17 държави. В резултат на неговата работа се учредява Комисия по международно право, чийто статут се одобрява на 21 ноември 1947 г. Този комитет е първият спомагателен орган на ОС на ООН, включващ към 18 ноември 1981 г. 34 представители.

Когато през 1949 г. Комисията по международно право избира основните теми на бъдещата си работна програма, тя изхожда от одобрен преди това меморандум. От 25 предложени в него въпроси са подбрани 14, които влизат в първоначалния дневен ред. Някои от тези 14 теми се доуточняват, т.е. разширява се предметът и се детайлизират някои елементи. През 1998 г. Комисията по международно право е представила окончателни проекти и доклади, които са материализирани в следните източници. Конкретно за Морското право те са:

А) Женевската конвенция за Открито море от 1958 г., подписана от 47 държави и влизаща в сила от 1962 г.;

Б) Женевската конвенция за териториалното море и прилежащата зона от 1958 г. - влизаща в сила от 1964 г. и подписана от 42 държави;

В) Женевската конвенция за континенталния шелф от 1958 г., подписана от 44 държави и влизаща в сила от 1964 г..

Интересен факт е малкият брой държави, подписали Женевските конвенции (от 42 до 47 при 86 държави участнички) и късният етап на влизане в сила вследствие забавена ратификация на конвенциите при нужен брой от 22 ратификации.

Всъщност Женевските конвенции се приемат в рамките на първата конференция за нормите и принципите на Международното морско право през 1958 г.

Втората конференция е през 1960 г., но тя не дава резултати. Голямо значение за Международното морско право дава Третата конференция от 1973 г. - 1982 г., която завършва с приемане на Конвенция на ООН по морско право, подписана в Монтегю Бей - Ямайка, състояща се от 320 члена и 9 приложения, която всъщност представлява доста сполучлив опит за кодификация на Международното морско право.

Международното право има продължителна и противоречива история на развитие. Генезисът на този институт е бил осеян със спорове още от 19 в., а в по-ново време те са засягали въпроса за суверенитета на крайбрежните държави върху този пояс като особено остри колизии има между държавите по отношение на неговата ширина. Този въпрос е бил в центъра на вниманието на три конференции - 1930 г. в Хага, 1958 г. и 1960 г. в Женева, но те така и не го решават.

Според чл. 1 от Женевската конвенция от 1958 г. териториалното море е пояс, долепен до брега и нищо повече относно ширината на този пояс. Според чл. 3 от Конвенцията от 1982 г. този пояс е с ширина не по-вече от 12 мили, измервани от изходната линия съгласно Конвенцията. [4]

В момента над 110 морски държави се придържат в своите законодателства около тази ширина. За изходните линии и начините им на отчитане и измерване Конвенциите от 1958 г. и 1982 г. се дублират. Всъщност според Опенхайн установената от Конвенцията от 1982 г. максимална ширина на териториалното море до 12 морски мили, като всеобща правна норма, е едно от най-забележителните постижения на Третата конференция в сравнение с неуредените от Женевските конференции проблеми. Конвенцията от 1982 г. прекратява всякакви спорове и спекулации на крайбрежните държави за разширяване на своя суверенитет върху значителни морски пространства в открито море.

Относно въпроса за делимитацията на териториалното море на държави със срещулежащи и принадлежащи брегове, двете конвенции са еднозначни (чл. 12 от Конвенцията от 1958 г. и чл. 15 от конвенцията от 1982 г.): "и там, където бреговете на две държави са срещулежащи или принадлежащи, нито една от двете държави няма право, ако между тях няма споразумение за противното, да разпростира еднакво разстояние от най-близките точки на изходните линии, от които се измерва ширината на териториалните морета на всяка от двете държави". Тази разпоредба не се отнася до исторически придобитите права или други обстоятелства, налагащи делимитиране на различно от посоченото в Конвенциите.

Друга проблематика от темата за териториалното море е тази за суверенитета на крайбрежната държава върху териториалното море, намерила решение в принцип на международното право - териториалното море се намира под суверенитета на крайбрежната държава. Въпреки това са се водили спорове за правния статут на териториалното море. Едни юристи смятат, че крайбрежната държава обладава правата на суверенитет над териториалното море, други твърдят, че тя има ограничен "функционален" суверенитет, а други пък са още по-дръзки и твърдят, че крайбрежната държава не е собственик, нито суверен на Териториалното море, а притежава само "пачка сервитутни". Тези различия се отразяват и в практиката на държавите. Конвенцията за териториално море и прилежащата зона от 1958 г. и Конвенцията на ООН по морско право от 1982 г. съдържат идентични по съдържание (чл. 1 от Конвенцията от 1958 г. и чл. 2 от Конвенцията от 1982 г.) и отговарящи на интересите на крайбрежните държави разпоредби относно суверенитета, т. е. държавата притежава териториално върховенство, т. е. държавен суверенитет както върху сухоземните си участъци, така и върху териториалното море. Тези разпоредби служат като основа за определяне на обема на нейните права по отношение на намиращите се в нейни пределе чуждестранни кораби и лица. Именно по силата на разпространения суверенитет върху териториалното море, крайбрежната държава има изключителното право да издава нормативни актове за регламентиране на режима в него. Тя установява правилата за корабоплаване, за радиотехническите средства, охраната, митническият, санитарният, фискалният и друг надзор. Като правило (закрепено и в двете конвенции - б.а.) крайбрежната държава забранява на чуждестранни кораби да се занимават с морски риболов, да извършват хидрографски и други операции без нейното изрично и специално разрешение. В същото време се отчита заинтересоваността и на другите държави от

използването на териториалното море, в чийто предели се намират най-удобните морски пътища и в търговско и в навигационно отношение. Предвид на това, както в Конвенцията от 1958 г. (чл. 14) така и в Конвенцията от 1982 г. (чл. 17) се признава на чуждестранните кораби правото на т. нар. "мирно преминаване" през териториалното море, при спазване на съответните изисквания. Приемайки това положение за "мирно преминаване", участниците в конференциите много правилно удовлетворяват и до днес интересите на крайбрежните държави и международното корабоплаване.

Правото на мирно преминаване през териториалните води, е възникнало и се е развило като международен обичай. Този обичай за първи път е бил преобразуван в международноправна норма в Конвенцията от 1958 г., чл. 14 - чл. 23. Това е един от сериозните успехи от тази първа конференция на ООН по Морско право, който е потвърден и в Конвенцията от 1982 г. Същата използва изходените положения на тази от 1958 г. относно териториалното море и прилежащата зона. Много от нормите са възприети, но в нея са включени и нови текстове. Редица от старите текстове са допълнени и конкретизирани, като се има предвид развитието на международното право и мореплаването, както и съвременните политически и териториални реалности.

Ако разгледаме чл. 14 от Конвенцията от 1958 г. определението на понятието "мирно преминаване" е доста по-повърхностно и общо, докато в чл. 19 от Конвенцията от 1982 г. са изброени 12 положения конкретизиращи характера на този вид преминаване. [5]

Друг пример за по-обстойния преглед на Конвенцията от 1982 г. са разпоредбите, касаещи преминаването на военни и подводни съдове, за които в Конвенцията от 1958 г. са определени само 3 разпоредби.

Освен това в Конвенцията от 1982 г. има и непозната до тогава разпоредба със следното съдържание: "Държавата на знамето носи международна отговорност за всяка загуба или щета…" (чл. 31 от Конвенцията от 1982 г.), т. е. тук вече се илюстрира и института за отговорност на държавите относно преминаването им през териториалното море на крайбрежна държава, отговорност, която през 1958 г. е била само частично и непълно обоснована и конкретизирана, ставаща причина за доста противоречива съдебна практика на държавите.

По отношение на юрисдикцията на крайбрежната държава върху чуждестранните кораби по време на пребиваването им в териториалното й море Конвенциите от 1958 г. и 1982 г. са идентични и разпоредбите им се свеждат до две основни юрисдикции: наказателна и гражданска. Дори залегналото в Конвенцията от 1958 г. правило за режима на изключителната икономическа зона се установява след консенсус на Третата конференция.

Следващият институт, разработен и кодифициран на Първата конференция е този за континенталния шелф. Конвенцията за континентален шелф от 1958 г. се разработва в период, когато интересите на държавите към природните богатства на Морското дъно са били ограничени главно в плитките райони. По това време възможностите за експлоатация на природните богатства над 100 м. са били невъзможни. Поради тази причина разпоредбите на Конвенцията от 1958 г. за външния предел на шелфа са били формулирани по

такъв начин, че теоретически се е допускала възможност за неограничено разпространение на суверенни права на държавите за проучване и разработване на природните богатства на Морското дъно.

В хода на подготовката на Третата Конференция на ООН по морско право, специалният комитет на ООН за Морското дъно, търси по-точна формула за определяне на външния предел на шелфа, на база дълбочината на покриващите води или на определено разстояние от изходната линия на отчитане териториалното море на съответната държава. Тези критерии стоят в основата на по-широко и детайлизирано понятие на континентален шелф и по-конкретно за външната граница, съдържащо се в чл. 76 от Конвенцията от 1982 г. Формулировката на чл. 6 от Конвенцията от 1958 г. е породила доста спорни моменти в стремежа си за справедливост. Пораждат се множество конфликти относно разграничаване на континенталния шелф: в Северно море между ФРГ, Холандия и Дания 1965 г.; спорът между Франция и Англия за шелфа в Ламанша и прилежащия район на Атлантика. Но доста държави, използващи метода на средната линия, залегнал в чл. 6 на Конвенцията от 1958 г. и спомогнал за споразумение за разграничаване на шелфа на Северно море от съответните участници: Англия и Норвегия - 1965 г.; Англия и Холандия - 1965 г.; Англия и Дания - 1966 г. Съществуват и ред съглашения с отчитане на "особени обстоятелства". Например: съглашението между Иран и Катар от 1969 г.; Иран и Бахрейн за континенталния шелф в Персийския залив от 1974 г.

С оглед преодоляване на тези негативни последици, както и създаване на по-гъвкава и по-справедлива основа за решаване на въпросите, възникващи във връзка с разграничаване на континенталния шелф между държавите със срещулежащи и съседни крайбрежия, Третата конференция на ООН по морско право в приетата от нея Конвенция в чл. 83, акцентира на принципа за споразумението между спорещите държави. Ако възникне спор, то той се решава от Международен съд по справедливост.

За първи път проблемът за понятието " архипелаг " и статута на неговите води е бил на дневен ред през 1930 г., а по-късно през 1958 г. Но и в двата случая не се взема решение по този въпрос. За първи път уредба на този институт с правни норми се прави в Конвенцията от 1982 г. (чл. 46). Проблематиката е разработена с цел научни и практически нужди. Тук е важно да се подчертае, че постановките за архипелажни води изиграват огромно значение за корабоплаването и съответната делимитация на териториалното море, континенталния шелф и прилежащите зони. Освен това има и "приоритетно значение" според Международната морска асоциация за Открито море и юрисдикцията в такива реалии.

Понятието за Открито море според Конвенцията от 1982 г., е пространство, започващо от външния предел на териториалното море на крайбрежната държава, което в общи линии е идентично с понятието от чл. 1 от Конвенцията от 1958 г. [6] Основна разлика между двете конвенции е, че тази от 1958 г. признава суверенни права само върху териториалното море и вътрешните морски води, а тази от 1982 г. включва и едно ново понятие - "функционален суверенитет" - по отношение на изключителната икономическа зона, която е била

непозната до тогава и “континентален шелф”, който макар и обявен за суверенна част е бил доста мъгляво формулиран.

Но като голям плюс на Конвенцията от 1958 г. трябва да се отбележи чл. 2, който отразява свободите на открито море, които са възприети като сърцевина и основа на международноправния режим на Открито море и в Конвенцията от 1982 г. (чл. 87). Тези свободи са прогласени дори за правни принципи и са всеобщо признати в следствие обективната потребност на държавите за свободно ползване на морските пространства. В Конвенцията от 1982 г. има само две нови свободи, допълващи Конвенцията от 1958 г. - свободата за строеж на изкуствени острови и други съоръжения и свободата на научни изследвания. Това е продиктувано от научния прогрес и неговото влияние върху човечеството. Общо взето Конвенцията от 1982 г. копира разпоредбите на Конвенцията за открито море от 1958 г., без да внася някакви съществени промени и допълвайки тези разпоредби с нуждите на новото време.

Други два нови въпроса за морското право са приетите норми за затворени и полузатворени морета и “морското дъно” от Конвенцията от 1982 г. Регламентацията на затворените и полузатворените морета в чл. 122 и в чл. 123 е по - скоро дерелативна, докато въпросите за морското дъно са доста добре разработени, предвид факта, че това е един от възловите проблеми на Третата конференция на ООН по морско право и е бил предмет на продължителни и сложни дискусии. До приемане на Конвенцията от 1982 г. по линия на ООН е извършена значителна експертна работа за изясняване и оценка на редица принципи, определяща дейността на държавите по използването на морското дъно. За целта се създава и специален Комитет по морското дъно, на който в последствие се възлага и цялостната работа по подготовката на самата конференция. Регламентацията на този проблем се оценява като едно от най-забележителните нововъведения в кодификацията и прогресивното развитие на морското право според професор Ал. Янков.

Конвенцията на ООН по морско право от 1982 г. е всеобхватно кодифицирано морско право, която наред с традиционните институти, съдържащи се в Конвенциите от 1958 г., отделя особено място и на нови такива, както и на опазването на морската среда, научните изследвания, съвременните морски технологии и сътрудничество. Всъщност Конвенцията от 1982 г. представлява един универсален морски регулатор и всяка морска държава е заинтересована от него.

Заключение

От изложеното по горе, могат да бъдат направени следните **изводи:**

1. Относно териториалното море: Конвенцията от 1982 г. прекратява споровете за суверенитета на крайбрежната държава върху него и прибавя нови постановки относно свободите. Освен това, регламентира и доразвива отговорността на държавите при преминаването им през териториалното море. Конвенцията от 1958 г. с прогресивна мисъл залага като правна норма имунитета на военните кораби.

2. Относно прилежащата зона: Конвенцията от 1982 г. установява ширина от 24 морски мили за този пояс, а тази от 1958 г. - 12 морски мили.

3. Относно континенталния шелф: Конвенцията от 1982 г. формулира крайно понятие, което е доста по-разгърнато и по-ясно отколкото това от 1958 г., което позволяваше спекулации на търговско развитите държави.

4. Относно изключителната икономическа зона: в конвенцията от 1958 г. липсва такъв институт, а в тази от 1982 г. предвид новите изисквания на корабоплаването и търговията тя се регламентира.

5. Относно откритото море: Конвенцията от 1982 г. признава функционален суверенитет на крайбрежната държава върху този пояс, докато тази от 1958 г. не признава такъв. Трябва да се отбележи и преимуществото на Конвенцията от 1958 г., която за първи път установява свободите на откритото море, а Конвенцията от 1982 г. допълва две нови - за хидрографски изследвания и за изкуствените острови.

6. Относно полузатворените и затворените морета: Конвенцията от 1958 г. не познава такова понятие, а тази от 1982 г. просто го декларира и чрез аналогия на правото се формулират основните постановки.

7. Относно морското дъно: Конвенцията от 1958 г. не решава такъв проблем, защото развитието на корабоплаването и науката не е било на достатъчно ниво, а за Конвенцията от 1982 г. този проблем е бил възлов и доста експертен материал е бил разгледан преди окончателното му систематизиране и закрепване в правни норми.

8. Относно архипелага: участниците в Конвенцията от 1958 г. го поставят на дневен ред, но не намират решение, а Конвенцията от 1982 г. го регламентира и делимитира с цел големите нужди на корабоплаването.

В областта на търсенето и спасяването, и за опазване на природната среда Република България е подписала и прилага:

— Международна конвенция за безопасност на човешкия живот по море, 1974 г. /SOLAS/ [7];

— Международна конвенция за Търсене и Спасяване на море /SAR-79/ [8];

— Международна конвенция за предотвратяване сблъскванията на море /COLREG-72/ [9];

— Директиви на ЕС – 98/41/ЕС [10] и 2002/59/ЕС [11], с които се създава информационна и мониторингова система за корабния трафик в Общността.

За Черноморския регион в правното пространство действа Конвенцията за Черноморските Проливи, подписана в Монтрьо през 1936 г. Тя провъзгласява пълна свобода на търговското мореплаване в Проливите (Босфор и Дарданели) както в мирно, така и във военно време, ако самата Турция не е воюваща страна. В противен случай на свободно преминаване през проливите имат право само корабите на неутралните страни, които не съдействат на противниците на Турция. Въведени са ограничения за не черноморски държави относно типа на корабите (с водоизместване до 10 000 т и оръдия с калибър до 203-мм) и времето на престояване в Черно море (до 21 дни).

ЛИТЕРАТУРА

[1] https://www.ekoarhiv.bg/system/files/documents/710211_dogovor_zabrana_orazia_okean_KZP_1971.pdf, 18.10.2023 г.

[2] https://www.ciela.net/svobodna-zona-darjaven-vestnik/document/-20164608/issue/347/spogodba-za-spasyavane-na-kosmonavti-vrashtane-na-kosmonavti-i-vrashtane-na-obekti-izstrelyani-v-kosmicheskoto-prostranstvo-(ratifitsirana-s-ukaz-№-250-ot-6iii1969-g-dv-br-30-ot-1969-g-vlyazla-v-sila-na-16iv1969-g), 18.10.2023 г.

[3] https://legislation.apis.bg/doc/3938/0, 18.10.2023 г.

[4] https://legislation.apis.bg/doc/3938/0, 18.10.2023 г.

[5] https://legislation.apis.bg/doc/3938/0, 18.10.2023 г.

[6] https://www.ciela.net/svobodna-zona-darjaven-vestnik/document/-22526973/issue/2179/konventsiya-za-otkritoto-more, 18.10.2023 г.

[7] https://www.mtc.government.bg/sites/default/files/mejdunarodna_konv_za_bezop_coveskiq_jivot_na_more_1974_izm_1988.pdf, 18.10.2023 г.

[8] https://www.marad.bg/bg/node/985, 18.10.2023 г.

[9] https://www.marad.bg/bg/node/877, 18.10.2023 г.

[10] https://eur-lex.europa.eu/legal-content/bg/TXT/?uri=CELEX%3A31998L0041, 18.10.2023 г.

[11] https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32002L0059, 18.10.2023 г.

ОТНОСНО ПАДНАЛИТЕ СЪЮЗНИЧЕСКИ САМОЛЕТИ ПРЕЗ ВТОРАТА СВЕТОВНА ВОЙНА НА БЪЛГАРСКА ТЕРИТОРИЯ – РЕАЛИСТИЧЕН АНАЛИЗ

Станимир С. Станев, Орлин М. Георгиев

ON THE FALLEN ALLIED AIRCRAFTS DURING WWII ON BULGARIAN TERRITORY - A REALISTIC ANALYSIS

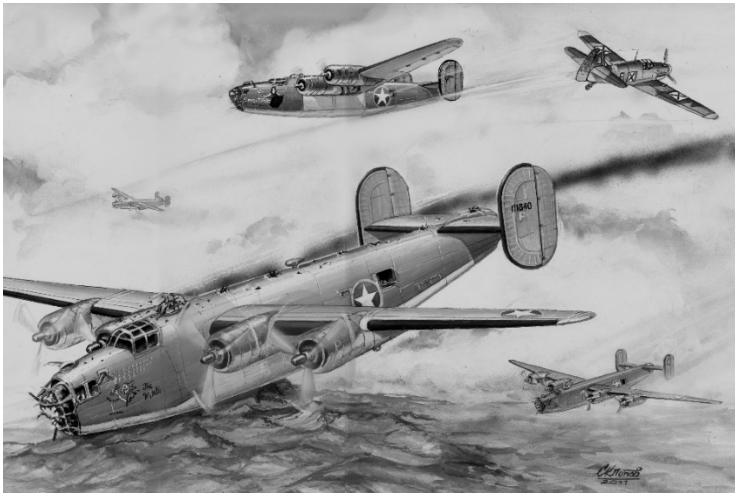
Stanimir S. Stanev, Orlin M. Georgiev

ABSTRACT: *Based on a long-term comprehensive analysis of foreign and domestic archival documents, interviews, witness statements and own field studies, the authors present data on the Allied aircraft shot down in Bulgaria during the WWII from September 1941 to September 1944. References are given for 60 planes fell in today's territory of the country. For the first time in the scientific community, the locations of the crashes of these planes are shown on a map of Bulgaria.*

KEYWORDS: *Bulgaria in WWII, Aviation history, USAAF loses, RAF loses, Fallen planes in Bulgaria, Maps of crashes.*

Увод

Военните събития през лятото на 1943 г. опровергават пропагандата на тогавашните български управници за „символична война“, която те на 13 декември 1941 г. обявяват на САЩ и Обединеното кралство под натиска на Германия. Средиземноморските съюзнически военновъздушни сили (MAAF), започват стратегическата операция „Point Blank“- тежки бомбардировки от американската и английската авиации на цели в Германия и нейните съюзници, включително България. Военновъздушните сили на армията на САЩ (USAAF) бомбардират денем, а кралските военновъздушни сили (RAF- Royal Air Force) действат предимно нощем. В края на войната в България в резултат от тези бомбардировки са убити 1828 души и 2372 ранени. Столицата София е в руини - разрушени и повредени са над 12000 сгради [1]. Въпреки недостатъчния брой изтребители и липса на боен опит, българските летци, заедно с действията на противовъздушната артилерия (ПВА) се опитват с променлив успех, да противодействат на противниковата авиация, за да намалят разрушенията и жертвите в българските градове. Геройски загиват 16 български пилоти. Немската авиация също участва в защитата на София. На 10 януари 1944 г. загива капитан Герхард Венгел (Gerhard Wengel) – командир на 1 група от изребителна ескадра 5 (I./JG 5 „Eismeer“) на Луфтвафе, базирана на летище Враждебна.



Фиг. 1. *Художествено представяне на поразяването на първия американски бомбардировач B-24D с надпис „Вещицата“(“The Wittch”), на 1 август 1943 г. от български изтребител, пилотиран от поручик Стоян Стоянов. Картината от художника Стоян Костадинов Попов бе любезно предоставена на авторите*

За въздушните битки по време на Втората световна война над България и съседните балкански страни има много публикации. Един от спорните въпроси, по които се отличават, са данните за загубите на съюзническата авиация над България, изразени в паднали самолети, убити и пленени членове на екипажи.

Основната цел на настоящата статия, е да представи резултати, потвърдени на базата на дългогодишни изследвания на авторите в архивни документи, документални публикации, мемоари, документирани свидетелски показания на съвременници и чрез теренни обхождания, за загубите на съюзническата авиация и достоверна информация за местата на паднали съюзнически самолети в резултат на бойни действия на сегашната територия на България за времето от 1 август 1943 г. до 31 август 1944 г.

1. Паднали самолети на съюзническата авиация (САЩ Великобритания, СССР)

В трудовете на нашите изследователи К. Скотунов, И. Бориславов, Д. Недялков, М. Христов, Й. Миланов, Р. Руменин, Н. Сладкаров и др. броят паднали самолети на съюзниците варира от 57 до 147 [2]. По-малък брой – 53 паднали самолети (41 бомбардировача и 12 изтребителя), намираме в американски архивни документи [3]. Авторът на излязлата през 2006 г. чуждестранна книга за военнопленническия лагер в Шумен, бившия военнопленник в него Робърт Джонсън (Robert Johnson), написана след нашите

разговори при посещението му в Шумен през 2004 г., посочва за американските загуби общо 60 бомбардировача и изтребителя [4]. През 2018 г. излезе от печат илюстрираната двутомна книга на унгарския изследовател Denes Bernad (Денеш Бернар), за българската изтребителна авиация, плод на негови двадесетгодишни изследвания. В нея Денеш, с когото ние коментирахме загубите на съюзната авиация, преди нейната публикация, дава списък за 113 поразени американски изтребителя и бомбардировача. Той е включил в този списък и самолети, които само са били повредени, или са паднали извън териториите под българско управление. Все пак прави уговорката, че този списък със загуби не е изчерпателен. Той препоръчва по-нататъшни изследвания, по-специално на подробностите за изчезнали самолети и тези, повредени във въздушен бой, които са се върнали в авиобазата, от която са излетели [5].

През 2011 година бе първата публикация на Станимир Станев и Рандъл Ханъм с резултати за броя на падналите съюзнически самолети на територията под български контрол от 1941 до септември 1944 г. [6]. В нея бе прието отчитането на загубите да става по достоверни източници за територии, намиращи се под контрола на българската армия. За тези територии се представиха общо 95 съюзнически самолета, за които има информация за паднали самолети или загуби на членове на екипажи, и за 85 паднали в тези територии самолети (тогава не бяха отчетени 2 съветски самолета).

Този принцип за отчитане на загубите в посочените териториални граници е възприет и от Румен Руменин в неговата книга „Летящи крепости над България“. Той посочва 114 паднали самолети на американците и англичаните на тези територии [1].

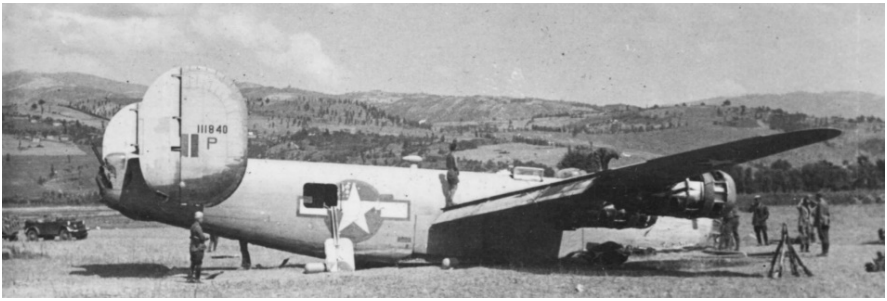
Някои от причините за различията относно броя на свалените самолети се посочват от Румен Руменин - непълни архивни данни, грешки при отчитане на въздушните победи, унищожени архиви. През войната местните административни органи са били задължени да докладват за всички произшествия, в това число и за падналите самолети и парашутисти. Има случаи, в които един паднал самолет е отчитан 2 или 3 пъти в архивни документи от наши военни, базирани на сведенията от кметовете на съседни села, между които е паднал самолета. В книгата на Руменин също има такива примери. По сведения от архивите, които е използвал, той е посочил, че на 24 юни 1944 год са паднали 4 самолета край село Дичево, Слистренска област (старото име е Половник Тошково до 1951 г.) [1], докато реално на около 9 км североизточно от селото е паднал само един бомбардировач (пилот Ван Поперинг), между селата Нова Попина и Поляна.

На базата на сведения, вероятно от кметовете на селата Горно Пещене, Тишевица, Вировско и Горна Кремена от област Враца, Руменин е отбелязал падането на 4 американски самолета на 11 юни 1944 г. В една от нашите експедиции с американци от отдела за военнопленници и изчезнали при акция на Пентагона (USDod/DPMO) установихме, че на 11.06.1944 г. е паднал само един американски самолет край село Горно Пещене. Има още няколко подобни дублирания на сведения – за Самоков, Костелево, Кнежа и др., но задачата ни тук не е да обсъждаме тези пропуски. Всъщност неговият списък бе стартовата точка в края на 90-те години, откъдето започнаха изследванията на Станимир Станев и

възможностите за надграждането му. Едва ли Румен Руменин, на когото трябва да благодарим отново, че добросъвестно е събирал данни от архивите, си е поставил трудната задача да анализира всеки от тези случаи и да ги сверява с топографски карти на България, Сърбия и Северна Македония.

Но това направиха авторите на настоящата статия в края на 2023 г. Рискувайки да влезем в спор с някои „диванни експерти“, публикуваме обобщените данни от нашите проучвания и изследвания.

За първите проведени въздушни боеве от нашата авиация на 1 август 1943 г. от района на връх Ком до района южно от Цариброд (днешен Димитровград в Сърбия), за падналите извън сегашната територия на България 4 американски бомбардировача B-24D са признати победи на поручик Стоян Стоянов, неговия воден подпоручик Иван Бонев, поручик Христо Кръстев и неговия воден подпоручик Петър Бочев [7] (фиг. 2 и фиг. 3).



Фиг. 2. *Поразената от поручик Стоянов „Вещица“ след аварийното кацане на 1 август 1943, заобиколена от български военни [архив на Симеон Цветков]*

Фиг. 3. *Съветски торпедоносец Ил-4Т от 5 ГВМТАП на КЧФ с мина АМГ-1. Самолет от същия тип е свален на 15 септември 1943 г., този ден е носел две английски мини (получени по „лend-лиз“) тип A-I-IV*

Първият съюзнически самолет, паднал на територията на днешна България, е съветския бомбардировач „Ил-4Т“ (фиг. 4). На 14 септември 1943 г. той е поразен от германски нощен изтребител Ме-110 след завръщане от мисия по дълбочинно миниране на р. Дунав между Свищов и Русе. Пада южно от село Професор Иширково, Силистренско [8]. В следващите текстове той има условен номер **1(5F).**

Фиг. 4. *Септември 1943: Останки от сваления Ил-4Т в двора пред кметството в с. Професор Иширково (любезно от РИМ-Силистра)*

На базата на анализа на достъпните американски [9] и наши архивни документи **[**10, 11, 12, 13, 14, 15, 16], мемоарна литература [17], интервюта, свидетелски показания и собствени проучвания, авторите предлагат в следващата таблица 1, обобщени данни за загубите на „англо-американската“ и съветската авиация на териториите под българско управление до началото на септември 1944 г.

Съставянето на таблицата бе продължителен, и вероятно, още незавършен процес, започнал от данните, публикувани в книгата на Румен Руменин [1]. При това за достоверен факт за паднал самолет се приеха данни от следните източници на информация:

— най-малко 2 различни български архивни документа (основно от справки в Държавния военно исторически архив (ДВИА) - В. Търново), касаещи

един и същи случай на катастрофа по време, място и тип на самолета, в това число и резултат от разследване на органи на МВР;

— официалени американски доклади за изчезнали екипажи – (MACR – Mission Air Crew Reports) или английски документ (RAF Form 441A) за изчезнал самолет и официални чуждестранни публикации;

— първостепенни свидетелски показания, получени чрез интервюта на мястото на катастрофа;

— резултати от теренно проучване на екип от специалисти от отдела за издирване на изчезнали военни на САЩ (DPMO) или от екип на Българската армия (БА).

Дневниците на българските и чуждестранните военно въздушни сили (ВВС), описващи победите на летците, мемоари и исторически четива без посочени източници са взети само са сведение, поради често субективния им характер. Поради това, че някои от тях не са потвърдени, тези сведения се класифицират като „съобщение за случай на катастрофа(ССК)“ [1]. По същия ред се процедира и със сведения от непреки (второстепенни) свидетели. Не са включени паднали самолети в Румъния и други страни, от които няма намерени убити или пленени на посочените територии, независимо от причината за свалянето им.

Типовете свалени съюзнически самолети са:

От американските бомбардировъчни групи (съответстват на авиополкове в други ВВС) (BG - Bombng group) най- много загуби има 376-та BG, а от ескадрилите - от 343 ескадрила (Squadron) на 98-ма BG. Най-много загуби изтребители има от 82-ра изтребителна група (82 FG). Типовете паднали самолети са:

— от USAAF: Бомбардировачи: B24 - B24D, B24G, B24H, B24J; B17 - B17F, B17G; Изтребители: P38 - P38F, P38G, P38J; P51 - P51B, P51C, P51D;

— от RAF: Wellington Mk.X; Liberator VI.

— от ВВС на ЧФ на СССР: Ил-4Т; А-20 „Boston 3“.

Проучванията на авторите доказват, че за **91 съюзнически самолети** летяли над териториите под българско управление, има документирани загуби на самолети и личен състав, до началото на септември 1944 г. Не всички от самолетите обаче са паднали в тези граници. Според нашите последни проучвания, потвърдени от независими източници и архивни документи, там са паднали **общо 83 съюзнически самолети.** От тях **69** са на американските въздушни сили (USAAF)**, 12** са на въздушните сили на британската общност (под общо английско командване на RAF, 205-та група)**, и 2** съветски самолета от ВВС на Черноморския флот.

Ние смятаме, че от всичките 91 самолета, броят на падналите съюзнически самолети в границите на съвременна България е **60** изтребителя и бомбардировача. Получените резултати от новите проучвания коригират броя на падналите самолети в наши предишни научни публикации [6]. Това е минималния брой доказани загуби към 2023 г., като е възможно броят им да се увеличи при поява на нови веществени доказателства. Тези резултати се отличават значително от данните в публикациите на уважавани от нас автори,

които са направени най-вероятно поради липса на обективни данни за действията на нашата авиация и противовъздушна артилерия, и доклади за победи чрез субективни преценки.

Интересен, но в същото време е спорен въпросът, какъв е реалният принос на българската изтребителна авиация и противовъздушната артилерия за посочените загуби на съюзическата авиация.

Наши автори посочват, че изтребителната ни авиация е свалила между 47 до 54 противникови самолета [3]. Посочената бройка в заповед № 78/12 декември 1944 г., че само противовъздушната артилерия е свалила през войната 69 вражески самолета [18], според нас не е коректна.

Таблица 1.

Принадлежност/Тип на самолета/ Брой	**Модификация**	**Паднали самолети,брой**
USAAF / B-24 / 39	**B-24 D**	5
„Liberator“	**B-24 G**	14
	B-24 H	12
	B-24 J	8
USAF / B-17/ 9	**B-17 F**	4
„Flying fortress“	**B-17 G**	5
CW (Common wealth)		
(RAF,SAAF,RAAF) / 12		
„Wellington“(„Wimpy”)	Wellington Mk. X	10
„Liberator“	Liberator B. VI	2
СССР, ВВС ЧФ / 2	Ил-4Т	1
	A-20G	1
Общо бомбардировачи		62
USAAF P-38/ 15	P-38 F	2
„Lightning“	P-38 G	6
	P-38 J	7
USAAF P-51/ 6	P-51 B	4
„Mustang“	P-51 C	1
	P-51 D	1
Общо изтребители		21
Общо паднали		**83**

След направения анализ на данните от американските доклади за причините за катастрофите на техните изтребители и бомбардировачи може да се направи извода, че в разглежданите от нас територии под български контрол, от 83 паднали самолета, българските изтребители са свалили 23 американски самолета в дните, които са летели [5, 7]. Противовъздушната артилерия е свалила от 3 до 4 американски самолета и 1-2 английски самолета при нощните им бомбардировки над страната.

Анализът на загубите на противника може да се продължи и в посоката на недоказаните загуби, като се отчетат падналите над територията на Югославия и Албания, както и в Адриатическо море съюзнически самолети. От получените от колеги-изследователи списъци (Милош Боянич от Белград и Дан Мелинте от Букурещ) на загуби, причинени над Румъния и България самолети, и от действията на германската авиация и зенитна артилерия, защитавайки важни обекти с известно приближение тези загуби, причинени от действията на нашите изтребителите и противовъздушната артлерия, към посочения по – горе брой от 83 самолета, може да се добавят над 25 паднали самолета на съюзническата авиация. От тези 25 вероятно 13 са поразени над България, отчитайки дните, когато са действали българските изтребители и противовъздушната артилерия [5, 7].

Следват кратки справки за съюзническите самолети, паднали на територията на днешна България. За всеки самолет справката започва с пореден номер, който съответства и на номера от представната в т. 2 карта с локациите. В скоби след този номер е посочен и съответният му индекс, присвоен от Станимир Станев и Марк ЛаСкот с цел бърза връзка в други техни публикации с разработената от тях база от данни за загиналите и пленени членове на екипажите [19]. В текста следва датата на катастрофата на самолета и по-конкретно описание на мястото на падане на самолета, уточнено от авторите на базата на сравнение на данни от редица достоверни източници. Следват типа на самолета, серийният му номер, неговата войскова принадлежност – номер на бомбова (BG) или изтребителна група (FG), номер на ескадрилата (Sq); званието и името на пилота; броят на членовете на екипажа; броят на загиналите (KIA- Killed in action) и пленените у нас членове на екипажа (POW- Prisoner of war) и в скоби номера на доклада за изчезнал при акция екипаж от ВВС на САЩ - USAAF - (MACR). Следва описание на целта на мисията на самолета и причината за неговата катастрофа. За някои самолети в текста има характеристика на мисията или посочване на конкретна причина за падането му.

1(5B): 14.IX.1943, обл. Силистра, 5 км Ю/З от село Професор Иширково (старо име- с. Кочина), (43°57'34"N 27°8'5"E). **Ил-4Т** от 5 ГМТАП, КЧФ (СССР); пилот ст. лейтенант Д.Бабий, екипаж 4: 3 KIA и 1 POW в Германия. След миниране на р. Дунав м/у Свищов и Русе свален от германски нощен изтребител Ме-110.

2(11B): 20.XII.1943, обл. София, 5 км Ю/И от Панчарево, местност „Урвич“, към с. Долни Пасарел. **B-24J** сер.номер 4273428, от 376 BG/515 Sq/; пилот 2L Robert Brown, екипаж 10: 9 KIA и 1 POW (MACR 1592). Цел - София, свален чрез насрещен таран в дясното крило от поручик Димитър Списаревски. Загиналите са погребаии в с. Панчарево. Опашният стрелец Робърт Ренър е военнопленник в лагера в Шумен.

3(13F): 20.XII.1943, обл. Перник, 20-25 км Ю/Ю-З от София. към с. Извор. общ. Радомир. **P-38F** сер.номер 432151 от 82 FG/96 FSq/; пилот 2L George Mitchell, POW (MACR 1600). Цел - София, свален от подпор. Никола Начев.

4(14F): 20.XII.1943, Столична общ., 20-25 км Ю/Ю-И от София, 5 км С/З от с. Долни Пасарел. **P-38G** сер.номер 432532 от 82 FG/97 FSq/; пилот 2L John McLendon, POW (MACR 1601). Цел - София, свален от поручик Виктор Павлов.

5(12F): 20.XII.1943, обл. Перник, 25-30 км Ю/Ю-З от София, общ. Радомир. **P-38G** сер.номер 432413 от 82 FG/97 FSq/; пилот 2L Edward Tinker, POW (MACR 1599). Цел - София, свален от подпор. Георги Кюмюрджиев.

6(16B):10. I.1944, обл. Перник, 2 км Ю/З от с. Радибош, общ. Радомир. **B-17F** сер.номер 425170 от 99BG/347Sq/; пилот 2L Dale Shupe, екипаж 10: 9 POW и 1 KIA (MACR 1819). Цел - София, свален съвместно от български изтребители и противовъздушната артилерия.

7(17B):10. I.1944, обл. Перник, 2 км С/З от село Кладница, в м. „Голо бърдо". **B-17F** сер. номер 425811 от 2BG/20Sq/; пилот 2L Thomas Finch, екипаж 10: 7 KIA и 3 POW (MACR 1824).Цел - София, свален съвместно от български изтребители и противовъздушната артилерия.

8(18F): 10. I.1944, обл. София, 200 м източно от с. Гълъбовци общ. Сливница, местност. „Валозите". **P-38G** сер.номер 432458 от 14FG/48Sq/; пилот Cpt. George Richards, KIA (MACR 1816). Цел - София, свален от български изтребител (кап. Чудомир Топлодолски).

9(22B): 30. III.1944, обл. Перник, с. Кошарево- с. Станьовци, общ. Брезник. **B-17 G** сер.номер 4231683 от 2BG/20Sq/; пилот 2L Leroy Rigney, екипаж- 10: 10 KIA (MACR 3364). Цел-София, свален от български изтребител (подпор. Христо Костакиев). Според американски източници паднал след катастрофа в облаците с бомбардировач номер 10 (23B).

10(23B): 30. III.1944, обл. Перник, с.Кошарево - с. Станьовци, общ. Брезник. **B-17 G** сер.номер 4231851 2BG/20Sq; пилот 1L Fred Wickham, екипаж - 10: 10 KIA (MACR 3370). Цел - София, поразен от взривилия се в облаците летящ над него бомбардировач, поразен от българският изтребител наподпоручик Костакиев. Според американски източници, 9 (22B) пада надолу и удря с лявото си крило в кабината му и го разбива.

11(26B): 5. IV.1944, обл. Монтана, с. Златия (с. Куле Махала), общ. Вълчедръм. сер. номер 4231182 от 301BG/419Sq/; пилот 2L Jess Coppedge, екипаж 10: 10 POW в Румъния (MACR 3882). Цел - Плоещ, свален от изтребител в Румъния.

12(27F): 15. IV.1944, обл. Русе, с. Тръстеник - с. Мечка, общ. Иваново. **P-38J** сер.номер 42104102 от 14FG/37Sq/; пилот 2L John Ingram, пилотът намерен на 1,5 км източно от Тръстеник, до пътя за с. Пиргово (MACR4371). Цел - Букурещ, свален от изтребител в Румъния.

13(28F): 15. IV.1944, обл. Русе, 1600-2000 м източно от от с. Сандрово, общ. Русе. **P-38J** сер.номер 4267965 от 14FG/37Sq/; пилот 2L Joseph Garrity, POW (MACR 4368). Цел - Букурещ, свален от изтребител в Румъния.

14(29F): 15. IV.1944, обл. Русе, с. Пиргово, общ. Иваново. **P-38J** сер.номер 42104151 от 14FG/37 Sq/; пилот 1L Robert Zimmerman, POW (MACR 4378). Цел - Букурещ, свален от изтребител в Румъния.

15(30F): 17. IV.1944, обл. Перник, до с. Друган, общ. Радомир. **P-51B** сер.номер 42106479 от 31FG/309Sq/; пилот 2L Raymond Dameron, POW(MACR 4230). Цел - София, Свален чрез таран от поручик Неделчо Бончев.

16(31B): 15.V.1944, Черно море, източно от Констанца или Шабла. **A-20 „Бостън 3“** от 13 ГМТАП на КЧФ (СССР) пилот капитан В. Мейев, екипаж 4: 2 KIA, 2 MIA. Цел – Констанца - Сулина, свален от германски изтребител над Черно море. Координати съгласно доклад на Luftwaffe: 98728 (Координатите са дадени по системата Gradnetz (GNMV), използвана от Луфтвафе за отблязване на местата на победите. Вероятно мястото е в трапеца 34Ost, или 24Ost.) [20].

17(32B): 6.V.1944, обл. Видин, 700 м С/З от с. Войница, общ. Кула. **B-24H** сер.номер 4252282 от 455BG/742Sq/; пилот 1L William Beck, екипаж 10: 7 KIA и 3 POW (MACR 5459). Цел - Кампина (Румъния), свален от изтребители в Румъния.

18(33B): 6/7. V.1944, обл. Видин, С/И от с. Вълчек, общ. Кула, в подножието на възвишението Върголия. **Wellington Mk.X** ном. LN982’Q от 205 група на RAF/40Sq/; пилот FS K.C.J. Martin, екипаж 5: 5 POW. Цел - Букурещ, преди целта 2 двигателя отказват и екипажът напуска самолета.

19(34B): 7/8. V.1944, обл. Перник, 7 км Ю/З от гр. Земен, местност „Черепиш“, западно от с. Блатешница, общ. Земен. Wellington Mk.X номер LN804’T’ от 205 група на RAF /40Sq/; пилот W/O T. Bradshaw, екипаж 5: 1 KIA, 4 се приземили в Югославия, 80 км Ю/З от Турну Северин. Четиримата са спасени поотделно от селяни и от четници на Дража Михайлович. Цел - ж.п. мост 4-5 км западно от Филиаси (Румъния), свален от румънски 20 мм зенитни оръдия, прикриващи моста.

20(35B): 13.V.1944, обл. Враца, с. Галиче, общ. Бяла Слатина.**Wellington Mk.X** номер HE 956’N от 205 група на RAF /150Sq/ пилот Hinchcliffe, екипаж 5: 5 в Румъния. Цел - Букурещ. Причина за падане – неизвестна.

21(37B): 18.V.1944, обл. Враца, с. Бърдарски геран, общ. Бяла Слатина. **B-24J** сер.номер 4264347 от 455BG/743Sq/; пилот 2L Thomas Markham, екипаж 10: 1 пленен и разстрелян край с.Литаково, 9 POW (MACR 5057). Цел - Плоещ, свален съвместно от противовъздушната артилерия и изтребители в Румъния.

22(38B): 18. V.1944, обл. Враца, местност “Гроба“ - „Големия връх“, 5,5 км Ю/З от с. Веслец, общ. Мездра. **B-17G** сер.номер 4231825 463BG/775Sq/; пилот 1L Louis Menge, екипаж 10: 10 MIA, от тях 8 разстреляни (MACR 5791). Цел - Плоещ, свален от изтребители в Румъния.

23(39F): 18. V.1944, обл. Кюстендил, 5 км Ю/И от с. Джерман, местност „Беш бунар“, общ. Дупница. **P-38J** сер. Номер 42104063 от 14FG/49Sq/; пилот 2L Paul Wingert, KIA. (MACR 5042). Цел – неизвестна, причина за падането - неизвестна.

24(41F): 10. VI.1944, обл. София, с. Грълска Падина, общ. Драгоман. **P-38J** сер. номер 4328704 от 1FG/71Sq/; пилот 2L Carl Hoenschell, MIA, идентифициран 2002 KIA (MACR 5634). Цел - Плоещ, свален от германски изтребители.

25(43B): 11. VI.1944, обл. Враца, 4 км южно от с. Горно Пещене. **B-24G** сер. номер 4278260 от 461BG/767Sq/; пилот 1L Robert Heald, екипаж 10: 10 POW (MACR 5641). Цел - Гюргево, свален от противовъздушната артилерия в Румъния.

26(44B): 11. VI.1944, обл. Русе, 5 км С/И от гр. Русе (към с. Долно Абланово). **B-24H** сер. номер 4129251 от 451BG/724Sq/; пилот 2L Charles Haun, екипаж 10: 2 KIA, 8 POW (MACR 5668). Цел - Гюргево, свален от изтребители в Румъния.

27(45F): 11. VI.1944, обл. Перник, кв. Върба (с. Върба, Радомирско) Радомир. **P-38J** сер.номер 4328636 от 82FG/95Sq/; пилот 2L Leonard Wood, POW (MACR 5756). Цел - Констанца, свален от изтребител, възможно български.

28(46F): 11. VI.1944, обл. Перник, към с. Долна Диканя, общ. Радомир. **P-38J** сер. номер 328678 от 82FG/95Sq/; пилот 2L Dan Wylie, POW (MACR 5759). Цел - Констанца, свален от изтребител, възможно български

29(47B): 11. VI.1944, обл. Плевен, 2,6 км Ю/И от село Санадиново, общ. Никопол. **B-24H** сер. номер 4264500 от 455BG/743Sq/; пилот 2L Earl Brawninger, екипаж 10: 2 POW, 1 MIA, 7 POW в Румъния.(MACR 5771). Цел - Гюргево, причина за падането – авария в двигател.

30(48B): 11. VI.1944, обл. Русе, близо до с. Екзарх Йосиф, общ. Борово (35-50 км Ю/З от Русе). **B-24H** 4252671 от 484BG/826Sq/; пилот 2L Clarance Odle, екипаж 10: 2 KIA, 8 POW (MACR 6014). Цел - Гюргево, свален от румънски и германски изтребители.

31(49B): 11.VI.1944, обл. Кютендил, с. Лисец, под местността „Връшник“, 1 км Ю/З от с. Блатец, общ. Соволяно. **B-24G** сер.номер 4278290 от 449B/716Sq/; пилот 2L James Gudjer, екипаж – 10: 6 KIA, 4 POW(MACR 6021) Цел - Констанца, свален от румънски и германски изтребители.

32(53F): 11.VI.1944, обл. Софийска, местност Зелин (с. Зелин, Ботевградско), общ. Ботевград. **P-51B** сер, номер 437024 от 52FG/2Sq/; пилот 2L Joseph Riley, KIA (MACR 5777). Цел - Констанца, свален от румънски и германски изтребители.

33(54B): 12. VI.1944, обл. Монтана, между селата Сталийска махала и Трайково (с. Криводол), общ. Лом. **Wellington Mk.X**, номер LN870, от 205 група на RAF/231 Wing/70Sq RAAF; пилот W/O Marstin: екипаж - 5: 5 POW. Цел - Карлово, свален от германски нощен изтребител.

34(56B): 23. VI.1944, обл. Пловдив, между с. Сухозем, и Отец Паисиево, общ. Калояново. **B-17F** сер.номер 425951 от 97BG/341Sq/; пилот 2L Edwin Anderson, екипаж - 10: 1 KIA, 9 POW (MACR 6406). Цел – Плоещ, ударен най-напред в Румъния от противовъздушната артилерия и изтребители, свален от български и германски изтребители, излетели от Карлово.

35(57B): 23.VI.1944, обл. Монтана, 2 км Ю/З от с. Дива Слатина, общ. Г. Дамяново; **B-17G** сер.номер 4237813 от 301BG/32Sq/; пилот 2L John Muirhead, екипаж – 10: 1 KIA, 2 MIA, 7 POW (MACR 16203). Цел - Плоещ, след авария свален от германски изтребител.

36(62B): 24. VI.1944, обл. Силистра, м/у с. Нова Попина и Поляна, общ. Ситово. **B-24G** сер. номер 4278380 от 450BG/722Sq/; пилот 2L Henry Van Popering, екипаж - 10: 6 POW, 4 POW в Румъния (MACR 6365). Цел – Плоещ, свален от румънски и германски изтребители.

37(63B): 24. VI.1944, обл.София, гр. Самоков (с. Доспей махала, 1 км западно от гр. Самоков). **B-24H** сер. номер 4128846 от 449BG/717Sq/; пилот 1L Robert Anderson, екипаж – 10: 10 POW (MACR 6403). Цел - Плоещ, причина авария и сваляне от български изтребители.

38(64B): 24. VI.1944, обл. Пазарджик, гр. Стрелча (4 км източно от село Стрелча, общ. Панагюрище, 2-3 км от местност „Корубата“). **B-24J** сер. номер 42100259 от 98BG/343Sq/; пилот 2L Wilson Stallings,екипаж – 11: 1 MIA, 9 KIA, 1 POW.(MACR 6437). Цел - Плоещ, свален от румънски изтребители.

39(67B): 28. VI.1944, обл. Пловдив, 2 км Ю/И от с. Чурен, общ. Родопи. **B-24H** сер. номер 4252701 от 485BG/828Sq/; пилот 2L John Crouchley, екипаж - 10: 1 KIA (до 2017 - MIA), 9 POW (MACR 6820). Цел- Букурещ, свален от германски изтребители.

40(68B): 29. VI.1944, обл. В.Търново, с. Илаков рът, общ. Елена. **Liberator B.VI** номер EV970’F от 205 група на RAF/31Sq/ SAAF; пилот Mj. J.A. Mouton, екипаж - 7: 2 KIA, 4 POW, 1 - POW в Румъния. Цел- Гюргево, свален от германски нощен изтребител Ю-88.

41(70B): 29. VI.1944, обл. Русе, между с. Новград и с. Беляново, общ. Ценово. **Wellington Mk.X** номер MF194’F от 205 група на RAF/70Sq RAAF; пилот - FS L.Fallon: екипаж- 5: 4 KIA, 1 POW. Цел - Гюргево, свален от германски нощен изтребител Ю-88.

42(71B): 29. VI.1944, обл. Русе, с. Николово (с. Липник, общ.Гагаля). **Liberator B.VI** номер EW104’Y от 205 група на RAF/31Sq/ SAAF; пилот Lt D.J.S. Haggie, екипаж- 7: 7 KIA. Цел - Гюргево, свален от германски нощен изтребител Ю-88.

43(72B):3.VII.1944, обл. Монтана, между с. Владимирово (с. Люта) общ. Бойчиновци, и с. Якимово- 2 км южно от него (с. Котеновци), общ. Берковица. **B-24H** сер. номер 4251157 от 376BG/512Sq/; пилот 2L William Holgate, екипаж - 10: 10 POW в Румъния (MACR 6339). Цел - Гюргево, причина за падането – авария или атака от румънски изтребители.

44(73B): 3. VII.1944, обл. Враца, между с. Остров и с. Горни Вадин, общ. Оряхово (на около 30 км източно от Оряхово). **B-24H** сер.номер 4295388 от 376BG/512Sq/; пилот 1L George Hillman, екипаж - 11: 11 POW (MACR 6363). Цел - Гюргево, свален от зенитната артилерия на Румъния.

45(75B): 3. VII.1944, обл. Русе, 3 км южно от Русе. **B-24G** сер. номер 4278154 от 450BG/722Sq/; пилот 1L Kenneth Wilson, екипаж - 10: 1 KIA, 2 MIA, 7 POW(MACR 6758). Цел - Гюргево, свален от зенитната артилерия в Румъния.

46(80B): 22.VII.1944, обл. Ловеч, м/у с. Гостиня и Къкрина, 3 км Ю/И от Гостиня, местност „Келалиската нива“, общ.Ловеч. **B-24G** сер. номер 4278343 от 98BG/343Sq/; пилот 1L Francis Puntenny, екипаж - 11: 1 KIA, 6 POW,4 POW в Румъния. (MACR 7054). Цел - Плоещ, свален от румънски изтребители.

47(82F): 31.VII.1944, обл. Плевен, с. Ставерци, общ. Долна Митрополия. **P-51D** сер.номер 4413364 от 325FG/318Sq/; пилот 1L BobieWinn, POW (MACR 7155). Цел - Букурещ, свален от румънски изтребители.

48(83B): 10.VIII.1944, обл. Плевен, 3 км източно от Ново село (сега Санадиново), общ. Никопол. **B-24G** сер.номер 4278320 от 376BG/515Sq/; пилот 1L Donald Rigs; екипаж - 10: 10 POW (MACR 7185). Цел - Плоещ, свален от зенитната артилерия в Румъния.

49(84B): 10.VIII.1944, обл. Плевен, край Плевен (според някои източници пада в колодрума в Плевен). **B-24G** сер. номер 4278464 от 376BG/514Sq/; пилот 2L Craig Morrow; екипаж - 10: 8 POW, 2 - POW в Румъния (MACR 8087). Цел - Плоещ, свален от зенитната артилерия в Румъния.

50(85B): 10.VIII.1944, обл. Видин, южно от с. Чорлево (сега Дреновец), местн. „Камен дол“, общ. Ружинци. **Wellington Mk.X** номер LN972'W от 205 група на RAF/142Sq/; пилот Lt Noel Catherine; екипаж – 6: 6 POW. Цел - Плоещ, свален от германски нощен изтребител Ю-88.

51(86B):10.VIII.1944, обл. Монтана, с. Долно Линево, общ. Лом. **Wellington Mk.X** номер LP189'H от 205 група на RAF /142Sq/ FS C.G. Hill, екипаж - 5: 5 KIA. Цел - Гюргево, свален от германски нощен изтребител Ю-88.

52(87B):17.VIII.194, обл. Враца, между селата Лик и Липница, местност „Китката“, общ. Мездра. **B-24J** сер.номер 4278504 от 454BG/738Sq/; пилот 1L John Mason; екипаж - 10: 2 KIA, 8 POW (MACR 7456). Цел - Плоещ, свален от зенитната артилерия в Румъния.

53(88B): 17.VIII.1944, обл. Монтана, 500-1000 метра С/З от с. Комарево, местност „Недобала“ общ. Берковица, С/И от Берковица. **B-24G** сер.номер 4278182 от 454BG/738Sq/; пилот 1L Joe Crawford, екипаж – 9: 2 KIA,7 POW (MACR 7628/32). Цел - Плоещ, свален от зенитната артилерия в Румъния.

54(90B):17.VIII.1944, обл. Монтана, 3 км южно от с. Расово, в местността „Лозята“, общ. Медковец (м/у с.Расово и с.Медковец): 43°41'18.0"N 23°14'13.3"E. **B-24G** сер.номер 4278206 от 376BG/512Sq/; пилот 2L James McConnaughey; екипаж - 10: 10 POW (MACR 7634/38). Цел - Плоещ, свален от зенитната артилерия в Румъния.

55(91B): 17.VIII.1944. обл. Перник, с. Габров дол, общ. Земен. **B-24G** сер.номер 4278203 от 456BG/745Sq/; пилот 1L J.J.Walker, екипаж - 9: 5 POW, 4 POW в Румъния. (MACR 7672). Цел - Плоещ, свален от зенитна артилерия в Румъния.

56(92F): 17.VIII.1944, обл. Враца, около с. Гложене, общ. Козлодуй. **P-51B** сер.номер 42106455 от 31FG/308Sq/; пилот 1L Bennard Shipp, POW (MACR 7864). Цел - Плоещ, причина за падането – отказ на горивната система.

57(93B): 17.VIII.1944, обл. Враца, с. Игнатица, общ. Мездра. **B-24J** сер.номер 4440489 от 376BG/512Sq/; пилот 1L HenryFord; екипаж - 12: 1 KIA, 11 POW Румъния (MACR 7631/37). Цел- Плоещ, свален от зенитната артилерия на Румъния.

58(95B): 18.VIII.1944, обл. Враца, 10 км западно с. Гложене, общ. Козлодуй, в местността „Златията“.**B-24G** сер.номер 4278295 459BG/758Sq/; пилот Cpt. Allie Peoples, екипаж - 9: 9 POW (MACR 7693). Цел - Плоещ, причина за падане – авария на два двигателя.

59(96B): 18.VIII.1944, обл. Враца, 3 км южно от с. Михайлово (с. Долна Гнойница) общ. Хайредин. **B-24J** сер.номер 4299858 от 98BG/343Sq/; пилот 1L Raymond Baker;екипаж - 11: 1 KIA, 10 POW (MACR 15306). Цел - Плоещ, свален от зенитна артилерия в Румъния.

Фиг. 5. *Паднал бомбардировач B-24J до с. Бърдарски геран, общ. Бяла Слатина (номер в текста 21(37B) (любезно от Денеш Бернар и Николай Братоев - Крижицки)*

Фиг. 6. *Останки от самолета B-24, свален с таран от поручик Списаревски (номер 2(11B)*

60(97F): 26.VIII.1944, обл. Враца, Ю/И от с. Нефела. **P-51B** от 332FG/99Sq/ „Red tails“; пилот 2L Henry Wise, POW. Цел - Плоещ, причина за падането е авария в

двигателя на връщане от целта. Според ген. Йордан Миланов е свален от поручик Стоян Стоянов. Пилотът е единственият афроамерикански пленник в лагера в Шумен, отношението към него както от охраната, така и от останалите пленници е било коректно.

Фиг. 7. *Юни 1944: Крило от свалениият край Самоков бомбардировач B-24 (37(63B)*

Фиг. 8. *Останки в полите на Витоша от самолет B-17F, вероятно номер 7(17B)*

Времето неумолимо изтрива бледите следи на отдавна минали събития, но все още се появяват и материални доказателства за тях. При участието на Станимир Станев от 2007 до 2016 г. в американските експедиции по търсенето на останките на загиналия американски пилот лейтенант Краучли, мястото на гибелта му бе установено по множеството останки от самолета му в борова гора в Родопите край с. Чурен, общ. Родопи, обл. Пловдив [21].

Фиг. 9. *Останки от самолета на лейтенант Краучли (39(67B)(архив на авторите)*

Засега е известен само един артефакт, останал от английски бомбардировач „Wellington“. През февруари 2021 Митко Митков от Лом е намерил стандартна кофа, която е имало във всеки английски самолет и служела на екипажа в полет (Elsan toilet bucket).

Последният известен случай на намирането на самолетни останки от войната е от април 2022 г. Трактористът Калоян Костадинов от с. Поляна изважда при оран между селата Нова Попина и Поляна, област Силистра, добре запазена лопата от витло от американски бомбардировач. Нашето проучване по архивни документи и по каталога на частите на B-24 показа, че то е от бомбардировача B-24 G, с пилот лейтенант Хенри Ван Попъринг, паднал в този район на 24 юни 1944 г. (номер **36(62B**).

2. Карта на локациите на падналите съюзнически самолети

След уточняване на местата на падането на самолетите, за пръв път в научната общност у нас от авторите се публикува разработена на базата на карта на страната [22], карта с тези локации (фиг. 11).

На представената карта ориентировъчното място на падане на всеки самолет е маркирано с четири лъчева звезда, последвана от текстово поле с

пореден номер, за да се направи връзка с пояснителната информация за него. След поредния номер е посочена датата на падане и типа на самолета. Следва силуета на конкретния самолет.

Фиг. 10. *Лопата от самолетно витло на B-24G (номер36(62B) и кофа от Wellington (номер 51(86B)(любезно от Митко Митков)*

За по-голяма яснота на фиг. 13, 14, 15, 16 и 17 са представени увеличени части от цялата карта на фиг. 11.

Най-голяма част от самолетите са паднали в Западна България – в сегашните Пернишка и Врачанска области (фиг. 13 и 14).

На 20 декември 1943 г. при защита на София загиват геройски двама български пилоти. Поручик Димитър Списаревски, от 3-та ескадрила на 6-ти изтребителен авиополк, в 12.55 часа сваля с челен таран американски „Либърейтър“. Подпоручик Георги Кюмюрджиев, от 3-та ескадрила на 6-ти изтребителен авиополк, атакува и сваля изтребителя с пилот лейтенант Едуард Е. Тинкър, но веднага след това е свален от водения (wingman) на л-т на Тинкър - лейтенант Фоли.

На картата на фиг. 12 е показано местоположението на падналите съюзнически и наши самолети след битката на 20.12.1943 г.

С номер Б1 на картата, северно от с. Долни Пасарел, 25 км югоизточно от София е маркирано мястото на падане на изтребителя на поручик Списаревски (фиг. 18), а с номер Б2, южно от с. Радибош, на 7 км югозападно от Радомир – на подпоручик Георги Кюмюрджиев.

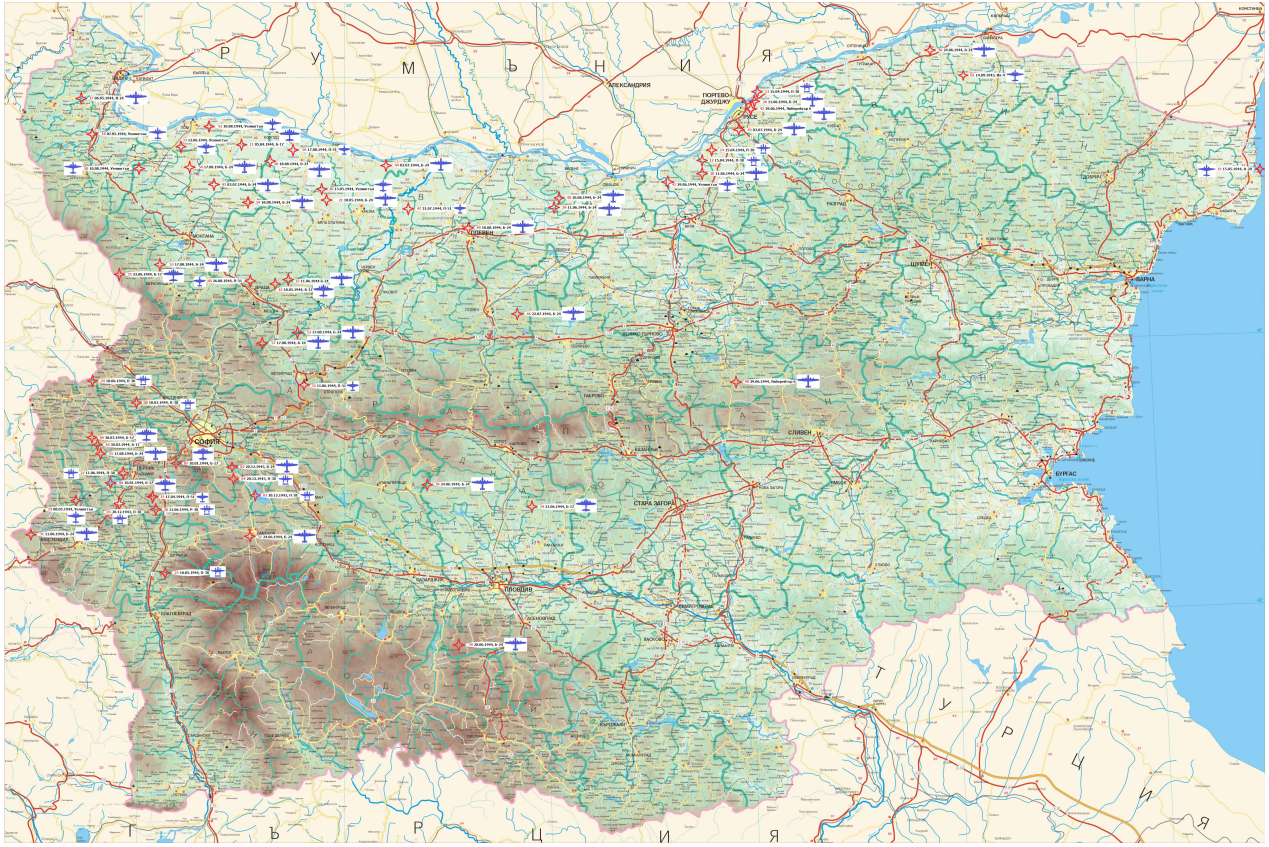
С номер 2 е показано мястото на падане на поразения след тарана на Списаревски, „Либърейтър“, с надпис на носа 92 „Big Nig“. С номер 3 е маркиран първият свален в този бой изтребител, с пилот лейтенант Джордж Мичел, в района на с. Горни Пасарел (През 1954 г. с. Горни Пасарел е изселено и потопено от водите на яз. Искър и вече не съществува). Номер 4 е мястото на падане на изтребителя с пилот Джон МкЛендън, а с номер 5 – на самолета на лейтенант Едуард Тинкър.

Заключение

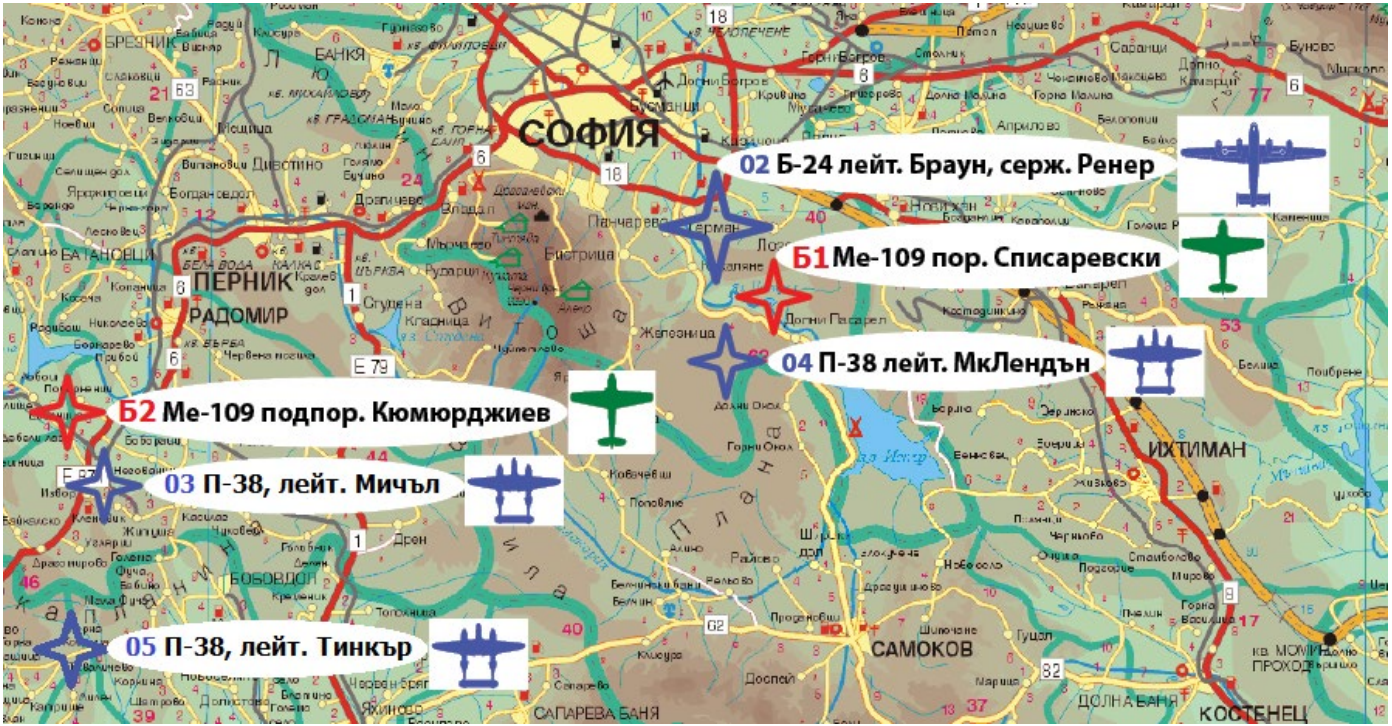
В настоящата статия се представят резултатите от авторските проучвания за доказани загуби на самолети на съюзническата авиация на територията на нашата страна. Обосновано е коригирането от преднишна публикация на авторите [6] количество – 95 самолети на съюзниците, от които има паднали самолети и загуби на личен състав на териториите под българско управление, на 91 броя в тази статия, и от 85 паднали на тези територии – на 83 сега.

За пръв път в научната общност у нас от авторите се публикува допълнена административна карта на страната [22] с показани местата на падане на 60 изтребителя и бомбардировача на съюзниците в сегашните граници на България. Съставената за пръв път у нас карта със загубите на съюзническата авиация ще допринесе за последващи военно-археологични проучвания, и уточняване на факти по гибелта или пленяване на съюзнически авиатори у нас по време на Втората световна война.

Освен намирането на допълнителни данни за паднали съюзнически самолети, перспективно е търсенето на артефакти от местата на катастрофи и на наши изтребители през Втората световна война. Такъв е случаят с намерения неотдавна в Самоковаско двигател от Messerschmitt Bf 109 G6 [23].

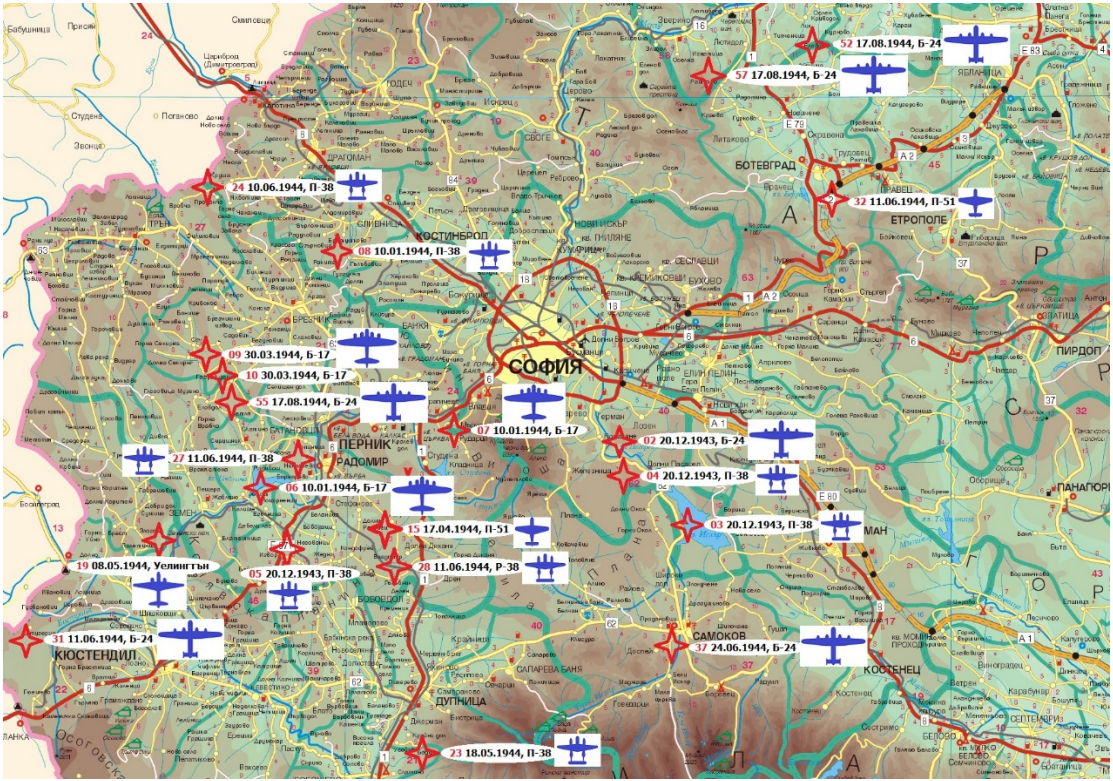


Фиг. 11. *Съставената от авторите карта на локациите на падналите съюзнически самолети*



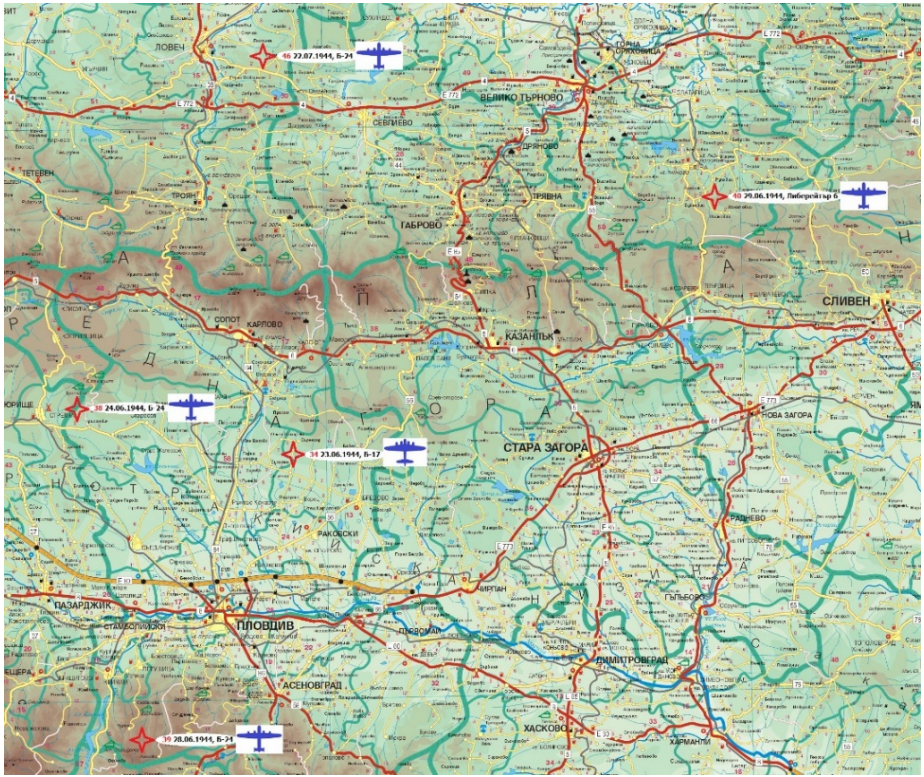
Фиг. 12. *Местоположение на падналите съюзнически и наши самолети след битката на 20.12.1943 г.*

Фиг. 13. *Северозападният участък от разработената карта*

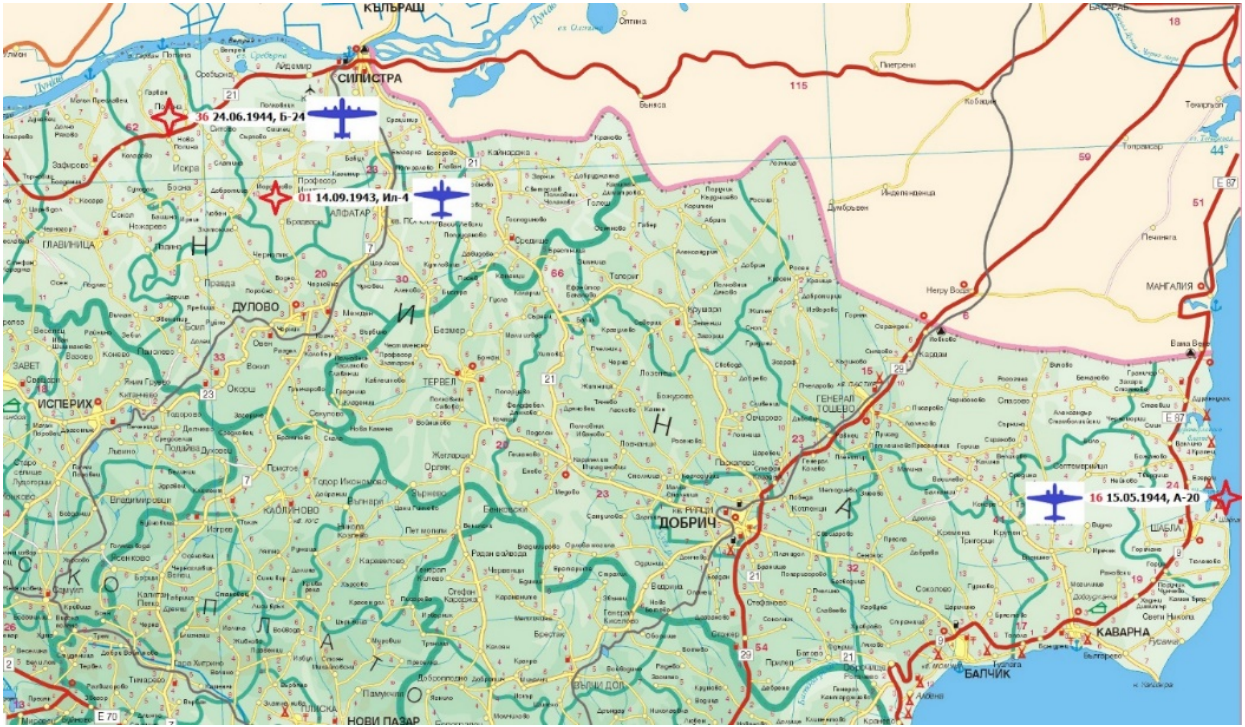


Фиг. 14. *Западният участък от разработената карта*

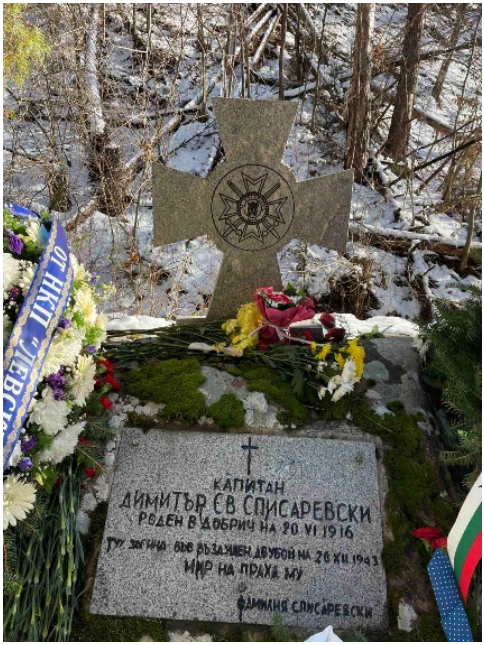
Фиг. 15. *Северната част на разработената карта*



Фиг. 16. *Централната част на разработената карта*



Фиг. 17. *Североизточната част от разработената карта*



Фиг. 18. *Лобното място на поручик Списаревски (личен архив на авторите)*

ЛИТЕРАТУРА

[1] Руменин Р. „Летящи крепости над България“. Изд. Хр.Ботев, София,1990.

[2] Христов М. „Българските въздушни войски във втората световна война 1941 – 1945 г.“ - Дисертация за получаване на образователно-научната степен „Доктор”,София, ВА „Г.С.Раковски”; Недялков, Д. 130 години българи в небето. (Кратка история на българската военна авиация). Прозорец, С.2022. ISBN 978-619-243-230-0.

[3] Report on Operation Freedom. !5th Air force historial monograph, Roll A6088, Maxwell AFB, Ala.p.427

[4] Johnson R. Gidi Gidi Boom Boom (The true story of the plane and crew in WWII Europe). San Ramon, Falcon Books.

[5] Bernad D. Bulgarian Fighter Colours 1919-1948. vol. 2 (White Series), MMPBooks.2020. ISBN- 978-8365958198.pp.230-260.

[6] Станев С., Ханъм Р. Към въпроса за падналите през 1943/44 г. англоамерикански самолети в България и контролираните от българската войска територии.Сборник научни трудове, научна конференция с межд.участие „40 години Шуменски университет“,ФХН, Секция История и теология, Шумен, 2011.

[7] Миланов Й. Авиацията и въздухоплаването на България през войните 1912/1945 (част втора). С., ВИК „Св. Г. Победоносец”, 1997.

[8] Великов Г. По пътя към безсмъртието. Второ допълнено издание, Силистра, 2012. 58 стр. ISBN 978-954-8198-44-8.

[9] Missing Air Crew Reports of the U.S. Army AirForces, 1941-1948, National Archives and Records Administration, College Park, MD.

[10] Списък на падналите самолети в България от английските Кралски въздушни войски, ДВИА, ф.38, оп..2, а.е.118, стр.607.

[11] Сведение за падналите англо-американски самолети в Сърбия и Македония, ДВИА, ф.38, оп. 2, а.е.118, стр.596.

[12] Сведение за падналите на българска територия англо-американски самолети, ДВИА, ф.28, оп. 1, а.е.204, стр.469

[13] Сведение за падналите на българска територия американски самолети ДВИА, ф.38, оп. 2, а.е.118, стр.609

[14] Списък на падналите самолети от англо-американски произход, ДВИА, ф.20, оп. 3, а.е.118, стр.7

[15] Сведение за падналите на българска територия американски самолети ДВИА, ф.20, оп. 3, а.е. 101, стр. 8-13

[16] Арх. МВнР, КИСП, а.е.1172, л. 48-52.

[17] Димитров И. По волята на победителите (съглашението за примирие и лагери в България). С., НКИА ООД, 1996.; Димитров, И. Американското военно гробище в с. Слатина, Софийско. Военноисторически сборник, бр. 2, 1992, стр. 76-89.

[18] История на зенитната артилерия и зенитно-ракетните войски в българската армия. ВК "Св. Георги Победоносец".С.,1995 г.

[19] Stanev S., Lascotte M. 289 days near Shumen.Konstantin Preslavski University Press, Shumen, 2012. ISBN 978-954-577-570-3. 166 p.

[20] http://www.cieldegloire.fr/jg_052k.php

[21] Whiting J. Long road home for Lt. Crouchley. Vagabond (Bulgarian English magazine), Issue 155-156 (2019), pp.26-29. ISSN 1312-8590.

[22] Карта на България, Сфера ИК, https://treasures.zonebg.com/bulgaria.htm

[23] Hristov H., Tsankov Ts. A new look at the capabilities of the HWK 109-509 series rocket engines. Scientific Conference with international participation MATTEH 2020, Conference proceedings, Vol. 2, Shumen, 2020, ISSN 1314-3921, pp. 359-368.

РАЗРАБОТВАНЕ НА ИЗЧИСЛИТЕЛЕН МОДЕЛ НА КОМПЛЕКСЕН ПОКАЗАТЕЛ НА НАДЕЖДНОСТТА НА СИСТЕМА ОТ ПРОГРАМИРУЕМИ УСТРОЙСТВА В ПРОИЗВОДСТВЕНО ПРЕДПРИЯТИЕ

Даниел Р. Денев

DEVELOPMENT OF A COMPUTATIONAL MODEL OF A COMPLEX INDICATOR OF THE RELIABILITY OF A SYSTEM OF PROGRAMMABLE IN A MANUFACTURING ENTERPRISE

Daniel R. Denev

ABSTRACT: *With the development of the industry, the creation and management of production units becomes a top priority for every industrial enterprise. For the control process, emphasis is placed on programmable devices and industrial networks. Through them, manufacturing enterprises face two main questions, "What reliability could they provide?" and "Is it possible to improve the current devices they use." Based on this, the present article aims to develop a computational model of a complex indicator of the reliability of a system of programmable devices. The choice is based on the fact that many enterprises rely on the rapid processing of information and greater reliability of programmable devices.*

KEYWORDS: *Complex indicator, Reliability, Risky technical system, Programmable devices.*

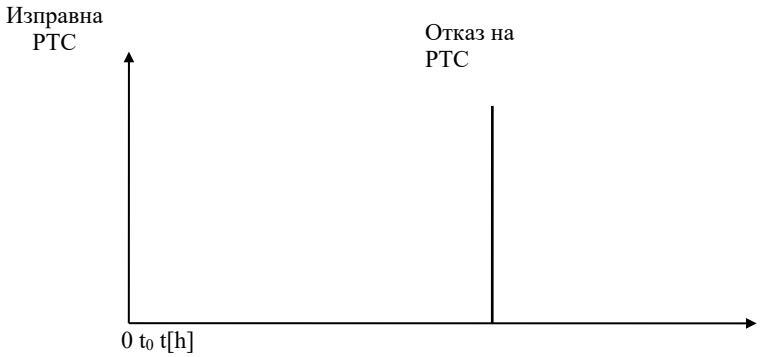
Въведение

Както е показано в литература [1, 2, 3, 4], процесът на управление на техническото състояние на РТС, разгледан като комплекс от мероприятия, имащи производствен и експлоатационен характер, се състои от следните многократно повтарящи се етапи:

1. Получаване на информация за състоянието на конкретната рискова техническа система или отделна система от него;
2. На основата на получената информация вземане на решение за необходимостта от управление на нейното състояние, характера, времето и мястото за прилагане на управляващото въздействие;
3. осъществяване на управляващото въздействие върху РТС или отделна нейна подсистема в съответствие с взетото решение.

От изброеното следва, първо, че процесът на управление се явява информационен процес (два от трите етапа са свързани с получаване и обработка

на информация) и второ, че тъй като резултатите на всеки предшестващ етап се явяват база за следващите, качеството на първите етапи имат определящо значение при разработването и усъвършенстването на управлявания процес. На фиг. 1 е показана рискова техническа система работеща до първи отказ.



Фиг. 1. *Рискова техническа система работеща до първи отказ*

Изчислителен модел на комплексен показател

Комплексен показател на надеждност на РТС (в частност програмируемите устройства и техниката) се явява *вероятността за нормално функциониране* $\mathrm{P}_{\mathrm{НФ}}(\tau, t)$, изразяваща вероятността, че в произволен момент τ изделието е работоспособно и ще продължи да работи безотказно още за определен интервал от време t, т.е. в интервала $\tau, \tau + t$.

Този обобщен показател на надеждност, при програмируеми устройства в индустрията може да се дефинира като „вероятност, че плановото задание (изработката на изделие или обработката на информация) няма да бъде провалена по вина на електронния компонентен състав". Той се определя от:

$$\mathrm{P}_{\mathrm{НФ}}(\tau, t) = K_{\Gamma}(\tau).P_{\mathrm{БР}}(\tau, \tau + t) \quad \textbf{(1)}$$

където: $K_{\Gamma}(\tau)$ - коефициента на готовност на РТС в момент τ;

$P_{\mathrm{БР}}(\tau, \tau + t)$ - ВБР на РТС в интервал $(\tau, \tau + t)$,.

При установен процес на ТЕ (стационарен случаен процес), когато в интервала $(\tau, \tau + t)$ не се е появил нито един отказ, $\mathrm{P}_{\mathrm{НФ}}(\tau, t)$ се нарича коефициент на оперативна готовност $K_{\mathrm{ОГ}}(t)$, който се определя от израза:

$$K_{\mathrm{ОГ}}(t) = K_{\Gamma}(t).P_{\mathrm{БР}}(t) \quad \textbf{(2)}$$

Коефициентите на оперативна готовност $K_{\text{ОГ}}(t)$ и коефициентът на готовност $K_{\text{Г}}(t)$ са предвидени в стандартите като нормируеми комплексни показатели. Кой от двата трябва да се избере, зависи от начина на функциониране на съответното изделие[2].

За изделия с висока безотказност е подходящ $K_{\text{Г}}(t)$, защото от времето за възстановяване ще зависи най-много ефективността от тяхното използване.

За изделия, при които безотказността е по-ниска и има решаващо значение, подходящ ще бъде $K_{\text{ОГ}}(t)$.

Пример: Чрез експлоатационни наблюдения на група еднотипни възстановяеми изделия е установено, че са получени общо $n = 5$ отказа(таблица 1), като сумарната отработка между отказите е $\sum_{i=1}^{n} t_{0i} = 525h$, сумарното време за възстановяване е $\sum_{i=1}^{n} t_{Bi} = 23{,}5h$ и сумарния престой в планови ТО и ремонти в наблюдавания интервал е $\sum_{i=1}^{j} t_j = 93{,}5h$. Приема се, че е налице установен процес на нормална експлоатация, при който потоците на събитията (откази, възстановявания) са стационарни. Да се определят показателите на надеждност при време за работа $t_P = 30h$ и време за възстановяване $t_B = 3h$.

Таблица 1. *Числови показатели*

Параметър	**Стойности**
Брой откази	5
Сумарната отработка между отказите	$525h$
Сумарното време за възстановяване	$23{,}5h$
Сумарния престой в планови ремонти	$93{,}5h$
Време за работа	$30h$
Време за възстановяване	$3h$

Решение: За показателите за безотказност се получава:

$$n\,.\,h_{\text{Дневно}},\ 5\,.\,3{,}5h_{\text{Дневно}} = 17{,}5h_{\text{Дневно}} \quad \textbf{(3)}$$

$$30_{\text{Дни}}\,.\,17{,}5h_{\text{Дневно}} = 525h \quad \textbf{(4)}$$

$$\bar{T}_0 = \frac{\sum_{i=1}^{n} t_{0i}}{n} = \frac{\sum_{i=1}^{5} t_{0i}}{5} = \frac{525}{5} = 105h \quad \textbf{(5)}$$

$$\bar{\omega} = \frac{1}{\bar{T}_0} = \frac{1}{105} = 9.10^{-3}h^{-1} \quad \textbf{(6)}$$

$$\text{P}_{\text{БР}}(t) = exp\left(-\bar{\omega}.t_p\right) \quad \textbf{(7)}$$

$$\text{P}_{\text{БР}}(t) = exp(-9.10^{-3}.30) = 0{,}7633795\ \approx 0{,}763 \quad \textbf{(8)}$$

За показателите за ремонтопригодност се получава:

$$\bar{T}_B = \frac{\sum_{i=1}^{n} t_{Bi}}{n} = \frac{\sum_{i=1}^{5} 3h}{5} = \frac{23{,}5}{5} = 4{,}7h \quad \textbf{(9)}$$

$$\bar{\mu} = \frac{1}{\overline{T_B}} = \frac{1}{4,7} = 0,2127h^{-1} \quad \textbf{(10)}$$

$$\mathrm{P}_B(t_B) = 1 - \exp(-\bar{\mu}.t_B) \quad \textbf{(11)}$$

$$\mathrm{P}_B(t_B) = 1 - \exp(-0,2127\,.\,3) = 0,47181 \quad \textbf{(12)}$$

За комплексните показатели на надеждност се получава:

$$K_{\mathrm{ТИ}}\frac{\sum_{n=1}^{n} t_{0i}}{\sum_{n=1}^{n} t_{0i}+\sum_{n=1}^{n} t_{Bi}+\sum_{n=1}^{k} t_j} = \frac{525}{525+23,5+93,5} = \frac{525}{642} = 0,81776 \quad \textbf{(13)}$$

$$K_{\Gamma} = \frac{\sum_{n=1}^{n} t_{0i}}{\sum_{n=1}^{n} t_{0i}+\sum_{n=1}^{n} t_{Bi}} = \frac{525}{525+23,5} = \frac{525}{548,5} = 0,95716 \quad \textbf{(14)}$$

$$K_{\mathrm{ОГ}}(t) = K_{\Gamma}.P_{\mathrm{БР}}(t) = 0,957\,.\,0,763 = 0,73067 \quad \textbf{(15)}$$

В теорията на надеждността са разработени модели за оценяване на функцията вероятност за нормално функциониране $\mathrm{P}_{\mathrm{НФ}}(\tau, t)$ и за случаите, когато могат да възникнат и да бъдат отстранени в процеса на работа един и повече откази. За електронния компонентен състав в системите от програмируеми устройства тези модели са приложими, когато случайното време $\mathrm{T}_{\mathrm{В}}$ за отстраняване на отказ не превишава определено допустимото време $t_{\mathrm{В.ДОП}}$ за престой на контролера в неизправно състояние, т.е. $\mathrm{T}_{\mathrm{В}} \leq t_{\mathrm{В.ДОП}}$. Такъв модел, отнасящ се за програмируеми устройства, е изложен в [3]. В него е прието, че сумарното време за възстановяване работоспособността при възникналите n на брой откази на поточната линия е много по-малка от разглежданото време на работа на контролера в режим обработка на информацията и изпълнение на задание $t_{\mathrm{ВД}}$, т.е. $\sum_{n=1}^{n} t_{Bi} \ll t_{\mathrm{ВД}}$.

При определяне на вероятността за нормално функциониране $\mathrm{P}_{\mathrm{НФ}}(\tau, t)$ се приема, че за времето $t_{\mathrm{ВД}}$ не трябва да се получи нито един отказ. Ако се допусне, че в установен процес на експлоатация на програмируемите устройства, след момента τ в интервала $(\tau, \tau + t)$ се е появил един отказ, който ще бъде отстранен от персонала за подръжка преди изтичането на времето $t_{\mathrm{ВД}}$, то за пресмятане на вероятността за нормално функциониране е предложена формулата:

$$\mathrm{P}_{\mathrm{НФ}}\left(t, t_{\mathrm{ВД}}\right) = K_{\Gamma}.P_{\mathrm{БР}}(t).\left\{1 + [1 - P_{\mathrm{БР}}(t)].P_{\mathrm{В}}(t_{\mathrm{ВД}})\right\} \quad \textbf{(16)}$$

Пример: При установен процес на експлоатация на дадена серия програмируемите устройства (Siemens Simatic S7-300 – фиг. 2) е известно, че коефициентът на готовност е $K_{\Gamma} = 0,99$; вероятността за безотказна работа за определено време за извършване на операция $t_{\mathrm{ВД}}$ е $P_{\mathrm{В}}\left(t_{\mathrm{ВД}}\right) = 0,8$, а вероятността за възстановяване на работоспособността на контролера в производственото предприятие $t_{\mathrm{ВД}}$ е $P_{\mathrm{В}}\left(t_{\mathrm{ВД}}\right) = 0,96$. Да се определи вероятността за нормално

функциониране на $\mathrm{P}_{\mathrm{НФ}}(t, t_{\mathrm{ВД}})$ на програмируемо устройство от тази серия, ако е допустимо появяването и отстраняването за време $t_{\mathrm{ВД}}$ само на един отказ.

Фиг. 2. *Програмируемо устройство Siemens Simatic S7-300*

Решение: След заместване в (16) се получава:

$$\mathrm{P}_{\mathrm{НФ}}(t, t_{\mathrm{ВД}}) = K_{\mathrm{Г}}.P_{\mathrm{БР}}(t).\{1 + [1 - P_{\mathrm{БР}}(t)].P_{\mathrm{В}}(t_{\mathrm{ВД}})\} = \\ = 0{,}99.0{,}8.[1 + (1 - 0{,}8).0{,}96] = 0{,}944 \quad \textbf{(17)}$$

При положение, че в същия период не се допуска появата на никакъв отказ, вероятността за нормално функциониране $\mathrm{P}_{\mathrm{НФ}}(t, t_{\mathrm{ВД}})$ (в случая това е коефициентът на оперативна готовност $K_{\mathrm{ОГ}}$) ще бъде:

$$\mathrm{P}_{\mathrm{НФ}}(t, t_{\mathrm{ВД}}) = K_{\mathrm{ОГ}} = 0{,}99.0{,}8 = 0{,}792 \quad \textbf{(18)}$$

В разгледания пример в резултат на допускането за възстановяване на работоспособността на контролера в производственото предприятие се получава така, че функцията $\mathrm{P}_{\mathrm{НФ}}(t, t_{\mathrm{ВД}})$ ще се повиши и при време t нейната стойност ще бъде с 6% по-висока $(0{,}96 : 0{,}792 = 1{,}21)$. При допускане на възможност за отстраняване на повече от един отказ в производствени условия, това повишение ще бъде съответно по-голямо.

Пригодността на изделията да бъдат възстановявани в процеса на експлоатация води до повишаване на вероятността за нормално функциониране $\mathrm{P}_{\mathrm{НФ}}(t, t_{\mathrm{ВД}})$, което компенсира в известна степен недостатъчното ниво на тяхната безотказност, изразена чрез вероятността за безотказна работа $P_{\mathrm{БР}}(t)$ от (8). Това подчертава голямото значение на средствата за сигнализация и откриване на откази, на съвършенството на схемните и функционални решения, на възможността за бърза и лесна замяна на често отказващи елементи и т.н., при постоянно обслужваните програмируеми устройства, каквито са самите контролери, комуникационните блокове, а в известна степен и сигналните блокове и датчици.

При икономическите пресмятания могат да се дефинират и други комплексни показатели като: коефициент за стойността на експлоатацията, себестойност на извършената превозна работа и др. В такива показатели, освен разходите, пряко свързани с надеждността, участват и разходите за закупуване, приходите от извършената работа, икономичността, производителността и други технически параметри по предназначение [4].

Заключение

Въз основа на изчислителният модел може да се обобщи и заключи, че е представен ефикасен метод, чрез който предприятията в индустрията да пресмятат своя надеждностен показател, спрямо броя на своите програмируеми устройства и тяхното времето за работа. След оформянето на крайните решения производствените предприятия добиват обща представа за устройствата който притежават и тяхната полева надеждност. Предвидена е бъдеща разработка в която алгоритъма да бъде съкратен и предлага по-удобно изчисление. Необходимо е да се направи и анализ на отказите. [5, 6]

ЛИТЕРАТУРА

[1] Петров Н. Надеждността като технико-икономически проблем при кибернетизация на обществото. 2015, Дисертация за присъждане на НС „Доктор на икономическите науки“, ВСУ „Черноризец Храбър“, ISBN 978-954-92960-8-2,400с.

[2] Петров Н. Надеждността и рискът като световен кибернетичен проблем. 2019, Студия РБ „Г. Раковски“, ISBN 978-954-90476-0-8, 48 с.

[3] Попчев И. Шест теми и литература по управление на риска. 2012, НБУ, София.

[4] Petrov N., Dimitrov V., Dimitrova V. Reliability of Technology Systems in Industrial Manufacturing. 2019, Monograph, „AkiNik Publications”, New Delhi, India, ISBN: 978-93-87072-59-6.

[5] Цанков Ц. С. Съвременни методи за управление на ресурси в компютърни индустриални мрежи. Университетско издателство „Епископ К. Преславски“, Шумен, 2022, 150 с., ISBN 978-619-201-618-0.

[6] Arabadzhieva-Kalcheva N., Tsankov Ts. Failure Modes and Effects Analysis – FMEA. Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 58-62.

НАБЛЮДЕНИЕ С WIRESHARK И ИЗПОЛЗВАНЕТО МУ В КОМУНИКАЦИОННИТЕ МРЕЖИ

Даниел Р. Денев

SURVEILLANCE WITH WIRESHARK AND ITS USE IN COMMUNICATION NETWORKS

Daniel R. Denev

ABSTRACT: *This science paper illustrates the functionality of Wireshark as a network snooping tool. This is proven through an experimental setup that describes the detection performance of a malicious packet in each network. Testing was done by experimenting on a real-time network analyzed by Wireshark. This article highlights Wireshark's performance as a network protocol analyzer and also highlights its flexibility as an open source utility to allow developers to add possible features to intrusion detection devices.*

KEYWORDS: *Firmware, RAID Системи, WireShark.*

Въведение

През последните години се наблюдава голям скок в използването на мобилни устройства. Следователно изследванията в областта на мобилните и повсеместните компютри са от първостепенно значение. Сигурността е една от основните грижи на потребителите на такива устройства. Във всяка типична мрежа, кабелна или друга, малко вероятното и нежелано влизане на злонамерени потребители и/или злонамерени пакети с данни са основен проблем, що се отнася до сигурността на мрежата. Пакетите данни са основните единици на всички комуникационни системи. Следователно сигурността на мрежата предполага сигурност на пакетите с данни. Пакетът данни е най-основният комуникационен блок, включващ рационализиран поток от безкрайни други реплики, за да се предаде информация от едно устройство на друго[1, 2]. Пакет от данни се съдържа в сегмент от данни, който съдържа друга информация, като използвания протокол, адреса на хардуера на местоназначението и т.н. Накратко, самоличността на всеки пакет, идващ от всеки ненадежден източник, може да бъде открита чрез изучаване на съдържанието му. Това проучване за откриване и само преглеждане на съдържанието на сегмент от данни и неговия пакет се нарича пакетно снифиране. Когато се изготвя регистър на тази информация, техниката се нарича регистриране на пакети. Анализаторът на пакети е компютърен софтуер или хардуер, който може да прихване и регистрира трафик, преминаващ през цифрова мрежа или част от мрежа. Докато потоците от данни преминават през мрежата, снифърът улавя всеки пакет и в крайна сметка декодира и анализира

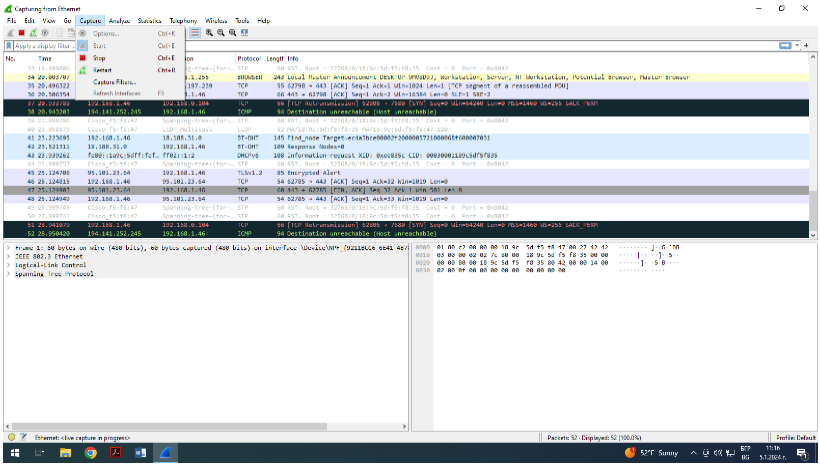
съдържанието му според подходящата спецификация. Тази статия анализира процеса на подслушване на пакети и регистриране на пакети. Wireshark е често достъпен анализатор на мрежови протоколи с отворен код. В тази статия използваме Wireshark, за да проучим функционалността на анализатора на пакети. Използването на Wireshark става много удобно за откриване на подозрителни пакети от всеки ненадежден източник. Всеки снифър/регистратор на пакети с добавена функционалност за откриване на злонамерени записи в мрежа се нарича система за откриване на проникване (IDS). [3, 6]

Софтуерна програма Wireshark

Wireshark е най-популярният анализатор на мрежови протоколи в света? Той има богат и мощен набор от функции и работи на повечето компютърни платформи, включително Windows, OS X, Linux и UNIX. Мрежови специалисти, експерти по сигурността, разработчици и преподаватели по целия свят го използват редовно. Той е свободно достъпен като отворен код и е издаден под GNU General Public License версия 2. Разработен е и се поддържа от глобален екип от експерти по протоколи и е пример за разрушителна технология. Преди това Wireshark беше известен като Ethereal. Wireshark е безплатно компютърно приложение за проследяване на пакети. Използва се за отстраняване на неизправности в мрежата, анализ, разработка на софтуер и комуникационни протоколи и обучения. През юни 2006 г. проектът беше преименуван от Ethereal поради проблеми с търговската марка. Wireshark има инструменти за улавяне, преглед и анализ на пакети с данни. Wireshark има усъвършенствана поддръжка за анализ на безжични протоколи, за да помогне на администраторите да отстраняват проблеми с безжичните мрежи. С подходяща поддръжка на драйвери, Wireshark може да улавя трафик „от въздуха“ и да го декодира във формат, който помага на администраторите да открият проблеми, които причиняват лоша производителност, прекъсваща връзка и други често срещани проблеми.

Инструменти за улавяне

Традиционното мрежово подслушване в Ethernet мрежа е сравнително лесно за настройка. В споделена среда работна станция за анализ, работеща с Wireshark, започва ново улавяне на пакети, което конфигурира картата в безразборен режим и изчаква, докато бъде уловено желаното количество трафик. Един възел може да бъде свързан към мрежа чрез множество механизми, жични и безжични, покриващи много топологии и използващи голямо разнообразие от протоколи. Wireshark предоставя на потребителите възможността да уловят пакетите, пътуващи през цялата мрежа на определен интерфейс в определен момент. Един от основните инструменти е инструментът за заснемане. Опцията за интерфейс, както е показано на фигура 1 по-долу, изброява всички налични интерфейси на възела и може да активира улавяне за всеки от тези възли. Разделът му с опции предоставя по-сложен подход за всеки интерфейс. Елементите от менюто GO предоставят възможностите за преминаване на пакети в списъка за улавяне на трафик.



Фиг. 1. *Инструмент за улавяне*

Инструменти за обработка на файлове

Wireshark предоставя невероятна гъвкавост спрямо други IDS/IPS устройства в областта на поддръжката на регистрационни файлове. Регистрационните файлове могат да бъдат заснети на почасов или седмичен курс въз основа на изискванията на мрежата и способността за работа с устройства. По този начин файловете могат лесно да бъдат заснети през възел за бърза обработка и прехвърлени към по-бавна база данни. Друг интересен аспект е функцията за експортиране на заснетия файл в различни други и по-разбираеми формати - обикновен текст, пост скрипт, CSV и т.н. въз основа на използвания инструмент за анализатор (фиг. 2, 3) [4, 6].

Тестване на проблеми

Целта на експеримента по-долу е да се тества наличието на неоторизиран пакетен достъп до сървърния възел. Тоест възелът, на който е отказан неоторизиран достъп, от външен или експериментален възел, който представлява един или група злонамерени възли в сценарий в реално време (RTS). В текущата експериментална настройка имаме четири възела, всеки изобразяващ възможен възел или набор от възли в ситуация в реално време. Тук имаме четири възела, свързани с превключвател (не се конфигурира). Възлите са както следва:

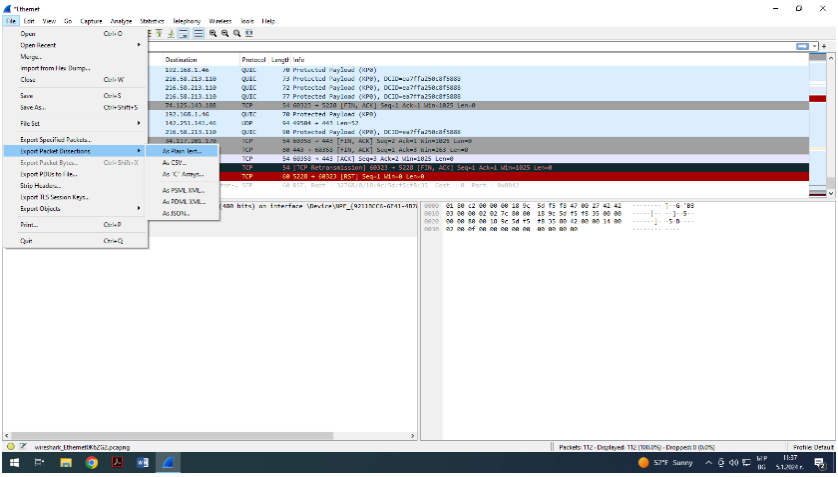
ANALYSER: Това е компютърът с Wireshark, инсталиран в него и работещ в безразборен режим;

IP ADDRESS: 10.0.0.12, Мрежова маска 255.0.0.0

SERVER NODE: Това е възелът, който очакваме да защитим от външно проникване (въпреки че в сценария за IDS ще можем да открием всяко проникване само на сървъра);

IP ADDRESS: 10.0.0.7, Мрежова маска 255.0.0.0

INTERNAL NODE: Това са възлите, които могат да работят както на сървъра, така и да се свързват към външната мрежа; IP адрес: 10.0.0.9 Мрежова маска: 255.0.0.0
EXTERNAL NODE: Това е възможният нарушител и във филтриран режим очакваме да видим всички възможни опити за проникване от този възел на сървъра; IP адрес: 10.0.0.5 Мрежова маска 255.0.0.0
INTIAL STATE (Unfiltered Capture): В това състояние не е използван израз за филтриране, така че целият трафик, преминаващ през анализатора, се показва тук. UDP трафикът тук протича от:
EXTERNAL NODE to **SERVER NODE:** 10.0.0.5 TO 10.0.0.7
EXTERNAL NODE to **INTERNAL NODE:** 10.0.0.5 TO 10.0.0.9
INTERNAL NODE to **SERVER NODE:** 10.0.0.9 TO 10.0.0.7



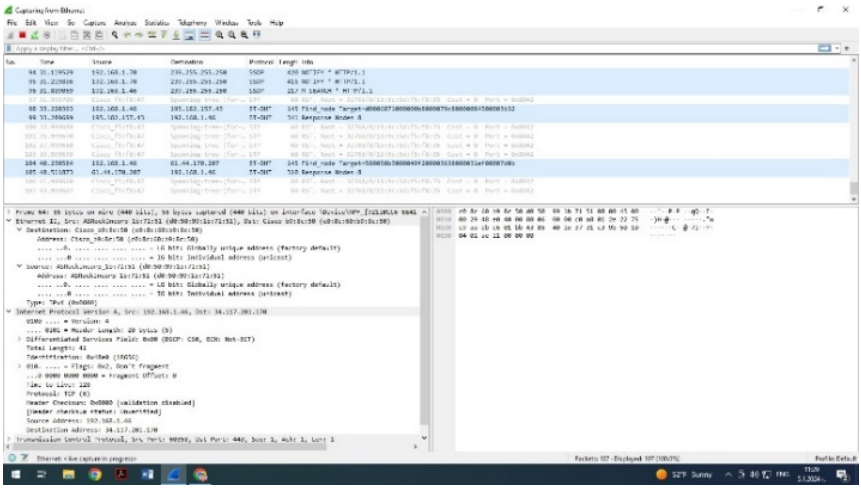
Фиг. 2. *Инструмент за анализиране*

По-долу са графиките, получени при наблюдение на трафика между гореспоменатите възли по време на нефилтрирано тежко и леко улавяне улавяне (фиг. 4) [5, 7].

FINAL SET UP:
Filter queries used:
IP.SRC == 10.0.0.5 and IP.DST == 10.0.0.9
IP.SRC == 10.0.0.9 and IP.DST == 10.0.0.7
UDP
Operators used:
Logical AND:- and
Logical Negation:- !
Logical OR: - or

Final Query: - udp and !
(ip.src == 10.0.0.5 and ip.dst == 10.0.0.9)
and
(ip.src == 10.0.0.9 and ip.dst == 10.0.0.7)

В резултат на тази заявка ще се филтрира целия трафик от външния възел към сървърите и ще покаже, че върху заснетия файл остават всички пакети с данни и няма да бъдат наблюдавани. В случай на нежелан достъп до сървъра външният възел ще бъде маркиран и ще се забележи. Wireshark сам няма да може да генерира аларма или да предприеме действие за сигурност срещу неоторизиран достъп, за това действието е оставено на потребителя, но може да поддържа проследяване на неоторизиран достъп до последно. С използването на други помощни софтуерни програми потребителя е възможно да улесни работата на WireShark, където те да генерират предупреждения.



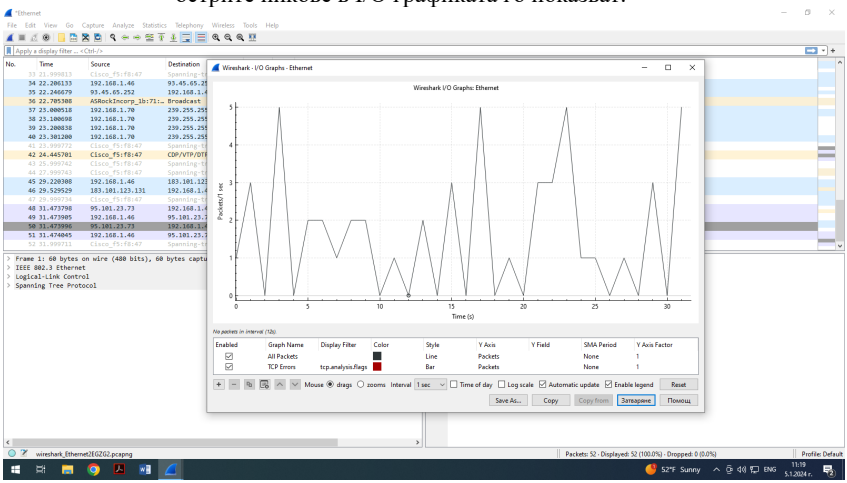
Фиг. 3. *Снифинг с Wireshark*

В резултат на тестовата програма се залага на филтър за откриване нарушители проследяващи личния комуникационен трафик.

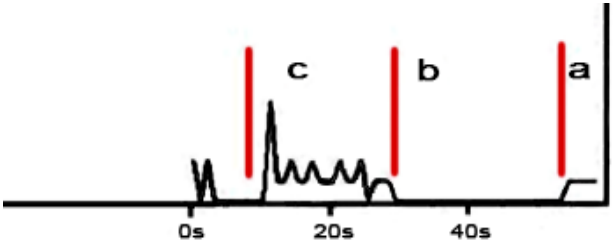
Регионите в графиката на фиг. 5 са обяснени:

- **Регион А:** Това е регионът на маяка и контролния поток на трафика в началото на мрежата и който не показва резки пикове.
- **Регион В:** Дейността по мрежата е от вътрешния възел на сървъра към външния възел и помежду им. Така че улавянето не се изобразява и този регион липсват някакви данни.

- **Регион C:** Злонамерената дейност започва в този момент и е придружена от UDP активност в панела за улавяне на пакети и острите пикове в I/O графиката го показват.



Фиг. 4. *Уловен трафик по време на експериментална постановка*



Фиг. 5. *Пренос на данни през 3 региона*

Заключение

Горният експеримент потвърждава необходимостта от IDS/IPS устройства във всяка типична локална мрежа. Също така подчертахме възможностите на Wireshark в интерпретацията на пакети данни и обработката на данни. Wireshark в този експеримент е използван предимно при филтриране на ACL (списък за контрол на достъпа). Много други варианти на филтриране са налични в програма Wireshark, като филтриране въз основа на размера на пакета, филтриране въз основа на използвани протоколи, филтриране на поднизове и т.н. По този начин, с правилно използване на команди за филтриране и допълващи помощни програми, Wireshark може да се развие в цялостен софтуер за откриване на проникване.

ЛИТЕРАТУРА

[1] Цанков Ц. Съвременни методи за достъп до ресурсите в комтюпърни индустриални мрежи. 2022, Шумен, ISBN 978-619-201-618-0

[2] Цонев И. Компютърни мрежи. 2013, Шумен

[3] Ahmedova D., Konstantinova E., Tsankov Ts. The use of packet sniffing tools in computer networks security. International Scientific Conference "Defense Technologies" DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 401-406.

[4] Konstantinova E., Karadocheva M., Tsankov Ts. The invisible Internet and cyber security. International scientific conference 2019, "Vasil Levski" National military university, "Artillery, aircraft defense and CIS" faculty, Shumen, 2019, ISSN 2367-7902, pp. 519-524.

[5] Scantlebury A. A model for the local area of a data communication network - Objectives and hardware organization 2010, ACM Symp. Data Communication, Pine Mountain.

[6] Simeonova I. Definition of information security as a main channel of administrative security. Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921.

[7] Stolze M., Pawlitzek R., Wespi A. Visual Problem-Solving Support for New Event Triage in Centralized Network Security Monitoring: Challenges, Tools and Benefits. 2003, Conference IT-Incident Management and IT-Forensics (IMF).

ОБЩА КОНЦЕПЦИЯ НА СОФТУЕРНО-ДЕФИНИРАНИТЕ МРЕЖИ

Мустафа Б. Узун, Валентин Т. Атанасов

COMMON CONCEPTION OF SOFTWARE-DEFINED NETWORKS

Mustafa B. Uzun, Valentin T. Atanasov

ABSTRACT: *Software-defined management networking (SDN) is an advanced approach to computer networking, separating the control plane from the data plane. An SDN centralized controller manages network devices through programmed interfaces which could be called Southbound Interface (SBI) and Northbound Interface (NBI) according to their purpose. SBI communicates with devices from the information plane, while NBI interacts with high-level applications. This architecture allows for centralized control, providing a dynamic, abstracted view of the network. SDN's use of standardized protocols, such as OpenFlow, ensures interoperability through which it introduces other SDN implementation innovations. This concept achieves automated network management, streamlining and facilitating network operations, improving response time to changing network conditions. This report provides a brief overview of SDN, focusing on its core principles, interfaces, and transformative impact on network management.*

KEYWORDS: *Software-defined networking, SDN, Northbound Interface, NBI, Southbound Interface, SBI, network automation, OpenFlow.*

Въведение

Софтуерно-дефинираният мрежов модел SDN (Software-defined networking) е трансформационна точка в областта на компютърните мрежи, която предопределя начина, по който се проектират, управляват и поддържат компютърните мрежи [1, 11]. SDN се различава от традиционните мрежови архитектури, като разделя управляващата равнина (Control Plane) от информационната равнина (Data Plane), позволявайки динамично и централизирано програмно управление на мрежата. Това разделение позволява по-гъвкава и ефективна мрежова инфраструктура, която се справя с ограниченията на традиционните мрежови архитектури.

Базовата концепция на SDN включва централизация на мрежовия контрол чрез софтуерен слой, наречен SDN контролер [2]. Този контролер управлява активния процес на трафик в мрежата, чрез предоставяне на един глобален изглед

на цялата мрежа и динамично управление на информационните потоци. SDN въвежда два основни интерфейса за взаимодействие с контролера:

— Северен граничен интерфейс (NBI);
— Южен граничен интерфейс (SBI).

Връзката между слоевете се осъществява посредством API (Application Programming Interface), а NBI интерфейсът служи за достъп и управление на контролера, също така се допуска автоматизиране чрез скриптове на езици като Java и Python. SBI осъществява предаването на информация от контролера към индивидуалните мрежови елементи, включени в мрежата, като маршрутизатори и комутатори. Едно от най-популярните решения е комуникационният протокол OpenFlow.

Внедряването на SDN дава начало на един нов подход в автоматизираното управлението на компютърните мрежи. Чрез централизиране на контрола и абстрахиране от инфраструктурния слой, SDN позволява на мрежовите оператори да автоматизират рутинните задачи, да оптимизират използването на ресурсите и бързо да реагират на променящите се условия в мрежата [3]. Този преход към автоматизирано управление е от съществено значение за справяне с нарастващата сложност на съвременните мрежи и изискванията за ефективни и гъвкави мрежови услуги.

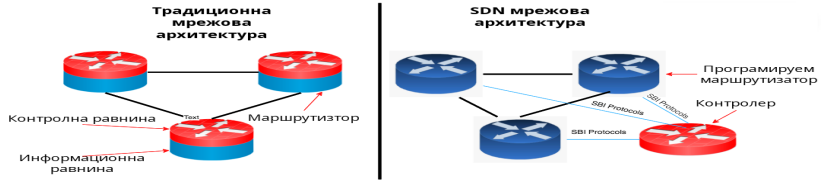
Различни протоколи играят ключова роля в реализацията на SDN, улеснявайки комуникацията между SDN контролера и мрежовите устройства [1]. Тези протоколи, като OpenFlow, предоставят средствата за динамична конфигурация и управление на мрежовите елементи. Използването на стандартизирани протоколи гарантира съвместимост и насърчава отворена система, стимулирайки иновациите и развитието на разнообразни приложения за SDN. Чрез представеното по-горе се полага основата за изследване на SDN модела, подчертавайки неговите основни принципи, интерфейси и ролята на протоколите при реализиране на възможни решения за автоматизирано управление на мрежи. Следващите части от доклада ще разгледат основните концептуални части, образуващи архитектурата на SDN, както и тяхното предназначение.

SDN концепция

Традиционните мрежови архитектури разчитат на разпределен контрол, където всяко мрежово устройство взема автономни решения. Този децентрализиран подход може да доведе до сложни конфигурации и да попречи на адаптивността към променящите се изисквания. За разлика от тях, софтуерно дефинираната мрежа централизира контрола чрез програмен слой, като я прави по-гъвкава и по-лесна за управление. Разделянето на равнината за управление от информационната равнина, за разлика от интегрирания подход в традиционните архитектури, улеснява динамичното програмиране на мрежовите устройства от инфраструктурния слой.

Централизираният контрол на SDN опростява управлението на мрежата и позволява по-ефективно използване на ресурсите [2]. Освен това се отбелязва, че стандартизираните протоколи, като OpenFlow, обуславят оперативната

съвместимост, посредством което се улеснява създаването на иновации и разработване на различни приложения [1]. Чрез сравнението на фиг. 1 се показват архитектурните разлики и промените между традиционните мрежови архитектури и разглежданият SND архитектурен модел.



Фиг. 1. *Сравнение между традиционна мрежова архитектура с SDN архитектурен модел.*

Равнини на абстракции

Равнинните абстракции се използват за да се дефинират съответните интерфейси за формиране на модулна скалируема система. Модулна скалируема система е тази, която позволява повторно използване на код. Реализацията може да бъде модифицирана, но ако интерфейсът остане същия, това не засяга други части на софтуерната система. Равнинните абстракциите имат големи предимства за изграждане на скалируеми софтуерни системи, като се изисква модулност, базирана на абстракция [4]. Абстракцията е подобна като при традиционните компютърни системи, които са изградени от собствена операционна система, апаратно и програмно обезпечение в многослоен модел, с възможност за избор на подходяща функция във всеки слой. SDN разполага с подходящи абстракции на контролната равнина, като тя може да се раздели на три основни части:

— Абстракция на равнината за предаване: Това в компютърните мрежи се отнася до частта на мрежовите елементи, която се грижи за предаването на мрежовите данни от един интерфейс към друг, в съответствие с правилата на каналните или мрежовите протоколи например IP или Ethernet. Тази равнина изпълнява действията, необходими за предаване на мрежови пакети от един интерфейс на устройството към друг и гарантира, че тези пакети ще достигат до правилния адрес или интерфейс в мрежата. Абстрахирането на равнината на предаване крие сложността на нейното изпълнение, свързани с контролните решения. Използва се отворен интерфейс за управление на мрежовите елементи, което означава, че се постига унифициране на управлението на мрежовите елементи без значение от техния производител.

— Абстракция на състоянието на мрежата: Причината за сложността на управлението и контрола на традиционните мрежи са времеемки и ресурсоемки алгоритми за разпределение, като например протоколът за динамично маршрутизиране OSPF. Идеята е да се абстрахира този тип сложни алгоритми и да се придаде общ мрежов изглед на контролера, за да се опростят функциите на приложението. Вместо да се позволи на мрежовите елементи да комуникират помежду си, SDN контролерът използва специфичен протокол например OpenFlow, gNMI, gNOI и други, за да комуникира с мрежовите елементи с цел

извличане, изпращане или промяна на информация за мрежата, при което се формира изглед или топологична карта. От информацията, изпратена до маршрутизаторите и комутаторите зависи предаването и пренасочването на данните.

— Абстракция на контролната равнина: SDN контролерът предоставя интерфейси, чрез които приложенията могат да получат достъп. Външните приложения могат да манипулират мрежата чрез API, посредством контролера, като се използва Java или REST подходи. Разработчиците могат да конфигурират и контролират мрежата, без да се налага да пишат софтуер, който да поддържа апаратната част и системното обезпечение на различни производители на мрежово оборудване.

След прилагане на всички описани нива на абстракции, контролерът ще започне да работи като мрежова операционна система NOS (Network Operation System). При тези операции той ще се свързва с мрежовите устройства чрез API, известен като (Southbound API), където приложенията са съставени от кодове, записани в контролера, като се използва API, предоставен от NOS, наречен (Northbound API).

SDN слоеве

SDN архитектурата може да се дефинира като седем слоен модел, както е показано на фиг. 2. Всеки слой има свое специфично приложение и може да взаимодейства със съседни си такива . Съществува определен клас модели като южни „Southern“, мрежови операционни системи, северни „Northern“ мрежови API, които винаги се представят в SDN архитектурата. Други модели могат да бъдат въведени само в определени случаи и при определени изисквания, като хипервайзори - или езици за програмиране [5,6]. На фигура 2. се илюстрират тези слоеве.

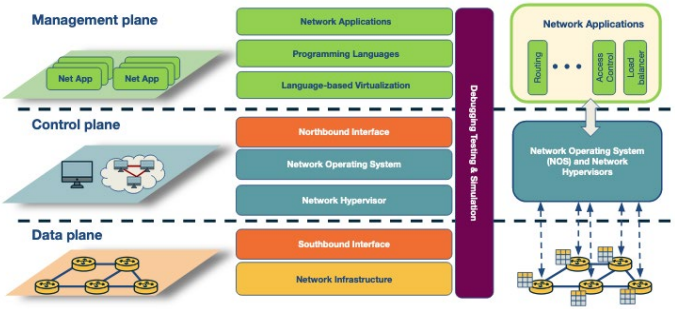
Мрежова инфраструктура: Традиционното мрежово оборудване се развива, като самостоятелна и стабилна основа без централизиран контрол или вземане на решения извън предефинираната конфигурация. Мрежите от ново поколение са изградени върху отворени и стандартизирани концепции и протоколи, за да гарантират оперативна съвместимост между различни производители на мрежово оборудване. Освен това отворените интерфейси позволяват на единиците на контролера да програмират хетерогенни устройства, което е трудно постижимо в традиционните мрежи [7].

Южен граничен интерфейс: Южните гранични интерфейси (SBI) са свързващите връзки между контролните и мрежовите елементи. SI определят комуникационната процедура между мрежовите елементи и контролната равнина. Този протокол установява метода на взаимодействие на елементите на контролната и информационната равнина. От друга страна, тези API все още са сигурни по отношение на развиващите се елементи на физическата или виртуална инфраструктура на подструктурата [5]. SDN използва различни интерфейси и протоколи, за да позволи комуникация и контрол в мрежата. Популярността на конкретни интерфейси и протоколи може да варира в зависимост от конкретната

SDN архитектура и изисквания за тяхното внедряване. Най-популярните SBI интерфейси и протоколи са:

— Интерфейси: OpenFlow, NETCONF (Network Configuration Protocol), RESTful APIs (Representational State Transfer), gRPC (gRPC Remote Procedure Calls);

— Протоколи: OpenFlow, BGP-LS (Border Gateway Protocol - Link State), VSDB (Open vSwitch Database Management Protocol), OF-Config (OpenFlow Configuration and Management Protocol).



Фиг. 2. *SDN слоест модел*

Мрежови хипервайзори: Мрежовата виртуализация представлява абстракция на определена мрежа, която е отделена от основното физическо оборудване. Това позволява на множество виртуални мрежи да работят върху споделена инфраструктура, където всяка виртуална мрежа може да има своя топология, а не имплицитна физическа мрежа. Flow Visor е първоначалният опит за виртуализиране на SDN. Както е показано на фиг. 3, Flow Visor действа като посредник между контролера и мрежовите инструменти, за да осигури концептуален слой, който споделя информационната равнина OpenFlow, като се позволява на множество контролери да контролират собствената си част. Основното предназначение на Flow Visor е да определи кой да контролира пакетите, изпратени от комутатора, и да провери и установи правилата (policy), които да бъдат зададени от контролерите [6, 8].

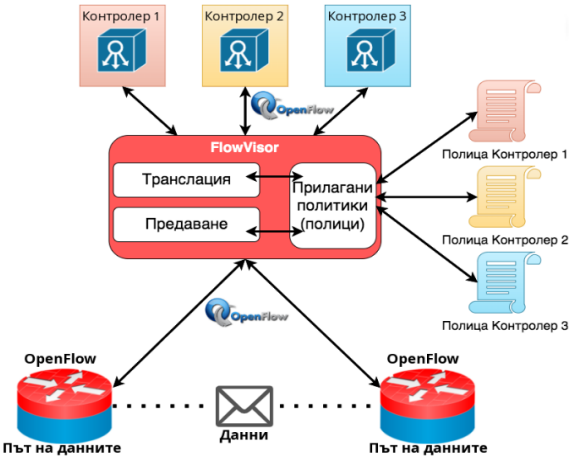
Мрежови операционни системи: Мрежовата операционна система е основният елемент в SDN архитектурата. Подобно на операционната система, контролерът абстрахира детайлите на протокола SDN от контролера към устройствата, където приложенията по-горе могат да комуникират с тези SDN устройства, без да „*знаят*“ разликата. Този централизиран контрол от NOS трябва да улесни управлението на мрежата и да опрости претоварването при решаване на мрежови проблеми. Основните функции на контролера включват:

— Откриване на устройство на краен потребител;

— Откриване на мрежово устройство;

— Управление на топологията;

— Управление на потока.



Фиг. 3. *Мрежов хипервайзор Flow Visor*

Северни гранични интерфейси: Северните интерфейси осигуряват абстракция, която позволява на мрежовите приложения да не зависят от определени програмни реализации, за да се опрости програмното управление на мрежата. Обратно на южния интерфейс, северният интерфейс е предимно софтуерна система, където приложения за маршрутизиране се изграждат програмно чрез езици като Python или Java, което позволява по-бързо развитие, по-ниски инвестиционни разходи и по-лесно отстраняване на неизправности в сравнение с Southbound API [9]. Контролерът уведомява приложението за процедури и събития, които се случват в мрежата. Събитията може да се отнасят до отделен обработван пакет или процес, който е установен от контролера, или промяна на състоянието в топологията, като прекъсване на връзката. Приложенията изискват различни подходи в отговор на събитието. Това може да включва премахване на промяна или препращане на пакета в случай на настъпило събитие. Най-популярните NBI интерфейси са:

- RESTful API (Representational state transfer);
- RESTCONF (RESTful Network Configuration Protocol);
- gRPC (gRPC Remote Procedure Calls);
- JSON-RPC ;
- XML-RPC.

Езици за програмиране: Една от главните идеи за създаване на SDN концепцията е да се постигне унифициране чрез езиците за програмиране, които са API от високо ниво, разширяващи концепцията за самата мрежа. По-този начин разработчиците не трябва да познават програмните особености на отделните мрежови елементи, и като цяло да са по-малко ангажирани с елементите на мрежовата инфраструктура [9]. Езици като Pyretic, Python и Frenetic са предназначени за SDN.

Мрежови приложения: Мрежовите приложения прилагат контролна логика, която се предава на мрежовите устройства, препоръчва какво е инсталирано на мрежовите устройства и определя тяхното поведение. Мрежовото приложение се счита за „*мрежов мозък*“. Той се регистрира като слушател за определени събития, както бе посочено по-горе, след което контролерът извиква метода за обратно извикване на приложението, когато възникне такова събитие, както и да ги прилага към външни входове, като например изпълнение на методи за защита. [9]. За да постигне тази цел на мрежовото маршрутизиране в компютърните мрежи, приложението за маршрутизиране трябва, въз основа на топологията, да вземе решение и да избере маршрут, който ще се използва и същевременно да инструктира контролера да приложи съответните правила за маршрутизиране във всички маршрутизиращи устройства по избрания път от A до B [10].

Въпреки голямото разнообразие от случаи на използване, повечето SDN приложения могат да бъдат обобщени в един от петте изброени класа: *контрол на трафика, мобилност и безжична връзка, измерване и наблюдение, сигурност и надеждност и мрежи на центрове за данни*[6]. Протоколите в мрежовите приложения обуславят три източника на информация за мрежови операционни системи:

— Първо, съобщенията, базирани на събития, се изпращат от препращащи устройства към контролера, когато се създаде връзка или промяна на порта.

— Второ, статистическите данни за потока се генерират от препращащите устройства и се събират от контролера.

— Трето, входящите съобщения от пакети се изпращат от препращащи устройства към контролера, когато те не знаят какво да правят с нов входящ поток или защото има изрично действие „изпрати до контролера“ в съответстващия запис на таблицата на потока. Тези информационни канали са основните средства за предоставяне на информация за нивото на потока на мрежовата операционна система [9].

Заключение

Софтуерно-дефинираните мрежи променят мрежовата архитектура чрез въвеждане на динамичен и централизиран подход към управлението. Слоевете на абстракция, които обхващащ Southbound Interface за комуникация с информационната равнина и Northbound Interface за взаимодействие с приложенията, играят ключова роля за текущия успех и основа за бъдещо развитие на SDN. Тези слоеве на абстракция подобряват модулността и правят възможно скалирането на мрежи от всякакъв мащаб, позволявайки ефективно повторно използване на кода и високата адаптивност на системата. Използването на стандартизирани протоколи, като OpenFlow, гарантира оперативна съвместимост и полага основи за бъдещи иновации. Разделянето на равнините за управление и данни позволява внедряването на различни приложения, без да се нарушава основната инфраструктура.

Облачните системи изискват адаптирането и на компютърните мрежи към тях. SDN съвместимостта с хипервайзори подобрява интеграцията им във

виртуализирани среди, допринасяйки за по-добра гъвкавостта и ефективност на съвременните мрежи. Както беше представено по-горе, слоестият модел на SDN, който се явява стъпка в еволюирането на традиционните компютърни системи, осигурява солидна основа за автоматизирано мрежово управление и бързо адаптиране към развиващите се мрежови изисквания.

ЛИТЕРАТУРА

[1] McKeown, N., et al., OpenFlow: Enabling Innovation in Campus Networks, ACM SIGCOMM Computer Communication Review, volume 38, number 2, 2008.

[2] Kreutz, D., et al., Software-Defined Networking: A Comprehensive Survey, Proceedings of the IEEE, volume 103, issue 1, 2015, doi:10.1109/JPROC.2014.2371999.

[3] Gude, N., et al.,NOX: Towards an Operating System for Networks, ACM SIGCOMM Computer Communication Review, 2008.

[4] McKeown, N., Anderson, T., Balakrishnan, H.; Parulkar, G.; Petrson, L.; Rexford, J.; Shenker, S.; Turner, J., OpenFlow: Enabling Innovation in Campus Networks, volume 38, issue 2, 2008, pp 69–74, https://doi.org/10.1145/1355734.1355746.

[5] Kreutz, D., Jiangshan., Y., Esteves-Veríssimo, P. Magalhães, C., Ramos, F. M.V., The KISS principle in Software-Defined Networking: A framework for secure communications, IEEE Security & Privacy, volume 16, isssue 5, 2018, doi:10.1109/MSP.2018.3761717.

[6] Azodolmolkly, S., Software Defined Networking with OpenFlow, Birmingham, 2013, ISBN 978-1-84969-872-6.

[7] Oppenheimer, P., Cisco Press "Top Down Network Design. Cisco Press. Indianapolis, 2011, ISBN-13: 9781587140013.

[8] Ramos., F., Kreutz., D., Verissimo., P., Software-Defined Networks: On the Road to the Softwarization of Networking, Cutter IT Journal, volume 28, issue 5, 2015. pp. 6-13, ISSN : 1554-5946.

[9] Casado, M.; Foster., N., Guha, A., Abstractions for software-defined networks, CM Commun, volume 57, issue 10, 2014, pp. 86 – 95, https://doi.org/10.1145/2661061.2661063.

[10] Mininet. An Instant Virtual Network on your PC, 2018, (Accessed 1.12.2023 URL: http://www.mininet.org).

[11] Denev D., Tsankov Ts. Development of a Virtual Private Network in Computer Networks and Communication Environments. 2020, International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 71 July, ISSN 2367-5721, pp. 11-19.

КОНТРОЛ НА РАБОТНАТА ГЕОДЕЗИЧЕСКА ОСНОВА

Мирем Е. Ниязи-Юсуф

CONTROL OF THE WORKING GEODESIC BASE

Mirem E. Niyazi-Yusuf

ABSTRACT: *Control is a quality check of the cadastral map and cadastral registers, including through repeated measurements. Control of the working geodetic base is an important stage in the creation of a cadastral map and cadastral registers.*

KEYWORDS: *Control, Cadastral map, Geodetic base.*

Контролът на работната геодезическа основа (РГО) се осъществява в три етапа:

1. Съгласуване на проекта на РГО;
2. Контрол на изпълнението на РГО;
3. Приемане на РГО;

Съгласуване на проекта на РГО

Работната геодезическа основа се създава като планова и височинна мрежа, вкл ючена в точки от ДГМ, ГММП и станциите на инфраструктурните ГНСС мрежи.

За създаването на РГО за урбанизираните територии се изработва проект, който се съгласува със службата по геодезия, картография и кадастър. В проекта се посочват и начините за определяне на точките от РГО, както и номерирането им. Извън урбанизирани територии РГО се създава само за частите от територията, за които ще се извършват геодезически измервания.

Съгласуваният проект може да бъде допълван и променян от изпълнителя в процеса на изпълнението му. Броят на изключените от проекта точки не може да бъде по-голям от 10 на сто. [1]

Контрол на изпълненеието на РГО

Контролът на изпълнението на РГО включва:

1. проверка на данните от измерванията и обработката им;

2. полска проверка по отношение изпълнението на проекта на РГО и на изискванията на чл. 23 от Наредба № РД-02-20-5 от 15 декември 2016 г. и

преизмерване до 10 на сто от точките на РГО за оценка на точността на определените координати.

Проверката на данните от измерванията и обработката им се извършва от Службата по геодезия, картография и кадастър (СГКК) с контролна компютърна програма. Форматът на файловете от измерванията и обработката им при прилагане на класически технологии е съгласно приложение № 3 от [2], а за GPS-измерванията – в RINEX-формат. Величините, които се проверяват с контролната компютърна програма при прилагане на класически технологии, са съгласно приложение № 4 от [2]. Програмно съставеният протокол се подписва от лицето, извършило проверката.

Полската проверка на РГО се извършва от длъжностни лица в СГКК, определени от началника на службата., по един от следните методи, съгласувано със СГКК:

1. чрез включени полигонови ходове - при прилагане на класически технологии или чрез определяне на затворени фигури - при GPS-измервания, като всяка точка се определя с минимум два вектора;

2. чрез абриси на станции от РГО;

3. чрез комбинация от двата метода.

За извършената проверка се съставя доклад, който включва оценка на преизмерените точки по следните величини:

1. грешките в абсолютното положение и разликите в надморските височини – при полската проверка чрез включени полигонови ходове;

2. средните квадратни грешки за посока от абрисите на станциите и относителните грешки на дължините - при полска проверка чрез абриси на станции от РГО.

Изпълнителният директор Агенцията по геодезия, картография и кадастър може да възложи извършването на контрола и на лица с правоспособност по чл. 19, ал. 1 от Закона за кадастъра и имотния регистър (ЗКИР)

Когато повече от 5 на сто от грешките в абсолютното положение и разликите в надморските височини превишават 7 см в урбанизирани територии, съответно 14 см в неурбанизирани територии, или средните квадратни грешки за посока превишават 6 mgon, или относителните грешки в дължините превишават 1:4000, в доклада се отбелязва, че РГО по точност не отговаря на нормативните изисквания. [2]

За извършения контрол на изпълнението на РГО се представят материали и данни съгласно приложение № 2 от [2].

1. Обяснителна записка, която съдържа наименованието на обекта, методите на измервания и обработката им, изпълнителя, състава на работния колектив, датата.

2. Задание за извършения контрол.

3. Становище относно стабилизирането и сигнализирането на точките от РГО.

4. Данните от полските измервания с GPS в RINEX-формат.

5. Данните от полските измервания с тотална станция.

6. Резултатите от изравнението на РГО.

7. Регистър на проверените точки, който включва координатите, определени при контрола, координатите, определени от изпълнителя, и координатните разлики.

8. Статистически анализ на координатните разлики.

Всички данни и материали се представят в цифров и текстов вид. Форматът на представяне на данните е съгласно приложение № 3 от [2] - при измерване с класически технологии или в RINEX-формат при измерване с GPS

Приемане на РГО

Приемането на РГО се извършва от комисията на СГКК, назначена със заповед на изпълнителния директор на АГКК.

Комисията разглежда и оценява представените от изпълнителя материали и данни, доклада от проверката и протокола от проверката на данните от измерванията и обработката им. За направените констатации и взетите въз основа на тях решения комисията съставя протокол в пет екземпляра: по един екземпляр за комисията, за изпълнителя, за правоспособното лице, извършило контрола, и два екземпляра за Агенцията по геодезия, картография и кадастър.

Когато в изпълнението на РГО има несъответствия с нормативните изисквания, комисията не приема представените данни и материали и определя срок за отстраняването им.

Когато се констатират съществени несъответствия с нормативните изисквания, комисията не приема представените данни и материали, което се отбелязва в протокола.

За приемане на РГО изпълнителят представя в Службата по геодезия, картография и кадастър следните материали:

1. Обяснителна записка, която съдържа:

1.1. Обща характеристика - наименование на обекта с географско и топографско описание.

1.2. Хидрография, релеф и климатична характеристика - водни течения, водни площи, характер на релефа с наклони в различните райони.

1.3. Общи сведения за вида, гъстотата и разположението на изходните точки.

1.4. Координатна и височинна система, в която са определени точките на РГО.

1.5. Данни за ползваните съществуващи и новоизградени точки - начин на стабилизиране, измерване, изчисление и оценка на точността.

1.6. Методи на измерване и обработка.

1.7. Изпълнител, състав на работния екип, година и месец на измерването и други характерни особености.

2. Схема на РГО в графичен вид в подходящ мащаб, кратен на 500, и в цифров вид със следното съдържание:

2.1. Извънрамково оформяне.

2.2. Точките с техните условни знаци и номера.

2.3. План на наблюдение - хорди, бази, посоки, разстояния.

2.4. Землищната граница.

2.5. Границите на урбанизираните територии.

2.6. Пътищата, улиците и наименованията на някои поважни улици.

2.7. Разграфката и номенклатурата на кадастралните листове в М 1:5000 - със син цвят.

2.8. Координатните кръстове.

3. Реперни карнети в графичен и цифров вид.

4. Данните от полските измервания с GPS.

5. Данните от полските измервания с тотална станция.

6. Резултатите от изравнението на РГО - разделно GPS измервания и ъглови и дължинни измервания.

7. Регистър на геодезическата основа по образец, одобрен от изпълнителния директор на АГКК - в цифров вид.

Всички данни и материали се представят в цифров и текстов, съответно графичен вид. Форматът на представяне на данните от преките геодезически измервания е съгласно приложение № 3 от [2] или в RINEX-формат.

ЛИТЕРАТУРА

[1] Наредба № РД-02-20-5 от 15 декември 2016 г. за съдържанието, създаването и поддържането на кадастралната карта и кадастралните регистри-обн. ДВ. брой 4 от 13 януари 2017 г., заедно с ПриложенияНаредба 19.

[2] Наредба № 19 от 28.12.2001 г. за контрол и приемане на кадастралната карта и кадастралните регистри (по чл. 50 ЗКИР), Обн. ДВ. бр.2 от 8 Януари 2002г.

[3] Закон за кадастъра и имотния регистър, изм. и доп. ДВ. бр.8 от 25 януари 2023г.

ПРОГРАМНО УПРАВЛЕНИЕ НА КОМПЮТЪРНИ МРЕЖИ ЧРЕЗ ИЗПОЛЗВАНЕ НА МОДЕЛИ С ПРОТОКОЛИТЕ NETCONF И RESTCONF

Мустафа Б. Узун, Валентин Т. Атанасов

PROGRAM MANAGEMENT OF NETWORKS TROUGH MODELS BASED ON NETCONF AND RESTCONF PROTOCOLS

Mustafa B. Uzun, Valentin T. Atanasov

ABSTRACT: *This study explores model-driven network configuration programmability in the context of network automation management, focusing on key protocols such as NETCONF, YANG, and RESTCONF. The integration of these protocols enables automation of the computer network management, enhancing efficiency and scalability. The model-driven approach leverages declarative specifications, facilitating a clear separation of concerns between data and operations. This abstraction enables the creation of programmable network models, streamlining configuration and management tasks. The study investigates the impact of model-driven programmability on the reliability and agility of network operations. By evaluating the interoperability and standardization of these protocols, the research contributes insights into advancing automated network management systems, fostering a more responsive and adaptive networking infrastructure.*

KEYWORDS: *Networking, SDN, NETCONF, YANG, RESTCONF, Network automation.*

Въведение

Мрежовите устройства се управляват основно чрез команден ред CLI (Command Line Inreface). За наблюдение на мрежата все още широко се използва SNMP (Simple Network Management Protocol). Въпреки, че CLI са ефективен подход, те в определени случаи са със запазени права. Налице са и различия при производителите на мрежовото оборудване. Това определя необходимостта от квалифицирана човешка намеса. Като една от слабостите при тях е слабата мащабируемост при големи мрежови среди. Със значителното нарастване мащабите на съвременните компютърни мрежи се ускорява разработването на алтернатива на по-ограничения, като възможности протокол SNMP, за създаване на общ стандартен начин за управление и наблюдение на мрежовите устройства в лицето на протоколите NETCONF и RESTCONF. Моделирането на конфигурационни данни заменя ръчната конфигурация, тъй като предоставя

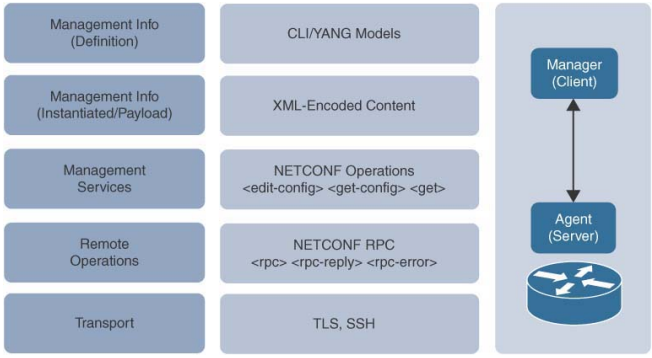
базиран на стандарти, програмен метод за записване на тези данни и събиране на статистически и оперативни данни от мрежовите устройства. Моделите на данни YANG са разработени специално, за да отговорят на необходимостта от стандартизация и общ подход в управлението на компютърните мрежи. Програмното управление на мрежи, чрез използване на модели с NETCONF и RESTCONF, позволява да се автоматизира конфигурирането и контрола на мрежовите устройства. Този подход за автоматизирано управление на мрежи е част от концепцията SDN (Software-defined Networking) за програмно дефинирани мрежови архитектури описан в [4].

Водещи производители на мрежово оборудване, като Cisco, Huawei, Juniper и други са вече интегрирали този протокол в някои от техните продуктови линии. Като пример може да се даде с Cisco IOS XE, мрежова операционна система предназначена за управление на по-големи по мащаб мрежи, Cisco NX-OS, мрежова операционна система за центрове за данни и Cisco IOS модели поддържащи NETCONF, RESTCONF и gRPC.

NETCONF

Протоколъта NETCONF определя механизма за установяване на данни за връзка и обмен между мрежовия администратор и мрежовите устройство, но не определя формат на данните [6]. Определянето на формата се извършва с езика за моделиране на данни YANG (Yet Another Next Generation) [3].

Протоколът NETCONF дефинира транспорт през SSH (Secure Shell) и включва операции и хранилища за данни за конфигурации, които позволяват управлението на мрежови устройства. Опциите за удостоверяване на NETCONF са същите като за всяка SSH комуникация. Могат да се използват потребителско име и парола, както и SSL сертификати, точно както CLI команди с SSH. Стекът на архитектурата на протокола и неговата връзка с YANG са показани на фиг.1



Фиг.1. Стек на архитектурата NETCONF и връзката с YANG.

NETCONF използва комуникационен модел клиент/сървър. Сървърната страна се разгръща на мрежовото устройство чрез NETCONF агент, който действа като API от северния интерфейс на SDN модела. Клиентите, свързващи

се с агента, изпращат частични или пълни конфигурационни данни и получават данни за състоянието и работата от устройството. Всяка система, която прилага протокола, може да бъде клиент, някои често срещани са Cisco NSO и ncclient (Python) [1].

Основната цел на NETCONF е да се транспортират полезни данни между клиент и сървър. Полезните данни могат да бъдат конфигурационни, оперативни и известяващи. NETCONF поддържа известявания, които са подобни на SNMP trap съобщения [1].

Съобщенията, изпратени с NETCONF, използват извиквания на отдалечени процедури RPC (Remote Procedure Call). Клиентът или приложението за управление изпраща своето XML-форматирано съобщение до сървъра, като заявката се вмъква в <rpc> XML елемент, а сървърът връща резултати в рамките на <rpc-reply> елемент [6]. Протоколът NETCONF предоставя малък набор от операции на ниско ниво, част от които са представени в таблица 1.

Таблица 1. *Операции в NETCONF*

NETCONF операции	
<get>	Извличане на информация за работеща конфигурация и състояние на устройството
<get-config>	Извличане на цялото или част от указаното хранилище на конфигурационни данни
<edit-config>	Зареждане на цялата или част от конфигурация в указаното хранилище на конфигурационни данни
<copy-config>	Заменяне на цялото хранилище на конфигурационни данни с друго
<delete-config>	Изтриване на хранилище на конфигурационни данни
<commit>	Копиране хранилището на потенциални данни в текущото хранилище на данни
<lock> / <unlock>	Заключване или отключване на цялата система за съхранение на данни за конфигурация
<close-session>	Нормално прекратяване на сесията NETCONF
<kill-session>	Принудително прекратяване на сесията NETCONF

YANG

YANG е език, използван за моделиране на данни за протокола NETCONF. Модулът YANG дефинира йерархия от данни, които могат да се използват от базирани на NETCONF операции. Този език позволява пълно описание на всички данни, изпратени между NETCONF клиент и сървър. YANG моделира йерархичната организация на данните като дърво, в което всеки възел има име и или стойност, или набор от дъщерни възли. YANG предоставя ясни и кратки описания на възлите, както и взаимодействието между тези възли [2]. В (1) се показва код в YANG модел за назначаване на IP адрес в мрежово устройство.

YANG постига баланс между моделиране на данни на високо ниво и описва метод за представяне на данни в компютърните мрежи на ниско ниво, когато информацията се предава по мрежата във формата на битове „bits-on-the-wire“.

Този подход се използва за кодиране и декодиране на данни, когато те се изпращат или получават по мрежата. Идеята зад този подход е да се изложи информацията на ниво, при което данните се представени чрез бинарни стойности. Този вид кодиране е специфичен начин за преобразуване на данни в последователност от битове, които може да бъде лесно интерпретирани и обработвани от устройствата в мрежата.

YANG структурира моделите на данни в модули и подмодули. Един модул може да импортира данни от други външни модули и може да включва данни от подмодули. Йерархията може да бъде разширена, позволявайки на един модул да добавя възли с данни към йерархията, дефинирана в друг модул [1, 2].

```
module router-config {                                                    (1)
 yang-version 1.1;
 namespace "urn:example:router-config";
 prefix rc;

 import ietf-inet-types {
  prefix inet;
 }

 organization "Example Organization";

 container router {
  list interfaces {
   key name;
   leaf name {
    type string;
   }
   container ip {
    leaf address {
     type inet:ipv4-address;
    }
    leaf subnet-mask {
     type inet:ipv4-prefix;
    }
   }
  }
 }
}
```

Модулът YANG съдържа три типа изрази [2]:

- *Изявления за дефиниране на данни* (Data Definition Statements): Тези изявления определят структурата и типовете данни, които могат да бъдат използвани в рамките на модула. Те биха могли да определят типът на поддържаните данни и как те са организирани.

- *Изявления за обработка на данни* (Data Handling Statements): Тези изявления определят начина, по който данните се обработват в рамките на модула. Това включва правила за валидация, обновление и извличане на данни.
- *Изявления за известия* (Notifications Statements): Тези изявления се използват за дефиниране на събития или известия, които могат да бъдат генерирани от модула. Те предоставят начин за информиране при определени събития, които се случват в системата.

YANG дефинира четири типа възли за моделиране на данни [3]:

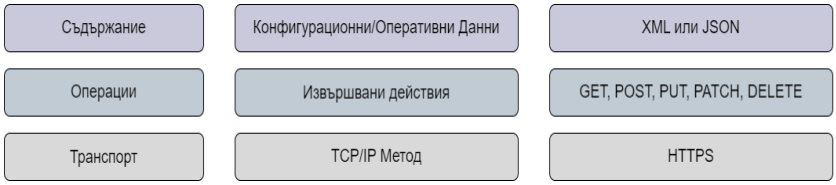
- *Leaf nodes*
- *Leaf-list nodes*
- *Container nodes*
- *List nodes*

RESTCONF

RESTCONF, като базиран на HTTP протокола, осигурява програмен интерфейс за достъп до данни, дефинирани в YANG и използвайки концепциите за хранилище на данни, дефинирани в протокола за мрежова конфигурация (NETCONF) [4].

По принцип RESTCONF предоставя REST-подобен интерфейс към модела NETCONF/YANG. Въпреки че NETCONF осигурява значителни подобрения спрямо SNMP, той не предоставя мрежови интерфейси с добър REST API интерфейс. NETCONF намира своята еволюция в RESTCONF, но запазва своята самостоятелност.

RESTCONF предоставя API, който се привежда в съответствие с API на други УЕБ приложения, за да осигури входна точка за разработчиците [1]. На фиг. 2 е показан стекът на протокола RESTCONF.



Фиг.2. Протоколен стек RESTCONF

Подобно на други REST API, RESTCONF използва HTTPS протокола за капсулиране и изпращане на съобщения. Удостоверяването се осъществява с помощта на типични модели за удостоверяване на HTTP, като основно удостоверяване, при което потребителските имена и паролите са кодирани в Base64 и се предават от клиента към сървъра чрез заглавка за удостоверяване.

REST API обикновено прилагат CRUD (създаване, извличане, актуализиране и изтриване) операции, като използват HTTP методи. RESTCONF картографира NETCONF операциите в HTTP методи, както е показано на таблица 2 [1].

Таблица 2. *NETCONF операции в HTTP методи*

RESTCONF/NETCONF	
GET	<get>, <get-config>
POST	<edit-config> (operation=”create”)
PUT	<edit-config> (operation=”create/replace”)
PATCH	<edit-config> (operation=”merge”)
DELETE	<edit-config> (operation=”delete”)

Наличните RESTCONF методи и съответните им NETCONF операции са както следва [4]:

- HTTP GET изпраща в заявката RESTCONF от клиента за извличане на данни и метаданни за конкретен ресурс. Прилага се в операциите NETCONF <get> и <get-config>. Методът GET се поддържа за всички типове ресурси, с изключение на операционните ресурси.
- HTTP POST се използва за NETCONF RPC и за създаване на ресурс от данни. Семантичният му смисъл е като при операцията NETCONF <edit-config> с operation= “create”.
- PUT се използва за създаване или замяна на съдържанието на целевия ресурс. Това е еквивалент на операцията NETCONF <edit-config> с operation=“create/replace”.
- PATCH осигурява рамката на механизъм за корекция на ресурси. Това е еквивалент на операцията NETCONF <edit-config> с operation=“merge”.
- HTTP DELETE се използва за изтриване на целевия ресурс и е еквивалент на NETCONF <edit-config> с operation=“delete”.

Алгоритмични подходи

Може де бъде представен следният подход за конфигуриране на IP адрес от интерфейс на маршрутизатор с операционна система IOS XE/NX-OS, посредством RESTCONF, YANG и NETCONF, като се следват изложените по-долу стъпки:

Стъпка 1 - дефиниране на YANG модел с цел описване на промените в конфигурацията, които трябва да се направят. Конфигурацията следва да се съхрани във файл *interface-config.yang***.**

```
module interface-config {                                    (2)
 yang-version 1.1;
 namespace "urn:example:interface-config";
 prefix "ifc";
 import ietf-inet-types { prefix "inet"; }
 import ietf-interfaces { prefix "if"; }
 organization "Example Organization";
 container interfaces {
  list interface {
   key "name";
   leaf name {
    type if:interface-ref;
```

```
    }
    container ipv4 {
     leaf address {
      type inet:ipv4-address;
     }
     leaf subnet-mask {
      type inet:ipv4-address;
     }
    }
   }
  }
 }
```

Стъпка 2 - компилиране на YANG модела в YANG модул. Възможно е да бъдат използвани инструменти като pyang за тази цел.

```
pyang -f yang -p . interface-config.yang -o interface-config.yang
```
(3)

Стъпка 3 - Създаване на XML полезен товар

```
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <interfaces xmlns="urn:example:interface-config">
  <interface>
   <name>GigabitEthernet0/0</name>
   <ipv4>
    <address>192.168.1.1</address>
    <subnet-mask>255.255.255.0</subnet-mask>
   </ipv4>
  </interface>
 </interfaces>
</config>
```
(4)

Стъпка 4 - NETCONF клиентски скрипт – използва се NETCONF клиент, като например ncclient (Python), за да се изпрати XML полезният товар към мрежовото устройство. Показаният в (5) код е генериран от ncclient.

```
router_ip = "your_router_ip"
router_port = 830
router_username = "your_username"
router_password = "your_password"
xml_payload = """
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <interfaces xmlns="urn:example:interface-config">
  <interface>
   <name>GigabitEthernet0/0</name>
   <ipv4>
    <address>192.168.1.1</address>
    <subnet-mask>255.255.255.0</subnet-mask>
   </ipv4>
  </interface>
```
(5)

```
 </interfaces>
</config>
"""
with manager.connect(
  host=router_ip,
  port=router_port,
  username=router_username,
  password=router_password,
  allow_agent=False,
  look_for_keys=False,
  hostkey_verify=False,
) as m:
   response = m.edit_config(target="running", config=xml_payload)
   print(response)
```

Заключение

Интегрирането на програмно управление на компютърни мрежи чрез модели с помощта на протоколи NETCONF, YANG и RESTCONF демонстрира значителен напредък в автоматизираното управление на компютърни мрежи и автоматизация на мрежите. Декларативният характер на тези протоколи, съчетан със стандартизирани модели на данни, оптимизира процесите на конфигуриране и подобрява цялостната надеждност на системата. Проучването извежда значението на оперативната съвместимост и стандартизацията при тези подходи за постигане на по-ефективната им интеграция. Положителна страна този подход е възможността за мащабиране на мрежата.

ЛИТЕРАТУРА

[1] Jackson, C., Gooley, J., Iliesiu, A., Malegaonkar, A., Cisco Certified DevNet Associate: DEVASC 200-901 Official Cert Guide, Cisco Press, 2021, ISBN 13-978-01-3664296-1.

[2] Claise, B., Clarke, J., Lindblad, J., Network Programmability with YANG: The Structure of Network Automation with YANG, NETCONF, RESTCONF, and gNMI, Addison-Wesley Professional, 2019, ISBN 13-978-0135180396.

[3] YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF), (Посетен на 02.12.2023) (https://datatracker.ietf.org/doc/html/rfc6020).

[4] RESTCONF Protocol, (Посетен на 02.12.2023) (https://datatracker.ietf.org/doc/html/rfc8040).

[5] Software-Defined Networking (SDN): Layers and Architecture Terminology, (Посетен на 02.12.2023) (https://datatracker.ietf.org/doc/html/rfc7426).

[6] Network Configuration Protocol (NETCONF), (Посетен на 02.12.2023) (https://www.rfc-editor.org/rfc/rfc6241.html).

УПРАВЛЕНИЕ НА ВРЪЗКАТА ЗА WDM МРЕЖИ С МАРШРУТИЗИРАНЕ НА ДЪЛЖИНА НА ВЪЛНАТА

Екатерина М. Христова, Цветослав С. Цанков

LINK MANAGEMENT FOR WDM NETWORKS WITH WAVELENGTH ROUTING

Ekaterina M. Hristova, Tsvetoslav S. Tsankov

ABSTRACT: *With the rapid growth of the Internet, the demand for bandwidth for data traffic is increasing. It turns out that dynamic light path establishment, or light flow establishment on demand, will allow ISPs to respond quickly and cost-effectively to customer requirements.*

KEYWORDS: *Multiplexing, Optical fiber, Packet switching, Signal-to-noise ratio, Wavelength, WDM.*

Едно от предизвикателствата, свързани с изискванията за проектирането на мрежи с маршрутизирана дължина на вълната с динамичен трафик, е да се разработят ефективни алгоритми и протоколи за установяване на светлинни пътища. Алгоритмите трябва да избират маршрути и да задават дължини на вълните към връзки, като използват ефективно мрежовите ресурси и увеличават броя на установените светлинни пътища. Сигналните протоколи за създаване на светлинни пътища трябва ефективно да управляват разпространение на контролни съобщения, както и информация за състоянието на мрежата за своевременно установяване на начини за връзка. Обикновено се използва Протокол за мрежов контрол и за управление за извършване на RWA и задачите за сигнализиране. Друг проблем при установяването на динамичен светлинен път е инициализацията на заявки за установяване или отстраняване на светлинен поток. Съществуват редица възможни подходи за генериране на заявка за връзка.

Например, клиент може да инициира заявка за връзка чрез щракване върху уеб страница или чрез извикване доставчика на услугата. Заявка за връзка също може да бъде инициирано от IP рутер или друго мрежово устройство, което идентифицира търсене между две OXC-и. Полагат се много усилия за развитие на протоколите за създаване на светлинни пътеки при поискване. Взаимното свързване на оптични домейни (ODSI) работи за стандартизиране на интерфейси, което би позволило клиентски мрежи и устройства да взаимодействат с оптична мрежа. ODSI рамката не посочва как действително се установяват светлинните

пътища в рамките на оптичната мрежа, а просто определя как клиентът ще поиска светлинен път или ще освободи светлинен път от оптичната мрежа. [3, 4, 5, 6]

Превключването на Многопротоколни Етикети (MPLS) е контролна рамка, която се разработва като стандарт за позволяване на бързо превключване в IP мрежи. MPLS контролните механизми могат да се използват за създаване на път с превключване на етикети (LSP) между два несъседни IP рутера, позволяващи пакетите да заобикалят рутери в междинни възли. Основният сигнализиращ механизъм за установяване на LSP в MPLS е Протоколът за Разпространение на Етикети (LDP). Концепцията за MPLS може да бъде разширена до оптични мрежи с дължина на вълната като MPAS (мултипротоколно ламбда превключване). Работната група за интернет инженеринг (IETF) разработва Многопротоколно превключване на етикети (GMPLS), обобщена контролна рамка за установяване на различни видове връзки, включително светлинни пътища, в IP базирани мрежи. [1, 2, 12, 13, 15, 21]

Правени са много промени на съществуващи протоколи за маршрутизиране и сигнализиране, които да поддържат GMPLS. По-специално, IETF се фокусира върху подобренията на Open Shortest Path First (OSPF) протокол за маршрутизиране и базиран на ограничения Routing Label-Distribution Protocol (CR-LDP), както и Протокола за сигнализиране и резервиране на ресурси (RSVP). OSPF е протокол за състояние на връзката при който състоянието на всяка връзка в мрежата периодично се излъчва до всички възли под формата на информационни реклами (LSA). След това възлите могат вземат своите решения за маршрутизиране въз основа на тази информация. RSVP е IP протокол, който се използва за сигнализиране на нуждите от ресурси и се прилага от междинни рутери. CR-LDP е протокол, който позволява разпределението на контролните съобщения за създаване на потоци чрез превключване на етикети. CR-LDP използва маршрутизиране с ограничения и работи заедно с TCP за надеждност. Докато фокусът на IETF е върху няколко конкретни протокола, самият GMPLS не е ограничен до нито едно маршрутизиране или протокол за сигнализизация. Освен това, протоколи като OSPF, CR-LDP и RSVP са гъвкави и могат да се адаптират за внедряването на различни маршрути и сигнални схеми за създаване на светлинни потоци. [3, 4, 5, 6, 7, 26, 27, 34]

1. Фиксирано маршрутизиране и Маршрутизиране с фиксиран алтернативен път

Два примера за алгоритми, които използват статични маршрути са с фиксиран маршрут и с фиксиран алтернативен маршрут. При фиксираното маршрутизиране има единичен фиксиран маршрут предварително определен за всяка двойка източник-дестинация. При маршрутизирането с фиксиран алтернативен път има множество фиксирани маршрути предварително изчислени

за всяка двойка източник-дестинация и съхранявани в подреден списък в маршрутизиращата таблица. Когато пристигне заявка за връзка, има един маршрут, избран от набора от предварително изчислени маршрути. Два от тези подхода са много по-лесни за прилагане в сравнение с адаптивните схеми за маршрутизиране, но страдат от провал на връзката. [8, 9, 10, 11, 14]

2. Адаптивно маршрутизиране, базирано на глобална информация

Подходите за адаптивно маршрутизиране увеличават вероятността за установяване на връзка чрез използване на информация за състоянието на мрежата. За случая, в който глобалната информация е налична, решенията за маршрутизиране могат да бъдат направени с пълното знание кои дължини на вълните са налични на всяка връзка. За намиране на оптимален маршрут, може да бъде създадена система със стойност, оценяваща всяка връзка въз основа на наличието на дължина на вълната, като се изпълнява алгоритъм за маршрутизиране с най-ниска стойност. [1, 13, 21]

Адаптивното маршрутизиране с глобална информация може да бъде внедрено по централизиран или разпределен начин. В централизиран алгоритъм, една централизирана единица, като мрежов мениджър, поддържа информацията за състоянието на мрежата и отговаря за намиране на маршрути и заявяването на създаване на светлинни пътеки. Тъй като една централизирана единица управлява цялата мрежа, няма нужда от висока степен на координация между възлите. Тази централизирана единица става възможна слабост в системата.

Алгоритъм за разпределено адаптивно маршрутизиране, базиран на глобалната информация може да бъде реализиран по редица начини. При подхода *връзка-състояние* всеки възел в мрежата трябва да поддържа пълно състояние на мрежова информация. След това всеки възел може да намери маршрут за заявка за връзка по разпределен начин. Всеки път, когато състоянието на мрежата се промени, всички възли трябва да бъдат информирани. Следователно, установяването или премахването на светлинен път в мрежа довежда до излъчване на съобщение за актуализация до всички възли в мрежата. Необходимостта от излъчваните съобщения за актуализация може да доведат до значителени контрол, особено ако светлинните пътища се обработват с висока скорост. Освен това, възможно е даден възел да е с остаряла информация и да вземе неправилно решение за маршрутизиране въз основа на тази информация.

Подходът *разстояние-вектор*, а именно подход на разпределено маршрутизиране с глобална информация, също е възможен. Този подход не изисква всеки възел да поддържа цялостна информация за състоянието на мрежата, а вместо това да поддържа таблица за маршрутизиране, която показва следващото прескачане до местонахождението и разстоянието до там. Подходът разчита на разпределен алгоритъм на Белман-Форд за поддържане на таблицата.

Схемата също изисква актуализация на информацията за маршрутизиращата таблица всеки път, когато се установи или прекъсне връзка. Тази актуализация се осъществява, като всеки възел периодично изпраща актуализации на маршрута на своите съседи или когато състоянието на изходящите връзки на възела се промени. [20, 28, 32, 36, 37]

Друга форма на адаптивно маршрутизиране е този с най-малко претоварен път (LCP). Задръстването на дадена връзка се измерва с броя на дължини на вълните, налични на връзката. Връзки, които имат по-малко налични дължини на вълната се считат за по-заети. Задръстванията по пътеката се обозначават със задръстването на най-натоварените връзка. Подобно на алтернативно маршрутизиране, за всяка двойка източник-местонахождение, предварително е избрана последователност от маршрути. При пристигането на заявка, се избира най-малко натоварения път сред предварително определени маршрути. Използването на маршрутизиране по най-краткия път и после LCP за прекъсването на равенството работи по-добре от използването на LCP самостоятелно. [29, 35]

Въпреки че схемите за маршрутизиране, базирани на глобални познания, трябва да се справят със задачата да поддържат потенциално голямо количество информация за състоянието, което се променя постоянно, тези схеми често вземат най-оптималните решения за маршрутизиране, ако информацията за състоянието е актуална. По този начин схемите, базирани на глобални знания, могат да бъдат много подходящи за мрежи, в които светлинните пътища са доста статични и не се променят много с времето. [14, 15, 33]

3. Адаптивно маршрутизиране, базирано на локална информация – маршрутизиране на отклонение

При схемата на маршрутизирането с отклонение или маршрутизирането на алтернативна връзка за маршрутизиране се избира от алтернативни връзки чрез прескачане, вместо маршрути от-край-до-край. Маршрутизирането се изпълнява, като всеки възел поддържа таблица за маршрутизиране, която показва за всяка дестинация една или повече алтернативни изходящи връзки за достигане до тази дестинация. Тези алтернативни изходящи връзки са предварително изчислени и могат да бъдат подредени така, че заявката за свързване да избира предпочитано определени връзки пред други връзки, стига ресурсите за дължина на вълната да са налични за тези връзки. Ако ресурсите не са налични на предпочитаната връзка, тогава за маршрута се избира алтернативна връзка. Освен статична таблица за маршрутизиране, всеки възел ще поддържа информация само относно състоянието на използването на дължината на вълната на собствените си изходящи връзки. Следователно в мрежата няма съобщения за актуализиране и търсенето на честотна лента за управление е значително намалено. [17, 18, 19, 22]

Като цяло, ако има множество възможни дължини на вълната между възел-източник и възел-местоназначение, тогава е необходим алгоритъм за определяне на дължина на вълната. Един пример за проста, но ефективна евристика за определяне на дължината на вълната е First-Fit. При него дължините на вълните се индексират и светлинният път се опитва да избере дължината на вълната с най-нисък индекс, преди да се опита да избере дължина на вълната с по-висок индекс. Чрез този метод съществуващите връзки ще бъдат опаковани в по-малък брой общи дължини на вълните, оставяйки по-голям брой дължини на вълните на разположение за по-дълги светлинни пътища. [30, 31]

4. Сигнализация и запазване на ресурси и паралелна резервация

За установяване на светлинен път, е нужен протокол за сигнализиране за обмен на контролна информация между възли и за резервиране на ресурси по пътя. В много случаи протоколът за сигнализиране е близко-интегриран с протоколите за маршрутизирането и присвояване на дължината на вълната. Протоколите за сигнализация и резервация могат да бъдат категоризирани и класифицирани въз основа на това дали ресурсите се резервират паралелно за всяка връзка, на база на мрежовите устройства по маршрута, или се запават при пренасочването по протежение на обратния път. Протоколите също ще се различават в зависимост дали е налична глобална информация или не. [7, 34]

Схемата, която използва маршрутизиране на състоянието на връзката, предполага, че всеки възел поддържа глобална информация за мрежовата топология и за текущото състояние на мрежата, включително информация относно дължините на вълните използвани за всяка връзка. Въз основа на тази глобална информация, възелът може да изчисли оптимален маршрут до местоназначението на дадена дължина на вълната. Изходният възел след това се опитва да запази желаната дължина на вълната на всяка връзка в маршрута чрез изпращане на отделно контролно съобщение до всеки възел в маршрута. Всеки възел, който получи съобщение за заявка за резервация, ще направи опит да запази определената дължина на вълната и ще изпрати потвърждение или отказ обратно към източника. Ако изходният възел получи потвърждения от всички възли, той може да създаде светлинен поток и започва комуникация с местоназначението. Предимството на паралелната схема за резервация е, че скъсява времето за установяване на сигнал чрез паралелното обработване на заявките за резервация. [16, 23, 24]

5. Резервация чрез мрежови устройства и предварителна резервация

Алтернатива на паралелната резервация е чрез пренасочване по мрежови устройства, при която се изпраща поетапно контролно съобщение по избрания маршрут. При всеки междинен възел управляващото съобщение се обработва

преди да бъде препратено към следващия възел. Когато контролното съобщение достига местоназначението, то е обработено и изпраща обратно към изходния възел. Действителното резервиране на ресурси може да се изпълнява или докато контролното съобщение пътувайки в посока напред към местоназначението си, или докато управляващото съобщение пътува в обратна посока обратно към източника. [25, 30, 31, 33]

В схемите за предварителна резервации, ресурсите се запазват по пътя към местоназначението един-по-един. Методът на резервирането на дължини на вълните зависи от това дали глобалната информация е достъпна за изходния възел. Ако изходният възел поддържа пълна информация за състоянието на мрежата, тогава ще бъде наясно кои дължини на вълните са налични за всяка връзка. Ако се приеме, че информацията за състоянието е актуална, изходният възел може да изпрати съобщение за установяване на връзка, запазвайки същата налична дължина на всяка връзка по пътя. Подходът за разпределеното маршрутизиране е подходящ пример за тази схема. [26, 27, 31]

За случая, в който възел знае само състоянието на своите непосредствени връзки, изходният възел може да използва консервативен резервиращ подход, като избира дължина на вълната и изпраща контролно съобщение към следващия възел, като се опитва да резервира тази дължина на вълната през целия път. Няма гаранция обаче, че избраната дължина ще бъде налична във всяка връзка по пътя. Ако нужната дължината е блокирана, изходният възел може да избере различна вълна и да опита отново да създаде връзка. Ограничението на този подход е, че може да доведе до повече време за обработка, тъй като може да отнеме няколко опита, преди даден възел да може да установи светлинен поток. [5, 35]

Алтернативен подход за увеличаване на вероятността за създаване на път в тази схема е да се използва агресивен метод за резервиране, която използва ненужно количество ресурси. Когато съобщението за резервация пристига до възел, той запазва всички дължини на вълните, които са налични за всички връзките, преминати до момента. Когато съобщението за заявката достигне целевия възел, местоназначението след това избира една дължина на вълната от дължините на вълните запазен по цялата пътека и освобождава резервите за останалите вълни. [5, 6, 7, 27, 34, 36]

6. Обратна резервация

За предотвратяване на свръх резервирането на ресурси, резервации могат да се правят след като контролното съобщение е достигнало местоназначението и е насочено обратно към източника. Такива схеми са наричани схеми за обратно резервиране. При тях, възелът-източник изпраща контролни пакети до местоназначението, без да резервира никакви ресурси. Тези контролни пакети ще се събират информация за използването на дължина на вълната по един или

повече пътища и дестинацията след това ще използва тази информация за вземане на решение за маршрут и дължина на вълната. След това дестинацията изпраща съобщения за резервация до изходните възли по избрания маршрут и това съобщение за резервация ще запази подходящите мрежови ресурси по пътя. [1, 4, 5, 6, 7, 26, 29, 37]

ЛИТЕРАТУРА

[1] Denev D. 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, pp. 75-79

[2] Denev D. Synthesis and Analysis of Linear Discrete and Time Invariant Systems Used in the Field of Communications using Matlab and Signal Processing Toolbox, Journal scientific and applied research, vol. 22, 2022 International Journal, 2022, ISSN 1314-6289, pp. 72-80

[3] S. Yao, S. Dixit, and B. Mukherjee, "Advanced in photonic packet switching: an overview," IEEE Communications Magazine. pp. 84-94, Feb. 2000.

[4] R. Ramaswami and K. N. Sivarajan, Optical Networks: A Practical [8] A. Mokhtar and M. Azizoglu, "Adaptive wavelength routing in all-optical networks," IEEE/ACM Transactions on Networking, vol. 6, pp. 197-206, Apr. 1998.

[5] 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.

[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] 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.

[8] Ivan Ivanov, Victor Lilov, Daniel Denev, Traffic Reporting and the Ability to Optimize LAN, MATTEH 2018, CONFERENCE PROCEEDING, vol. 1 Communication and Computer Technologies, ISSN 1314-3921, pp. 331-335

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

[10] Denev D. Analytical Study of the Delay Introduced as a Result of Encryption/Decryption of Voice Transmitted over a VPN Networks, Journal scientific and applied research, vol. 20, 2021 International Journal, 2021, ISSN 1314-6289, pp. 73-77

[11] Denev D. Comparative Analysis Between Wireless and Li-Fi, MATTEH 2022, CONFERENCE PROCEEDING, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 89-94

[12] Denev D. Low Energy Real-Time Routing, Annual University Scientific Conference, Proceedings of National Military University „Vasil Levski“, Veliko Tarnovo, 2022, ISSN 2367-7481, pp. 1267- 1276

[13] Chlamtac, A. Ganz, and G. Karmi, "Purely optical networks for terabit communication," in Proc. IEEE INFOCOM '89, vol. 3, (Washington, DC), pp. 887-896, Apr. 1989.

[14] S. Subramaniam and R. A. Barry, "Wavelength assignment in fixed routing WDM networks," in Proc. IEEE International Conference on Communications (ICC '97), vol. I, (Montreal, Canada), pp. 406-410, June 1997.

[15] X. Zhang and C. Qiao, "Wavelength assignment for dynamic traffic in multi-fiber WDM networks," in Proc. 7th International Conference on Computer Communications and Networks, (Lafayette, LA), pp. 479-485, Oct. 1998.

[16] B. Ramamurthy and B. Mukherjee, "Wavelength conversion in WDM networking," IEEE Journal on Selected Areas in Communications, vol. 16, pp. 1061-1073, Sept. 1998.

[17] J. Iness and B. Mukherjee, "Sparse wavelength conversion in wavelength-routed WDM networks," Photonic Network Communications, vol. 1, pp. 183-205, Nov. 1999.

[18] S. Subramaniam, M. Azizoglu, and A. K. Somani, "All-optical networks with sparse wavelength conversion," IEEEJACM Transactions on Networking, vol. 4, pp. 544-557, Aug. 1996.

[19] D. W. Matula, G. Marble, and J. D. Isaacson, Graph Theory and Computing (R. C. Read ed.), ch. Graph Coloring Algorithms, pp. 109-122. New York and London: Academic Press, 1972. ch. 10.

[20] D. W. Matula, "k-components, clusters and slicings in graphs," SIAM Journal of Applied Mathematics, vol. 22, 1972.

[21] A. Birman, "Computing approximate blocking probabilities for a class of all-optical networks," IEEE Journal on Selected Areas in Communications, vol. 14, pp. 852-857, June 1996.

[22] H. Zang, L. Sahasrabuddhe, J. P. Jue, S. Ramamurthy, and B. Mukherjee, "Connection management for wavelength-routed WDM networks," in Proc. IEEE Globecom '99, vol. 2, (Rio de Janeireo, Brazil), pp. 1428-1432, Dec. 1999.

[23] J. Garcia-Luna-Aceves, "Distributed routing with labeled distances," in Proc. IEEE INFOCOM '92, vol. 2, (Florence, Italy), pp. 633-643, May 1992.

[24] B. S. Davie, P. Doolan, and Y. Rekhter, Switching in IP Networks: IP Switching, Tag Switching and Related Technologies. San Francisco, CA: Morgan Kaufmann, 1998.

[25] Management enhancements," IEEE Communications Magazine, vol. 39, pp. 144-150, Jan. 2001.

[26] R. Perlman, Interconnections, Second Edition: Bridges, Routers, Switches, and Inter-networking Protocols. Addison Wesley Professional Computing Series, Oct. 1999.

[27] R. Ramaswami and A. Segall, "Distributed network control for optical networks," IEEE/ACM Transactions on Networking, vol. 5, pp. 936-943, Dec. 1997.

[28] J. Anderson, B. T. Doshi, S. Dravida, and P. Harshavardhana, "Fast restoration of ATM netowrks," IEEE Journal on Selected Areas in Communications, vol. 12, pp. 128-138. Jan. 1994.

[29] W. D. Grover and D. Stamatelakis. "Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration," in Proc. IEEE International Conference on Communications (ICC '98), (Atlanta, GA), pp. 537-543, June 1998.

[30] J. Zhang, K. Zhu, L. Sahasrabuddhe, S. J. B. Yoo, and B. Mukherjee, "On the study of routing and wavelength assignment approaches for survivable wavelength-routed WDM mesh networks," SPIE Optical Networks Magazine, in press, 2002.

[31] C. Xin, Y. Ye. S. Dixit, and C. Qiao, "An enhanced route assignment mechanism in optical control plane," in Proc. SPIE (Opticomm 2001: Denver, CO, Aug. 2001), vol. 4599, pp. 104-111, 2001.

[32] M. R. Garey and D. S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness. New York, NY: W. H. Freeman Company, 1979.

[33] D. E. Knuth, J. H. Morris, and V. R. Pratt, "Fast pattern matching in strings," SIAM Journal on Computing, vol. 6, no. 1, pp. 323-350, 1977.

[34] S. Dana, S. Sengupta, S. Biswas, and S. Datta, "Efficient channel reservation for backup paths in optical mesh networks," in Proc. IEEE Globecom '01, (San Antonio, TX), pp. 2104-2108, Nov. 2001.

[35] A. S. Arora and S. Subramaniam, "Converter placement in wavelength routing mesh topologies," in Proc. IEEE International Conference on Communications (ICC '00), (New Orleans, LA), pp. 1282-1288, June 2000.

[36] S. Subramaniam, M. Azizoglu, and A. K. Somani, "On optimal converter placement in wavelength-routed networks," IEEE/ACM Transactions on Networking, vol. 7, pp. 754766, Oct 1999.

[37] I. Chlamtac, V. Elek, A. Fumagalli, and C. Szabo, "Scalable WDM access network architecture based on photonic slot routing:' IEEE/ACM Transactions on Networking, vol. 7, pp. 1-9, Feb. 1999.

WDM МРЕЖИ С МАРШРУТИЗИРАНЕ НА ДЪЛЖИНА НА ВЪЛНАТА В ПРАКТИКАТА

Екатерина М. Христова, Даниел Р. Денев

WDM WAVELENGTH ROUTING NETWORKS IN PRACTICE

Ekaterina M. Hristova, Daniel R. Denev

ABSTRACT: *Creating light streams in wavelength-routed WDM networks requires the implementation of control and management protocols to perform routing and set wavelength functions, as well as to exchange signaling information and backup resources.*

KEYWORDS: *Multiplexing, Optical fiber, Packet switching, Signal-to-noise ratio, Wavelength, WDM.*

1. Протоколи

Предполага се, че сигналните съобщения са доставени в контролна мрежа с комутация на пакети. Тази контролна мрежа се реализира в извънлентов канал за наблюдение, който управлява самостоятелна дължина на вълната. Контролният слой има същата топология като физическата мрежа и всички пакети се маршрутизират по най-кратките пътища. Тъй като контролната мрежа е с комутация на пакети, методът за сигнализиране, консумира много контролирана честотна лента и включва по-дълго забавяне при установяване на връзка в сравнение с метода за поетапното сигнализиране. За запознаване отблизо с проблемите с маршрутизацията, методът за сигнализиране се променя в поетапна сигнализация. Освен това, в модифицираният подход на състояние на връзката, всеки възел изчислява сам своето следващо пренасочване въз основа на информацията за топологията. Пълният маршрут се определя в изходния възел. Следователно единствените разлики между сравняваните подходите са актуализирането на информацията и изпълнението на RWA. [1, 2, 3, 20, 26, 32]

Обобщени са двата подхода в процес на разглеждане:

- *Маршрутизиране:* И в двата подхода то се извършва с глобална информация. Въпреки това, в подхода със състоянието на връзката, всеки възел поддържа база данни за топологията на мрежата и състоянието на дължината на вълната; LSA се използва за актуализиране на топологията и информация за използване на дължина

на вълната. В подхода с разпределеното маршрутизиране протоколът вектор-разстояние се изпълнява, за да запази актуални маршрутизиращите таблици.

- *Определяне на дължина на вълната:* Използва се подход за First-Fit и в двата случая.
- *Процедури за сигнализиране:* Подобна процедура за сигнализиране се използва и за двата подхода. След като изходния възел определя маршрута или следващото пренасочване, той изпраща съобщение RESERVE до следващото мрежово устройство. Всеки междинен възел ще разгледа исканите ресурси. Ако ресурсите са налични, възелът ще ги резервира и ще изпрати съобщението RESERVE до следващото устройство; в противен случай възелът изпраща RESERVE-NACK обратно към източника. След като местоназначението получава съобщение RESERVE, то проверява дали има резервен приемник на желаната дължина на вълната. Ако възелът има такъв, той изпраща RESERVE-ACK обратно към предното устройство. В противен случай изпраща RESERVE-NACK. Комутаторите се конфигурират, когато възелът получи RESERVE-ACK. Той също отговаря за доставката на RESERVE-ACK към предходната спирка по маршрута. Ако даден възел получи RESERVE-NACK, той освобождава запазените ресурси. Когато източникът получи съобщението RESERVE-NACK, отново изпълнява RWA и опитва да установи връзката по друг маршрут и дължина на вълната. Ако такива не могат да бъдат намерени, връзката се блокира. Когато източник получава RESERVE-ACK, създаването на връзката е успешна и източникът може започне да изпраща данни през връзката. За да се предотврати твърде много повторни опити за заявка за връзка, се използва параметър M за контролиране на максималния брой опити. Връзката се блокира след $M^{\text{ти}}$ неуспешен опит.
- *Процедури за актуализиране:* И двата подхода използват постепенни актуализации. При подхода на състоянието на връзката всеки LSA съдържа информация за един канал на една връзка. При подхода на разпределено маршрутизиране всеки възел пази копие от таблицата за маршрутизиране на всеки съсед и всяко съобщение за актуализиране съдържа само наскоро променените записи в таблицата за маршрутизиране на изпращащия възел. [12, 21, 27, 28, 31]

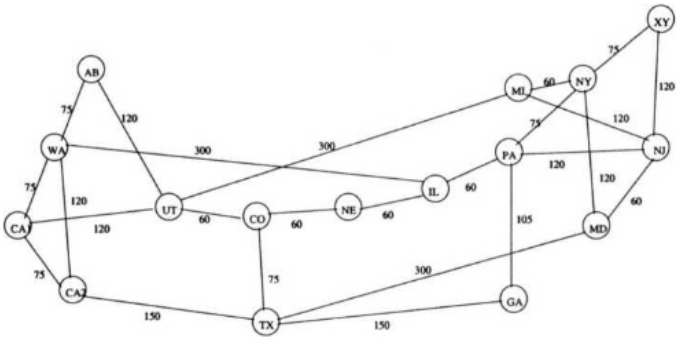
2. Сравнение

Сравнява се производителността на двата подхода чрез симулация в мрежата за цялата страна – NSFNET, показана на фиг. 1. NSFNET има 16 възела,

25 връзки, а дължините на връзките варират от 750 км до 3000 км. Всяка връзка е двупосочна оптична връзка и числото на връзките на Фиг. 3.1 представлява дължината на връзките в единици от 10 км. Трябва да се има предвид, че дължините на връзките са зададени само за симулационни цели и не отразяват реалните географски разстояния. [4, 11, 13, 14, 15, 22, 25]

Предполага се следното:

- Броят на дължините на вълните на всяка връзка, W, е 8.
- Трафикът се разпределя равномерно между всички двойки възли.
- Времето за задържане на връзката е експоненциално разпределено със среда 100 ms.
- Времето за обработка на съобщението във възел Pе 10 μs.
- Времето за конфигуриране, тестване и настройка на кръстосана връзка, C, е 500 μs.
- Времето за предаване или превключване на пакет в контролната мрежа R, е 0.
- Най-краткият път, получен при адаптивното маршрутизиране, се определя като пътят с минимален брой пренасочвания. При равномерен трафик и ниско натоварване, средното забавяне на разпространението между два възела е $D = 14.7\ ms$, а средното разстояние за пренасочване е $H = 2.28$. Сигналните съобщения се насочват по пътя с най-кратко забавяне на разпространението в контролната мрежа.
- Броят на приемо-предавателите на всяка дължина на вълната във всеки възел, TR, е параметър за симулацията. TR = 1, 2, 3.
- Не се извършва повторен опит, когато връзката е блокирана.



Фиг. 1. *NSFNET: национална мрежа*

За да се проучи поведението на мрежата при различни натоварвания, скоростта на пристигане на заявките за връзка се променя като параметър в симулацията. Натоварването се измерва в Ерланги, което може да се изчисли чрез умножаване на скоростта на пристигане на връзката със средното време за задържане на връзката. Следователно, натоварването се отнася до средния брой връзки, измерени във всеки момент от време в мрежата, ако няма блокиране.

3. Забавяне при установяване на връзка

Забавянето при установяване на връзка е времето, необходимо за установяване на връзка, след като пристигне заявката. Когато мрежата е много слабо натоварена (т.е. най-краткият път е достъпен за всички връзки) и няма повторни опити, тогава следните елементи допринасят за средните закъснения при настройване и на двата подхода за управление на връзката:

- 2 закъснения на разпространение от източника до възела на местоназначението, $2D$,
- $2H + 1$ закъснения при обработка на съобщения, $(2H + 1)P$
- време за конфигурация на комутатора, C.

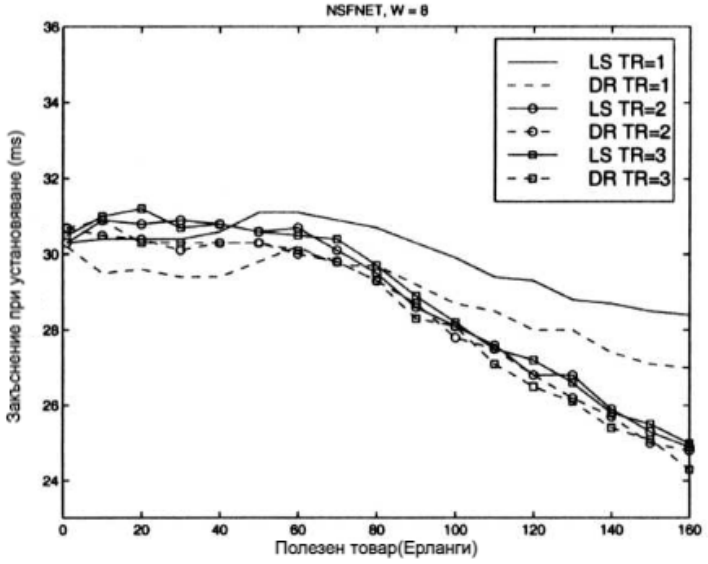
Следователно, времето за установяване на връзката при слабо натоварване е: $T_D = 2D + (2H + 1)P + C = 30.02\,ms$. Фиг. 2 показва закъсненията при настройка спрямо натоварването в NSFNET, с различен брой приемо-предаватели (TR). Наблюдава се, че при много ниско натоварване, закъсненията при настройка са доста близки до тази долна граница. С увеличаване на натоварването най-кратките пътища може да станат недостъпни и трябва да се изберат по-дълги пътища. Следователно забавянето при установяване на връзка може да се увеличи с увеличаване на натоварването. Степента на блокиране на опитите обаче също се увеличава, при увеличаване на натоварването. Връзка, която обхваща повече мрежови устройства, е по-вероятно да бъде блокирана от връзка, която обхваща по-малко такива устройства; по този начин, тъй като натоварването продължава да нараства, закъсненията при установяване на връзката ще намалеят. [6, 16, 17, 18, 24, 29]

Интересно е да се отбележи, че подходът на разпределено маршрутизиране дава по-ниски забавяния при установяване на връзката, отколкото подходът на състоянието на връзката. И двата подхода се опитват да намерят пътя с минимален брой пренасочвания. При подхода на състоянието на връзката, ако има множество пътища до местоназначението, единият се избира произволно. Въпреки това, при подхода на разпределено маршрутизиране, таблиците за маршрутизиране се обменят между съседни възли, като по този начин таблицата за маршрутизиране от път с по-кратко забавяне на

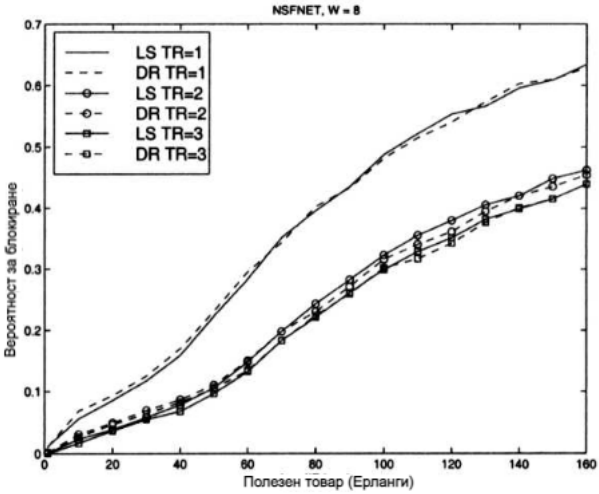
разпространение ще достигне първа до възел. Следователно сред пътищата на един и същ брой пренасочвания, пътят с най-кратко забавяне на разпространението ще бъде записан в таблицата за маршрутизиране. [5, 7]

4. Вероятност за блокиране

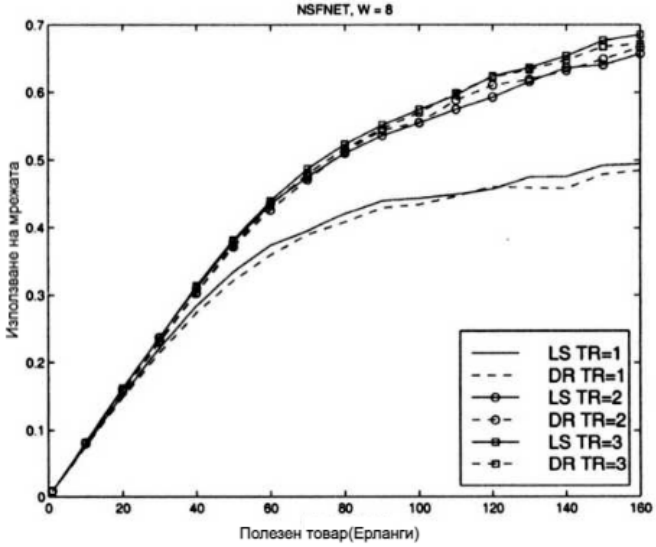
Вероятността за блокиране се отнася до вероятността връзката да не може да бъде създадена поради конкуренция за ресурси по желания маршрут. Фиг. 3 показва вероятностите за блокиране спрямо натоварването за двата подхода. Показано е, че блокирането в подхода на състоянието на връзката е малко по-ниско, отколкото при подхода на разпределено маршрутизиране при ниско натоварване, но малко по-високо при известно високо натоварване. Тези разлики се дължат на факта, че при ниско натоварване подходът за състояние на връзката има по-точна информация за маршрутизиране, която идва от по-кратки стабилизиращи закъснения (фиг. 4). При високо натоварване и двата подхода може да нямат актуална информация за маршрутизирането, но закъсненията при настройката при подхода за състояние на връзката са по-големи. Следователно, при високо натоварване в подхода на състоянието на връзката ресурсите се запазват за по-дълъг период от време. [11, 13, 15]



Фиг. 2. *Закъснение при установяване на връзка при полезен товар за NSFNET и 8 дължини на вълната*

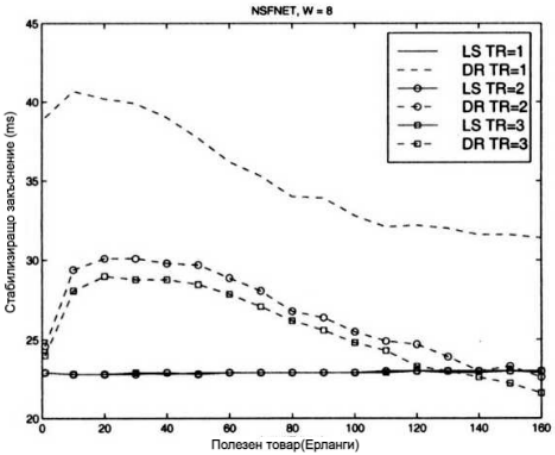


Фиг. 3. *Вероятност за блокиране на полезен товар за NSFNET и 8 дължини на вълната*



Фиг. 4. *Използване на мрежата на полезен товар за NSFNET и 8 дължини на вълната*

На фиг. 5 е графиката на използването на мрежата спрямо натоварването, получено чрез симулация. Когато всеки възел е само един приемо-предавател на всяка дължина на вълната (TR = 1), се наблюдава, че мрежата се насища при около 50% от натоварване от 160 Ерланга (където около 60% от връзките са блокирани). Когато са налични повече приемници (TR > 1), използването на мрежата е близо до 70% за натоварване от 160 Ерланга (където около 45% от връзките са блокирани). Тази производителност не е ограничение на подходите за маршрутизиране, а по-скоро ограничение на броя на приемо-предавателите във всеки възел (когато TR = 1), както и ограничението за непрекъснатост на дължината на вълната. [9, 10, 19, 23]



Фиг. 5. *Стабилизиращо закъснение на полезен товар за NSFNET и 8 дължини на вълната*

5. Време за стабилизация

Времето за стабилизиране е времето, необходимо на възлите да актуализират информацията за топологията след установяване или прекъсване на връзката. При подхода на състоянието на връзката времето за стабилизиране е равно на времето, необходимо на съобщението за актуализиране на възел (LSA) да бъде доставено до най-отдалечения възел, което се обозначава като T_i за възел i. T_i може да се изчисли по следния начин. За всеки възел i в мрежата и $j \neq i$, се намира най-краткия маршрут чрез минималното забавяне на разпространението от i до j. Означава се броя на мрежовите устройства по този маршрут с H'_{ij} и забавянето на разпространението с d_{ij}. Ако времето за предаване/превключване на LSA е R, тогава времето, необходимо на i достигане LSA на възела j е $H'_{ij} +$

$d_{ij} = d_{ij}$, тъй като $R = 0$. Намира се jза всеки възел i такъв, при който d_{ij} е максимално. Така:

$$T_i = \max_j d_{ij} \quad (1)$$

Средното време за стабилизиране в подхода за състояние на връзката тогава ще бъде

$$\frac{1}{N} \sum_i T_i = 23{,}2 \text{ ms} \quad (2)$$

за NSFNET, където Nе броят на възлите в мрежата. От симулацията се наблюдава, че средното стабилизиращо забавяне е в диапазона [22,8 ms, 23 ms] за NSFNET. Стабилизиращото забавяне за подхода с разпределено маршрутизиране се изучава само в симулация, тъй като забавянето в този случай е трудно за моделиране. Подходът на разпределено маршрутизиране има по-големи стабилизиращи закъснения от подхода на състоянието на връзката в повечето случаи. Това е така, защото при подхода на разпределено маршрутизиране обикновено са необходими няколко кръга обмен на информация, за да се стабилизира мрежата, особено в отговор на „лоши“ новини. [5, 7, 8, 30]

Разпределеното маршрутизиране има предимство при по-кратки закъснения при установяване на връзка и при високо натоварване, по-ниска вероятност за блокиране. Подходът за състояние на връзката също има предимство при инженеринга на трафика. Тъй като всеки възел поддържа глобална информация за мрежата, може да се приложи изрично маршрутизиране. Този атрибут може да добави повече толерантност към грешки в мрежата. Например, лесно и бързо е да се изчислят два несвързани маршрута в изходния възел. Той също така прави възможна споделена защита с познанията за пълна мрежова топология. [13, 30]

ЛИТЕРАТУРА

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

[2] 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.

[3] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath communications: An approach to high-bandwidth optical WAN's," IEEE Transactions on Communications, vol. 40, pp. 11711182, July 1992.

[4] 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.

[5] Цанков Ц. Съвременни методи за достъп до ресурсите в комтюпърни индустриални мрежи. 2022, Шумен, ISBN 978-619-201-618-0

[6] 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.

[7] A. Birman and A. Kershenbaum, "Routing and wavelength assignment methods in single-hop all-optical networks with blocking," in Proc. IEEE INFOCOM '95, vol. 2, (Boston, MA), pp. 431-438, Apr. 1995.

[8] S. Even, A. ltai, and A. Shamir, "On the complexity of timetable and multicommodity flow problems," SIAM Journal of Computing, vol. 5, pp. 691-703. 1976.

[9] J. Yates, J. Lacey, D. Everitt, and M. Summerfield, "Limited-range wavelength translation in all-optical networks," in Proc. IEEE INFOCOM '96, vol. 3, (San Francisco, CA), pp. 954-961, Mar. 1996.

[10] R. Ramaswami and G. H. Sasaki, "Multiwavelength optical networks with limited wavelength conversion," in Proc. IEEE INFOCOM '97, (Kobe, Japan), pp. 489-498, Apr. 1997.

[11] A. Copley, "Optical domain service interconnect (ODSI): Defining mechanisms for enabling on-demand high-speed capacity from the optical domain," IEEE Communications Magazine, vol. 38. pp. 168-174, Oct. 2000.

[12] A. Banerjee, J. Drake, J. Lang, B. Turner, K. Kompella, and Y. Rekhter, "Generalized multiprotocol label switching: An overview of routing and

[13] J. P. Jue and G. Xiao, "An adaptive routing algorithm with a distributed control scheme for wavelength-routed optical networks," in Ninth International Conference on Computer Communications and Networks, (Las Vegas, NV), Oct. 2000.

[14] Tsankov Ts., Staneva L., Vardeva I., Iliev D. Generalized net model of a communication network using the Port Knocking method. Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 29-34.

[15] X. Yuan, It Melhem, R. Gupta, Y. Mei, and C. Qiao, "Distributed control protocols for wavelength reservation and their performance evaluation," Photonis Network Commu¬nications, vol. 1, no. 3, pp. 207-218, 1999.

[16] Gerstel and R. Ramaswami, "Optical layer survivability: a services perspective," IEEE Communications Magazine, vol. 38, pp. 104-113, Mar. 2000.

[17] A. Fumagalli, I. Cerutti, F. Masetti, R. lagannathan, and S. Alagar, "Survivable networks based on optimal routing and WDM self-healing rings," in Proc. IEEE INFOCOM '99, vol. 2, (New York, NY), pp. 726-733, Mar. 1999.

[18] S. Ramamurthy, L. H. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks;' IEEE/OSA Journal of Lightwave Technology, in press. 2002.

[19] M. Clouqueur and W. D. Grover, "Mesh-resotratble networks with complete dual failure resotratbility and with selectively enhanced dual-failure restorability properties," in Proc. SPIE (Opticomm 2002: Boston, MA, Aug. 2002), vol. 4874, pp. 1-12, 2002.

[20] W. He, M. Sridharan, and A. K. Somani, "Capacity optimization for surviving double-link failures in mesh-restorable optical networks," in Proc. SPIE (Opticomm 2002: Boston, MA, Aug. 2002), vol. 4874, pp. 13-24, 2002.

[21] Цанков Ц., Ненков Н. Възможностите на отдалечени клиенти в архитектурата клиент-сървър. Сборник статии от XII международна научна конференция „Инновации в технологиях и образовании“, филиал на КузГТУ в г. Белово, 2019, ISBN 978-5-00137-063-5, с. 342-346.

[22] C.-F. Su and X. Su, "Protection path routing on WDM networks," in Proc. Optical Fiber Communication Conference and Exhibit (0F("01), vol. 2, (Anaheim, CA), p. Tu02, Mar. survivable WDM networks?' J. High Speed Networks, vol. 10, no. 2, pp. 109-125, 2001.

[23] G. Ellinas, E. Bouillet, R. Ramamurthy, J. Labourdette, S. Chaudhuri, and K. Bala, "Routing and restoration architectures in mesh optical networks," SPIE Optical Networks Magazine, in press, 2002.

[24] P.-H. Ho and H. T. Mouftah, "A novel routing protocol for WDM mesh networks," in Proc. Optical Fiber

[25] Communication Conference and Exhibit (OFC"02), (Anaheim, CA), p. TuG4, Mar. 2002.

[26] D. Dunn, W. Grover, and M. MacGregor, "Comparison of k-shortest paths and maximum flow routing for network facility restoration," IEEE Journal on Selected Areas in Communications, vol. 12, pp. 88-99, Jan. 1994.

[27] M. Azizoglu, S. Subramaniam, and A. K. Somani, "Converter placement on wavelength- routed network paths," in Proc. SPIE'97, vol. 3230, pp. 265-276, Nov. 1997.

[28] D. Papadimitriou. F. Poppe, and et al., "Inference of shared risk link groups." IETF Draft, Nov. 2001.

[29] I. Chlamtac, A. Fumagalli, and G. Wedzinga, "Slot routing as a solution for optically transparent scalable WDM wide area networks," Photonic Network Communications, vol. 1, pp. 9-21, June 1999.

[30] Iliev M., Bedzheva M., Boyanov P., Bedzhev B., Tsankov Ts. Requirements to the Personal Work Stations in the University’s Computer Laboratories. 29-th Annual Conference of the European Association for Education in Electrical and Information Engineering – EAEEIE 2019, Ruse, ISBN 978-1-7281-3222-8.

[31] D. Hunter, M. Chia, and I. Andonovic, "Buffering in optical packet switches," IEEE/OSA Journal of Lightwave Technology, vol. 16, pp. 2081-2094, Dec. 1998.

[32] D. Bertsekas and R. Gallager, Data Networks. New Jersey: Prentice Hall, 2 ed., 1992.

МЕТОДИ ЗА УПРАВЛЕНИЕ НА ПРОЕКТИ

Добринка П. Добрева

METHODS FOR PROJECT MANAGEMENT

Dobrinka P. Dobreva

ABSTRACT: *A good knowledge of the processes, tools and techniques of different methodologies is a factor for effective project management. In this regard, the purpose of the report is to review existing project management methods.*

KEYWORDS: *Project management, Standard, Methods.*

Въведение

Проектът е временна организационна структура, която може да създаде уникален продукт или услуга в рамките на определени ограничения като време, цена и качество. Проектите са различни от нормалната ежедневна работа и изискват специална временна организационна структура, за да: дефинират обхвата на проекта и резултатите, създадат бизнес обосновка за инвестицията, идентифицират заинтересованите страни по проекта и да определят основен екип на проекта, създадат плановете на проекта, наблюдение и контрол на проекта (напредък, промени, рискове, проблеми, качество и т.н.) и предаване на резултатите и административно приключване на проекта [3].

Целта на всеки проект е да представи нов продукт или услуга или да промени съществуващ. Постигане на целта се очаква да донесе ползи на организацията. Проектът може да се разглежда и като процес на трансформация, превръщащ идеите в реалност.

Управлението на проекта е задължително да се извършва на етапи в определена последователност, за да се подобри контрола и качеството. В края на всяка фаза се прави преглед на резултатите и работата на екипа по проекта. По този начин се установява дали проектът преминава към следващата фаза, подлежи ли на преразглеждане и се анализира как да се подобри работата на всички участници [4].

Проектите не съществуват изолирано, те се влияят от два съществени фактора, вътрешната и външната среда. Един проект зависи от три основни компонента: процеси, хора и инструменти, всички интегрирани и повлияни от вътрешната среда (организацията) и външната среда (света), което се приема за екосистемата на проекта. Успехът на управлението на проекта зависи от баланса на трите компонента. Когато един от компонентите не се познава или управлява ефективно, цялата система ще загуби.

Следователно доброто познаване на процесите, инструментите и техниките на различните методологии е фактор за ефективното управление на проекти. В тази връзка, целта на доклада е да се разгледат съществуващите методи за управление на проекти.

Изложение

Управлението на проекти може да се опише като дейности по планиране, организиране, осигуряване, наблюдение и управление на необходимите ресурси и работа за постигане на конкретни цели и задачи на проекта по ефективен и ефикасен начин.

Жизненият цикъл на управление на проекти е процедура, която прави проектите успешни. Освен това, този цикъл позволява на ръководителите да планират внимателно всяка задача и дейност, за да увеличат максимално перспективите за успех. Проектът обикновено е внимателно обмислена дейност, която следва жизнен цикъл с ясно изразено начало и край [5].

Има различни методи за управление на проекти. Представените по-долу методи не са изчерпателни. Всеки метод подхожда по различен начин към проекта.

1. *Гъвкаво управление на проекти*

Това е един от най-ранните стилове на методи за управление на проекти. Използва се стратегията „стъпка по стъпка“, която предоставя предимства по пътя, за да се постигнат резултати.

2. *Водопадно управление на проекти*

Проектът се основава на цикъла на Деминг и поставя акцент върху поетапността, контрола и вземането на решение за времето, парите и качеството. Този вид проекти се организират предварително и се изпълняват директно, като се очаква, че нищо няма да се промени [3, 5].

3. *Канбан управление на проекти*

Метода насърчава по-малко промени в проекта. Използва се за визуализиране на цялостния работен процес на проекта. Той следи напредъка на проектните задания във времето и идентифицира проблеми, като предоставя обратна връзка за постигане на най-значимите резултати [3, 5].

4. *Scrum управление на проекти*

Scrum Техниката е друга форма на стратегия за управление на проекти. Основата на тази система позволява на екипите да си сътрудничат, като се събират и обсъждат възникнали въпроси. Този подход използва бърза разработка и тестване, за да предостави резултати възможно най-скоро, като същевременно избягва грешки [3, 5].

5. *Six Sigma управление на проекти*

Този подход набляга на повишаване на стандарта за завършване на проекта. Екипа категоризира всички проблеми, преди да бъдат коригирани, докато проектът напредва. Подхода се стреми към значителни финансови печалби и набляга на използването на анализ на данни за повишаване на удовлетвореността на клиентите [3, 5].

Фиг. 1. *Six Sigma управление на проекти*

Фиг. 2. *Lean Project Management*

6. *Lean Project Management*

Клиента е основният фокус на този подход. Подхода има за цел да произведе резултати възможно най-бързо като завърши проекта, без да срещне никакви проблеми. Подходът набляга на използването на минимални ресурси (труд, оборудване и консумативи).

7. *Prince2 управление на проекти*

Фиг. 3. *Prince2 управление на проекти*

Метода е създаден през 1989 г. от Британската централна компютърна и телекомуникационна агенция (ССТА) и е подходящ за всички видове проекти. Методът се основава на практически опит с различни методи за управление на проекти и практически примери. Prince2 има ясни взаимоотношения с управлението на програмата и стандарта за качество ISO 9001. Метода се фокусира върху постигането на ефективни резултати, като същевременно минимизира всякакви опасности. Методологията Prince2 разделя проекта на отделни задачи. Може да изпълнява задачи една по една, което спомага за по-прецизното изпълнение на задачите без никакви грешки [3, 5].

8. Body Of Knowledge (BOK)

Професионалните организации в Холандия и в други европейски страни обединяват знанията си по управление на проекти в така нареченото „Body Of Knowledge“ (BOK). Тези „знания“ могат да се използват за образование и обучение, за тестване на знанията на ръководителите на проекти и за сертифициране на ръководители на проекти [1].

9. Метод на критичната верига

Метода е разработен от д-р Е. Голдрат и наречен „Управление на критични вериги на проекти и управление на буфери“. Учения отбеляза, че в почти всеки метод за управление на проекти на ниво задача е вграден допълнителен запас за безопасност, за да се предпази от всякакви проблеми несигурности. И тъй като практиката показва, че всеки служител на проекта винаги изразходва времето, което му е отредено (законът на Паркинсон), всеки проект в крайна сметка се сблъсква с проблеми. Особено ако се сбъдне и законът на Мърфи: „Всичко, което може да се обърка, ще се обърка и то в най-неблагоприятния момент в най-катастрофалната форма“ [1, 2].

Метода на критичната верига показва най-бързото време, в което можем да завършим проект, като се вземат предвид както зависимостите от задачите, така и наличието на правилните ресурси. Метода се фокусира върху проекта като цяло, а не върху отделни задачи. „Буферите на задачите“ се обединяват като създават „буфер на проекта“ в края на проекта. По този начин общият запас на безопасност остава видим за ръководителя на проекта и клиента. Наблюдението на буфера на проекта е удобен начин за непрекъснато наблюдение на състоянието на проекта.

Метода може да се разглежда като допълнение към други методи за управление на проекти.

Заключение

Проектите са съставени от свързан набор от дейности, предприети за създаване на уникален продукт или услуга в рамките на определени изисквания. Този специфичен характер на проектите улеснява изолацията от средата, като ръководителите могат да се фокусирате единствено върху изпълнението на дейностите.

Проектите за развитие трябва да работят в по-широка среда и ръководителите на проекти трябва да разглеждат проектите в този по-широк контекст. За да бъдат ефективни при управлението на сложни ситуации, ръководителите трябва да имат цялостен поглед върху проекта и да разбират

взаимодействието му със средата. Като приемат този холистичен поглед върху проектите, ръководителите са по-добре подготвени да разберат външните фактори, които ще повлияят на развитието на проекта.

Управлението на проекти използва системен анализ като подход за решаване на проблеми, той изисква определяне на обхвата на проекта, разделянето му на съставни части и идентифициране и оценка на неговите проблеми, възможности, ограничения и нужди. Анализа разглежда възможните решения за подобряване на текущата ситуация, идентифицира оптимално решение и план за действие и непрекъснато проверява плана срещу всякакви промени в околната среда.

Традиционните методи за анализ включват линейни причинно-следствени връзки. Възприемайки системен подход, проектите могат да видят целия комплекс от двупосочни взаимовръзки. Вместо да се анализира даден проблем по отношение на вход и изход, ръководителите разглеждат цялата система-входове, процеси, изходи, обратна връзка и контроли. Тази по-голяма картина осигурява по-полезни резултати от традиционните методи и позволява на проекта да вижда промяната като непрекъснат процес.

В литературата има разнопосочни мнения относно използването на методите за управление на проекти. Някои автори считат, че тези методи обогатяват арсенала от инструменти на ръководителя на проекта, а други, че методите са склонни да създават бюрократични проблеми, което е в противоречие с целта на управлението на проекти.

Поради това, ръководителите трябва добре да познават методите за управление на проекти и да търсят баланс между теорията и практиката.

ЛИТЕРАТУРА

[1] Методи за Управление на проекти, https://bg.itpedia.nl/2011/10/11/projectmanagementmethoden-op-een-rij/.

[2] Ръководство за начинаещи за управление на проекти. 2019, https://www.microsoft.com/bg-bg/microsoft-365/business-insights-ideas/resources/guide-for-project-management.

[3] PM² Project Management Methodology. Guide, European Commission, Brussels/Luxembourg, 2016.

[4] https://fairbulgaria.com/%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BD%D0%B0-%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B8-%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5/

[5] https://www.mindonmap.com/bg/blog/what-is-project-management/.

ИНСТРУМЕНТИ И ТЕХНИКИ ЗА УПРАВЛЕНИЕ НА ПРОЕКТИ

Добринка П. Добрева

PROJECT MANAGEMENT TOOLS AND TECHNIQUES

Dobrinka P. Dobreva

ABSTRACT: *Effective project management requires a good knowledge of the processes, tools and techniques of different methodologies. In this way, managers and teams can make decisions about project needs and trade-offs between project dimensions such as time, cost, scope, and quality to achieve set goals.*

KEYWORDS: *Project management, Life cycle, Phases, Tools, Techniques.*

Въведение

Успехът на управлението на проекти зависи от баланса на трите компонента: процеси, хора и инструменти. Те са интегрирани и повлияни от вътрешната и външната среда на организацията.

Процесите определят работата, която трябва да бъде извършена, което от своя страна води до изискванията за умения на хората.

Хората, отговарящи за управлението на проекта следват процесите и процедурите, за да гарантират качеството на услугите, предоставяни от организацията. Компонентът на хората се влияе от възнаграждението и ценностите на организацията и от външния пазар на труда, който поставя условия за намиране на квалифициран персонал.

Инструментите, техниките и устройствата се избират от организациите с цел да улеснят управлението на проекта, да постигнат целите му и да улеснят договорните му задължения. Сред инструментите са техники за контрол на бюджетите, проследяване на напредъка на проекта и оценка на изпълнението. Инструментите включват наличната технология за управление на информацията, генерирана от проекта, и подобряване на неговия анализ, за да позволи на проекта да взема правилните решения.

Идеалният инструмент за управление на проекти спомага компанията да спечели предимство чрез възможността да се ориентира във вътрешната организация и да реагира бързо на промените в бизнес обстановката. Приемането на такъв инструмент е от полза на всички заинтересовани страни.

В тази връзка, в доклада ще бъдат разгледани някои от използваните инструменти и техники за управление на проекти, полезни за справяне с различни предизвикателства при управлението на проекти.

Изложение

Проектите работят като част от система и включват висока степен на несигурност. Чрез използване на холистичен подход ръководителите могат да интегрират всички вътрешни и външни проблеми в своето планиране. Това им помага да виждат проектите като поредица от взаимно свързани фази, което осигурява успех на проекта.

Добра практика е проектите да се разделят на няколко фази (т.н. жизнен цикъл на проекта). Тези фази варират от една индустрия в друга, но като цяло те включват фаза на иницииране, планиране, внедряване, мониторинг и затваряне. Проектът трябва да завърши успешно всяка фаза, преди да премине към следващата, този подход към проектния цикъл осигурява по-добър контрол на управлението и изгражда подходящите връзки с общата среда [4].

Институтът за управление на проекти (PMI) е най-голямата световна асоциация за застъпничество за управление на проекти и програми. Института създава насоки и изисквания за работа на жизнения цикъл на проекта. Използването на предписаните PMI принципи за управление намалява риска и въздействието на скъпи пропуски, промени и грешки в проекта.

Всеки проект има разпознаваеми начални и крайни точки, които могат да бъдат свързани с времева скала. Жизненият цикъл на проекта включва всички дейности по проекта от началната точка до окончателното завършване на проекта.

Фиг. 1. *Жизнен цикъл на проекта [3]*

Жизненият цикъл на проекта има четири фази. Всяка фаза представлява период от време, през който се изпълняват определени дейности. В началото проектите се фокусират върху дейности по иницииране и планиране, по средата върху дейности по изпълнение, мониторинг и контрол, а в края върху дейности по приемане, преход и затваряне.

Общите етапи и фази при управление на проекти са [2, 3, 5]:

1. Фаза иницииране. Управлението на проекта започва, когато екипът или мениджърът инициира проект. През този етап се дефинират желаните резултати, формулира се целта, създава се бизнес казус, определя се обхвата на проекта и се дава начало на проекта.

2. Фаза планиране. През този етап се разработва обхвата на проекта и се определя подходящия подход за изпълнение, определя се график за различните включени задачи и оценка на необходимите ресурси, разработват се детайлите на плановете на проект и се планира работата.

3. Фазата на изпълнение. През този етап се извършват дейности по осигуряване на качеството, за да се гарантира че проектът се придържа към договорените стандарти за качество. Координира се работата по проекта, координират се хората и ресурсите, разрешават се конфликти и проблеми. През периода се изготвят и предават резултатите от проекта в съответствие с плановете на проекта.

4. Заключителната фаза. През етапа се координира официалното приемане на проекта, докладва се за цялостното му изпълнение, публикуват се препоръки за проекта и се извършва административно затваряне на проекта.

През по-голямата част от жизненият цикъл се извършва монииторинг и контрол на цялостната дейност и управлението на проекта. Мониторингът е за измерване на текущите дейности по проекта (къде се намираме във връзка с плана) и мониторинг на променливите на проекта (разходи, време, усилия) спрямо плановете на проекта. Контролирането е свързано с идентифициране коригиращи действия за справяне с отклонения от плановете и правилно справяне с проблеми и рискове.

При управлението на проекти се използват следните инструменти и техники [2]:

1. Анализ на PESTEL

Анализът се използва, за да се разбере как околната среда може да повлияе на проект или цел. PESTEL означава: политически, икономически, социални, технологични, екологични и правни фактори. Анализът на PESTEL помага да се идентифицират външните фактори, които влияят върху организацията и биха могли да окажат влияние върху целите, планирането или изпълнението на проекти.

Този тип анализ е важен в контекста на бизнес обосновката и управлението на риска и ще подхрани процеса на проектиране на достатъчно изчерпателен план, за да идентифицира и да се справи с потенциални рискови сценарии (заплахи/възможности), произтичащи извън организацията или проекта.

2. Анализът „Произвеждане или купуване“

Анализът помага на организацията да вземе нформирано решение за това какво да възложи и какво да не възложи. Ръководителите често са изправени пред дилемата да направят или да купят, имайки предвид наличността и уменията на наличните ресурси. Факторите, които трябва да бъдат взети под внимание при анализа на марката или покупката, включват сравнение на разходите, технология и бизнес процеси, информация, свързана с доставчика, и системи за поддръжка. Решаващо значение за вземане на решение включват ефективност на разходите, проблеми с интелектуалната собственост, проблеми с контрола на качеството или проблеми с ненадеждността на доставчика. Потенциалните причини за решение

за покупка включват съображения за разходите, липса на технически опит, технически опит на доставчиците и/или недостатъчни вътрешни ресурси.

3. Матрица на интерес/влияние на заинтересованите страни (SIIM)

Тази техника се използва за улесняване и документиране на анализа на интереса и влиянието на всяка заинтересована страна в проекта. Важно е да се познават заинтересованите страни и тяхното значение за проекта, за да се запази поверителността на информацията.

Интересът показва нивото на интерес на заинтересованата страна към проекта. Той се измерва като степента на ентусиазъм, показан от заинтересованата страна в подкрепа на проекта. Заинтересованите страни могат да бъдат положителни, неутрални или отрицателни към проекта.

Влиянието показва властта, която заинтересованата страна има върху планирането и изпълнението на дейностите. Колкото по-голяма е властта за вземане на решения на дадена страна, толкова по-голямо е влиянието ѝ. Най-често хората, които могат да вземат решения относно финансирането на проекта и/или ресурсите, имат голямо влияние.

4. Матрица на риска (вероятност/въздействие)

Матрицата за оценка на риска съчетава оценките на вероятността и въздействието на всяка заплаха. В резултат на това рисковете на проекта са идентифицирани.

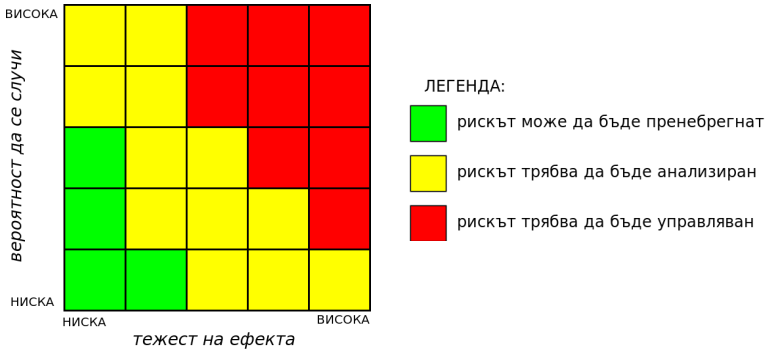
Матрицата служи за определяне допустимото ниво на риск. Тя може да се използва и за да се даде приоритет на определени ресурси, заплахи или ответни действия. Вертикалната ос от лявата страна на матрицата за оценка на риска (таблица 1) показва сериозността на събитието. Това са степените на риска (римски цифри I до IV) или нивата на въздействие. Хоризонталната ос в горната част на матрицата показва вероятностните нива (с главни букви „A“ до „E“). Точката, където тежестта на реда и вероятността на колоната се пресичат, определя нивото на риска [1].

Таблица 1. *Матрица за оценка на риска*

Случайни събития		**Вероятност**				
Тегло/ Въздействия	Степен	Често A	Възможно B	Случайно C	Рядко D	Невъзможно E
Катастрофално	I	**ЕН**	**ЕН**	**Н**	**Н**	**М**
Критическо	II	**ЕН**	**Н**	**Н**	**М**	**L**
Ниско	III	**Н**	**М**	**М**	**L**	**L**
Пренебрежимо	IV	**М**	**L**	**L**	**L**	**L**

ЕН – изключително висок риск (Extremely High Risk)
Н – висок риск (High Risk)
М – умерен риск (Moderate Risk)
L – нисък риск (Low Risk)

Нивото на риска е определено въз основа на вероятност и въздействие, като рисковете най-често се степенуват на „висок“, „среден“ и „нисък“ (фиг 2), но могат да имат и 4 или 5 степени, за да се определи тяхното значение и приоритетност.



Фиг. 2. *Матрица на риска*

Колкото по-високо е нивото на риска, толкова по-голяма е необходимостта от разработване на план за реагиране на риска. Матрицата е проектирана като инструмент за допълване на регистъра на риска.

Въз основа на склонността към риск на организацията могат да бъдат разработени адекватни стратегии за реагиране на риска за всеки идентифициран риск.

5. Структура на разпределението на работата (WBS)

WBS е йерархично разделение на проекта на по-малки работни компоненти, които могат да се използват за възлагане на работа или за оценка на усилията и разходите. Добре направеният WBS трябва да бъде лесен за разбиране, да бъде пълен и трябва да улеснява наблюдението на напредъка по време на изпълнение. Най-често използваните техники за декомпозиция на WBS включват разделяне на проекта по фази или етапи, по резултати или резултати, по работни пакети или въз основа на организацията, нейните отдели и бизнес звена.

6. Структура на разбивката на резултатите (DBS)

Структурата на разбивката на резултатите е съществена част от продуктово базираното планиране. Може да се използва за идентифициране и документиране на резултатите от даден проект и техните взаимозависимости. Това води до йерархично дърво на резултати и поддоставки (физически, функционални или концептуални), които съставляват целия проект. По този начин се помага на екипа на проекта да идентифицира пълния набор от резултати, които съставляват проекта.

DBS е подобен на WBS, но се използва на различна стъпка в процеса на планиране. PBS може да предшества WBS и идентифицира желаните резултати,

които след това се използват при създаването на WBS (идентификация на задачите и дейностите, необходими за доставянето на тези резултати).

Може да се каже, че DBS определя какво ще произведе проектът, а WBS определя каква работа трябва да бъде извършена, за да бъдат произведени.

7. Оценки на усилията и разходите

Техниката за оценка на усилията и разходите произлиза от WBS, като всеки работен елемент (задача) се оценява по отношение на усилия и разходи. Усилието обикновено се измерва в човекодни или човек месеца. Тази работа се извършва в тясно сътрудничество със собствениците на задачите или други експерти в рамките на основния екип на проекта, за да се осигурят по-прецизни оценки и участие от страна на членовете на екипа, отговарящи за изпълнението на работата.

Висококачествената структура на разпределението на работата формира основата за висококачествени оценки.

8. Триточкови оценки с помощта на PERT

Триточковата оценка е част от набора от инструменти PERT (техника за оценка и преглед на проекти) и обикновено се използва във връзка с мрежови диаграми, за да предостави средно претеглена стойност на продължителността на дейността или разходите. Очакваната продължителност/цена и стандартното отклонение на продължителността или цената на проекта се изчисляват въз основа на три точки от данни, а именно оптимистична оценка на продължителността или разходите, най-вероятна оценка и песимистична оценка.

След това тези оценки се претеглят, за да се осигури средно претеглена стойност на усилията, разходите или продължителността. В допълнение, тези оценки могат да се използват за изчисляване на стандартно отклонение, използвано за оценка на нивата на достоверност на претеглената средна стойност за дейност, както и за изграждане на прости статистически модели на времето и цената на задачата. Този метод може да се приложи за прогнозиране и намаляване на риска и за присвояване на буфери/непредвидени обстоятелства на задачи.

Привличането на експерти повишава точността на триточковите оценки и намалява степента на несигурност на проекта.

9. Планиране на проекта

Графикът на проекта има за цел да идентифицира зависимостите между задачите, да присвои ресурси за всяка задача, да идентифицира началните и крайните дати на задачите и да определи общата продължителност на проекта.

Графикът може да се направи предварително за целия проект или за части от него, като отделни етапи или повторения. Могат да се използват различни методи и представяния за планиране: списък с дати/крайни срокове, план за крайъгълен камък, лентови диаграми, мрежови диаграми и свързани лентови диаграми (диаграми на Гант), като всички те могат да се виждат взаимно допълващи се.

Веднъж одобрен, графикът на проекта е базов – всяка следваща промяна в графика трябва да следва процеса на управление на промените и съответните управленски договорености.

10. Изравняване на ресурсите

Изравняването на ресурсите е техника, използвана за анализиране на небалансираното използване на ресурсите на проекта и за разрешаване на конфликти, свързани с разпределението на ресурсите (човешки, материални, технически и др.).

Изравняването на ресурсите се фокусира върху ефективно/оптимално разпределение на ресурсите, за да може проектът да бъде завършен в рамките на определения график. Ръководителите на проекти анализират зависимостите между проекти или дейности, за да гарантират, че дейностите могат да бъдат изпълнени своевременно. Като се вземат предвид идентифицираните ограничения, може да се извърши изравняване на ресурсите. Изравняването на ресурсите може например да изисква забавяне на конкретни задачи, докато ресурсите са налични.

Някои IT инструменти (Microsoft Project), предоставят функционалност за автоматично изравняване на ресурсите, като правят едно от трите ограничения на проекта (цена, обхват или време) променливо.

11. Диаграми на Гант

Диаграмата на Гант е често срещана техника за управление на проекти, използвана за представяне на графика, фазите и дейностите на даден проект в едно изображение. Той се фокусира върху последователността на проекта, продължителността, зависимостите и състоянието по начин, който е лесен за разбиране.

Диаграмата на Гант представлява реда, в който дейностите трябва да бъдат извършени, и предоставя общ преглед на напредъка, който е постигнат във всеки един момент. Диаграмата се използва за съобщаване на график на проекта по визуален начин, но и за показване на напредъка и текущото състояние на графика чрез добавяне на засенчвания на процент завършеност и вертикална линия „днес“. Основната сила на тази техника е способността ясно да показва състоянието на всяка дейност с един поглед.

12. Метод на критичния път (CPM)

Методът на критичния път е техника за моделиране, която използва математически базиран алгоритъм за изчисляване на общата продължителност на даден проект. CPM изчислява най-дългия необходим път (най-дългата продължителност) на планираните дейности от началото до края на проекта, известен още като критичен път на проекта. Тази техника помага да се разбере кои дейности имат критично влияние върху общата продължителност на проекта. На тази база дейностите могат да бъдат приоритизирани, за да се съкрати продължителността на критичния път.

13. Метод на критичната верига (CCM)

Методът на критичната верига е техника за моделиране, използвана за планиране и планиране на набор от дейности или проекти. Подобен е на метода CPM, но взема предвид ресурсите и тяхното изравняване, както и поведението на ръководителя на проекта, когато се оценява продължителността на дейностите в даден проект.

Техниката се основава на наблюдението, че оценките на времето за дейности за проекти са двойно повече от времето, необходимо за завършване на дейностите. Причините, които водят до забавяне, могат да включват неизползване на ранното приключване на дадена дейност, темп на членовете на екипа, за да запълнят наличното време за изпълнение на задача, изчакване до последния момент, за да се съсредоточи наистина върху задачата, и др.

CCM приема, че оценките на ръководителя на проекта за продължителността на дейностите са подплатени и незабавно пристъпва към намаляването им. След това се добавят допълнителни буфери, за да се отчете намаляването на проектните оценки.

14. Управление на спечелената стойност (EVM)

Управлението на спечелената стойност е техника, използвана за наблюдение и контрол на изпълнението на проекти, предоставяйки обективен поглед върху изпълнението въз основа на финансовите данни на проекта. Разходите и стойността се измерват в разходни единици. EVM предоставя относително обективни показатели за проактивно управление на ефективността на проекта. Някои индикатори отразяват постигнатия напредък или отклонения от плана от гледна точка на разходите или стойността на работата, докато други индикаторите се фокусират върху прогнозирането на общото бюджетно отклонение или върху производителността, необходима за завършване на проекта по график.

15. Анализ на Парето

Анализът на Парето е официална техника за идентифициране на проблемите, които причиняват повечето проблеми в даден проект. Принципът на Парето гласи, че обикновено 80% от ефектите идват от 20% от причините.

Като се съсредоточава върху тези основни проблеми (20%), анализът на Парето може да бъде полезен за управление на риска или качеството, тъй като помага да се съсредоточи върху онези рискове или проблеми с качеството с най-голямо въздействие върху даден проект. По този начин методът улеснява приоритизирането на необходимото смекчаване или непредвидени действия.

16. Поуки

Целта на официалните извлечени поуки и препоръките след проекта е да се даде възможност на екипите по проекта и постоянната организация като цяло да се възползват от опита, придобит по време на проекта. Също така е важно да се съберат идеи и препоръки за работа след проекта, свързана с работата на доставения продукт/услуга, като разширения, поддръжка, идеи за последващи проекти и др.

Заключение

За ефективното управление на проекти е необходимо доброто познаване на процесите, инструментите и техниките на различните методологии. По този начин ръководителите и екипите могат да вземат решения относно нуждите на проекта и компромисите между измеренията на проекта като време, цена, обхват и качество, за постигане на поставените цели. Като критичен фактор за успеха

може да се посочи ефективното управление на изискванията, тъй като те са отправната точка за цялата работа по проекта и влияят върху риска, продължителността и бюджета на проекта.

Тъй като всеки проект е уникален, за да се гарантира, че методологията ефективно обслужва нуждите на проекта, е необходимо известно ниво на приспособяване и/или персонализиране. Приспособяването се прави с цел адаптиране на методологията към специфичните нужди на проекта, като същевременно се вземат предвид организационните процеси, политики и култура. Приспособяването има повече смисъл на ниво организация, но незначително приспособяване може да се извърши и на ниво проект.

ЛИТЕРАТУРА

[1] Диманова Д. Управление на риска. УИ „Епископ Константин Преславски“, Шумен, 2016, ISBN 978-619-201-095-9.

[2] PM² Project Management Methodology. Guide, European Commission, Brussels/Luxembourg, 2016.

[3] PMI Project Management Principles, pmiprojectmanagementprinciples20141006-141006181426-conversion-gate01.pdf.

[4] Project management for development organizations. 2015, www.pm4dev.com.

[5] https://www.mindonmap.com/bg/blog/what-is-project-management/

НАЗЕМНО ЛАЗЕРНО СКАНИРАНЕ – ТЕХНИЧЕСКИ СРЕДСТВА И СФЕРИ НА ПРИЛОЖЕНИЕ

Найлян М. Салиева

TERRESTRIAL LASER SCANNING – TECHNICAL MEANS AND AREAS OF APPLICATION

Naylyan M. Salieva

ABSTRACT: *Terrestrial laser scanning is a relatively new technology for precise remote studies of objects from the earth's surface and has been successfully applied in various fields. In this method, information about distant objects is obtained and processed using active and optical systems using the reflection and scattering of light in transparent and semi-transparent media. In the present work, the technical means and areas of application of terrestrial laser scanning are considered.*

KEYWORDS: *Terrestrial laser scanning, Areas of application, Technical means.*

1. Въведение

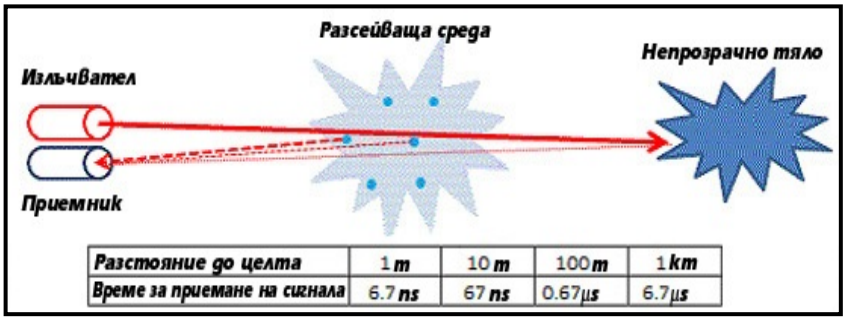
Наземното лазерно сканиране представлява сравнително нова технология за прецизни дистанционни изследвания на обекти от земната повърхност и се прилага с успех в различни области. При този метод се получава и обработва информация за отдалечени обекти с помощта на активни и оптически системи, използващи отражението на светлината и нейното разсейване в прозрачни и полупрозрачни среди. В настоящата разработка се разглеждат техническите средства и сферите на приложение на наземното лазерно сканиране.

2. Изложение

Геодезията е наука за събиране, обработка и представяне на информация за формата, размерите и гравитационното поле на Земята и за формата, размерите и положението на отделните участъци от земната повърхност, както и разположените върху тях обекти. Особено значение в съвременното ѝ развитие и приложение придобива наземното лазерно сканиране, при което се извършва 3D заснимане на земната повърхност, изследване на опасни геодинамични процеси и ефектите от тях, снимане и документиране на инженерни, архитектурни обекти и паметници на културата, за проектиране и изследването им и други.

2.1. Същност на наземното лазерно сканиране.

Наземното лазерно сканиране е един съвременен начин за бързо и точно определяне на 3D координатите на точки от околното пространство чрез извършване на геодезически измервания, като се използва лазерна светлина и нормален растер без контакт с обекта от земната станция. При този метод данните за обектите се набират бързо и подробно. Принципът на работата на наземните лазерни скенери се основава на отразяването на лазерен лъч от повърхността на сканирания обект и връщането му обратно към скенера, който се регистрира от специален сензор (фиг. 1) [1].



Фиг. 1. *Схема на технологията лазерно сканиране*

Методът наземно лазерно сканиране представлява електронно-оптична дистанционна технология за заснемане на обекти без необходимост от пряк достъп до тях, което го прави незаменим при анализиране на трудно достъпни терени, агресивни и опасни среди. В резултат на това заснемане се създават цифрови модели на изследваните обекти, като се осигурява изключително висока точност на отразяване на реалния свят. Понятието LASER в превод означава светлинно усилване на стимулирана радиационна енергия (Light Amplification by Stimulated Emission of Radiation – LASER), което представлява оптически квантов генератор и източник на монохроматична, насочена светлина, изпускащ тънък, кохерентен сноп с голяма яркост, постоянна дължина на вълната и фаза. Освен наземно лазерно сканиране съществува и въздушно лазерно сканиране при един и същ основен принцип на действие, като разликата между двата метода е в местоположението на лазерния скенер [2, 7].

2.2. Технически средства, прилагани при наземно лазерно сканиране.

Техническите средства прилагани за реализиране наземното лазерно сканиране се наричат лазерни скенери или LiDAR системи. Първите прототипи се разработват през 80-те години на 20-ти век и след това те имат огромно развитие и реализация. Технологията, свързана с тяхното използване, е наречена сканиране [2].

Лазерните скенери работят с електромагнитни вълни във видимата и инфрачервената част на спектъра. За разлика от радарите те имат възможност за регистриране на изключително дребни частици – водни капки, аерозоли и молекули, с размери от порядъка на 10 μm до 250 nm. Базират се на

безрефлекторното измерване на разстояние между сензора или излъчвателя на скенера и наземния обект. Същността на метода се състои в това, че излъчвателят представлява мощен светлодалекомер, работещ на принципа – обратна връзка, излъчващ непрекъсната серия от електромагнитни импулси в различни направления. Това позволява за кратък период от време да бъдат измерени разстоянията и посоката до голямо количество точки от земната повърхност с гъстота, зависеща от честотата на излъчваните и приемани отразени импулси, която достига до 400 KHz. В резултат на лазерното сканиране се формира т.нар. облак от точки, при което заснетият обект се представя като съвкупност от крайно число точки, местоположението на всяка от които е определено в пространството с тройката координати X, Y и H в зададена координатна система. Търсената геометрична информация за сканирания обект се извежда изцяло при последващата обработка от 3D облаци от точки чрез специализиран софтуер [5].

Поради факта, че обектите от земната повърхност отразяват в различна степен електромагнитните вълни с различна дължина на вълната, в зависимост от своето предназначение, различните лазерни системи използват вълни с различна дължина, като често използваните вълни са тези с дължина 532 nm (при топографско заснимане на дъното на различни водоеми), 1064 nm (при изследване на заснежени и заледени или влажни повърхности) и 1550 nm (при изследване на сухи, скалисти и други подобни повърхности).

Функционалното устройство на скенерите за наземно лазерно сканиране се състои от три основни системи:

— система за управление и администриране на данни;

Системата за управление и администриране на данни представлява компютър, който е свързан със системите за измерване, и е предназначена за управление на системите за измерване и запаметяване на данните, като служи и за последваща обработка на данните.

— система за измерване на посоки;

Системата за измерване на посоки се състои от система от огледала, полигони от огледала и призми и е изградена, така че източникът на лъчение на далекомера е подвижен или пътят на лазерния лъч се изменя от подреждането на огледалата. В зависимост от това каква маса е в движение (огледала, призми, рамки), се определя броят на сканираните точки за единица време, както и скоростта на сканиране. Колкото по-малка е тази маса, толкова по-голяма е скоростта на сканиране и с това броят на точките за единица време.

— система за измерване на дължини.

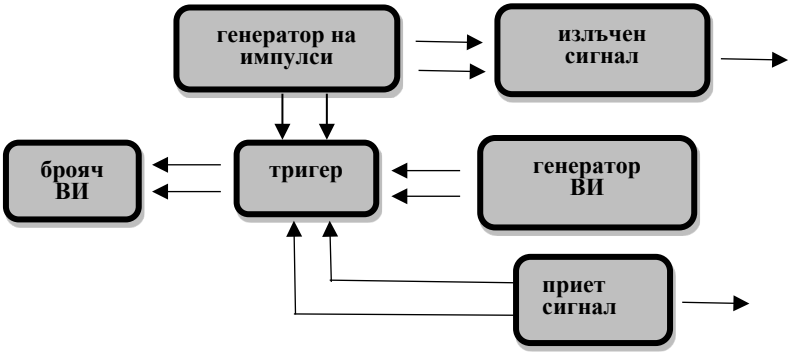
Системата за измерване на дължини работи или на импулсивния принцип или на сравнение на излъчената и приетата отразена фаза на дължината на вълната – фазов принцип. Съществува и трета система на оптическа триангулация, чрез измерване на два ъгъла в скенера от постоянна база [1].

2.3. Класификация на лазерните скенери.

Съобразно начина на измерване на разстояния, лазерните скенери се класифицират като импулсни, фазови и чрез триангулация, тъй като зависимост от своята конструкция могат да използват един от трите метода за измерване на разстоянията:

— импулсен метод (Time Pulsed Method) – времеви импулсен метод, базиращ се на точното измерване на времето между излъчения и отразения светлинен импулс;

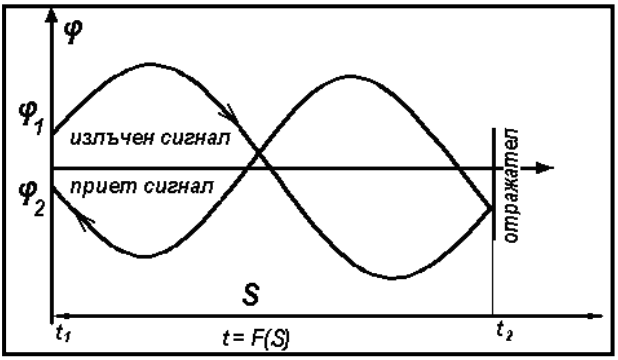
Този тип системи работят на принципите на импулсния далекомер (фиг. 2), при който излъчването на светлината се осъществява във вид на много кратки импулси, притежаващи голяма концентрация и енергия. При този тип далекомери времето за преминаване на двойно измереното разстояние – от излъчвателя до отражателя, и обратно, се измерва непосредствено с помощта на брояч на количеството времеви импулси (ВИ) между момента на излъчване на сигнала и момента на приемане на отразения сигнал [1].



Фиг. 2. *Принципна схема на импулсен далекомер*

— фазово сравнителен метод (Phase Comparison Method) – базира се на измерването на фазовите разлики между непрекъснатия изходящ и входящ вълнов поток;

Принципът на работа на фазовия далекомер се илюстрира с фиг. 3, на която са показани: излъченият сигнал, притежаващ фаза на амплитудата в момента на излъчване φ1, и приетият отразен сигнал, притежаващ фаза φ2.



Фиг. 3. *Излъчен и приет модулиращ сигнал при фазовия далекомер*

На база зависимостта между ъгловата честота на трептене и фазата на сигнала в момента на неговото излъчване и фазата на същия сигнал в момента на обратното приемане след преработка се получава формулата за определяне на измереното разстояние по фазовата разлика на излъчения и приет отразен сигнал, която има вида:

$$S = \frac{v\Delta\varphi}{4\pi f} \quad (1)$$

където v е скорост на разпространение на светлината, $\Delta\varphi$ е измерена фазова разлика между излъчения и приетия модулиращ сигнал и f – честота на трептене на модулиращия сигнал [1].

— чрез триангулация.

При метода на триангулация се излъчва лазерен лъч от източника на излъчване, който се отразява обратно към приемащия край, когато срещне целевия обект. Точката на излъчване, целевият обект и приемащата точка образуват триъгълник. Чрез измерване на ъгъла на триъгълника може да се измери разстоянието от инструмента до целта [1].

В зависимост от зрителното поле се класифицират като скенери с обикновена камера (Camera-View-Scanner), скенери с панорамна камера (Panorama-View-Scanner) и хибридни скенери.

Скенерите с обикновена камера притежават постоянен отрез от образа, както една обикновена фотокамера и трябва ръчно да се насочват към обекта на сканиране. При тези апарати отклонението на визирния лъч е чрез ротиращо се огледало.

Скенерите с панорамна камера имат хоризонтално зрително поле от 360 градуса. При панорамните скенери измерването на ъглите и разстоянията се извършва в хоризонтален обхват от 360 градуса, а във вертикално отношение до 180 градуса. По конструкция те са подобни на електронния тахиметър, тъй като измерването на посоките на визирния лъч става с движение на мерната глава, носеща оптиката [1].

Съществуват мобилни лазерни скенерни системи, чрез които се извършва лазерно сканиране със скенери, поставени на движеща се платформа – жп., автомобил, кораб и др., както и скенери, които се държат в ръка при измерване [1].

2.4. Сфери на приложение на наземното лазерно сканиране.

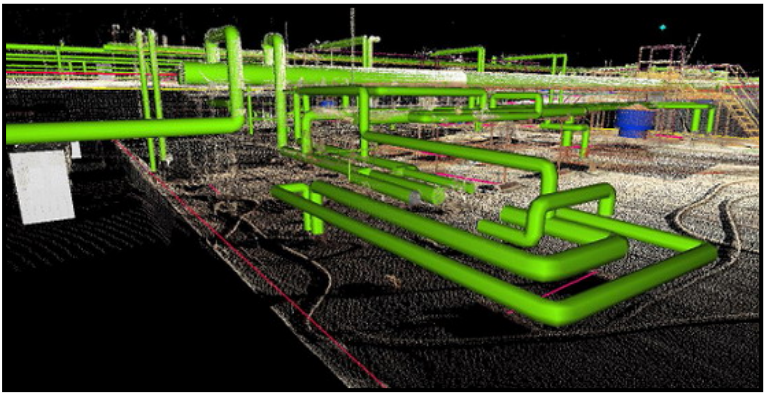
Наземното лазерно сканиране намира редица приложения при събиране на геопространствени данни за местността с цел геодезически, топографски, хидрографски, инженерно-проучвателни, електроенергетични и редица други изследвания на заобикалящия ни свят:

— за изследване на деформации по геодезически методи;

На базата на цифрови модели на терена, създавани през определени периоди от време чрез наземно лазерно сканиране, може да се правят оценки за промени в топографията и тяхното влияние върху околната среда [2].

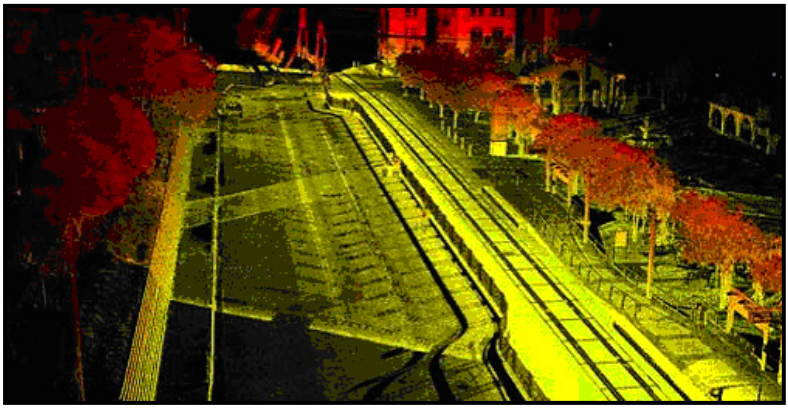
— в строителството;

Чрез наземно сканиране и документиране в реално време на изгражданите сгради, съоръжения или машини се спестява време и труд.



Фиг. 4. *Модел на промишлени съоръжения, заснети чрез наземно лазерно сканиране*

Също така за определяне на точна оценка на състоянието на пътни или ж.п. съоръжения, на базата на предварително създадени тримерни модели, може да се установи степента на износване и необходимостта от рехабилитация [2, 6].

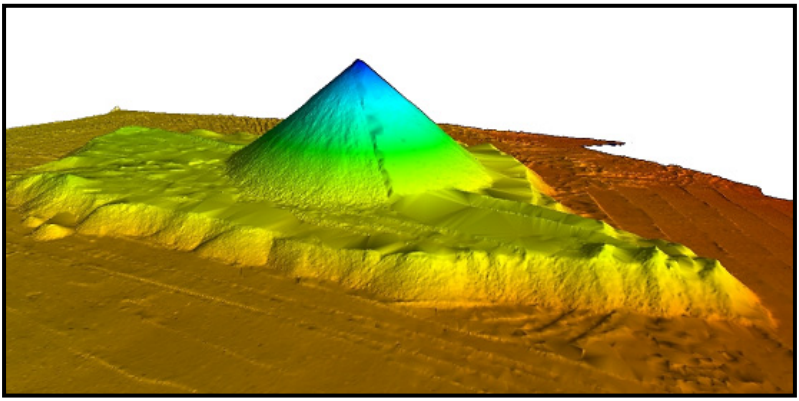


Фиг. 5. *Тримерен модел на железопътна инфраструктура*

— при работа в опасни и труднодостъпни терени;

Наземното лазерно сканиране е несравним с традиционните методи за повишаване на техническата безопасност в открити рудници, намаляването на необходимото производствено време и нуждата от физически достъп до обекта. Намира приложение и при определянето на обеми и създаване на тримерни модели с доста по-висока точност и в значително по-кратки срокове. В България

наземно лазерно сканиране се прилага успешно в рудничен комплекс „Елаците Мед“АД [2].



Фиг. 6. *Тримерен модел на насипище в открит рудник*

— при изграждането и поддържането на различни инженерни съоръжения – мостове, тунели [2];

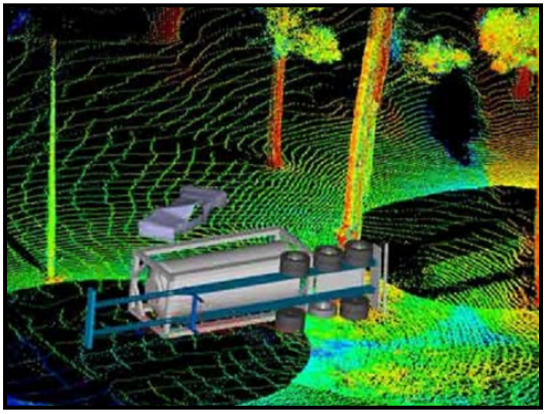
— в архитектурата и фотограметрията;

Наземните лазерни скенери се използват в областта на архитектурата за създаване на цифрови модели на сгради, подлежащи на реконструкция, като често допълват и въздушното лазерно сканиране при изготвяне на тримерен модели на градската среда, на базата на които се оценява влиянието на новопроектирано строителство върху облика на града [2, 4].

Фиг. 7. *Тримерно наземно лазерно сканиране на храм-паметник „Св. Александър Невски“*

— в анимацията за получаване на тримерни компютърни модели [2];
— в археологията за моделиране на ценни предмети на изкуството [2];
— при разследване на катастрофи.

Чрез дигитализиране и тримерно моделиране на сцената на инцидента могат да бъдат установени причините за произшествието, както и средства за евентуалното му избягване [2].



Фиг. 8. *Сцена на пътно-транспортно произшествие.*

3. Изводи.

Между класическия метод за събиране на геопространствени данни и наземното лазерно сканиране е възможно да се направи аналогия като видове геодезическо заснимане. Разликата между тях не е само в количествените измерения, произтичащи от преимущества на лазерното сканиране по отношение на производителността, но и в реализирането им на две различни идеологии за местността. Сравнението между класическия метод за събиране на геопространствени данни и наземното лазерно сканиране е представено в табл. 1 [3].

След анализ на данните от табл. 1 може да се направи извод, че при изпълнението на земната топографска снимка с класически средства, всяка точка съдържа точно определено семантично съдържание и още в момента на нейното създаване тя вече се явява част от предварително формулирана схема, която по-късно по определени правила ще бъде преобразувана в топографски план. Докато лазерното изображение е извън тези ограничения. Полученият в резултат от лазерното сканиране облак от точки, е много по-богат по съдържание, което прави информацията, съдържаща се в него, значително по-универсална при нейното използване. Положението и ориентацията на сензора, който регистрира постъпващите на входа електромагнитни вълни в избраната координатна система, се определя от наличната в комплекса навигационна апаратура, осигуряваща непрекъснат запис на пространствените координати на сканиращия блок X,Y,Z и трите ъглови елемента ω, φ, κ – елементите на външно ориентиране [3].

Таблица 1. *Съпоставка между класическия метод за събиране на геопространствени данни и наземното лазерно сканиране [3, 5]*

Параметър за сравнение	**Данни, получени чрез класическа земна топографска снимка**	**Данни, получени от наземно лазерно сканиране**
Максимално достижима точност на определяне на пространствените координати	по добра от 1 cm	15 cm – 30 cm
Плътност на данните	- плътност на разположението на точките се определя от мащаба на изпълнение на топографската снимка и характера на обекта; - плътността е ограничена от производителността на снимачния екип, която практика е няколко стотин точки на ден;	- на практика до 3 - 5 лазерни точки на кв. м. от земната повърхност; - реалната плътност се определя от производителността на скенера (в настоящия момент тя достига 50 - 100 хиляди измервания за секунда) и условията на снимане – скорост и височина на полета;
Пространствено положение на точките	точките се избират по правило върху реалната земна повърхност;	точките от отразяването на лазерните лъчи покриват както реалната земна повърхност, така и всички обекти, разположени върху нея – покриви на здания, стълбове и проводници на въздушни електрически линии, водоеми, растителност и др;
Характер на пространственото разпределение на точките върху земната повърхност	изборът на мястото на подробната точка се определя от оператора във всеки конкретен случай съобразно топологическите особености и обекта на заснемане;	разпределението на лазерните точки по земната повърхност носи случаен характер;

Предимствата на наземното сканиране пред конвенционалните методи са многобройни, например:

— заснемане с висока скорост;
— безконтактно заснемане на трудно достъпни обекти;
— финансова икономичност;
— високо ниво на автоматизирана обработка;
— отлична визуализация на сканирания обект;
— съхраняване на точната геометрия на обектите;
— моделиране на сканирани обекти;
— създаване на фасадни планове и др.

В съвременния свят технологията на наземното лазерно сканиране ще се използва все по-широко в различни области като метод за събиране на пространствени данни и създаване на тримерни цифрови модели [2].

ЛИТЕРАТУРА

[1] Милев Г., Милев И. Основи, системи и технологии в инженерната геодезия, София: Съюз на геодезистите и земеустроителите в България, 2017.

[2] Камбуров А. Технологията LiDAR и нейното приложение за наземно 3D лазерно сканиране, Геомедия, 2010.

[3] Михайлов Пл., Петров Д. Съвременни технически средства и технологии за събиране на геопространствени данни за местността, Шумен: Университетско издателство „Епископ Константин Преславски“, 2014, ISBN 978-954-577-933-6.

[4] Малджански, Пл. Развитие на методите за заснемане и обработка на данни в архитектурната фотограметрия, София: „ТЕС Дизайн“, 2012, ISBN 978-954-2994-02-2.

[5] Ниязи-Юсуф М., Оценка на актуалността на съдържанието и точността на действащите кадастрални планове. Шумен: Университетско издателство „Епископ Константин Преславски“, Годишник: Технически науки, том XI Е, 2021, ISSN: 1311-834X.

[6] Ниязи-Юсуф М., Геодезическа основа на кадастрална карта. Шумен: Университетско издателство „Епископ Константин Преславски“, Годишник: Технически науки, том XI Е, 2021, ISSN: 1311-834X.

[7] Лалев Х., Цанков Ц., Николов И. 3D лазерно сканиране. Научна конференция МАТТЕХ 2010, Шумен, 2010/2011, ISSN 1314-3921.

ОСНОВНИ СПЕЦИФИКАЦИИ НА ПРОТОКОЛА OPENFLOW

Мустафа Б. Узун, Валентин Т. Атанасов

MAIN SPECIFICATIONS OF OPENFLOW PROTOCOL

Mustafa B. Uzun, Valentin T. Atanasov

ABSTRACT: *The OpenFlow protocol, one of the key components of Software-Defined Networking, is outlined as a transformative force in the field of computer networks. This protocol facilitates dynamic network management by separating the control plane from the data plane, enabling centralized control for improved programmable management and automation. Once standardized through RFCs, OpenFlow allows operational compatibility and establishes the foundation for a versatile ecosystem. OpenFlow's distinctive features, including support for Software-Based Infrastructure through Southbound Interfaces, deviate from traditional hardware-centric models. SBI emphasizes the use of software applications, aligning with the network automation paradigm. This shift streamlines administrative tasks and promotes adaptability in the face of changing network conditions.*

KEYWORDS: *OpenFlow, SDN (Software Defined Networking), SBI, Southbound Interface, Network automation.*

Въведение

Протоколът OpenFlow е основно звено за SDN (Software Defined Networking), чрез който се разделя контролната от информационната равнина. За да се насърчи развитието на SDN и да се насърчи разработване на протоколи, като OpenFlow, беше създаден ONF (Open Networking Foundation) през март 2011 г. [8]. Тази организация се фокусира главно върху разработването на SDN базирани модели, чрез внедряване на протокола OpenFlow, с цел установяването на нов мрежов стандарт. Основните му изследователски постижения включват дефиниране на основна архитектура на SDN, стандартизиране на протокола за конфигурация и управление OpenFlow. След първото издание на спецификацията на протокола през октомври 2009 г., ONF публикува версии 1.1, 1.2, 1.3, 1.4 и най-новата му версия OpenFlow 1.5 през януари 2015 г. [1] Хронологията на разработените версии и актуализации на OpenFlow се обобщават на фиг. 1.

OpenFlow е най-популярният отворен стандарт, работещ на SBI (Southbound Interfaces) на SDN. Той предоставя обща спецификация за внедряване на комуникационни устройства с поддръжка на OpenFlow, осигуряващ

комуникационни канали между контролната равнина и комуникационни устройства, като например комутатори, маршрутизатори, контролери и др. Тези информационни канали са основните средства за предоставяне на информация за преминаващите потоци към мрежовата операционна система [5].

Фиг. 1. *Историческо развитие на протокола OpenFlow*

Чрез изграждане на информационни канали OpenFlow осигурява необходимата информация за мрежовите операционни системи. Тези канали могат да бъдат разделени условно на три типа [3].

1. Съобщенията, базирани на събития, се изпращат от комуникационните устройства към контролера, когато се създаде връзка или има промяна в състоянието на порта.
2. Статистическите данни за потока се генерират от комуникационните устройства и се събират от контролера.
3. Съобщенията за входящите пакети се изпращат от комуникационните устройства към контролера, когато те не знаят какво да правят с нов входящ поток или защото има изрично действие „изпрати до контролера“ в съответстващия запис на таблицата на потока.

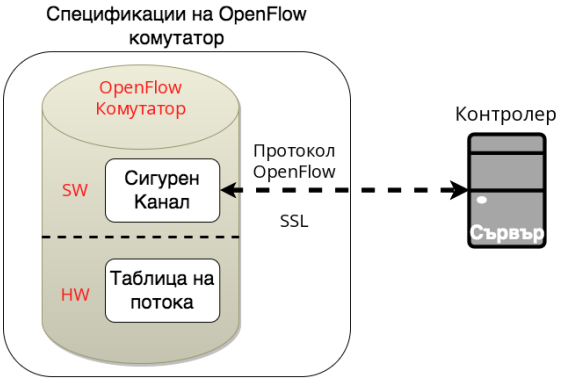
Основните компоненти на протокола OpenFlow се състоят от порт, таблица на потока комуникационен канал, алгоритми за управление на потоци и съобщения. Принципа за обработка и групиране на данни на SDN комуникационно устройство, след като получи пакет е първо да търси съвпадащи записи на потока в локалната таблица на потока.

Предварително групираните данни се сравняват с първата таблица на потока, но могат да се сравнят и преминат през множество таблици. Това преминаване през множество таблици (филтри) се наричат конвейери [2]. За да се изясни по-добре как тези процеси се изпълняват може да се разгледа спецификацията на OpenFlow комутатор, и да се разгледат основните етапи през, които комутационния процес преминава.

Спецификация на OpenFlow комутатор

За разлика от традиционното (Ethernet) комутиране, което се базира на CAM (Content Addressable Memory) и TCAM (Ternary Content Addressable Memory) таблици [5], OpenFlow използва потоци известни, като flows, при които принципът на комутация е по-сходен с TCAM отколкото с CAM. На Фиг. 2 се показва пример на OpenFlow комутатор, като комутационният процес може да се раздели на три части[7]:

- *Таблица на потока*: Това е основният градивен елемент на OpenFlow. Всеки пакет, който влиза в комутатора, преминава през една или повече таблици на потока. Като по този начин се взема решение за всяко последващо действие, според всеки запис на потока.
- *Сигурен канал:* Той свързва комутатора с централизираното управление наречено *контролер*, който позволява изпращане на инструкции и пакети между контролера и комутатора. Протоколът описва обмена на съобщения, който се извършва между контролер OpenFlow и устройство OpenFlow. Обикновено протоколът използва SSL (Secure Socket Layer) или алтернатива, като защитата на транспортния слой TLS (Transport Layer Secuirity), осигурявайки защитен OpenFlow канал.
- *OpenFlow протокол*: Това е най-популярният протокол, опериращ в южната граница SBI (South Bound Interfaces) описан в общия модел на SDN, който предлага отворен и надежден начин за осигуряване на информационен канал между контролера и OpenFlow комуникационното оборудване



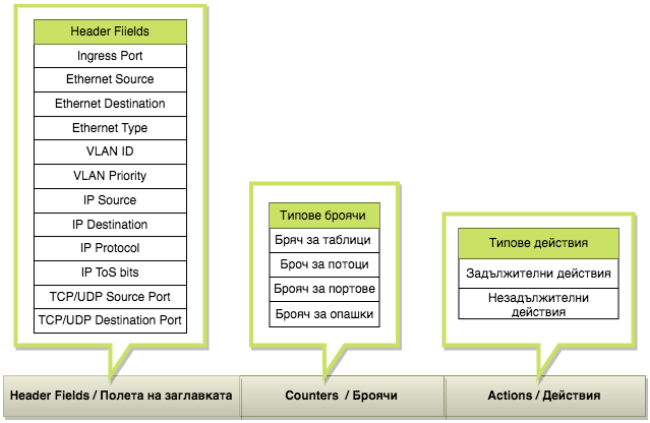
Фиг. 2. *Спецификация на OpenFlow комутатор*

Основната идея е проста - повечето съвременни Ethernet комутатори и маршрутизатори имат таблици със *запис за управление на потоци*, които поддържат скорости според заложените им спецификации към комуникационни устройства, изпълняващи функции на защитни стени, NAT, QoS и др.

Таблици на потока

Основният градивен елемент на OpenFlow е таблицата на потока. Всеки пакет, който влиза в устройство, преминава през една или повече таблици на потока. Таблицата на потока (Flow Table) съдържа набор от правила или записи, определени чрез потоците flows. Всеки поток (фиг. 3) е асоцииран с определен вид мрежов трафик и съдържа информация за начина, по който трябва да бъде обработен този вид трафик. Всяко правило в таблицата на потока включва съвпадащи (Matching) критерии както и инструкции за действия, които трябва да се предприемат, когато се открие поток, който отговаря на тези критерии [6]. Таблицата на потока състои от следните три елемента:

- *Header Field:* Поле на заглавката или полета за съвпадение с информация, намираща се в заглавката на пакета, входния порт и метаданните, използвани за съпоставяне на входящите пакети.
- *Counters*: Броячи, използвани за събиране на статистика за конкретен поток като брой получени пакети, брой байтове и продължителност на потока.
- *Actions*: Набор от инструкции или действия, които да бъдат приложени след съвпадение, които диктуват как да се обработват съвпадащи пакети. Например, действието може да бъде препращане на пакет към определен порт.



Фиг. 3. *Потоци на OpenFlow*

„Header Field“ (Поле на заглавката)

Всеки запис в заглавката на таблицата на потока се състои от шест компонента, които определят правилата за съвпадение и други основни правила за съответния поток:

1. *Поле за съвпадение:* Използва се за сравнение на пакети, за които е намерено съвпадение на стойностите на полето.
2. *Приоритет:* Относителен приоритет на записите в таблицата.

3. *Броячи:* Обновяване на стойностите на съвпадащи пакети.
4. *Инструкции:* Действия, които трябва да се предприемат, ако възникне съвпадение.
5. *Таймаут:* Максималното време за изчакване, преди потокът да бъде премахнат от комутатора.
6. *Бисквитки:* В основата си, т.н. бисквитки (cookies) позволяват на контролера да асоциира допълнителна информация с определен поток, като например политики за качество на обслужване (QoS), маршрутизационни правила или други контролни параметри.

„Counters“ (Броячи)

Броячите (Counters) в OpenFlow представляват механизъм за отчитане на различни статистики, свързани с обработката на мрежов трафик от страна на OpenFlow поддържащи устройства. Тези броячи предоставят информация за различни събития, като брой пренесени пакети, обем на трафика, брой грешки и други статистики, които са полезни за мониторинг и управление на мрежовия трафик. В рамките на OpenFlow, броячите се свързват с правила (Flow Entries) за потоци в (Flow Table) на комутаторите.

Това позволява на администраторите да следят и анализират как се обработва мрежовият трафик в реално време. Броячите могат да бъдат конфигурирани за определени потоци или групи от потоци, позволявайки детайлен мониторинг на трафика спрямо зададени правила. Основната цел на броячите в OpenFlow е да предоставят информация за ефективността и състоянието на мрежата, което е от съществено значение за динамичната управленска парадигма на софтуерно дефинираните мрежи (SDN). В табл.1 са показани различните видове броячи и тяхното предназначение [2].

Таблица 1. *OpenFlow броячи*

Table	Flow	Port	Queue
• Активни записи • Сравнение на пакети • Съвпадения	• Получени пакети • Получени байтове • Продължителност (секунди) • Продължителност (наносекунди)	• Получени пакети • Изпратени пакети • Получени байтове • Изпратени байтове • Анулирани получени пакети • Анулирани пакети при предаване • Грешки при получаване • Грешки при предаване • Грешки при получаване по нечетност • Грешки при получаване с препълване • Грешки в CRC	• Предадени пакети • Предадени байтове • Грешки при предаване с препълване

„Actions“ (Действия)

Всеки запис на поток е свързан с или повече *действия*, които диктуват как устройството обработва съвпадащи пакети. *Действията* (Actions) в спецификацията на OpenFlow са определени като задължителни и незадължителни (табл.2). Различните производители на комуникационно оборудване не изискват незадължителните действия като такива.

Действията в OpenFlow представляват инструкции или операции, които се предприемат от комутаторите в мрежата в резултат на съвпадение с определени правила в таблиците на потока "Actions". След това се определя какво трябва да се направи с пакетите, които отговарят на конкретно правило за определен поток [8].

Примери за "Actions" в OpenFlow:

- Предаване (Forwarding): Определя къде да бъде изпратен пакетът, като се задава портът на изходящия интерфейс.
- Промяна на MAC или IP адреса: Променя MAC адреса на източника или получателя или IP адрес в заглавието на пакета.
- Ограничение на скоростта (Rate Limiting): Задава ограничение на трансферната скорост за определен поток (flow).
- Изпращане на пакет към контролер: Предоставя възможност за изпращане на пакети към централния контролер за допълнителна обработка.
- Промяна на VLAN тага: Актуализира VLAN тага на пакета.

Таблица 2. *OpenFlow „Actions“*

Forward	Drop	Modify Field
Задължителен	**Задължителен**	**Незадължителен**
• All • Controller • Local • Table • In Port		
Незадължителен		
• Normal • Flood		

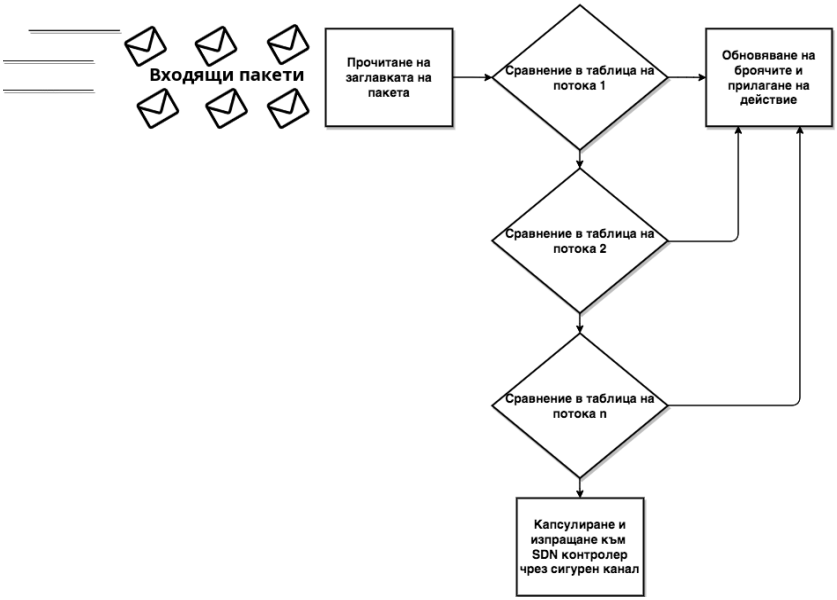
Действията позволяват на администраторите посредством контролери да определят как точно да се управлява мрежовият трафик в съответствие с вида на потоците и правилата, които са конфигурирани в (Flow Table).

Това предоставя висока степен на гъвкавост и контрол в софтуерно дефинираните мрежи. На фиг. 4 се показва общата логическата блок схема, която илюстрира начина на управление на потоци (flows), чрез *действия* [6].

Всеки входящ пакет в SDN се сравнява за съвпадения с определения поток, като се използват Ethernet полетата на подателя и получателя. Процесът на сравнение може да продължи и с другите полета на протокола в зависимост от полето за типа на пакета (Ethertype).

Като за пример може да даде тип на протокола 0x8100 (VLAN), след това сравнението продължава за полето (VLAN ID) и (VLAN Priority). Подобно на това и с типа 0x806 (ARP), сравнението може да продължи с IP адресите на изпращача и получателя.

За всеки запис, за който е намерено съвпадение без приложен мрежова „джокер“ маска (Wildcard), има присвоен по-голям приоритет от този със (Wildcard). Всеки (Wildcard) запис има свой собствен приоритет.



Фиг. 4. *Поток на пакети в комутатор OpenFlow*

Ако се открият много записи с еднакъв приоритет, тогава устройството може да избере произволно реда, по който ще се сравнят. На фиг. 5 е даден пример за процеса на търсене на съвпадения в потока и последващи действия (Actions) според откритите такива.

Port#	Src. MAC	Dest. MAC	Eth. type	VLAN ID	VLAN Priority	IP Src.	IP Dst.	IP protocol	IP ToS	L4 Src. Port	L4 Dst. Port	Action
*	*	*	*	*	*	*	8.8.8.8	*	*	*	*	Port 1/1

Маршрутизиране (целия трафик за 8.8.8.8 се маршрутизират към физически порт 1/1

Port#	Src. MAC	Dest. MAC	Eth. type	VLAN ID	VLAN Priority	IP Src.	IP Dst.	IP protocol	IP ToS	L4 Src. Port	L4 Dst. Port	Action
*	*	*	*	*	*	*	*	*	*	*	22	Drop

Дискарт на трафика (трафик с номер на порт на получател 22 се дискартват)

Port#	Src. MAC	Dest. MAC	Eth. type	VLAN ID	VLAN Priority	IP Src.	IP Dst.	IP protocol	IP ToS	L4 Src. Port	L4 Dst. Port	Action
*	*	*	*	*	*	4.4.4.4	*	*	*	*	*	Port 1/1, 1/3

Дублиране (трафика за 4.4.4.4 се дублира на входящия порт 1/1 и порта за мониторинг 1/3)

Фиг. 5. *Поток на пакети в комутатор OpenFlow*

Заключение

В заключение би могло да се направи следното обобщение - Автоматизираното управление на мрежи с концепцията на софтуерно дефинирани мрежи, основано на протокола OpenFlow, представлява стъпка към значително повишаване ефективността на проектирането, конфигурирането и управлението на мрежова инфраструктура. SDN осигурява централизирана и програмируема контролна „*плоскост*“, като допълнително подчертава гъвкавостта и динамиката в мрежите.

Протоколът OpenFlow играе ключова роля, като дефиниран стандарт за комуникация между централния контролер и комутаторите, позволявайки централизирано управление и възможност за програмно управление на мрежовите устройства. Тази комбинация улеснява бързата адаптация към променящите се условия, повишава ефективността на трафика и подобрява общата сигурност на мрежата.

ЛИТЕРАТУРА

[1] Göransson, P., Black, C., Timothy C., Software Defined Networks: A Comprehensive Approach Second Edition, Morgan Kaufmann, 2017, ISBN: 978-0-12-804555-8.

[2] Azodolmolkly, S., Software Defined Networking with OpenFlow, Packt Publishing, 2013, ISBN 978-1-84969-872-6.

[3] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Petrson, L., et al, OpenFlow: Enabling Innovation in Campus Networks, ACM SIGCOMM Computer Communication Review, vol. 38, number 2, 2008, pp 263-297, https://doi.org/10.1145/1355734.1355746.

[4] Hucaby, D., CCNP Switch 642-813 Official Certification Guide. Indianapolis: Cisco Press, 2010, ISBN-13 978-1-58720-243-8.

[5] Casado, M., Foster, N., Guha, A., Abstractions for software-defined networks, Communications of the ACM, vol. 57 issue 10, 2014, 86–95, https://doi.org/10.1145/2661061.2661063.

[6] Tiawari, V., SDN and Openflow for beginners with hand on labs, (Посетен на 10.10.2023) (http://www.2doubleccies.com/downloads/SDN-and-Openflow.pdf).

[7] An Instant Virtual Network on your PC, 2018. (Посетен на 10.10.2023) (http://www.mininet.org).

[8] ONF. OpenFlow Switch Specification. December 31, 2009. (Посетен на 10.10.2023) (https://opennetworking.org/wp-content/uploads/2013/04/openflow-spec-v1.0.0.pdf).

МАРШРУТИЗАЦИЯ И ПРИСВОЯВАНЕ НА ДЪЛЖИНА НА ВЪЛНАТА ЗА ОЦЕЛЯВАЩИ МРЕЖИ

Цветослав С. Цанков, Екатерина М. Христова

ROUTING AND WAVELENGTH ASSIGNMENT FOR SURVIVABLE NETWORKS

Tsvetoslav S. Tsankov, Ekaterina M. Hristova

ABSTRACT: *In wavelength-routed networks, after the light flow is established, the failure of a node or link can result in the failure of all light paths that cross it. This necessitates the development of appropriate protection and recovery schemes that reduce data loss in the event of a failure.*

KEYWORDS: *Multiplexing, Optical fiber, Packet switching, Signal-to-noise ratio, Wavelength, WDM.*

Протоколите от виско ниво (като ATM, IP и MPLS) имат свои собствени процедури за възстановяване. Времето за възстановяване на горните слоеве обаче е значително голямо (от порядъка на секунди), докато времето за възстановяване на повредата при оптичния слой трябва да е от порядъка на милисекунди за намаляване на загубите на данни. Освен това е полезно да се разгледат механизмите за възстановяване на повреди в оптичния слой поради следните причини: (а) той може ефективно да мултиплексира защитни ресурси (като резервни дължини на вълните и влакна) сред няколко мрежови приложения от по-висок слой и (б) оцеляването на оптичния слой осигурява защита на протоколите от високо ниво, които може да нямат вградено възстановяване при грешки. [1, 2, 15, 16, 17, 20, 21]

По същество има два вида механизми за възстановяване на грешки. Ако резервни ресурси (маршрути и дължини на вълните) са предварително изчислени и резервирани предварително, той се нарича схема за защита. В противен случай, когато възникне повреда, ако трябва да се осигури динамично друг маршрут и свободна дължина на вълната за всяка прекъсната връзка, се нарича схема за възстановяване. Схемата за възстановяване обикновено е по-ефективна по отношение на ресурсите, докато схемата за защита има по-бързо време за възстановяване и гарантира пълно възстановяване на мрежата. Механизмите и подходите за защита и възстановяване могат да се комбинират, за да се използват предимствата и на двете. Механизмите за защита могат да се използват

за борба в сценарии за единичен отказ, докато възстановяването се прилага, ако две или повече повреди възникват едновременно. В действителност сценариите с двойна повреда са редки и възможността за възстановяване при двоен отказ може да бъде много скъпа. [3, 4, 18, 25, 26, 31]

От гледна точка на топологията на мрежата схемите за защита могат да бъдат класифицирани като Ring-защита и Mesh-защита. Схемите за Ring-защита включват: Автоматично защитно превключване (APS) и Самовъзстановяващи пръстени (SHR). И двете схеми могат допълнително да бъдат разделени на две подгрупи: защита на пътя и защита на връзката. При защита на пътя, след като възникне повреда на връзката по основния път, движението се пренасочва през несвързан резервен маршрут. При защитата на връзката трафикът се пренасочва само около пропадналата връзка. Защитата на потока обикновено изисква по-малко ресурси и по-ниско забавяне на разпространението за възстановителния маршрут, докато защитата на връзката може да осигури по-бързо възстановяване, тъй като няма изискване за сигнализиране по цялото трасе. [5, 19]

При схемата „защита на пътя“, за всеки установен светлинен път, има два несвързани пътя на защита: основен (работен) път и резервен (защитен) път. Светлинният поток се създава през основния път. В случай на повреда на връзката, светлинният път се превключва на предварително запазен или предварително установен резервен път. Основният и резервният път не са свързани, докато резервните пътища на различните връзки могат и да споделят общи дължини на вълните и общи връзки. [1, 2, 15, 16]

Ако не е разрешено споделяне между резервни пътища, тогава се появява специализирана схема за защита на светлинния път. Комутаторите на резервните пътища могат да бъдат конфигурирани в началото, т.е. когато светлинният път е установен на основният път. По този начин, не е необходимо конфигуриране на комутатора при възникване на повреда. Този тип възстановяване може да бъде много бързо, но ресурсите не се използват много ефективно.

Ако споделянето между резервни пътища е разрешено, докато отговарят на определени ограничения, комутаторите на резервните пътища не могат да бъдат конфигурирани до момента на възникване на повреда. Времето за възстановяване при тази схема е по-дълго, но общото използване на ресурсите е много по-добре оптимизирано, отколкото предната схема. Разбира се, необходимо е повече сигнализиране за възстановяване от повреда. Тази схема се нарича „защита на споделен път“. [36, 37, 38]

При защитата на връзката, светлинният поток се създава чрез основен път. За всяка връзка по светлинния път, резервна верига (или защитна верига) е резервирана на връзката. Ако връзката се провали, трафикът по светлинния път се пренасочва около тази връзка в резервната верига. Ако не е възможно преобразуване на дължина на вълната в мрежата, дължината на вълната, запазена

за резервните вериги, трябва да бъде същата като тази на основния път. Ако не е разрешено споделяне, т.е. дължина на вълната, използвана за резервна верига може да се използва само за възстановяване на дължина на вълната на конкретна връзка, схемата за защита е специализирана. В противен случай, схемата за защита е със споделена връзка. Трябва да се отбележи, че при схемата „защита на връзката“, на една и съща връзка може да има различни вериги за възстановяване.

Някои проучвания прилагат схеми за Ring-защита в мрежа с Mesh-топология. Един такъв подход е картографирането на планарен граф в насочени цикли и всяка насочена връзка да е защитена от насочен цикъл. Подходът е разработен върху пръстеновидна схема за защита на връзката. Предложена е и друга схема, базирана на пръстеновидния подход за защита, който работи по различен начин. „Капак на пръстена“ е измислен първо за Mesh-мрежа и схемата за защита на споделена връзка се използва в границите на пръстените, докато схемата за защита на дължините на вълните не се споделя между различни пръстени. По този начин, комутаторите могат да бъдат предварително конфигурирани и се насърчава известна степен на споделяне между защитни дължини на вълната. Концепцията на „*p*-цикли“ е друга Ring-форма на защита на връзката, където „*p*-цикъл“ е множество от връзки в Mesh-мрежа, образуващи цикъл, който пресича или покрива всяка връзка в мрежата. Следователно, всяка повреда на връзката може да бъде възстановена от „*p*-цикъл“. Въпреки че възстановяването с помощта на „p-цикли“ е с пръстеновиден характер, мрежа защитена от такива цикли, може да има ефективността на Mesh-мрежа на честотната лента. Фиг. 1 обобщава класификацията на схеми за защита и възстановяване. [6, 13, 14, 23, 29, 33]

Фиг. 1. *Схеми за защита и възстановяване*

В мрежа с маршрутизирана дължина на вълната трафикът може да бъде статичен или динамичен. При статичен трафик, заявките за свързване са достъпни наведнъж. RWA задачата трябва да е решена за всяка заявка за връзка, включително и първичните пътища и резервните пътища (резервните вериги). Този проблем може да бъде решен чрез Целочислено линейно програмиране (ЦЛП). Ограниченията на тази задача са броят на дължините на вълните на всяка връзка, броя на предавателите и приемниците във всеки възел, както и ограничението за непрекъснатост на дължината на вълната (ако не се използва преобразувател на дължина на вълната). Целта е да се намалят общия брой дължини на вълните, използвани за всички връзки в мрежата, което се обозначава с количество, наречено общ брой връзки с дължина на вълната или обща дължина – пробег. Алтернативната цел е да се увеличи максимално превозвания товар, т.е. да се блокират най-малък брой заявки. [5, 19, 22, 30, 32, 35]

При динамичен трафик, заявки за връзка постъпват една по една и всяка връзка съществува само с ограничена продължителност, наричана време за задържане на връзката. При фиксиран брой дължини на вълната на всяко влакно на връзката и фиксиран брой предаватели и приемници на всеки възел, целта е да се намали общата вероятност за блокиране на заявките, както и постигане на малки забавяния на разпространението на установените връзки. Нужен е протокол за контрол и управление, за да се установи и прекъсне светлинен поток, както и за извършване на възстановяване на повреда.

В маршрутизирана по дължина на вълната WDM Mesh мрежа, схемата със защитата по специализиран път може да гарантира липса на загуба на данни, тъй като данните се предават и по резервни пътища. Защитата чрез споделения път често се предпочита поради неговата ресурсна ефективност. Защитата на споделена връзка също е често предпочитан метод поради бързото си превключване. Защитата чрез специализираната връзка използва твърде много ресурси от дължина на вълната и често не е за предпочитане. [3, 26, 31]

RWA задачата в WDM Mesh мрежа с определена схема за защита е дадена по следния начин: при дадена физическа топология $G = (V, E)$, където V е множеството мрежови възли и E е набор от физически връзки, броя на дължините на вълните на всяко влакно и статична матрица на търсенето на трафик, нека се маршрутизира всяка заявка за връзка на физическата топология според схемата на защитата и да се зададе дължина на вълната на всеки път по такъв начин, по който общата стойност на мрежата е намалена или пропускателната способност на мрежата е увеличена. Предполага се, че G не съдържа дублирани ребра. Целта е да се сведе до минимум общия брой връзки с дължина на вълната. Използват се следните обозначения във формулировките на ILP. [5, 22, 30]

Като входове са дадени:

– N: брой възли в мрежата.

- E: брой връзки в мрежата.
- W: брой дължини на вълните, налични за всяка връзка (дължините на вълните са номерирани от 1 до W, същия номер са дължини на вълните на всички връзки.)
- Links = {$< i,j >$}: множество от еднопосочни връзки в мрежата.
- $\bigwedge_{N\ x\ N} = \{\ dem_{i,j}\}$: матрицата на търсенето на трафик, където $dem_{i,j}$ е броят на заявките за светлинни потоци между двойка възли (i,j).

ILP използва следните променливи:

- $F_{i,j}^{s,d,w}$ приема стойност 1, ако дължина на вълната w на връзката $i \rightarrow j$ се използва от някакъв основен път между двойка възли (s,d); в противен случай 0. Тези променливите се използват във всички ILP.
- $S_{p,q}^{s,d,w}$ приема стойност 1, ако дължината на вълната w на връзката $p \rightarrow q$ се използва от някакъв защитен път между двойка възли (s,d); в противен случай 0. Те се изпозват само в ILP2.
- $\delta_{p,q}^{s,d}$ приема стойност 1, ако дължината на вълната w на връзката $p \rightarrow q$ се използва от някакъв защитен път между двойка възли (s,d), когато връзката $i \rightarrow j$ е неуспешна; в противен случай 0. Те се използват при ILP2 и ILP3.
- $m_{p,q}^{w}$ приема стойност 1, ако дължината на вълната w на връзката $p \rightarrow q$ се използва от някакъв защитен път ; 0 в противен случай. Те се използват при ILP2 и ILP3.

ILP1: Защита чрез специализиран път

Един прост начин за решаване на задачата със защитата на специализирания път е маршрутизирането на $2 \times dem_{s,d}$ светлинни пътеки между двойка възли (s,d), тъй като в този случай и основната, и резервната пътека пренасят трафик. Това води до следната формулировка на ILP. Нека се обърне внимание, че няма разлика между основния и резервния път.

Цел: Намаляване на общия брой връзки с дължина на вълната.

$$\sum_{1\le s,d\le N}\sum_{w=1}^{W}\sum_{<i,j>\in Links} F_{i,j}^{s,d,w} \tag{1}$$

Предмет ($1 \le s,d \le N, 1 \le w \le W$ ако не е посочено): Търсенето между двойката възли (s,d) е удовлетворено по основните пътища.

$$2\ \times dem_{s,d} = \sum_{w=1}^{W}\sum_{\forall e:<s,e>\in Links} F_{s,e}^{s,d,w} \tag{2}$$

$$2\ \times dem_{s,d} = \sum_{w=1}^{W}\sum_{\forall i:<i,d>\in Links} F_{i,d}^{s,d,w} \tag{3}$$

$$F_{i,s}^{s,d,w} = 0\ \forall < i,s > \in Links$$

$$F_{d,e}^{s,d,w} = 0 \; \forall < d, e > \in Links$$

Запазване на потока при ограничение за непрекъснатост на дължината на вълната на основните пътища.

$$\sum_{\forall i:<i,j>\in Links} F_{i,j}^{s,d,w} \; - \; \sum_{\forall e:<j,e>\in Links} F_{j,e}^{s,d,w} \; = 0 \tag{4}$$

$$1 \; \leq j \; \neq s, d \; \leq \; N$$

Дължина на вълната на връзка може да се използва само от един основен път или един резервен път.

$$\sum_{1\leq s,d\leq N} F_{i,j}^{s,d,w} \; \leq \; 1 \;\; \forall < i, j > \in Links \tag{5}$$

Когато връзката е $i \; \rightarrow \; j$ е неуспешна, броят на неуспешните светлинни пътища между двойката източник-местоназначение (s, d) не трябва да надвишава търсенето между тях. [25, 26, 31]

$$\sum_{w=1}^{W} F_{i,j}^{s,d,w} \; \leq \; dem_{s,d} \; \forall < i, j > \in Links \tag{6}$$

ILP2: Защита чрез споделения път

Цел: Намаляване на общия брой връзки с дължина на вълната.

$$\sum_{w=1}^{W} \sum_{<i,j>\in Links} (m_{i,j}^{w} + \; \sum_{1\leq s,d\leq N} F_{i,j}^{s,d,w}) \tag{7}$$

Предмет (1 ≤ s, d ≤ N, 1 ≤ w ≤ W, ако не е посочено): Търсенето между всяка двойка възли (s, d) се задоволява по основните пътища.

$$dem_{s,d} \; = \; \sum_{w=1}^{W} \sum_{\forall e:<s,e>\in Links} F_{s,e}^{s,d,w} \tag{8}$$

$$dem_{s,d} \; = \; \sum_{w=1}^{W} \sum_{\forall i:<i,d>\in Links} F_{i,d}^{s,d,w} \tag{9}$$

$$F_{i,s}^{s,d,w} = 0 \; \forall < i, s > \in Links$$

$$F_{d,e}^{s,d,w} = 0 \; \forall < d, e > \in Links$$

Запазване на потока от данни при ограничение за непрекъснатост на дължината на вълната на първичните пътища.

$$\sum_{\forall i:<i,j>\in Links} F_{i,j}^{s,d,w} \; - \; \sum_{\forall e:<j,e>\in Links} F_{j,e}^{s,d,w} \; = \; 0 \tag{10}$$

$$1 \; \leq j \; \neq s, d \; \leq \; N$$

Ограничения за броя на пренасочените светлинни пътеки между двойка възли (s, d), когато връзката е $i \; \rightarrow \; j$ е неуспешна. [16, 17, 20, 21]

$$\sum_{w=1}^{W} F_{i,j}^{s,d,w} = \sum_{w=1}^{W} \sum_{\forall e:<s,e>\in Links} \delta_{s,e,i,j}^{s,d,w} \quad (11)$$

$$\forall < i,j > \in Links$$

$$\sum_{w=1}^{W} F_{i,j}^{s,d,w} = \sum_{w=1}^{W} \sum_{\forall p:<p,d>\in Links} \delta_{p,d,i,j}^{s,d,w} \quad (12)$$

$$\forall < i,j > \in Links$$

$$\delta_{p,s,i,j}^{s,d,w} = 0 \; \forall < p,s >, < i,j > \in Links$$

$$\delta_{d,e,i,j}^{s,d,w} = 0 \; \forall < d,e >, < i,j > \in Links$$

Запазване на потока от данни при ограничение за непрекъснатост на дължината на вълната на резервните пътища. [18, 25]

$$\sum_{\forall p:<p,q>\in Links} \delta_{p,s,i,j}^{s,d,w} - \sum_{\forall e:<q,e>\in Links} \delta_{q,e,i,j}^{s,d,w} = 0 \quad (13)$$

$$1 \le q \ne s,d \le N, < i,j > \in Links \; (4.20)$$

Основният път и неговият резервен път не трябва да са свързани чрез връзка.

$$\delta_{i,j,i,j}^{s,d,w} = 0 \; \forall < i,j > \in Links$$

Два светлинни потока, защитени от една и съща дължина на вълната w на една и съща връзка $p \rightarrow q$ не могат да преминат през една и съща връзка $i \rightarrow j$.

$$\sum_{1\le s,d\le N} \delta_{p,q,i,j}^{s,d,w} \le 1 \; \forall < p,q >, < i,j > \in Links \quad (14)$$

Ограничения, показващи дали дадена дължина на вълната w на връзката $p \rightarrow q$ се използва от някакъв защитен път.

$$m_{p,q}^{w} \le \sum_{1\le s,d\le N} \sum_{\forall <i,j>\in Links} \delta_{p,q,i,j}^{s,d,w} \quad (15)$$

$$\forall < p,q > \in Links$$

$$N \times N \times E \times m_{p,q}^{w} \ge \sum_{1\le s,d\le N} \sum_{\forall <i,j>\in Links} \delta_{p,q,i,j}^{s,d,w} \quad (16)$$

$$\forall < p,q > \in Links$$

Вълната w на $i \rightarrow j$ може да се използва само като основен път или защитени пътища.

$$m_{i,q}^{w} + \sum_{1\le s,d\le N} F_{i,j}^{s,d,w} \le 1 \; \forall < i,j > \in Links \quad (17)$$

Горната формулировка изпълнява защита от повреда, т.е. всеки сценарий на повреда съответства на различни пътища на защита, което усложнява контрола и управлението на връзката. На всяка връзка се присвояват някои защитни ресурси, независимо къде възниква повредата, като се добавят ограничения (18) до (20). Ограниченията показват дали дадена дължина на вълната w на връзката $p \rightarrow q$ се използва от някакъв защитен път между двойка възли (s, d).

$$S_{p,q}^{s,d,w} \leq \sum_{\forall<i,j>\in Links} \delta_{p,q,i,j}^{s,d,w} \quad \forall< p,q >\in Links \tag{18}$$

$$E \times S_{p,q}^{s,d,w} \geq \sum_{\forall<i,j>\in Links} \delta_{p,q,i,j}^{s,d,w} \quad \forall< p,q >\in Links \tag{19}$$

Основният път не трябва да има повече от един защитен път.

$$\sum_{\forall e:<s,e>\in Links} F_{s,e}^{s,d,w} \geq \sum_{\forall e:<s,e>\in Links} S_{s,e}^{s,d,w} \tag{20}$$

ILP2 предоставя общ „шаблон“ за формулиране на задачата с RWA чрез различни схеми на защита. ILP при защита на специализиран път, споделен път, специализирана връзка и защита на споделена връзка със или без ограничение за непрекъснатост на дължината на вълната могат лесно да бъдат извлечени от ILP2.

ILP3: Защита на споделена връзка

При сценарий за защита чрез споделена връзка, всяка връзка $i \rightarrow j$ на някакъв основен път p има защитна верига от възел i до j, която трябва да бъде на същата дължина на вълната като дължината на вълната на p.

$$F_{i,j}^{s,a,w} \& = \sum_{\forall e:<i,e>\in \text{Links}} \delta_{i,e,i,j}^{s,a,w} \tag{21}$$

$$\forall 1 \leq w \leq W, < i,j > \in \text{ Links}$$

$$F_{i,j}^{s,d,w} = \& \sum_{\forall p:<p,j>\in \text{Links}} \delta_{p,j,i,j}^{s,d,w} \tag{22}$$

$$\forall 1 \leq w \leq W, < i,j > \in \text{ Links}$$

Когато е налице ограничение за непрекъснатост на дължината на вълната, ограниченията за запазване на потока от данни, трябва да се поддържат за всяка дължина на вълната. [12, 28, 34]

ILP4: Защита чрез споделен път

Чрез разширяване на ILP1 се увеличава способността за преобразуване на дължината на вълната чрез отпускане на ограниченията за непрекъснатост на дължината на вълната, както следва. Запазва се потока по основните пътища.

$$\sum_{w=1}^{W} \sum_{\forall i:<i,j>\in Links} F_{i,j}^{s,d,w} - \sum_{w=1}^{W} \sum_{\forall e:<j,e>\in \text{Links}} F_{j,e}^{s,d,w} = 0 \quad 1 \leq j \neq s,d \leq N \tag{23}$$

Запазване на потока на данни по защитните пътища:

$$\sum_{w=1}^{W} \sum_{\forall p:<p,q>\in Links} \delta_{p,q,i,j}^{s,d,w} - \sum_{w=1}^{W} \sum_{\forall e:<q,e>\in \text{Links}} \delta_{q,e,i,j}^{s,d,w} = 0 \quad 1 \le q \ne s,d \le N, <i,j> \in Links \tag{24}$$

ILP5: Защита чрез споделена връзка

Този случай може лесно да бъде извлечен от ILP2. Освен същите направени промени, се отпускат ограниченията и за непрекъснатост на дължината на вълната в (25) и (26), както следва.

$$\sum_{w=1}^{W} F_{i,j}^{s,d,w} = \sum_{w=1}^{W} \sum_{\forall e:<i,e>\in \text{Links}} \delta_{i,e,i,j}^{s,d,w} \tag{25}$$

$$\forall 1 \le w \le W, <i,j> \in \text{Links}$$

$$\sum_{w=1}^{W} F_{i,j}^{s,d,w} = \sum_{w=1}^{W} \sum_{\forall p:<p,j>\in \text{Links}} \delta_{i,e,i,j}^{s,d,w} \tag{26}$$

$$\forall 1 \le w \le W, <i,j> \in \text{Links}$$

Евристични алгоритми

SWBF алгоритмите биват описани накратко както за мрежи с непрекъсната дължина на вълната, така и за мрежи с конвертируема дължина на вълната. В мрежа, конвертируема по дължина на вълната, „ширината“ на кандидат резервен път p_b за първичен път p_w се изчислява по следните уравнения.

$$width\ (p_b, p_w) = \underset{l_b \in p_b}{Min} width(l_b, p_w) \tag{27}$$

$$width(l_b, p_w) = \underset{l_w \in p_w}{Min}\ width(l_b, l_w) \tag{28}$$

$$\text{width}(l_b, l_w) = 1 - \frac{h_{l_b}^{l_w}}{\text{Max}_l\, h_{l_b}^{l}} \tag{29}$$

В уравненията l_b и l_w и l са връзки. В (29), $h_{l_b}^{l_w}$ е броят на дължините на вълните на връзка l_b, която може да се използва за защита на връзката l_w, и Max $h_{l_b}^{l}$ е общият брой дължини на вълните на връзката l_b които са запазени за защита. Като се вземе под внимание, че $h_{l_b}^{l_w} <$ Max $h_{l_b}^{l}$, $0 < width\ (l_b, l_w) < 1$. От уравнения (27) и (28), всички стойности на ширината са между 0 и 1.

Ако $h_l^l =$ Max $h_{l_b}^{l}$, тогава ширина (l_b, l_w) = 0 и трябва да се използва нова дължина на вълната i, ако l_b е избрано в резервния път за основния път, който

съдържа връзка l_w. Най-широкият път е пътят, който има най-голям брой дължини на вълните, които могат да бъдат повторно използвани (споделени). Ако съществуват два такива пътя, ще бъде избран по-късият. [7, 10, 11, 24, 27]

В мрежа с непрекъсната дължина на вълната се разширява определението за „ширина“ на път до „ширината“ на път на определена дължина на вълната. „Ширината“ на резервен път p_b по дължина на вълната λ^* за първичен път p_w се изчислява по следните уравнения.

$$\text{width}\,(p_b, \lambda^*, p_w) = \min_{l_b \in p_b} width(l_b, \lambda^*, p_w) \tag{30}$$

$$\&\ \text{width}\,(l_b, \lambda^*, p_w) = \min_{l_w \in p_w} width(l_b, \lambda^*, l_w) \tag{31}$$

$$\text{width}(l_b, \lambda^*, l_w) = \begin{cases} 0 & \text{ако } \lambda^* \text{ на } l_b \text{ защитава } l_w \\ 1 & \text{в противен случай} \end{cases} \tag{32}$$

При дадена заявка за свързване може първо да се приложи стандартен алгоритъм за най-кратък път, като алгоритъмът на Дейкстра, за изчисляване на основния път. Нека се вземе под внимание, че в някои мрежи, ако най-краткият път е избран като основен път за дадена двойка възли, не може да бъде намерен резервен път с несвързани връзки, въпреки че съществува двойка пътища с несвързани връзки в мрежата между двата възела .

След като основния път бъде намерен, за защита на споделения път, ширината на връзките в мрежата може да бъде изчислена с помощта на уравнения (28) и (29), или (31) и (32). Алгоритъмът на Белман-Форд може да се приложи с по-широк път или път с еднаква ширина, но по-къса дължина. Уравнения (27) и (30) се използват за изчисляване на ширината на път въз основа на ширината на връзките, през които преминава. [8, 9, 12, 28, 34]

Защита на споделена връзка

При защита на споделена връзка може първо да се приложи стандартен алгоритъм за най-кратък път, за да се изчисли основният път между дадена двойка възли. За всяка връзка в основния път се търси най-краткият и най-широк резервен път (наричан също резервен цикъл) между двата крайни възела. Ако мрежата е конвертируема по дължина на вълната, (29) се прилага за изчисляване на ширината на защитна връзка по отношение на защитената връзка. Следното уравнение показва как да се изчисли ширината на пътя p_b, който защитава връзката l_w:

$$\text{width}\,(p_b, p_w) = \min_{l_b \in p_b} width(l_b, p_w)$$

Ако мрежата е с непрекъсната дължина на вълната, същата дължина на вълната, използвана в основния път, ще се използва на резервните пътища. Нека

се приеме, че дължината на вълната λ* се използва на основния път. Уравнение (32) се използва за изчисляване на ширината на защитна връзка на дължина на вълната λ* по отношение на защитената връзка. Следното уравнение показва как да се изчисли ширината на пътя p_b, който защитава връзката l_wна дължина на вълната λ*:

$$\text{width}\,(p_b, \lambda^*, p_w) = \min_{l_b \in p_b} width(l_b, \lambda^*, p_w)$$

ILP формулировките и евристичните алгоритми на задачата с Маршрутизирането и присвояването на дължината на вълната (RWA) в WDM Mesh мрежи е с три защитни схеми: специализиран път, споделен път и защита чрез споделена връзка. Резултатите от евристиките на защитата на предназначения път и защитата на споделения път са много близки до тези от съответните ILP. Евристиката за защита на споделена връзка е по-малко оптимална в сравнение с другите евристики. [1, 2, 21]

ЛИТЕРАТУРА

[1] Denev D. Comparative Analysis Between Wireless and Li-Fi, MATTEH 2022, Conference proceeding, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 89-94

[2] Denev D. Low Energy Real-Time Routing, Annual University Scientific Conference, Proceedings of National Military University „Vasil Levski“, Veliko Tarnovo, 2022, ISSN 2367-7481, pp. 1267- 1276

[3] Denev D., Synthesis and Analysis of Linear Discrete and Time Invariant Systems Used in the Field of Communications using Matlab and Signal Processing Toolbox, Journal scientific and applied research, vol. 22, 2022 International Journal, 2022, ISSN 1314-6289, pp. 72-80

[4] Perspective. San Francisco, CA: Morgan Kaufmann, 2 ed., 2002.

[5] T. E. Stem and K. Bala, Multiwavelength Optical Networks: A Layered Approach. Reading, MA: Addison-Wesley, 1999.

[6] 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.

[7] D. Banerjee, Design and Analysis of Wavelength-Routed Optical Networks. PhD thesis, University of California, Davis, Department of Computer Science, 1996.

[8] R. A. Barry and S. Subramaniam, "The MAX-SUM wavelength assignment algorithm for WDM ring networks;' in Proc. Optical Fiber Communication Conference and Exhibit (OFC '97), (Dallas, TX), pp. 121-122, Feb. 1997.

[9] G. Jeong and E. Ayanoglu, "Comparison of

[10] wavelength-interchanging and wavelength- selective cross-connects in multiwavelength all-optical networks," in Proc. IEEE INFO COM '96, vol. 1, (San Francisco, CA), pp. 156-163, Mar. 1996.

[11] Ivan Ivanov, Victor Lilov, Daniel Denev, Traffic Reporting and the Ability to Optimize LAN, MATTEH 2018, CONFERENCE PROCEEDING, vol. 1 Communication and Computer Technologies, ISSN 1314-3921, pp. 331-335

[12] Denev D. 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, pp. 75-79

[13] Denev D., Analytical Study of the Delay Introduced as a Result of Encryption/Decryption of Voice Transmitted over a VPN Networks, Journal scientific and applied research, vol. 20, 2021 International Journal, 2021, ISSN 1314-6289, pp. 73-77

[14] E. Karasan and E. Ayanoglu, "Effects of wavelength routing and selection algorithms on wavelength conversion gain in WDM optical networks," IEEE/ACM Transactions on Networking, vol. 6, pp. 186-196, Apr. 1998.

[15] Gerstel, "Opportunities for optical protection and restoration," in Proc. Optical FiberCommunication Conference and Exhibit (OFC '98), vol. 2, (San Jose, CA), pp. 269-270, Feb. 1998.

[16] T. Wu, Fiber Network Survivability. Boston, MA: Artech House, 1992.

[17] T. Wu, "Emerging technologies for fiber network survivability," IEEE Communications Magazine, pp. 58-74. Feb. 1998.

[18] Gerstel and R. Ramaswami, "Optical layer survivability—an implementation perspective," IEEE Journal on Selected Areas in Communications, vol. 18, pp. 1885-1899, Oct. 2000.

[19] J. W. Suurballe and R. E. Tarjan, "A quick method for finding shortest pairs of disjoint paths," Networks, vol. 14, pp. 325-336, 1984.

[20] B. T. Doshi, S. Dravida, P. Harshavardhana, 0. Hauser, and Y. Wang, "Optical network design and restoration," Bell Labs Technical Journal, vol. 4, pp. 58-84, Jan.-Mar. 1999.

[21] G. Sahin and M. Azizoglu, "Optical layer survivability: single service-class case," in Proc. SPIE (Opticomm 2000: Richardson, TX, Oct. 2000), vol. 4233, pp. 267-278, 2000.

[22] S. Sengupta and R. Ramamurthy, "From network design to dynamic provisioning and restoration in optical cross-connect mesh networks: an architectural and algorithmic overview," IEEE Network, vol. 15, pp. 46-54, Jul.-Aug. 2001.

[23] H. Zang and B. Mukherjee, "Connection management for survivable wavelength-routed WDM mesh networks," SPIE Optical Networks Magazine, vol. 2, pp. 17-28, Sept. 2001.

[24] C. Guillemot, M. Renaud, P. Gambini, and et al., "Transparent optical packet switching: The european acts keops project approach," IEEE/OSA Journal of Lightwave Technology, vol. 16, pp. 2117-2134, Dec. 1998.

[25] I. Chlamtac, A. Fumagalli, L. G. Kazovsky, and et al., "Cord: contention resolution by delay lines," IEEE/OSA Journal of Lightwave Technology, vol. 14, pp. 1014-1029, June 1996.

[26] L. Zucchelli, M. Burzio, and P. Gambini, "New solutions for optical packet delineation and synchronization in optical packet switched networks," in Proc., 22nd European Conference on Optical Communication (ECOC '96), vol. 3, (Oslo, Norway), pp. 301304, Sept. 1996.

[27] J. lness, Efficient Use of Optical Components in WDM-Based Optical Networks. PhD thesis, University of California, Davis, Nov. 1997.

[28] K.-C. Lee and V. 0. K. Li, "A wavelength-convertible optical network," IEEE/OSA Journal of Lightwave Technology, vol. 11, pp. 962-970, May-June 1993.

[29] S. Ramamurty and B. Mukherjee, "Survivable WDM mesh networks, part I — protection," in Proc. IEEE INFOCOM '99, vol. 2, (New York, NY), pp. 744-751, Mar. 1999.

[30] R. R. lraschko and W. D. Grover, "A highly efficient path-restoration protocol for management of optical network transport integrity," IEEE Journal on Selected Areas in Communications, vol. 18, pp. 779-794, May 2000.

[31] G. Ellinas, S. Rong, A. Hailemariam, and T. E. Stern, "Protection cycle covers in optical networks with arbitrary mesh topologies;' in Proc. Optical Fiber Communication Conference and Exhibit (OFC '00), vol. Th, (Baltimore, MD), pp. 213-215, Mar. 2000.

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

[33] W. J. Goralski, SONET. New York, NY: McGraw-Hill, 2 ed., 2000.

[34] 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.

[35] 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.

[36] C. Huitema. Routing in the Internet. Englewood Cliffs, NJ: Prentice-Hall, 1995.

[37] S. Makam, V. Sharma, K. Owens, and C. Huang, "Protection/restoration of MPLS networks." IETF draft (work in progress), Oct. 1999.

[38] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part 11 - restoration," in Proc. IEEE International Conference on Communications (ICC '99), vol. 3. (Vancouver. Canada), pp. 2023-2030, June 1999.

СОЦИАЛНИТЕ МЕДИИ – ГЛОБАЛЕН ИЗТОЧНИК НА ИНФОРМАЦИЯ И МАНИПУЛАЦИЯ

Валентина С. Хорозова

SOCIAL MEDIA – A GLOBAL SOURCE OF INFORMATION AND MANIPULATION

Valentina S. Horozova

ABSTRACT: *The article discusses the role and impact of social media on security. A review and analysis of up-to-date statistical data and research of world-renowned and recognized companies in the field under consideration has been made. Attention has been paid to the total consumption of the Internet, of the users of social networks worldwide for the last years. Through the prism of their analysis, the main trends and perspectives are brought out. Next, the information that is created and disseminated through social networks in a global aspect is considered. The focus is mainly on manipulated information, and especially its role and influence on processes that take place both in social networks and cyberspace, and in real life. Based on this, proposals have been made to recognize misinformation and reduce its manipulative impact on a wide range of people.*

KEYWORDS: *Information, Socila media, Social networks, Manipulation, Disinformation, security.*

Въведение

Живеем в свят, в който социалните медии са неизменна част от живота ни. Постепенно те се превърнаха в ежедневие както за малките, така и за по-големите потребители на Интернет, както за ученици, студенти, така и за предприемачи, политици, дипломати, световни лидери, дори и престъпници. Освен основната си роля – канал за комуникация, социалните медии се трансформираха в глобализационен фактор, давайки възможност на всеки техен потребител да се превърне в гражданин на света, с перспектива да влияе или дори да предизвиква обществени процеси, нагласи, тенденции и прояви, които могат да варират от чисто благородни каузи до радикални прояви и действия, които далеч надхвърлят киберпространството и дори в нередки случай преодоляват национални, езикови бариери и ограничения.

Социалните медии – същност и тенденции за развитие

Според Cambridge dictionary социалните медии представляват уебсайтове и компютърни програми, които позволяват на хората да комуникират и споделят информация в интернет, използвайки компютър или мобилен телефон.[1]

Merriam-Webster dictionary приема социалните медии като форми на електронна комуникация (като уебсайтове за социални мрежи и микроблогинг), чрез които потребителите създават онлайн общности за споделяне на информация, идеи, лични съобщения и друго съдържание (като видеоклипове).[2]

Според Oxford dictionary социалните медии, това са уеб сайтове и софтуерни програми, използвани за социални мрежи. Застъпено е мнението, че социалните медии променят начина, по който хората общуват, работят и пазаруват. Безспорен пример за такива медии са Facebook и Twitter. [3]

Vocabulary dictionary тълкува социалните медии като уебсайтовете и приложенията, използвани за споделяне или създаване на онлайн съдържание, като съобщения, снимки и видеоклипове.[4]

За сведение, термина социални медии липсва в Българския тълковен речник.[5]

Както е видно от представените дефиниции, терминът социални медии носи със себе си и налага нова форма на комуникация, на споделяне на информация. Това предопределя дълбоки и същности промени в начина на живот на отделния човек, в начина на работа, в начина и пътя на развитие на света и цялото човечество.

Големият интерес към социалните мрежи и нарастващия им брои на потребители, ги предопределя като един от основните и търсени източници на всякакъв вид информация. Всичко това поставя на дневен ред друг проблем и поредица от въпроси – Каква част от информацията, която се създава, споделя и разпространява в социалните медии е достоверна? Каква част от нея е манипулирана и каква част от манипулираната такава цели да въведе в заблуждение широкия кръг от потребителите си и/или да провокира директни действия?

В търсене на отговор на така поставените въпроси, ще обърнем поглед към официалната статистика. Съгласно нея населението на света преминава 8 милиарда през ноември 2022 г. В началото на 2023 година достига 8,01 милиарда,

[1]https://dictionary.cambridge.org/dictionary/english/socialmedia?q=SOCIAL+MEDIA посетен на 30.01.2024 г.
[2]https://www.merriam-webster.com/dictionary/social%20media посетен на 30.01.2024 г.
[3]https://www.oxfordlearnersdictionaries.com/definition/english/socialmedia?q=SOCIAL+MEDIA+ посетен на 30.01.2024 г.
[4] https://www.vocabulary.com/dictionary/social%20media посетен на 30.01.2024 г.
[5]https://rechnik.chitanka.info/w/%D1%81%D0%BE%D1%86%D0%B8%D0%B0%BB%D0%BD%D0%B8%20%D0%BC%D0%B5%D0%B4%D0%B8%D0%B8 посетен на 30.01.2024 г.

а в началото на 2024 г. вече е 8,08 милиарда.[6] Тези данни сами по себе си са интересни, но разгледани през призмата на активността на киберпотребителите, са вече наистина впечатляващи, а именно:

- над 5,44 милиарда души използват мобилни телефони в началото на 2023 г., което се равнява на 68 процента от общото световно население;
- интернет потребители са над 5,16 милиарда, което означава, че 64,4% от общото население на света вече е онлайн;
- потребители на социални медии по света са 4,76 милиарда, което се равнява на малко под 60% от общото население на света. [7]

Тези данни прочетени през дигиталното състояние и употреба в България за 2023г., приемат следния вид:

- в началото на 2023 г. в България има 5,59 млн. интернет потребители;
- за гореспоменатия период потребителите на социалните медии в България са 4,42 милиона, което се равнява на 65,7 процента от общото население.
- клетъчни активните мобилни връзки в България за посочения период са общо 9,79 милиона, което се равнява на 145,5 процента от общото население.[8]

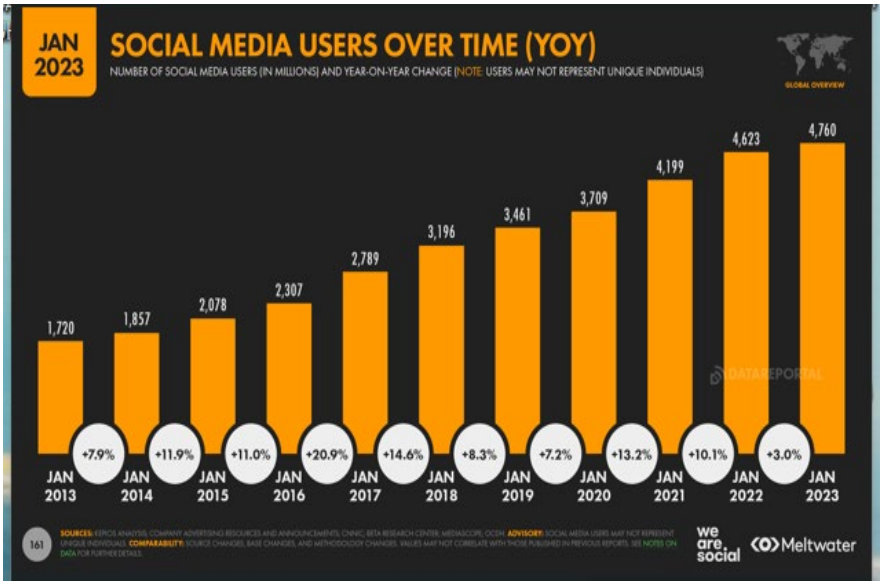
Посочените данни както в световен мащаб, така и за България, само загатват и леко разкриват, че силната вълна на дигитализация, на киберглобализация и на киберсвързаността, която започна по време на пандемията от Ковид-19 все още се наблюдава. Тя се характеризира с леко забавени темпове, но все още е факт. Интересът към социалните медии се превърна в трайно цифрово поведение на потребителите. Това се потвърждава и от официалните данни и анализ Kepios [9]. В тях се разкрива, че общият брой на потребителите на социалните медии в световен мащаб се е увеличил с близо 30% от началото на пандемията, което се равнява на повече от **1 милиард** нови потребители през последните 3 години.

Както е видно от фигура №1 тази тенденция се потвърждава и от официалния доклад за глобалния преглед: Digital 2023. Впечатление прави фактът, че интересът на потребителите се покачва почти двойно за периода от 2020 и 2021г. в сравнение с предходните дванадесет месеца. Тази обща положителна посока се затвърждава и за следващия разглеждан период - 2021 и 2022 г.

Въпреки установения голям ръст по време на пандемията от Ковид-19, ставаме свидетели на продължаващо положително отношение към социалните

[6] https://www.worldometers.info/bg/ посетен на 30.01.2024 г.
[7]https://datareportal.com/reports/digital2023globaloverviewreport?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=Bulgaria&utm_content=Global_Promo_Block посетен на 30.01.2024 г.
[8] https://datareportal.com/reports/digital-2023-bulgaria посетен на 30.01.2024 г.
[9]https://kepios.com/?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=Bulgaria&utm_content=Kepios_Home_Link посетен на 29.01.2024 г.

медии и отчитане на нови техни потребители. На фона на отчетения спад в различни аспекти на онлайн активността в световен мащаб, интересът към социалните мрежи продължава да отбелязва положителна стойност. Макар и с леки темпове (само 3 % за периода 2022 и 2023 г), важното обстоятелство тук е, че като цяло се отчита положителна нагласа сред потребителите, без да се забелязва отлив сред тях.



Фиг. 1. *Потребители на социалните медии по години*[10]

Посочените данни са напълно логично и естествено развитие на глобалните процеси и тенденции с оглед на лавинообразните революционни промени, през които преминава света и човечеството като цяло. За много кратък период от време – от средата на XX век Третата индустриална революция, известна още като информационна, поднася редица предизвикателствата (киберинформация, киберпространство, киберпрестъпления, кибер рискове и заплахи, хибридни войни, масова дезинформация и други).

Въпреки това, развитието в глобален аспект не спира. През 2011 г. според някои специалисти, изследователи и учени[11], вече сме на прага на поредното

[10]https://datareportal.com/reports/digital2023globaloverviewreport?utm_source=Data Reportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=Bulgaria&utm_content=Global_Promo_Block посетен на 30.01.2024 г.

[11] Клаус, Шваб. Четвъртата индустриална революция. Издателска къща „Хермес“, превод от английски Валентина Рашева-Джейвънс, 2016 г

революционно предизвикателство – Индустрия 4.0. Тя носи със себе си вълна от нови въпроси, нови колебания, нови дисбаланси в сферата на сигурността.

Социланите медии – източник на влияние и/или манипулация

Актуалните събития от последните години, показаха, че на международната сцена вече има нов, утвърден и все по-влиятелен фактор - именно социалните мрежи. Те постепенно разширяват силата и мощта си и се оформят като сериозен двигател върху формирането на обществените нагласи и процеси в редица държави. Новите достижения и технологии, заедно със социалните медии създават перспективи за събиране на данни, за наблюдение, дори в нередки случаи и контрол над гражданите.

Устойчивият интерес и положителна тенденция към социалните медии намират логично обяснение след като обърнем внимание на едни от последните изследвания на GWI[12]. В тях се посочва, че в световен мащаб се забелязва увеличаване на времето, в което потребителите на възраст между 16 и 64 години, прекарват ежедневно в социалните медии. Интересен факт, който заслужава внимание е, най-продължителното време, в което обикновения интернет потребител в активна трудова възраст, използва социални платформи, а именно рекордните 21 часа на ден.

В тази връзка, съвсем естествено е търсенето на най-доброто информационно обезпечаване от органа по назначаване в МВР, а именно: обявленията за конкурси за постъпване на работа в министерството, задължително се публикуват в специализирана страница в интернет или портал за търсене на работа, както и на страницата на МВР в интернет, раздел „Постъпване на работа в МВР – конкурси“[13].

Както е видно от фиг. 2, интернет потребителите прекарват все повече време в социалните медии. Тези данни напълно респондират с резултатите представени във фиг. 1.

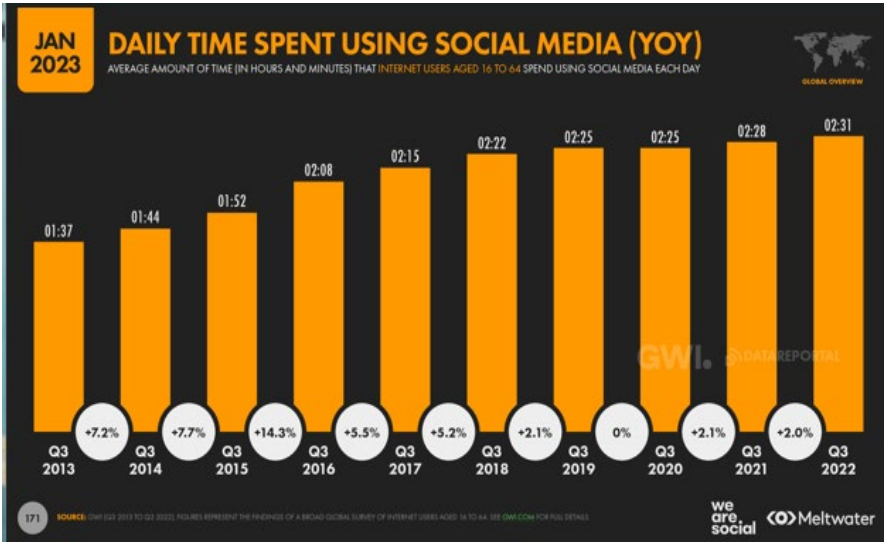
На фона на тези данни впечатление прави и фактът, че "намирането на информация" все още е водещата причина, поради която хората използват интернет днес. Едни от последните изследвания на GWI[14] установява, че 6 от 10 потребители на интернет в трудоспособна възраст (57,8%) все още се отнасят до онлайн ресурси, когато търсят информация, преди:

- връзка с приятели и семейство (53,7%);
- оставане в крак с новини и текущи събития (50,9%); и
- гледане на видеоклипове (49,7%).[15]

[12]https://www.gwi.com/bookdemo?utm_source=kepios&utm_medium=referral&utm_campaign=2023+Kepios+Global+Audiences посетен на 30.01.2024 г.
[13] Желев, Ант., Основи на държавната служба по Закона за Министерството на вътрешните работи, С., 2024, стр. 162-163.
[14]https://www.gwi.com/bookdemo?utm_source=kepios&utm_medium=referral&utm_campaign=2023+Kepios+Global+Audiences посетен на 30.01.2024 г.
[15] Пак там посетен на 30.01.2024 г.

Логичен ефект от глобалното използване на интернет и социалните медии е, че те заедно разкриват ново поле за информационен обмен. Особеното там е, че спецификите на социалните медии могат да бъдат използвани с деструктивни и подривни цели. Това предопределя и нова сфера на действие на:

- разузнаването, както на държавно, така и на частно ниво;
- организираната престъпност;
- тероризъм;
- психологически операции за въздействие;
- операции по целенасочено дезинформиране;
- операции по оказване на влияние;
- операции за пораждане и насаждане на полюсни настроения сред населението - страх, агресия, религиозна и етническа нетърпимост и конфликтност и други.



Фиг. 2. *Средно време (в часове и минути), което потребителите на интернет, на възраст между 16 и 64 години, прекарват в социални медии всеки ден*[16]

Според Cambridge dictionary манипулацията е контролиране на някого или нещо в своя полза, често несправедливо или нечестно.[17]

[16]https://datareportal.com/reports/digital2023globaloverviewreport?utm_source=Data Reportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023& utm_term=Bulgaria&utm_content=Global_Promo_Block посетен на 30.01.2024 г.
[17] https://dictionary.cambridge.org/dictionary/english/manipulation - посетен на 30.01.2024 г

Merriam-Webster предлага няколко тълкувания на термина манипулация. Релевантни за настоящето изследване са: 1. да управлявате или използвате умело; 2. да контролирате или да играете чрез изкусни, несправедливи или коварни средства, особено за собствена полза.[18]

Според Oxford dictionary манипулацията предполага поведение, което контролира или влияе на някого / нещо, често по нечестен начин, така че отсрещната страна да не го осъзнава. [19]

Vocabulary dictionary тълкува манипулацията като умело боравене, контролиране или използване на нещо или някой.[20]

Както е видно от предствените определение манипулацията преполага тайно оказване на влияние върху някой и/или нещо, в ползва за лична изгода или за постигане на лична цел. Пречупено през призмата на киберпространството и социалните медии, манипуаливното въздействие безспорно може да се превърне в опасно, трудно контролируемо оръжение.

Целият манипулативен процес и дезинформацията могат да бъдат продукт на тайни лица, групи и организации, с прикрити интереси, цели и мотиви. Процесът може да бъде окачествен като специфична форма на управление със силно въздействащ характер и ефект. Използват се широк спектър на похвати за оказване на въздействие, които намират добра почва в киберпространството и социалните медии.

За да постигне целта си, манипулативният процес е насочен върху убежденията на хората. Обект на въздействие при него е не разума, а емоциите на читателя. Чрез постепенно, поетапно, но постоянно наслагване на различни внушения се постига метода на повлияване върху хората. Възможно е манипулативният процес да бъде насочен не само към неприятелски, но и към неутрални и дори приятелски настроени групи и/или лица.

Напълно естествено е след като ставаме свидетели на появата на нов вид деструктивно и престъпно поведение в киберпространството с помощта на социалните медии, да се засили взаимодействието и координацията между службите за сигурност на различни държавни и международни институции. Доказателство за това сочи факта, че повече от половината от всички наказателни разследвания днес включват трансгранично искане за достъп до електронни доказателства (като данни от услуги за съобщения или имейл или социални медии)[21].

Заключение

[18]https://www.merriam-webster.com/dictionary/manipulation - посетен на 30.01.2024 г

[19]https://www.oxfordlearnersdictionaries.com/definition/english/manipulation?q=manipulation – посетен на 30.01.2024 г

[20] https://www.vocabulary.com/dictionary/manipulation - посетен на 30.01.2024 г

[21] Трендафилов, Ф. Служители за връзка в правоприлагащите организации, издател: Академия на МВР, 2023 г. ISBN 978-954-348-237-5, стр. 56

От всичко посочено до тук може да се направи изводът, че социалните медии и мрежи от обикновена комуникационна среда и канал за връзка вече са утвърден фактор не само в киберпространството. В последно време те са непредсказуем играч, с който се налага да се съобразяват почти всички актьори на социално-политическата сцена.

Прогнозата е, че социалните медии ще затвърдят характера си и значението си на възможен генератор на промени, на проводник на влияние(манипулативно, прикрито, тайно) върху формирането, протичането и насочването на обществени процеси от различен характер, сила и мощ, а от там и неизменна роля при гарантирането и поддържането на сигурността във всичките й нива.

Всичко това напълно обосновано описва прехода към нови институции за сигурност, които търсейки адекватен отговор и ефективно противодействие на разнородните, асиметрични и трудно предсказуеми процеси в киберпространството, ще разполагат и действат с нови методи и средства.

ЛИТЕРАТУРА

[1] Jelev, Ant., Basics of the civil service under the Law on the Ministry of the Interior, Sofia., 2024, ISBN 978-954-28-4552-2, page 162-163

[2] Klaus Shvab., The fourth industrial revolution. Hermes Publishing House, translated from English by Valentina Rasheva-Javons,, 2016 г

[3] Trendafilov, F., Law Enforcement Liaison Officers, Publisher: Ministry of Internal Affairs Academy, 2023 г. ISBN 978-954-348-237-5, page. 56

[4] https://dictionary.cambridge.org/dictionary/english/social-media?q=SOCIAL+MEDIA+ -посетен на 30.01.2024 г.

[5] https://www.merriam-webster.com/dictionary/social%20media - посетен на 30.01.2024 г.

[6] https://www.oxfordlearnersdictionaries.com/definition/english/social-media?q=SOCIAL+MEDIA+ посетен на 30.01.2024 г.

[7] https://www.vocabulary.com/dictionary/social%20media посетен на 30.01.2024 г.

[8] https://rechnik.chitanka.info/w/%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D0%BD%D0%B8%20%D0%BC%D0%B5%D0%B4%D0%B8%D0%B8 посетен на 30.01.2024 г.

[9] https://www.worldometers.info/bg/ посетен на 30.01.2024 г.

[10] https://datareportal.com/reports/digital-2023-global-overview-report?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=Bulgaria&utm_content=Global_Promo_Block посетен на 30.01.2024 г.

[11] https://datareportal.com/reports/digital-2023-bulgaria посетен на 30.01.2024 г.

[12] https://kepios.com/?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=Bulgaria&utm_content=Kepios_Home_Link посетен на 30.01.2024 г.

[13] https://www.gwi.com/book-demo?utm_source=kepios&utm_medium=referral&utm_campaign=2023+Kepios+Global+Audiences посетен на 30.01.2024 г.

[14] https://dictionary.cambridge.org/dictionary/english/manipulation - посетен на 30.01.2024 г

[15] https://www.merriam-webster.com/dictionary/manipulation - посетен на 30.01.2024

[16] https://www.oxfordlearnersdictionaries.com/definition/english/manipulation?q=manipulation – посетен на 30.01.2024 г.

[17] https://www.vocabulary.com/dictionary/manipulation - посетен на 30.01.2024

МОДЕЛ НА КУЛТУРА НА КОРПОРАТИВНА СИГУРНОСТ И МЕТОДИКА ЗА НЕЙНАТА ОЦЕНКА

Владимир В. Янков

CORPORATE SECURITY CULTURE MODEL AND METHODOLOGY FOR ITS ASSESSMENT

Vladimir V. Yankov

ABSTRACT: *An overview of the existing models for security culture shows that there is no developed comprehensive model and assessment tool for security culture in the corporate sphere. Available models of security culture are not applicable to the corporate sector, due to their complexity or because they do not cover all categories of security applicable to the corporate sector. This article offers an exemplary model of security culture in the corporate sector as well as the basics of a methodology for its assessment.*

KEYWORDS: *Corporate security culture, Security culture model, Security culture assessment.*

Въведение

Корпоративната сигурност е процес по управление на рисковете за сигурността в съставните стопански субекти. Ролята и е да защитава организациите, техните служители, собствените и клиентските ресурси от външни и вътрешни заплахи. Тези заплахи могат да включват кражба, измама, кибератаки, терористични атаки и други потенциални опасности. Крайната цел на корпоративната сигурност е да се осигури нормалното функциониране на компаниите, чрез намаляване тези рискове до приемливо ниво.

Човешкият фактор като цяло е допринесъл за всички инциденти свързани със сигурността. Те включват умишлени злонамерени действия, неумишлени грешки на персонала, въпроси свързани с проектирането и оформлението на софтуера и хардуера, неадекватни организационни процедури и процеси, както и грешки в управлението. Нарушенията сред персонала по отношение на сигурността, както неумишлени, така и преднамерени, не се осъществяват в изолирана среда. В повечето случаи те са резултат на нарушена организационна култура. Характеристиките на организационната култура, които са съотносими към сигурността формират културата на сигурност, като част от общата организационна култура в дружеството. Така културата на сигурност може да се определи като споделени вярвания и ценности в организацията, които определят как хората се очаква да мислят и да подхождат към сигурността. [1]

Приложими модели за култура на сигурност в корпоративния сектор и методи за нейната оценка

Културата на сигурност не трябва да бъде оставена да се развива безконтролно. Тя трябва да бъде подобрявана, което означава, че на първо място трябва да бъде изследвана и анализирана. Тъй като изследователите структурират по различен начин културното пространство, то организационните култури могат да бъдат представени чрез различни модели.

Прегледът на съществуващите модели за култура на сигурност показва, че няма разработен модел и инструмент за оценка на културата на сигурност приложим за корпоративната сфера. Обикновено при изследванията на културата на сигурност се прави разграничение между информационна сигурност и физическа сигурност, а моделите за култура на информационна сигурност (често погрешно описвана само като култура на сигурност) са много по-добре проучени и развити.

Най-изчерпателният модел и инструмент за оценка на културата на сигурност е разработен в ядрената област. Международната агенция за атомна енергия през 2008 г. разработи модел на култура на ядрена сигурност, базиран на модела на организационна култура на проф. Едгар Шайн, който беше успешно използван през 90-те години на 20-ти век за разработване на модел на култура на ядрена безопасност.

Проф. Шайн предлага културата в организациите да се разглежда на слоеве, състоящи се от основни предположения, възприети ценности и артефакти. Някои слоеве са пряко видими, докато други са невидими и трябва да бъдат изведени от това, което може да се наблюдава в организацията. Артефактите са видимите елементи в една култура и включват всички осезаеми, явни или вербално разпознаваеми елементи във всяка организация. Възприетите ценности са обявените от организацията ценности и правила на поведение. Споделените основни предположения са дълбоко вкоренени, приети за даденост поведения, които обикновено са несъзнателни, но представляват същността на културата. [2]

Фиг. 1. *Модел на Едгар Шайн за организационна култура*

Използвайки трите слоя култура на Едгар Шайн, моделът на МААЕ за култура на ядрена сигурност разделя артефактите на културата на три части, като дава общо пет елемента. Това са вярвания и нагласи, съответстващи на това, което Шайн нарича „основни предположения“, принципи за съзнателни решения и поведение, съответстващи на това, което Шайн нарича „приети ценности“, а „артефактите“ са представени като системи за управление (процеси, процедури и програми в организацията, които правят сигурността основен приоритет и оказват важно влияние върху функциите за сигурност), лидерско поведение (специфични модели на поведение и действия, предназначени да насърчават по-ефективна ядрена сигурност) и поведение на персонала (продукт на усилията на лидерите и на правилно работещи системи за управление). [1]

Фиг. 2. *Модел на МААЕ за култура на ядрена сигурност*

Вярванията и нагласите са тези убеждения и отношения, които се формират в съзнанието на хората с течение на времето и стават случайни фактори в поведението и влияят на начина, по който хората реагират на проблеми и събития на сигурността. Следващият слой са възприетите ценности и принципите, които ръководството декларира и които иска организацията да показва в действие. Културата се проявява предимно чрез артефактите, които изграждат третия и видим слой. Оборудването за физическа защита, поведението на персонала, писмените документи и работните процеси са видими артефакти на културата на сигурност.[3]

Базирайки се на този модел, МААЕ разработват и най-изчерпателната методика за оценка на културата на сигурност. Методиката използва 5 инструмента за оценка текущото ниво на култура на сигурност – анкети, интервюта, фокус-групи, преглед на документи и наблюдения.

Анкетите предоставят удобен начин за получаване на информация от голям брой служители. Проучванията могат да бъдат лесни и бързи за попълване, което помага да се сведе до минимум прекъсването на работата, като същевременно насърчава висок процент отговори. Този метод може да предостави верни данни, тъй като анонимните респонденти могат да изразяват критични възгледи без страх от неблагоприятни последици.

Интервютата играят важна роля в оценката на културата на сигурност като източник на данни, защото осигуряват гъвкавост, позволявайки да се задават последващи въпроси въз основа на отговорите на респондентите на предишни въпроси. Това осигурява начин за разбиране на по-дълбоките и по-малко осезаеми аспекти на културата на една организация.

Фокус групите могат да бъдат по-ефективни за изследване на по-широки въпроси, свързани със сигурността. Те също така могат да дадат голямо количество информация за сравнително кратък период от време. В сравнение с индивидуалните интервюта лице в лице, груповите дискусии имат предимството, че взаимодействията в групата често подтикват и поддържат дискусии с минимален принос от интервюиращия.

Основната цел на прегледа на документите е да се определи дали политиките и процедурите на организацията осигуряват достатъчна основа за насърчаване и поддържане на силна култура на ядрена сигурност. Прегледите на документи могат да дадат представа за това как ръководството определя своите приоритети и как възнамерява да осъществи своите политики, програми и процеси. В комбинация с анкети и интервюта, прегледът на документи помага на екипа за самооценка да оцени разликите между заявените политики и процедури и действителното поведение.

Целта на провеждането на наблюдения е да се запишат действителните резултати и поведение в реално време и при различни обстоятелства, особено при тренировки и учения за извънредни ситуации. Наблюденията са добре установен и доказан инструмент за управление на сигурността. [4]

Използвайки тези 5 инструмента за събиране на данни за видимия слой на културата, заедно с идентифицираните характеристики на системите за управление и лидерското поведение, както и поведението на персонала, е създадена изключително подробна методика за провеждане на оценка на културата на ядрена сигурност, която позволява да се преведе задълбочено изследване на културата на сигурност, включително до голяма степен на организационната култура.

Тази задълбоченост на методиката съответно създава и проблеми. Тя е създадена през 2017 година и оттогава досега е приложена напълно само в 2 държави – България в атомна централа и Индонезия в 3 изследователски реактора. Частично е приложена в 3 болници в Малайзия и в атомна централа в Армения. Това в голяма степен се дължи на сложността на методиката, породена от нейната задълбоченост, а оттам и необходимите средства и време за нейното цялостно провеждане. Опитът на България и Индонезия в нейното пълно прилагане показва, че е необходим екип от около 10 човека и между 6 месеца до 1 година за извършване на пълна оценка в средни до големи организации. Отделянето на

такъв ресурс за провеждане на оценка само на културата на сигурност би обезсърчило всяко корпоративно ръководство.

Анализът на характеристиките на модела на МААЕ за култура на ядрена сигурност показва, че в слоя на видимите артефакти, т.е. системите за управление и поведението на лидерите и персонала, има много елементи, които са съотносими към организационната култура. Това не е погрешно, защото културата на сигурност, бидейки част от цялостната организационна кутура, не се създава и развива самостоятелно. Но доколкото корпорациите обикновено обръщат внимание основно на корпоративната култура, то би било по-подходящо моделът на култура на корпоративна сигурност да е по-опростен и да добавя само характеристиките на организационната култура, които са съотносими към сигурността и са приложими за широкия кръг от области на корпоративната сфера. Методиката за неговата оценка може също да бъде опростена с използването само на основни инструменти за събиране на данни, като така може да бъде използвана като допълнение на вече съществуващите инструменти за оценка на организационната култура в корпорациите. Това, заедно с подходящо популяризиране, би насърчило въвеждането на инструменти за изследване и повишаване културата на сигурност в корпоративната сфера.

Примерен модел на култура на корпоративна сигурност

Моделът на Едгар Шайн за организационна култура е приложим за широк набор от ядрени съоръжения и организации и тъй като по-голямата част от съществуващите модели и рамки за култура на информационна сигурност също се основават на този модел, може да се заключи, че този модел ще бъде също така приложим и за корпоративния сектор. Следователно възможен вариант на модел на корпоративна сигурност би следвал същата структура на слоеве, състоящи се от основни предположения, възприети ценности и видими артефакти.

Доколкото дълбоко вкоренените вярвания и нагласи, както и принципите за вземане на осъзнати решения могат да произходят директно от модела на МААЕ за култура на ядрена сигурност, то в слоя на видимите артефакти трябва да останат само елементи, които са съотносими към сигурността и са приложими за широкия кръг от области на корпоративната сфера. Така от пълния набор елементи на система за управление трябва да останат само тези, които касаят сигурността и които гарантират, че са създадени организационни условия за формиране на подходяща култура на сигурност сред персонала.

Тъй като корпоративната сигурност е доста широко понятие и съществуват различни класификации на видовете сигурност, трябва да се определят категориите сигурност, за които е приложим моделът. Категориите на сигурност по отношение на основните ѝ компоненти се разделят на национална, политическа, социална, икономическа, психологическа, информационна, физическа сигурност и др. В обхвата на корпоративния модел на култура на сигурност ще влязат само последните две категории – физическа сигурност и информационна сигурност, като трябва да се определят общите компоненти за създаване на подходяща среда за развитие на добра култура на корпоративна сигурност.

И при физическата и при информационната сигурност на първо място трябва да има написани инструкции, правила, процедури, функционални задължения и отговорности за всички приложими дейности. И в двата случая трябва да има организирано обучение и тренировки по задълженията на персонала, каксаещи сигурността, включително за действия при извънредни ситуации. Защитата на класифицираната информация също е важен елемент за двете категории сигурност, така че трябва да присъства като елемент в модела на корпоративна сигурност.

Най-важната част от изследването на културата на сигурност се явява разбирането за нагласите на персонала по отношение на сигурността. Основните елементи, за които трябва да се изследват тези нагласи са мотивация, работа в екип и сътрудничество, ефективна комуникация, професионална компетентност, спазване на установените процедури, процесът на обратна връзка и проактивното отношение на всички към сигурността.

Мотивацията е ключов фактор за поведение и е изцяло зависим от възприемането на убежденията и ценностите. Тя може да се изледва както като част от оценката на културата на корпоративна сигурност, така и да се включи като елемент от изследването на мотивацията на персонала, ако съществува такова като практика в корпорацията.

Работата в екип също е от съществено значение за формиране на ефективна култура на корпоративна сигурност тъй като тя най-добре може да се развие в корпорации, където взаимоотношенията сред ръководството и персонала са положителни и професионални.

Ефективната комуникация е ключово междуличностно умение, което позволява да се постигне баланс между индивидуалните нужди и корпоративните цели и следва да бъде включена като елемент в модела.

Друга важна част от ефективна култура на корпоративна сигурност е процесът по поддържане на обратна връзка, чрез който персоналът на всички нива се насърчава да докладва за проблеми и да прави предложения за подобряване на сигурността.

Спазването на установените продеури е следващия елемент, който може да бъде оценен чрез изследване нагласите на персонала. За разлика от наличието на писани правила и процедури при прегледа на документи, на този етап ще се оцени дали процедурите са ясни, актуални, лесно достъпни и удобни за ползване, така че да не се налага персоналът да прибягва до отклонение от тях.

Последният предложен елемент е проактивното отношение на персонала. То има за цел да идентифицира и използва наличните възможности и да се предприемат превантивни действия срещу потенциалните проблеми и заплахи. Своевременното идентифициране на потенциални уязвимости позволява активни коригиращи действия.

От така предложените елементи може да се създаде примерен модел на култура на корпоративна сигурност (**Виж фиг. 3**). Характеристиките в този модел естествено не са изчерпателни и могат да се допълват от съответните субекти в корпорациите в процеса на изследването на културата на корпоративна сигурност.

Фиг. 3. *Примерен модел на култура на корпоративна сигурност*

Елементите от физическата и информационната сигурност в модела на корпоративна сигурност могат лесно да бъдат оценени чрез извършване на преглед по документи на съществуващите написани правила за физическа и информационна сигурност, наличието и достатъчността на функционалните задължения и отговорности, наличието на правила за защита на класифицираната информация, както и наличието на планове за действия в извънредни ситуации.

Възприятията на персонала по отношение на мотивацията, работата в екип и сътрудничество, ефективната комуникация, професионалната компетентност, спазването на установените процедури, процесът на обратна връзка и проактивното отношение, обаче трябва да бъдат оценени чрез допитване до персонала чрез някой от останалите методи. Най-лесният и бърз начин е като се проведе анкета сред персонала. Анкетата ще позволи да се съберат данни от максимално голям брой служители с минимални ресурси. Недостатъкът на този метод е, че той не позволява гъвкавост при събирането на данните, както и достигане до по-дълбоките слоеве на културата. Освен това анкетите понякога водят до противоречиви резултати, които е необходимо да бъдат допълнително проучени. Тези недостатъци могат да се решат чрез провеждане на интервюта. Те осигуряват гъвкавост, позволявайки да се задават последващи въпроси въз основа

на отговорите на респондентите и така спомагат за разбиране на по-дълбоките аспекти на културата.

Примерна методика за оценка културата на корпоративна сигурност

От дотук написаното може да се изведат следните основни стъпки, които да се използват като базисна методика за провеждане на оценка на културата на корпоративна сигурност:

Стъпка 1: Сформиране на екип за провеждане на оценката.

Първата стъпка е да се сформира и обучи екип за провеждане на оценката. Важно е членовете на екипа да не са само представители на звената за сигурност, а трябва да са членове на персонала от различни структурни звена, за да се избегне субективност при провеждане на оценката. Много ще е полезно, ако в екипа могат да бъдат включени служители, които имат практически опит в провеждане на оценки на корпоративната сигурност. В екипа също така е възможно да бъдат включени външни независими експерти, които ще консултират екипа, с цел намаляване на субективността, както и споделяне на опит при провеждане на оценки на корпоративната култура. При липса на подходящи членове на собствения персонал за включване в екипа, също така е възможно той да бъде сформиран изцяло от външни експерти.

Стъпка 2: Създаване на план за провеждане на оценката.

Планът трябва да обхване целия процес на оценка, като целта му е да се постигне максимална ефективност при минимални разходи и нарушения на работния процес. При планирането на процеса по оценка също така трябва да се изберат подходящите методи за събиране на данни като се вземат предвид всички фактори, които могат да нарушат процеса, като разполагаемостта на членовете на екипа, средствата отделени за оценката, провеждането на други оценки, като изследване на мотивацията сред персонала и др.

Стъпка 3: Събиране на данни.

Един от възможните варианти за събиране на данни е да се започне с преглед на документи на съществуващите написани правила за физическа и информационна сигурност, наличието и достатъчността на функционалните задължения и отговорности по отношение на двете категории сигурност, наличието на правила за защита на класифицираната информация, както и наличието на планове за действия в извънредни ситуации.

Оценката може да продължи с провеждане на анкета относно възприятията на персонала по отношение на мотивацията, работата в екип и сътрудничество, ефективната комуникация, професионалната компетентност, спазването на установените процедури, процесът на обратна връзка и проактивното отношение.

Следващият метод за събиране на данни може да е провеждане на интервюта, които ще спомогнат за изясняване на противоречиви резултати от другите методи, както и да се постигне разбиране на по-дълбоките аспекти на културата. Комбинираното използване на няколко метода за оценка спомага за извличането на изводи по време на анализа, което от своя страна улеснява търсенето на решения за подобряване на културата на сигурност.

Стъпка 4: Анализ на данните.

На този етап екипът систематизира събраните данни от стъпка 3, анализира получените разултати и прави изводи по отношение на основните вярвания и нагласи на персонала, които стоят зад видимите аспекти на културата.

Стъпка 5: Набелязване на мерки за подобряване културата на сигурност.

От направените изводи в стъпка 4, екипът предлага мерки за повишаване културата на корпоративна сигурност. Важно е да се отбележи, че с провеждането на оценка и набелязването на мерки не приключва процесът по повишаване културата на корпоративна сигурност. Това трябва да стане повтарящ се във времето процес, за да се верифицира ефективността на предложените мерки, както и да се гарантира, че културата на корпоративна сигурност няма да деградира с течение на времето.

Заключение

Адаптирането на съществуващите модели на култура на сигурност и методите за нейната оценка към корпоративната сфера ще подпомогне ръководствата на дружествата, чрез извършване на оценки и набелязване на последващи мерки, да повишат културата на корпоративна сигурност. Това от своя страна ще допринесе за по-ефективен режим на сигурност, разпростиращ се върху всички работещи в корпорациите. Този модел и методика също така ще даде възможност корпорациите да включат културата на сигурност в своите съществуващи програми за изследване и повишаване на корпоративната култура, което ще повиши ефективността на оценката, както и ще минимизира разходите за нейното провеждане.

ЛИТЕРАТУРА

[1] International Atomic Energy Agency, “Nuclear Security Culture: Implementing Guide,” IAEA Nuclear Security Series No. 7, IAEA, Vienna, 2008

[2] Schein, Edgar. The Corporate Culture and Leadership, 3rd ed. (San Francisco, CA: Jossey-Bass, 2004)

[3] International Atomic Energy Agency, “Self-assessment of Nuclear Security Culture in Facilities and Activities: Technical Guidance,” IAEA Nuclear Security Series No. 28-T, IAEA, Vienna, 2017

КОМПЛЕКСНИ СИСТЕМИ И МОДЕЛИ ЗА ОСИГУРЯВАНЕ НА СИГУРНОСТ В ОБЩИНИТЕ В БЪЛГАРИЯ
Холистичен подход за опазване на общинското благосъстояние

Илиана К. Симеонова

COMPREHENSIVE SYSTEMS AND MODELS FOR ENSURING SECURITY IN MUNICIPALITIES IN BULGARIA
A Holistic Approach to Safeguarding Community Welfare

Iliana K. Simeonova

ABSTRACT: *In recent years, the increasing reliance on digital technologies and the increasing complexity of urban systems have highlighted the importance of ensuring security in municipalities. Bulgaria, with its unique socio-economic and geopolitical landscape, faces specific challenges in protecting its municipalities against various threats. This report examines a range of systems and models designed to ensure security in Bulgarian municipalities, from cybersecurity frameworks to community policing initiatives.*

KEYWORDS: *Security in municipalities, Cyber security.*

Въведение

През последните години нарастващата зависимост от цифровите технологии и нарастващата сложност на градските системи подчертават значението на гарантирането на сигурност в общините. България със своя уникален социално-икономическа и геополитическа среда е изправена пред специфични предизвикателства при защитата на своите общини срещу различни заплахи.

Общините в България служат като жизненоважни субекти отговорни за местното управление, обществените услуги и развитието на общността. Тъй като тези субекти стават все по-взаимосвързани и дигитализирани, необходимостта от стабилни мерки за осигуряване на сигурност е от първостепенно значение за защита срещу киберзаплахи, физически уязвимости и непредвидени извънредни ситуации.

От тази гледна точка сигурността в общините се определя като динамично състояние на защитеност на система, при което е гарантирано нейното съществуване и са защитени надеждно жизненоважните ѝ интереси. [3, 4]

В тази връзка, целта на доклада е да направи цялостен преглед на различните системи и модели, прилагани в българските общини за гарантиране на сигурността – от рамки за киберсигурност и системи за реагиране при извънредни ситуации до инициативи за ангажиране на общността, като всеки аспект допринася за цялостната позиция на сигурността на тези администрации.

Изложение

В доклада се разглежда набор от системи и модели предназначени да гарантират сигурността в българските общини, от рамки за киберсигурност до инициативи за обществена полиция. Доклада се задълбочава в многостранните стратегии използвани за защита на обществените активи, критичната инфраструктура и благосъстоянието на гражданите. Възприемайки холистичен подход общините в България могат да се ориентират в развиващата се обстановка на заплахи и да насърчат устойчива и сигурна среда за своите общности.

Интегрирани системи за сигурност. Българските общини все повече внедряват интегрирани системи за сигурност, които обединяват системи за видеонаблюдение, контрол на достъпа, комуникационни мрежи и др. Тези системи позволяват наблюдение в реално време на обществени пространства, обекти от критичната инфраструктура и ключови съоръжения, като подобряват способността за бърза реакция срещу потенциални заплахи.

С нарастващата цифровизация на административните процеси и услугите на гражданите, общините в България трябва да дадат приоритет на информационната сигурност и киберсигурността. Това предизвикателство налага разработването и прилагането на стабилни рамки за киберсигурност, съобразени със специфичните нужди, пред които са изправени българските общини. [5]

Познаването на потенциалните заплахи е решаваща стъпка в разработването на ефективни рамки и управление на сигурността, които биха могли да компрометират поверителността и целостта на информацията в общинските системи.

Въз основа на добрите международни практики, този модел очертава ключови мерки за киберсигурност за общините в България, които включват сегментиране на мрежата, редовни оценки на уязвимостта, обучение на служители и внедряване на нови технологии.

Мерки за физическа сигурност в общините**.** Защитата на критичната инфраструктура е от решаващо значение за гарантиране на устойчивостта на общините. Тук се разглеждат мерките за физическа сигурност, включително контрол на достъпа, системи за наблюдение и сигурност на периметъра за защита на основните услуги.

За да реагират при извънредни ситуации и управление на бедствия, общините трябва да бъдат подготвени да реагират при различни извънредни ситуации, включително природни бедствия, аварии и катастрофи. Този модел разглежда създаването на ефективни планове за реагиране при извънредни ситуации, координиране и взаимодействие между общините и частите на единната спасителна система, както и осведоменост в реално време.

Общинска полиция и обществена безопасност. Създаването на общинска полиция е проактивен подход към обществената безопасност, който включва сътрудничество между правоприлагащите органи и общината. Този подход обсъжда прилагането на инициативи за общинска полиция в българските общини, насърчаване на доверието и чувството за споделена отговорност за сигурността.

Интегрирането на технологии, включително камери за наблюдение, криминален анализ и мобилни приложения, подобрява възможностите на правоприлагащите органи в българските общини. Изследва как технологията се използва за подобряване на времето за реакция, събиране на актуална информация и укрепване на партньорствата между общината и полицията.

Инициативи за интелигентен град за повишена сигурност.

Интелигентна инфраструктура. Инициативите за интелигентен град използват технологиите за повишаване на ефективността на общинските услуги и подобряване на качеството на живот на жителите. Тук се изследва как интелигентната инфраструктура, включително IoT устройства и сензори, може да бъде интегрирана в градското планиране за укрепване на мерките за сигурност, чрез поверителност на данните и управление.

Тъй като общините събират и анализират огромни количества данни за инициативи за интелигентни градове, гарантирането на поверителността на данните и управлението стават от първостепенно значение. Затова трябва да се разгледа прилагането на политики и рамки за защита на поверителността, като същевременно се извлича информация от събраните данни.

Няколко общини в България възприемат инициативата за интелигентен град. Ителигентното наблюдение и управление на трафика и анализите на данни допринасят за по-ефективното разпределение на ресурсите и подобрени възможности за реагиране при спешни случаи. Тази инициативи имат за цел да създадат по-безопасна и по-устойчива градска среда.

Казуси от практиката. Успешни внедрявания на сигурността в български общини.

Пловдив. Устойчивост на киберсигурността и публично-частни партньорства. Този казус изследва как община Пловдив е засилила своята устойчивост на киберсигурност чрез публично-частни партньорства. Сътрудничеството между местни фирми, държавни органи и експерти по киберсигурност създаде стабилна екосистема за сигурност. [6]

София. Град София успешно реализира инициативи за общинска полиция, интегрирайки технологии за повишаване на обществената безопасност. Този казус се задълбочава в конкретните използвани стратегии, подчертавайки положителното въздействие върху превенцията на престъпността и доверието на общността. [7]

Модели за оценка на риска. Прилагането на модели за оценка на риска е от решаващо значение и предвижда и смекчаване на потенциални заплахи за сигурността. Българските общини използват сложни модели, които отчитат фактори като природни бедствия, киберзаплахи и социална уязвимост. Тези

оценки насочват разработването на цели и стратегии за сигурност, свързани с местните нужди. [1]

Реагиране при извънредни ситуации и управление на кризи**.** Ефективната реакция при извънредни ситуации е от първостепенно значение за гарантиране на общинската сигурност. Българските общини инвестират в системи, които рационализират комуникацията, координацията и разпределението на ресурсите по време на кризи. Това включва интегрирането на информационни системи за улесняване на бързото вземане на решения и разгръщане на услуги за спешна помощ.

Предизвикателства и решения в общинската сигурност.

Бюджетни ограничения. Много общини са изправени пред бюджетни ограничения, които могат да ограничат прилагането на цялостни мерки за сигурност. Поради това трябва да се разгледат стратегии за оптимизиране на ресурсите, търсене на външно финансиране и приоритизиране на инвестициите в сигурността въз основа на оценки на риска.

Общините имат интерес от създаването на подходящи условия за развитие на инвестициите в района. В тази връзка общинският бюджет може да бъде определен като основен инструмент в релацията между общините и местния бизнес. От една страна, чрез бюджета се акумулират средства за функционирането на общината, но от друга – чрез общинските разходи се осигуряват блага, насочени към осигуряване потребностите на хората, бизнеса и организациите в района. [2]

Липсата на стандартизирани рамки за сигурност в българските общини поставя предизвикателства пред координацията и обмена на информация.

Бъдещи тенденции в общинската сигурност. Бъдещето на общинската сигурност включва засилено сътрудничество между общините, правоприлагащите органи и частни субект, като се обсъждат потенциалните ползи от платформите за сътрудничество и споделянето на информация за справяне с развиващите се заплахи.

Препоръки към общинските администрации.

Извършване на цялостни оценки на риска. Общините трябва да дадат приоритет на цялостните оценки на риска, за да идентифицират и приоритизират потенциалните заплахи. Тези оценки трябва да обхващат киберрискове, физически уязвимости и потенциални извънредни ситуации.

Инвестиране в програми за обучение и осведоменост. Гарантирането, че общинските служители са добре информирани относно мерките за сигурност е от решаващо значение. Необходимо да се провеждат обучение по киберсигурност, реагиране при извънредни ситуации и други обучения, свързани със сигурността на информацията.

Насърчаване на публично-частни партньорства. Сътрудничеството между общините и частните субекти може да подобри мерките за сигурност чрез използване на външен експертен опит и ресурси. Публично-частните партньорства могат да бъдат инструмент за разработване и прилагане на ефективни стратегии за сигурност.

Създаване на стандартизирани рамки за сигурност. За да улеснят координацията и споделянето на информация, общините трябва да работят за установяване на стандартизирани рамки за сигурност. Това може да включва национални насоки, които позволяват местно адаптиране въз основа на специфични нужди.

Заключение

В заключение, осигуряването на сигурност в българските общини изисква цялостен и адаптивен подход. От стабилни рамки за киберсигурност до инициативи за обществена полиция и технологии за интелигентни градове.

Общините трябва да се справят с разнообразен набор от предизвикателства. Като използват добри практики, преодоляват бюджетни ограничения и прилагат нововъведенията в технологиите. Българските общини могат да създадат устойчива и сигурна среда, която насърчава благосъстоянието на техните общности.

ЛИТЕРАТУРА

[1] Диманова Д. Управление на риска. УИ „Епископ Константин Преславски“, Шумен, 2016, ISBN: 978-619-201-095-9.

[2] Загорчева Д. Планиране и управление на собствените приходи на общините чрез симулатори за бюджетиране. УИ „Епископ Константин Преславски“, Шумен, 2021, ISBN: 978-619-201-485-8, с. 26.

[3] Кантарджиев И. Оценка на дейността на корпоративно контраразузнавателно звено. Университетско издателство „Епископ Константин Преславски“, Шумен, 2022, ISBN 978-619-201-643-2., с. 13.

[4] Denev D., Konstantinova E. Main Issues in the Protection of Information in the system of National and Corporate Security. 2020, MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 110-115.

[5] Konstantinova E., Karadocheva M., Tsankov Ts. The invisible Internet and cyber security. International scientific conference 2019, “Vasil Levski” National military university, “Artillery, aircraft defense and CIS” faculty, Shumen, 2019, ISSN 2367-7902, pp. 519-524.

[6] https://plovdivcentral.org/

[7] https://www.sofia.bg/

ПОДОБРЯВАНЕ НА АДМИНИСТРАТИВНАТА СИГУРНОСТ В ОБЩИНСКИТЕ АДМИНИСТРАЦИИ
Цялостен подход чрез модела „Монте Карло“

Илиана К. Симеонова

ENHANCING ADMINISTRATIVE SECURITY IN MUNICIPAL ADMINISTRATIONS
A Comprehensive Approach Using Monte Carlo Simulation

Iliana K. Simeonova

ABSTRACT: *In an era marked by rapid technological advancements and increasing cyber threats, municipal administrations are facing unprecedented challenges in safeguarding sensitive information and ensuring the security of administrative processes. This article delves into the realm of administrative security within municipal administrations, exploring the potential of the Monte Carlo model as a robust tool for improving security measures. By employing Monte Carlo simulation, municipalities can assess vulnerabilities, identify potential risks, and develop strategies to enhance their overall administrative security posture. This comprehensive approach aims to fortify municipal systems against cyber threats, thereby safeguarding the integrity, confidentiality, and availability of critical data.*

KEYWORDS: *Monte Carlo model, Municipal administration, Administrative security.*

Въведение

В епоха, белязана от бърз технологичен напредък и нарастващи кибер заплахи, общинските администрации са изправени пред безпрецедентни предизвикателства при опазването на чувствителната информация и гарантирането на сигурността на административните процеси.

Рискът от осъществяването на нерегламентиран достъп до класифицирана информация представлява потенциална заплаха за сигурността на общината. [1]

В доклада се разглежда административната сигурност в общинските администрации, прилагайки модела Монте Карло като стабилен инструмент за подобряване на мерките за сигурност и оценка на риска.

Използвайки модела Монте Карло, общините могат да оценят уязвимостите, да идентифицират потенциалните рискове и да разработят стратегии за подобряване на цялостната си административна сигурност. Този всеобхватен подход има за цел да укрепи общинските системи срещу кибер

заплахи, като по този начин защитава целостта, поверителността и наличността на критични данни.

Изложение

Общинските администрации играят решаваща роля в предоставянето на административни услуги на гражданите и управлението на различни функции, които допринасят за благосъстоянието на общностите.

По своята същност, общините са различни по територия, разположение, традиции, инфраструктура, размер и структура на населението, което предполага да имат различни социални, културни, образователни, екологични, здравни, инфраструктурни и други потребности. Основна задача на местната власт е да осигурява блага, формирани на база потребностите на общината, населението и бизнеса. [3]

Въпреки това, нарастващата зависимост от цифровите технологии и взаимосвързаните системи излага общинските администрации на множество заплахи. Неоторизирания достъп, нарушения на данните и други злонамерени дейности представляват значителни рискове за целостта и поверителността на чувствителната информация.

Административната сигурност е от съществено значение за общинските администрации, за да гарантират ефективно функциониране на операциите, да поддържат общественото доверие и поверителността на чувствителните данни. Пробивът в административната сигурност не само застрашава вътрешните процеси в общината, но може да има и дълбоки последици за гражданите, които обслужва.

В съвременните условия за осигуряване на ефективна работа е необходимо изграждането на база данни. Нейната основна функция е осигуряване на надеждно съхранение, обработка и достъп до информация. Перспективен вариант е изграждането на интегрирана система от база данни, която да осигурява на ръководството и структурите на организацията, необходимата информация за комплексно управление риска. [4, 5]

Модела Монте Карло и неговото практическо приложение в публичните администрации, в т.ч. общинските администрации на територията на Република България.

Както бе посочено, основната цел на доклада е да проучи потенциала на модела Монте Карло като инструмент за повишаване на административната сигурност в общинските администрации. Същността на метода на статистическите изчисления се заключва в построяването на модел на изследвания процес с помощта на случайни реализации, определянето на вероятностните му характеристики и приемането им за равни на величините, които са решения на поставените задачи. [2]

Чрез използването на модела Монте Карло общините могат да оценят настоящите си мерки за сигурност, да идентифицират потенциални уязвимости и да разработят стратегии за ефективно смекчаване на рисковете.

Разбиране на модела Монте Карло. Модела Монте Карло е статистическа техника, която използва произволна извадка за моделиране и анализ на сложни системи. Първоначално разработена по време на проекта Манхатън през 40-те години на миналия век, модела Монте Карло се е превърнала в мощен инструмент за вземане на решения, оценка на риска и оптимизиране на управленски решения.

В контекста на административната сигурност, модела Монте Карло може да се приложи за моделиране на потенциални заплахи, оценка на уязвимостите и симулиране на различни сценарии за измерване на ефективността на мерките за сигурност. Чрез включването на вероятностни елементи, този метод позволява на общинските администрации да вземат информирани решения и да разпределят ресурсите по-ефективно.

Първата стъпка за подобряването на административната сигурност с помощта на модела Монте Карло включва разработването на цялостен модел на заплахите. Това обхваща идентифициране на потенциални заплахи, както вътрешни, така и външни, които биха могли да компрометират сигурността на общинските системи.

Както е известно, заплахата и опасността са взаимно свързани. Опасността съществува в условия на неопределеност. Тя може да се разглежда като източник на потенциална вреда и обективна възможност за вредно въздействие. С нея се характеризира степента на изложеност на риск. Заплахата се определя като непосредствена опасност. Риск и заплаха има само при наличието на незащитеност на системата срещу нежелани вредни последици-уязвимост. Това всъщност е показател за ефективност на системата ни за сигурност. Често срещаните заплахи включват кибератаки, вътрешни заплахи и природни бедствия. [1, 6]

Модела Монте Карло разчита на точни данни, за да произведе значими резултати. Общинските администрации е необходимо да събират актуални данни за своите системи, мрежи и процеси. Това включва информация за поведението на потребителите, уязвимостите на системата и инциденти със сигурността.

След като източника на заплахата е установен и данните са събрани, следващата стъпка е да се конструира симулационният модел Монте Карло. Това включва дефиниране на променливите, задаване на вероятностни разпределения и задаване на параметри за симулацията. Моделът трябва точно да представя сложността на сценария за сигурността на общинската администрация.

Модела Монте Карло включва изпълнение на множество итерации за симулиране на различни сценарии за сигурност. Чрез въвеждане на случайни променливи и оценка на въздействието им върху системата, общините могат да получат представа за потенциални слабости и области, които изискват подобрение. Симулациите осигуряват количествена и качествена оценка на ефективността на съществуващите мерки за сигурност.

Административната сигурност е непрекъснат процес, който изисква непрекъснато подобряване.

Финансовото планиране и бюджетиране, чрез тези модели са отлични в прогнозирането на финансови резултати в несигурна среда. Общините могат да използват тези техники, за да симулират бюджетни сценарии, да оценят потенциалното въздействие на икономическите колебания. Правейки това, те могат да разработят по-устойчиви финансови планове, които да се адаптират към непредвидени обстоятелства.

Модела Монте Карло може да бъде интегрирана в протоколи за сигурност, за да се адаптира към развиващите се заплахи и тенденции. Периодичните симулации помагат на администраторите да останат проактивни при идентифицирането и справянето с възникващи предизвикателства пред сигурността.

Важна роля в административната сигурност има и човешкия фактор. Модела Монте Карло може да се използва за моделиране на въздействието на човешки грешки, като фишинг атаки или неоторизиран достъп от служители. Тази информация спомага за изготвяне на програми за обучение на служителите с цел повишаване на тяхната осведоменост и намаляване на риска от инциденти свързани със сигурността.

Успешни внедрявания. През последните години част от общините успешно използват възможностите на модела Монте Карло, за да подобрят административната си сигурност. Възникващите в процеса казуси подчертават специфичните предизвикателства, пред които са изправени администрациите. Възприетия симулационен подход и произтичащите от него подобрения в мерките за сигурност, са база за вземане на управленски решения. Проучването на добрите практики предоставя ценна информация за други общини, които обмислят подобни стратегии.

Едно от основните предизвикателства при прилагането на модела Монте Карло за административна сигурност е наличието и точността на данните. Общините може да се сблъскат с трудности при получаването на изчерпателни данни за инциденти свързани със сигурността, уязвимости на системата и поведение на потребителите.

Сложност на модела. Изграждането на точен и представителен модел Монте Карло изисква задълбочено разбиране на архитектурата за сигурност на общината. Сложността на тези модели може да създаде предизвикателства за администрациите с ограничени ресурси или опит в симулационните техники.

Тъй като технологиите продължават да се развиват, бъдещите насоки може да включват използването на изкуствен интелект и техники за машинно обучение в симулационни модели на Монте Карло. Това позволява по-точни прогнози и адаптивност в реално време към възникващи заплахи.

Общините могат да се възползват от сътрудничеството и споделянето на знания и добри практики в областта на административната сигурност. Споделянето на добри практики и знания, свързани с използването на модела на Монте Карло, може да насърчи колективен подход за справяне с общи предизвикателства.

Заключение

В заключение може да се обобщи, че интегрирането на модела Монте Карло в общинските административни протоколи за сигурност предлага стабилен и систематичен подход за идентифициране на уязвимостите, оценка на рисковете и разработване на целенасочени стратегии за подобрение. Като използват вероятностното моделиране, общините могат да подобрят цялостната си система за сигурност, като гарантират поверителността, целостта и наличността на критични данни. Тъй като технологиите продължават да се развиват, приемането на иновативни техники ще бъде от съществено значение за общинските администрации, за да изпреварят развиващите се кибер заплахи и да защитят доверието на общностите, на които служат.

ЛИТЕРАТУРА

[1] Диманова Д. Управление на риска. УИ „Епископ Константин Преславски“, Шумен, 2016, ISBN: 978-619-201-095-9, с. 27.

[2] Димитров Д., Митрев Д. Оптимизиране на управленските решения. УИ „Епископ Константин Преславски“, Шумен, 2012, ISBN: 978-954-577-622-9, с. 169-170.

[3] Загорчева Д. Планиране и управление на собствените приходи на общините чрез симулатори за бюджетиране. УИ „Епископ Константин Преславски“, Шумен, 2021, ISBN: 978-619-201-485-8, с. 24-25.

[4] Кантарджиев И. Методика за организиране на дейността на корпоративното контра разузнавателно звено. Сборник доклади от годишна университетска научна конференция 27-28 май 2021 г., Велико Търново 2021, с. 963.

[5] Denev D., Konstantinova E. Main Issues in the Protection of Information in the system of National and Corporate Security. 2020, MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 110-115.

[6] Konstantinova E., Karadocheva M., Tsankov Ts. The invisible Internet and cyber security. International scientific conference 2019, “Vasil Levski” National military university, “Artillery, aircraft defense and CIS” faculty, Shumen, 2019, ISSN 2367-7902, pp. 519-524.

ПРОЦЕСА НА УПРАВЛЕНИЕ НА ПРОМЯНАТА В БИЗНЕС ОРГАНИЗАЦИИТЕ

Мирослав Г. Петков

THE PROCESS OF CHANGE MANAGEMENT IN BUSINESS ORGANIZATIONS

Miroslav G. Petkov

ABSTRACT: *The purpose of the report is to examine the actions taken by the management team of a company during a change process in its sales team to overcome resistance to change from employees and successfully motivate them for the transition.*

KEYWORDS: *Change management, Resistance to change, Business organizations, Behavior of the management team and employees, Motivational approach.*

Въведение

Всяка промяна в самата си основа е свързана с някаква причина. Развитието на технологиите и дигитализацията на бизнеса по света налага промяна в компаниите. Промяната, която повечето компании правят е постепенна, тъй като ръководството преследва дългосрочни цели и предприема редица действия, свързани с ежедневието.

Поради намаляващите приходи, компаниите в сектора на услугите търсят нови възможности, за да запазят своята доходност и да получат ново устойчиво конкурентно предимство. Темата е от съществено значение за бъдещото развитие на компанията, тъй като изследването и оценката на различните възможни пречки за успешна промяна дава възможност на фирмата да подобри крайния си резултат чрез прилагане на констатациите.

Процесът на промяна е труден и води до много сътресения в отношенията между ръководителите и техните подчинени. В свое изследване, Davis и Coan [10] посочват, че най-важният фактор за извършване на промяна е начинът, по който средното ръководство на компанията ръководи и управлява своите подчинени. Според Tobore [23] най-естественият резултат, когато настъпи промяна, е съпротивата от страна на участващите служители. Ръководният екип носи отговорността да посрещне съпротивата на служителите и да приложи определени управленски действия, за да запази мотивацията на своите подчинени.

В тази връзка целта на доклада е да се оценят и разгледат различните лидерски стилове, които биха могли да доведат до осъществяването на успешна промяна.

Изложение

Appelbaum подчертава, че най-приложимите лидерски стилове за управление на промяната са трансформационни и транзакционни. И двата стила могат да бъдат правилният избор в зависимост от факторите на съпротива, които възникват сред служителите. В труда си, „Ефектът на лидерството върху съпротивата срещу промяна в една организация“, Katombe [14] подчертава основните причини за съпротива от страна на служителите, като набляга на: лични интереси, неразбиране на промяната, липса на доверие към ръководството, ниска толерантност и различна оценка.

Много автори и учени наблягат на темата за „управление на промяната“, като Patterson и Wigham [18], които подчертават важността на хората в една компания през целия процес на промяна.

Todnem [24] заявява, че предизвикателството „управление на промяната” е изключително сложен процес, причинен от факта, че основните промени идват най-вече в основните дейности, които пряко влияят върху външната и вътрешната среда на организацията (социална, икономическа, политически, междуличностна и лична).

Според Lines и др. [15], всички печеливши и успешни компании днес са в състояние на постоянна промяна. Те никога не спират своите процеси на промяна, защото вярват, че промяната е равна на развитие.

Prediscon и Roiban [19] определят основните фактори, които провокират промени в компаниите: конкуренция, световна политика, работна сила, технологии, социални тенденции.

В своя труд Stanleigh [22] улавя идеята, че най-голямото предизвикателство при управлението на промените възниква по време на сливания и придобивания. От друга страна Cameron и Green [7] заявяват в книгата си, че технологията е факторът, който активира най-много промяна както във външната, така и във вътрешната среда на фирмата.

Според Davis и Coan [10] всяка организационна промяна е процес, който включва различни групи от хора в рамките на компанията, които трябва да бъдат водени и управлявани.

Banker [5] посочва, че управлението е ключовата точка в процеса на промяна, което е подценявано от компаниите. По същия начин Fernandez и Rainey [11] посочват, че управлението на промените е свързано с управление и координация на следните три елемента: процеси, система за управление и хора. Всяка организационна промяна в една компания трябва да започне с план, който да се изпълнява на всички йерархични нива. В повечето случаи висшето ръководство инициира промяната и вярва в нея, но също така е много важно тя да бъде подкрепена от средното ръководство, тъй като те са мостът между високите нива и хората от фронт офиса.

Carter и др. [8] разграничават двата типа промяна: радикална и инкрементална (постепенна). Радикалната промяна е свързана с пълна трансформация или пълна промяна на основния продукт, мисията или визията на компанията. От друга страна, постепенната промяна включва промени, които се случват ежедневно. Изпълнението на този тип промени е по-бавно, на етапи във времето, което води до подобрения в екипната работа и комуникациите. На първо място, постепенните промени могат да бъдат свързани с внедряване на нова технология (система) в някои от отделите на компанията или могат да бъдат свързани с пускането на нов продукт.

Съпротива срещу промяната

Според Oreg [17], в процеса на промяна има група от хора, които инициират промяната. В повечето случаи тази група е висшето ръководство на компанията, което изпитва нужда от промяна, за да увеличи печалбите на компанията. Понякога причината за промяната е, че възниква някаква екстремна ситуация, но отново промяната е инициирана от висшето ръководство и комуникацията е отгоре надолу (Appelbaum и др.).

От друга страна, има друга група хора, които са противници на промяната. Aslam и др. [3] посочват в своето изследване, че незадоволените потребности водят до напрежение в индивида и респективно проява на защитно поведение като оттегляне, враждебност, заместване, компенсация.

Причините за подобно поведение могат да бъдат следните:

- Страх от новото и непознатото – в повечето случаи неизвестното засилва тревожността;
- Много хора смятат status que (статуквото) за зона на комфорт и се страхуват от промяната;
- Неразбиране на нуждите от промяна;
- Страх от провал – служителите се страхуват от новите изисквания и се съмняват дали ще могат да се справят;
- Индивидуални навици и стереотипи.

Al-Haddad и Kotnour [1] заявяват, че поведението на служителите е различно в зависимост от вида на промяната. Когато промяната е необходима поради екстремна или кризисна ситуация, тогава съпротивата ще бъде много по-голяма. Това се дължи на неразбиране, липса на сигурност и нестабилност от страна на служителите и изисква повече контрол от страна на ръководството. В тази ситуация има малко време за реакция и това увеличава отблъскването на непознатото. В случаите на промяна, предизвикана от кризисни ситуации, комуникацията между ръководители и подчинени липсва. Ръководството просто дава заповеди и се опитва да координира действията на служителите, за да постигне крайната цел (Sarkar и Osiyevskyy [20]).

Когато промяната е отдавна планирана, тогава съпротивата е по-малка. В тази ситуация служителите имат достатъчно време да бъдат добре информирани за промените. Въпреки това, съпротивата е най-естественият човешки навик по време на процеса на промяна (Tobore [23]).

Според Grama и Todericiu [12] има пет условия на съпротива срещу промяната: скептицизъм, песимизъм, съмнение, нетърпение и липса на мотивация.

Скептицизмът може да се разглежда в два аспекта, първо, мениджърите не са убедени дали техните подчинени ще приемат промяната, второ, служителите не вярват, че техните мениджъри са в състояние да завършат промяната. Jabbarian и Chegini [13] смятат, че песимизмът е по-крайна проява на скептицизъм, водеща до намалена активност. Съмненията в уменията на мениджъра често са причина за демотивация и водят до повишаване на несигурността. Процесът на промяна изисква време и ресурси, което създава нетърпение у служителите. Често е следствие от липсата на конкретни срокове за промяната. Според Maltseva и Klyushnikova [16] липсата на мотивация е най-честата форма на съпротива. Може да е резултат от неразбиране на целите или лоши взаимоотношения между служители и мениджъри.

Според Burnes и Bargal [6], по време на процесите на промяна в една компания, лидерите трябва да се придържат към един от класическите методи за планирана промяна. В своето изследване Burnes и Bargal (2017) поставят акцент върху тристепенния модел на промяната на Люин. Моделът разглежда промените като краткосрочни и определя, че след кратък период от време е напълно възможно хората да върнат старото си поведение. За да бъде успешна промяната в организацията, старите модели на поведение трябва да бъдат изхвърлени, преди да бъдат приети новите (Cummings и др., [9]).

Моделът на Кърт Левин от 1947 г. включва три основни етапа на промяна: размразяване, промяна и замразяване. Преди да започне промяната, тя трябва да премине през етапа на размразяване. Основната цел на този етап за ръководството и лидерите е да създадат усещане у своите служители как статуквото има негативен ефект върху развитието на компанията. Трябва да се направи цялостен анализ на старото поведение, процеси, структури на отделите и да се изложи на служителите, за да се убедят колко важна е промяната. Комуникацията на този етап има ключова роля, защото колкото повече служители знаят за промяната, толкова повече ще бъдат мотивирани за нея.

Втората стъпка е „промяна“, където всъщност се случва промяната (Bakari и др., [4]). Това е стъпката, при която служителите започват да се борят най-много срещу промяната. Това е най-трудната стъпка по модела и нейният успех зависи от нивото на подготвеност от предишния етап. През този етап на хората трябва да се казва и постоянно да им се напомня за причините, поради които се случва тази промяна и колко положително ще им се отрази тя след нея.

Последният етап от теорията на промяната е „замразяване“ или всички промени, които са направени в компанията, са приети и успешни. Люин нарича тази стъпка „замразяване“, защото това е моментът, в който хората трябва да възприемат промените като статукво. Награждаването и допълнителните бонуси за индивидуалните усилия са подходящи за укрепване на промяната (Cummings и др., [9]).

Липсата на ефективен мениджмънт може да доведе до провал и желаният резултат да не се постигне. Крайният успех на една промяна зависи от нивото на възприятие на служителите. Това може да стане чрез консултации и обучения.

Решаваща роля за крайния успех имат уменията на лидерите в компанията. Лидерите са тези, които трябва да допринесат най-много за правилната комуникация по промяната. Ефективната комуникация от страна на висшия мениджмънт към лидерите и съответно към служителите би могла да намали съпротивата.

За целите на доклада е направено анкетно проучване на търговски представители и ръководителите им в компания на българския пазар, за да разгледа поведението и на двете страни и да се открият пропуските в отношенията им. Проучването използва еднакъв въпросник, за да проследи двете различни гледни точки и да анализира по-добре процеса на промяна в компанията. Въпросника включва осем въпроса свързани с удовлетвореността на търговските представители от действията на техните ръководители по време на прилагането на промяната. Анализирайки отговорите на мениджърите, може да се отбележи, че тяхното мнение напълно съвпада с това на търговските представители. Shimoni [21] споменава в своето изследване, че повишаването на експертните познания на служителите по отношение на конкретната промяна увеличава шанса за по-добра и по-бърза промяна. В същия случай авторът споменава, че подобряването на знанията на хората влияе положително на тяхната естествена устойчивост към промяна.

Заключение

Доклада анализира поведението на търговците по време на процеса на промяна, за да се открият основните причини за съпротива. Оценява се нивото на мотивация сред търговските екипи, което помага на мениджърите да намерят най-добрия начин за стимулиране на своите подчинени. Решаваща роля за успешния преход има отношението на мениджърите.

На база на изложеното, основните мотиви за съпротивата на търговските представители срещу промяната, които всъщност са очаквани от мениджърите, са страхът от неизвестното и промяната на статуквото. Проучването показва, че подчинените, които оказват най-голяма съпротива, са хората от възрастовата група над 40 години.

Стилът на транзакционно лидерство е установен като най-подходящ стил за управление на промяната въз основа на отговорите по въпросниците. Конкретните изследвания показват, че този стил е подходящ за настоящия етап на промяната, но на мениджърите се препоръчва да внедрят някои елементи, свързани с трансформационния стил на лидерство, за да изградят повече доверие в своите подчинени, като положат усилия върху индивидуалния подход.

Поведението на търговците се проучва, за да се намери основната съпротива, която възниква в търговските представители по време на процеса на промяна. От друга страна се очаква изследването да открие болезнените точки в действията на ръководния екип. От съществено значение е ръководството да намери най-добрия начин за мотивиране на търговците по време на промяната, така че настоящото изследване се очаква да помогне на мениджърите да намерят най-полезния мотивационен модел, който може да бъде използван.

Подготвените въпросници от анкетата ще дадат възможност за анализ на множеството взаимодействия между възприятието на служителите за промяната, удовлетворението от работата, факторите на съпротива и нивото на мотивация. От друга страна, с разработването на отделна анкета може да се събират данни от мениджърите в търговските отдели.

Въпросите от анкетата предоставят информация свързана с възраст, пол, образование, работна позиция. Отношенията между мениджърите и техните подчинени, ефектът от промяната, нивото на ангажираност и удовлетвореност също ще заемат място във въпросниците.

ЛИТЕРАТУРА

[1] Al-Haddad, S. and Kotnour, T. (2015) Integrating the organizational change literature: a model for successful change. Journal of Organizational Change Management, 28(2), p.234-262.

[2] Appelbaum, S. H., Degbe, M. C., MacDonald, O. And Nguyen-Quang, T. S. (2015)

[3] Aslam, U., Ilyas, M., Imran, M. K. and Rahman, U. U. (2016) Detrimental effects of cynicism on organizational change: an interactive model of organizational cynicism (a study of employees in public sector organizations). Journal of Organizational Change Management, 29(4), p.580-598.

[4] Bakari, H., Hunjra, A.I. and Niazi, G.S.K. (2017). How does authentic leadership influence planned organizational change? The role of employees' perceptions: Integration of theory of planned behavior and Lewin's three step model. Journal of Change Management, 17(2), p.155-187.

[5] Banker, D. (2012), Organizational Change: Pragmatic approaches to Organizational Change Management, Amity Global Business Review, 7, p. 63–67.

[6] Burnes, B. and Bargal, D. (2017) "Kurt Lewin: 70 Years on", Journal of Change Management, 17(2), p. 91–100.

[7] Cameron, E. and Green, M. (2019) Making sense of change management: A complete guide to the models, tools and techniques of organizational change.

[8] Carter, M.Z., Self, D.R., Bandow, D.F., Wheatley, R.L., Thompson, W.F., Wright, D.N. and Li, J., (2014) Unit-focused and individual-focused transformational leadership: The role of middle.

[9] Cummings, S., Bridgman, T. and Brown, K.G. (2016). Unfreezing change as three steps: Rethinking Kurt Lewin's legacy for change management. Human relations, 69(1), p.33-60.

[10] Davis, M. C., and Phillipa Coan, (2015), Organizational change, p. 244-274.

[11] Fernandez, S. and Rainey, H.G. (2017). Managing successful organizational change in the public sector. In Debating Public Administration, p. 7-26.

[12] Grama, B. and Todericiu, R. (2016) Change, resistance to change and organizational cynicism. Studies in Business and Economics, 11(3), p. 47-54.

[13] Jabbarian, J. and Chegini, M. G. (2017) The effect of perceived organizational support on employee resistance to change: A study on Guilan Municipal staff. Journal of History Culture and Art Research, 5(4), p. 642-654.

[14] Katombe, M. (2018), The Effect of Leadership on the Resistance to Change in an Organization. OD Practitioner, 50(3), p. 47–55.

[15] Lines, B.C., Sullivan, K.T., Smithwick, J.B. and Mischung, J. (2015) Overcoming resistance to change in engineering and construction: Change management factors for owner organizations. International Journal of Project Management, 33(5), p.1170-1179.

[16] Maltseva, A.A. and Klyushnikova, E. (2017) Motivation of resistance to change in creative research teams: issues of scientists'typology. The Turkish Onlain Journal of Design and Communication. Special Edition, p.1916-1928.

[17] Oreg, S. (2018) Resistance to change and performance: Toward a more even-handed view of dispositional resistance. The Journal of Applied Behavioral Science, 54(1), p. 88-107.

[18] Patterson, K. and Wigham, G. (2019), Management of Change - what does a „good" system look like?, Loss Prevention Bulletin, 267, p. 7–10.

[19] Prediscan, M. and Roiban, R.N. (2014) The main forces driving change in the Romanian SME's. Procedia-Social and Behavioral Sciences, 124, p. 236-245.

[20] Sarkar, S. and Osiyevskyy, O. (2018) Organizational change and rigidity during crisis: A review of the paradox. European Management Journal, 36(1), p. 47-58.

[21] Shimoni, B., (2017) What is resistance to change? A habitus-oriented approach. Academy of Management Perspectives, 31(4), p. 257-270.

[22] Stanleigh, M. (2008) 'Effecting successful change management initiatives', Industrial & Commercial Training, 40(1), p. 34–37.

[23] Tobore, T. O. (2019), On Energy Efficiency and the Brain's Resistance to Change: The Neurological Evolution of Dogmatism and Close-Mindedness. Psychological Reports, 122(6), p. 2406–2416.

[24] Todnem By, R. (2005) Organisational change management: A critical review. Journal of change management, 5(4), p. 369-380.

НАЙ-ЧЕСТИТЕ ТИПОВЕ СОФТУЕРНИ УЯЗВИМОСТИ В КИБЕРСИГУРНОСТТА ПРЕЗ ПОСЛЕДНИТЕ ГОДИНИ И НАСОКИ ЗА ТЯХНОТО ОТКРИВАНЕ И ПРЕДОТВРАТЯВАНЕ

Стоян Р. Стоянов

THE MOST COMMON TYPES OF CYBERSECURITY SOFTWARE VULNERABILITIES IN RECENT YEARS AND GUIDELINES FOR THEIR DETECTION AND PREVENTION

Stoyan R. Stoyanov

ABSTRACT: *Cyber security research has seen significant growth in recent years. Some of it is oriented towards discovering ways to avoid the main application security threats. Such threats include software vulnerabilities. This paper aims to identify the most common types of software vulnerabilities in the last few years (2018-2023). In order to achieve this goal, the reports of several popular cybersecurity platforms specialized in software vulnerability detection and management are reviewed and analyzed. After analyzing the selected reports, important software vulnerabilities are identified according to their frequency of occurrence. In the study, software vulnerabilities are categorized and described with their main features. General guidelines for the detection and prevention of future problems related to software vulnerabilities are also provided.*

KEYWORDS: *Software vulnerabilities, Cyber security, Vulnerabilities scanning tools.*

Въведение

В днешният дигитализиран свят използването на софтуерни приложения навлиза все по-широко в живота ни при изпълнението на всякакъв вид дейности в личен и професионален план, като например бизнес, пазаруване, банкови транзакции, реклами, услуги и др. Това неминуемо води и до също толкова рязък скок в ръста на престъпленията, свързани с киберсигурността. Основната причина за това нарастване е огромното разнообразие от всякакъв вид софтуерни приложения (предимно уеб), които от своя страна може да притежават грешки в дизайна, които киберпрестъпниците да използват, за да получат незаконен достъп до системите. Ето защо киберсигурността се превръща във важен проблем за специалистите и разработчиците в областта.

Киберсигурността може да се дефинира като съвкупност от инструменти, техники, политики, мерки и насоки за сигурност, стратегии за намаляване на риска, действия, обучение, добри практики, проверка на сигурността и най-нови технологии, които могат да се използват за защита на киберпространството и активите на потребителите. В днешно време тя се е превърнала във въпрос от глобален интерес и значение и включва защита на информацията чрез откриване, предотвратяване и отговор на кибератаки. Важен аспект от задачите на киберсигурността е и откриването, отстраняването и предотвратяването на уязвимости, свързани със софтуера. [1, 20]

Уязвимостта е недостатък в даден продукт или система, който потенциално може да позволи на нападателя да подкопае поверителността, целостта или наличността на този продукт или система. Софтуерните уязвимости се появяват, когато приложенията съдържат грешки или бъгове, които се разглеждат от нападателите като възможност да се възползват от тези слабости, за да компрометират системата [2].

Ежедневно разработчиците на софтуер създават огромни количества нови приложения. Понякога това става толкова бързо, че тестовете за сигурност често са пропускани или извършвани неадекватно, както на етапа на разработване, така и на етапа на тестване. Липсата на познания за процесите и изискванията за разработване на сигурен софтуер задълбочава проблема. Използването на приложенията на различни платформи и устройства също създава уязвимости, които увеличават общия брой на свързаните с тях атаки.

Кратка история на софтуерните уязвимости

Първите компютри се появяват в началото на 40-те години на миналия век. Използвали са се ограничено и не са били свързани в мрежа. Поради липсата на обмен на данни между тях, не е имало и заплахи или атаки.

Терминът "хакерство" при компютърните системи се появява за първи път през 60-те години на миналия век. През 1965 г. е открита първата уязвимост в машината IBM 7094 Compatible Time-Sharing System (CTSS). През 1967 г. група студенти изследват нов компютър разработен от IBM. Те научават езика и получават достъп до различни части на системата, доказвайки, че компютърните системи имат уязвимости. Основите на киберсигурността започват в началото на 70-те години на миналия век с проект, наречен "The Advanced Research Projects Agency Network" (ARPANET) - първата мрежа с комутация на пакети преди появата на интернет. През 1971 г. Боб Томас създава първия вирус, наречен "Creeper", който може да се движи по мрежата ARPANET. След "Creeper" Рей Томлинсън създава "Reaper", който също може да се движи по ARPANET и да изтрива "Creeper". "Reaper" е първият пример за антивирусна програма. През 1979 г. известният хакер Кевин Митник е арестуван за първи път за киберпрестъпно поведение [2].

През 80-те години на XX век са наблюдавани няколко атаки, свързани с компютърни системи. През това десетилетие основно са използвани компютърни вируси. Появява се терминът "кибершпионаж". През 1985 г. Министерството на

отбраната (МО) на Съединените американски щати създава насоки за компютърна сигурност, наречени "Критерии за оценка на надеждни компютърни системи" (TCSEC), които по-късно са наречени "Оранжева книга". TCSEC е първото ръководство за сигурност на компютърните системи. [2, 21]

През 1986 г. германският хакер Маркус Хес прониква в системите на правителствата на САЩ, Източна Азия и Европа. Той успя да получи достъп до около 400 военни компютъра. През 1987 г. за първи път е пуснат търговски антивирусен софтуер. През 90-те години на XX век се наблюдава огромен ръст на компютърните системи и Интернет. Компютърният вирус и различните му версии стават много популярни.

През 1996 г. се появяват макровирусите. В края на 90-те години вирусите Melissa и ILOVEYOU заразяват милиони компютри по света. През 1995 г. Netscape въвежда протокола Secure Sockets Layer (SSL), който осигурява сигурността на потребителските връзки в компютърната мрежа.

В началото на века Интернет се разраства експоненциално, а компютрите стават все по-разпространени в работна и домашна среда. Но увеличеното използване на компютри води и до увеличаване на киберпрестъпността. Първата организирана хакерска група се появява през 2000 г., а компютърните червеи и троянските коне стават популярни методи за атака.

През 2010 г. са установени няколко пробива в сигурността на софтуера и протоколите на компютърните мрежи. В резултат на това физически лица загубват милиони долари, а големи компании и държави - милиарди годишно. През 2016 г. злонамереният софтуер Mirai използва уязвимост за IoT устройства, за да извършва DDoS атаки.

В периода 2010-2020 г. са популярни атаките, свързани с рансъмуер. Така например рансъмуерът WannaCry криптира компютърни системи и засяга 150 държави по света, а рансъмуерът LockerGoga блокира заразени системи и причинява щети за милиони долари. През 2020 г. рансъмуерът CovidLock криптира данни на устройства с Android и отказва достъп до тях.

През 2020 г. хакването на почти всичко в цифровия свят е възможно. Някои професионални уебсайтове дори предоставят автоматични приложения и инструменти за хакване като услуга. Навременните и ефективни кибератаки могат да доведат до огромни печалби, поради което големите компании и правителствата инвестират значителни средства в тази област [2].

Категории софтуерни уязвимости

Повечето кибератаки все още се дължат на грешки, уязвимости и недостатъци в приложния софтуер. Тези уязвимости и грешки се увеличават с всеки изминал ден. Водещите причини за уязвимостите и грешките, свързани със софтуера, могат да бъдат изброени, както следва [2]:

- Грешки при валидиране на входни данни;
- Проблеми с контрола на достъпа на потребителите;
- Непълно или неправилно удостоверяване;

— Проблем с директорията за миграция;
— Препълване на буфера;
— Проблеми, причинени от Structured Query Language (SQL);
— Cross-site scripting (XSS);
— Използване на компоненти с известни уязвимости;
— Проблеми с уеб услуги и API;
— Неправилно тестване на сигурността на софтуера.

Този списък включва много и най-различни софтуерни уязвимости, но ако трябва да ги обобщим и категоризираме, то най-честите попадат в следните категории:

- **XSS уязвимости**

XSS (Cross-site scripting) е вид уязвимост, която може да застраши уеб приложенията чрез инжектиране на злонамерен код. XSS се класира на 4-то, 4-то, 1-во, 3-то и 7-мо място в топ 10 на проекта OWASP съответно през 2004, 2007, 2010, 2013 и 2017 г. [7]. Уязвимостта XSS е много често срещана и разпространена уязвимост при Web приложенията. Експлоатирането ѝ може да доведе до много сериозни проблеми. В зависимост от това, дали предоставените от потребителя ненадеждни данни са включени в HTTP отговора, генериран от сървъра, или се намират някъде в DOM на HTML страниците, XSS уязвимостите могат да бъдат разделени на уязвимости от страна на сървъра и уязвимости от страна на клиента. XSS от страна на сървъра включва главно отразения XSS и съхранения XSS. Уязвимостта от страна на клиента се отнася до XSS, базиран на DOM [1].

- **XSS, базиран на DOM**, е известен и като XSS тип 0. Той се причинява от несигурен код от страна на клиента, а не от код от страна на сървъра. Този вид уязвимост може да възникне в страници, съдържащи JavaScript код, като *document.write()* или *eval()*. Нападателят създава връзка със зловреден JS код и я изпраща на жертвата. Когато жертвата кликне върху връзката, тя ще получи отговор без зловредния код. Зловредният код се изпълнява от страна на клиента и нападателят може да получи чувствителна информация от жертвата [1].

- **Съхраненият XSS** е известен също като XSS тип 1. Този вид уязвимост е вероятно да се случи в уебсайтове като форуми или блогове. Нападателят поставя зловредния код в своите заявки към уебсайтовете, а те съхраняват тези заявки директно в базите данни. Когато жертвата преглежда това съдържание, се задейства XSS атаката [1].

- **Отразеният XSS** е известен също като XSS тип 2. Процесът на отразената XSS атака е подобен на DOM-базираната, като разликата е, че зловредният код е включен в отговора на уебсайтовете. Нападателите обикновено вмъкват зловредни скриптове в URL адрес. Когато жертвата кликне върху връзката, тя ще получи отговор със зловреден код от уебсайта. След изпълнението на кода, нападателят ще получи достъп до чувствителни данни. За разлика от DOM базираните XSS уязвимости, отразеният XSS е уязвимост от страна на сървъра [1].

- **Инжектиране**

Инжектирането е вид уязвимост, която възниква, когато дадено приложение изпраща ненадеждни данни към интерпретатор като част от команда или заявка. Тези ненадеждни данни обикновено са входящи данни, получени от потребителя (като входящи данни от формуляри, параметри на URL адреси, HTTP хедъри и т.н.), които приложението не успява да обработи правилно, преди да ги включи в команда или заявка. Основната характеристика на грешките при инжектиране е, че те позволяват на нападателя да инжектира злонамерен код в системата, който след това се изпълнява от интерпретатора, което води до различни вредни резултати. Инжектиранията са особено опасни, тъй като могат да доведат до различни атаки, включително нарушаване или загуба на целостта на данните, отказ от услуга и пълно компрометиране на системата.

- **SQL инжектирането** е вид уязвимост при уеб приложенията, която позволява на нападателя да променя и вмъква SQL команди и да извлича данни от базата данни. В случай че потребителските данни не са достатъчно защитени, без проверка и кодиране на данните, нападателят може да получи достъп до чувствителни данни на потребителя, като например кредитна карта или друга чувствителна финансова информация. SQL инжектирането се счита за една от най-опасните заплахи за уебсайтовете, а също и за базите данни [3].

- **Препълване на буфера (Buffer overflow)**: Една от най-често срещаните опасности в съвременния софтуер. Появява се често в списъците на Bugtraq и CERT advisories. Предпочитани са при атаки с отдалечено проникване, защото дават възможност за инжектиране на код и изпълнението му на целевата система. Така може да се стартира системен шел с повишени привилегии и да се получи достъп до цялата файлова система, както и да се използва машината за бъдещи атаки срещу други системи. Когато този процес се автоматизира, той може да бъде използван за пускането на червеи [4].

- **Инжектиране на команди (Command Injection)**: Това се случва, когато дадено приложение предава несигурни данни, предоставени от потребителя (формуляри, бисквитки, HTTP хедъри и т.н.), на системната обвивка. Използвайки уязвимо приложение, нападателят може да изпълни произволни команди в операционната система на хоста.

- **LDAP инжектиране**: При този тип инжектиране нападателите използват уязвимости в софтуера на уеб приложение, за да конструират извлечения от LDAP (Lightweight Directory Access Protocol) въз основа на въведени от потребителя данни. Ако приложението не успее да обработи правилно подадения от потребителя вход, може да се окаже възможно нападателят да промени конструкцията на LDAP извлечението.

- **XML External Entity (XXE) инжектиране**: Тази атака се реализира, когато XML вход, съдържащ препратка към външна структура, се обработва от слабо конфигуриран XML анализатор. XXE атаките могат да доведат до разкриване на чувствителни данни, отказ от услуга, подправяне на заявки от страна на сървъра и други въздействия върху системата.

- **Инжектиране на код**: Включва инжектиране на код, който след това се интерпретира/изпълнява от приложението. В зависимост от случая това може да бъде цял скрипт или само част от него. Различава се от инжектиране на команда по това, че нападателят може да инжектира код, който след това се изпълнява от самото приложение.
- **XPath инжектиране**: Тази атака се осъществява в приложения, които използват предоставена от потребителя информация за конструиране на XPath заявки за XML данни. Чрез изпращане на специално създадени данни към сървъра атакуващият може да промени конструкцията на XPath заявките и евентуално да получи неоторизиран достъп до данни.

- **Разкриване на чувствителна информация**

Това включва недостатъчна защита на чувствителна информация, включително лични данни, финансова информация и удостоверения. Често срещаните проблеми включват слабо криптиране, неправилно съхранение на пароли и несигурно предаване на данни [5].

- **Нарушено удостоверяване**

Нарушеното удостоверяване (автентикация) е вид уеб уязвимост, която се появява поради неправилна конфигурация на управлението на сесиите. След приключване на процеса на автентикация се създава сесия, която се използва за предаване на данни между сървъра и даден потребител. Ако нарушител успее да получи достъп до активната сесия на конкретен потребител, заобикаляйки процеса на автентикация, сценарият се третира като проблем с експлоатиране на уязвимост от типа „нарушено удостоверяване“ [6].

- **Неправилна конфигурация на сигурността**

Поради широкия си обхват неправилното конфигуриране на сигурността е много често срещано явление. Тя включва проблеми като неправилно конфигурирани позволения, идентификационни данни по подразбиране, ненужно стартирани услуги и лошо конфигурирани хедъри за сигурност [5].

- **Незащитено десериализиране**

Тази уязвимост, макар и по-рядко срещана в сравнение с други, е все по-често идентифицирана и използвана в различни приложения. Тя може да доведе до отдалечено изпълнение на код, replay атаки и други експлойти.

- **Нарушен контрол на достъпа**

Неправилното прилагане на контрола на достъпа може да доведе до неоторизиран достъп до данни и функционалности, които би трябвало да са ограничени до определени потребители. Този вид уязвимост е често срещана в уеб приложенията.

Методология

В статията като източници на данни са използвани отчетите на няколко платформи за киберсигурност, откриване и управление на уязвимости. Това са EdgeScan, MaxPatrol 8 и HackerOne.

Edgescan е услуга за киберсигурност, която предоставя решения за непрекъснато управление на уязвимостите и тестване за проникване. Това е платформа за софтуер като услуга (SaaS), която съчетава автоматизирано сканиране с ръчен експертен опит в областта на тестването за проникване, за да идентифицира и управлява уязвимостите в сигурността на уеб приложения, облачни среди и мрежова инфраструктура. Edgescan е създаден, за да помогне на организациите да идентифицират и управляват ефективно уязвимостите, да осигурят проактивен подход към киберсигурността и да намалят риска от кибератаки. Той е особено полезен за компании, които търсят цялостен и непрекъснат подход към управлението на уязвимостите, съчетаващ автоматизация с експертен надзор [16].

MaxPatrol 8 е решение за управление на уязвимости и съответствие, разработено от Positive Technologies. То е предназначено за цялостен анализ на сигурността, оценка на уязвимостите, мониторинг на съответствието и мрежови одити в различни среди, включително мрежи, системи и приложения. MaxPatrol 8 обикновено се използва от организациите за подобряване на тяхната позиция по отношение на киберсигурността, осигуряване на съответствие с различни регулаторни стандарти и защита от широк спектър от заплахи за сигурността. MaxPatrol 8 е особено подходящ за големи и средни компании, които се нуждаят от цялостен подход към управлението на сигурността и съответствието. Като осигурява комбинация от оценка на уязвимостите, мониторинг на съответствието и управление на риска, той помага на организациите да се справят проактивно с предизвикателствата на киберсигурността [19].

HackerOne е платформа за киберсигурност, която свързва компаниите с изследователи в областта на киберсигурността и етични хакери, за да им помогне да идентифицират и отстранят уязвимости в сигурността. Тя е известна със своите услуги за възнаграждение за откриване и за координиране на уязвимости. Платформата е създадена, за да улесни отговорното докладване и управление на проблеми със сигурността, открити в продукти и услуги. HackerOne е широко признат в индустрията за киберсигурност и се използва от различни организации - от стартиращи компании до големи корпорации - за подобряване на тяхната сигурност. Като използват уменията на етичните хакери, компаниите могат проактивно да откриват и отстраняват уязвимости, намалявайки риска от използването им от злонамерени субекти [18].

За критерий дали една уязвимост може да се смята за една от най-често срещаните, е тя да попада в Топ 10 на най-често засичаните от дадената платформа.

Анализ на данните

В отчета на **MaxPatrol 8** са представени резултатите от автоматизираната оценка на сигурността на мрежовия периметър на избрани корпоративни информационни системи. Сканирането е извършено с помощта на системата за управление на уязвимостите и съответствието MaxPatrol 8 в режим Pentest. Докладът се отнася за 19-те най-представителни проекта на компанията от 2019

г. и първата половина на 2020 г. Сканирани са общо 3514 хоста, включително мрежови устройства, сървъри и работни станции [19]. Резултатите от сканирането показват следното:

— Разкриването на чувствителна информация е засечено в 100% от хостовете

— Нарушеното удостоверяване – в над 70% (Изброяване на потребители – 74% и недостатъчна авторизация – 63%)

— XSS уязвимости са открити в 58% от хостовете

— Също в 58% от хостовете са открити уязвимости от типа „незащитена десериализация“ (Изпълнение на произволен код).

— В 53% от случаите са открити уязвимости от типа „нарушен контрол на достъпа“ (Ескалация на привилегии).

Разгледаното тук проучване на **HackerOne** е проведено през септември 2022 г. и в него са участвали 5 738 хакери от цял свят [18]. Данните от платформата HackerOne обхващат периода юни 2021 г. - юни 2022 г. Различното тук е, че за разлика от другите класации, десетте топ уязвимости са подредени по размера на средствата, изплатени на хакери да открият тези уязвимости.

HackerOne Топ 10 на уязвимостите за 2022 г. е подреден така:

1. Cross-site Scripting - XSS
2. Неправилен контрол на достъпа
3. Разкриване на чувствителна информация
4. Несигурна директна препратка към обект (IDOR)
5. Неправилно удостоверяване на автентичността
6. Ескалация на привилегиите
7. Инжектиране на код
8. Неправилно оторизиране
9. SQL инжектиране
10. Фалшифициране на заявки от страна на сървъра

Обобщавайки тези резултати по категории виждаме, че първо място е заето от **XSS** уязвимостите, 2-ро и 6-то са за уязвимости от типа **нарушен контрол на достъпа**. На трето място са уязвимостите, свързани с **разкриване на чувствителна информация**, а на 5-то и 8-мо – с **нарушено удостоверяване**. На 7-мо и 9-то място са класирани уязвимости от типа **инжектиране**.

HackerOne са представили и отделни под-класации на уязвимостите в различните сектори на индустрията, като: правителствен сектор, финансови услуги, автомобилна индустрия, компютърен софтуер, криптовалути и блокчейн, интернет и онлайн услуги, търговия и телекомуникации. В тези под-класации почти всички позиции са заети от уязвимости от типа XSS, инжектиране, разкриване на чувствителна информация, нарушено удостоверяване и нарушен контрол на достъпа.

Докладът на **EdgeScan** за 2023 г. демонстрира състоянието на сигурността на full stack системите въз основа на хиляди оценки на сигурността и тестове за

проникване, извършени от платформата върху милиони активи през 2022 г. В него са анализирани уязвимостите, открити в системите на стотици организации в широк спектър от индустрии - от Fortune 500, до средни и малки компании. Докладите предоставят статистически модел на най-често срещаните слабости, с които се сблъскват организациите [16].

В доклада **XSS** уязвимостите са съответно на:

- 1-во място сред уязвимостите със средна степен на опасност при Web приложенията (19.1%)
- 2-ро място сред уязвимостите с висока степен на опасност при Web приложенията (12.9%)
- 3-то място сред уязвимостите с критична степен на опасност при Web приложенията (19.1%)

Уязвимостите с **инжектиране** са на:

- 1-во място сред уязвимостите с критична и висока степен на опасност при API интерфейсите – 27.3%
- 3-то място сред уязвимостите с висока степен на опасност при Web приложенията (XML инжектиране – 9.8% и дистанционно инжектиране на команди – 3.1%)
- 4-то място сред уязвимостите със средна степен на опасност при Web приложенията (Xpath инжектиране – 6.8% и Host Header инжектиране – 1.8%)
- 8-мо място сред уязвимостите с критична степен на опасност при Web приложенията (Обхождане на файловият път – 1.4%)

Уязвимостите с **разкриване на чувствителна информация** са класирани съответно на:

- 5-то място сред уязвимостите със критична и висока степен на опасност при API интерфейсите – 6.9%
- 7-мо място при уязвимостите с висока степен на опасност при Web приложенията – 3.6%
- 9-то място при уязвимостите със средна степен на опасност при Web приложенията – 2.5%

Уязвимости с **нарушено удостоверяване**:

- 1-во място при уязвимостите с висока степен на опасност при Web приложенията – 23.2% (нарушена автентикация – 14.7% и недостатъчна авторизация – 8.5%)
- 2-ро място при уязвимостите с критична степен на опасност при Web приложенията – 9.2% (Проблеми с авторизацията и привилегиите – 7.8% и слаби пароли – 1.4%)
- 3-то място при уязвимостите с критична и висока степен на опасност при API интерфейсите – 15.3%
- 4-то място при уязвимостите със средна степен на опасност при Web приложенията – 7.6% (Изброяване на потребители)

Уязвимости с неправилна конфигурация на сигурността:

— 6-то място при уязвимостите с висока степен на опасност при Web приложенията – 5.4% (Качване на зловреден файл)

Уязвимости с незащитено десериализиране:

— 1-во място при изложените към Интернет уязвимости с критично ниво на опасност – 3% (Apache Log4Shell)

— 3-то място при уязвимостите с критична степен на опасност при Web приложенията – 9.3% (Log4Shell – 5% и Spring4Shell – 4.3%)

Насоки и инструменти за откриване, отстраняване и предотвратяване на софтуерни уязвимости

Най-препоръчваният метод за отстраняване на грешки, недостатъци и уязвимости са **редовните актуализации** на софтуера. Но това не винаги осигурява решение. Често по време на софтуерните актуализации грешките и уязвимостите не се отстраняват. В някои случаи новите актуализации дори предизвикват нови проблеми. Най-ефективният начин да се сведат до минимум проблемите, свързани със софтуерни уязвимости, е да се изготви безгрешен **дизайн и изисквания** за конкретния софтуер, още преди написването на кода в жизнения цикъл на процеса на разработка. Ето защо е изключително важно разработчиците на софтуер да преминат обучение в което да се запознаят с изискванията и процеса на разработка на сигурен софтуер. Практиката първо бързо да се създаде софтуер, а чак след това да се правят опити за отстраняване на уязвимостите в сигурността му, не е правилен подход. Заплахите за сигурността и възможните атаки трябва да се вземат предвид още по време на разработването на софтуера, а всички блокове код трябва да се тестват ръчно и автоматично на всеки един етап. [2, 17]

Съществуват **инструменти**, които откриват уязвимости в сигурността на устройствата и софтуера в системите. Повечето от тях използват бази данни с уязвимости, за да извършват сканиране за конкретни такива. Тези бази данни могат да бъдат получени от реномирани лаборатории за тестване на сигурността или от известни бази, използвани за идентифициране на уязвимости в софтуера и хардуера. Ефективността на откриване на уязвимостите зависи от базата данни, която инструментът използва. Когато се избира инструмент за сканиране на уязвимости, трябва да се вземат предвид много характеристики, като например разнообразието от устройства, които може да сканира и методите на сканиране и предупреждение/отчитане [2]. По-долу са разгледани няколко от най-широко използваните днес инструменти за сканиране на уязвимости.

Invicti: Много точен автоматичен скенер, който определя уязвимостите в приложенията и API в интернет. Invicti допълнително потвърждава откритите уязвимости и доказва, че те са истински, а не фалшиво позитивни. Ето защо не е необходимо последващо ръчно потвърждаване. Наличен е за Windows и онлайн [8].

Acunetix: Напълно автоматизиран скенер за уеб уязвимости, откриващ над 4500 уязвимости в уеб приложения, SQL инжекции и XSS. Използва

усъвършенствани функционалности за управление на уязвимостите, класифицира рисковете според информацията чрез единна и консолидирана перспектива и комбинира резултатите от сканирането с такива от допълнителни инструменти и платформи [9].

Intruder: Този скенер се отличава със способността си да проследява средното време за отстраняване на уязвимост и да предоставя оценка на киберхигиената. Той сканира за различни уязвимости, включително неправилни конфигурации и липсващи пачове за сигурност. Intruder се интегрира с платформи като AWS, Google Cloud, GitHub и ServiceNow [11].

OpenVAS: Инструмент с отворен код, предназначен за централизирано сканиране и управление на уязвимости. Той е достъпен безплатно и обикновено е лицензиран под Общия публичен лиценз на GNU (GPL). Софтуерът е съвместим с редица операционни системи. OpenVAS разполага с редовно актуализиран механизъм за сканиране с тестове за мрежови уязвимости. Това е цялостен инструмент за оценка на уязвимостите, използван за идентифициране на проблеми, свързани със сигурността на сървъри и други мрежови устройства [12].

Nexpose: Инструмент с отворен код, който извършва проверки на мрежата и сканира за уязвимости. Използва се за наблюдение на излагането на уязвимости в реално време и за информиране за възникващи заплахи с помощта на нови данни. Приоритизира уязвимостите в сигурността и ги адресира по съответния начин. Инструментът автоматично идентифицира и сканира нови устройства, като оценява уязвимостите им при свързването им към мрежата. Nexpose може да бъде интегриран с фреймуърка Metasploit [13].

Nikto: Широко предпочитан уеб скенер с отворен код, използван за оценка на потенциални уязвимости и проблеми в уеб сървърите. Прави подробни тестове на уеб сървъри, за да идентифицира опасен софтуер или файлове, потвърждава, че версията на сървъра е актуална и идентифицира всякакви проблеми, влияещи на работата му. Nikto сканира различни протоколи, като HTTP, HTTPS и HTTPD. Може също и да сканира множество сървърни портове [14].

Wireshark: Признат и широко използван анализатор на мрежови протоколи. Инструментът открива проблеми в реално време и извършва анализи офлайн. Съвместим е с няколко платформи, включително Windows, Linux, Mac и Solaris, и може да изследва множество протоколи в големи подробности [15].

Burp Suite: Burp Suite е универсално решение за сигурност и тестване на приложения, което може да се адаптира към различни нива на изисквания на потребителите - от базово тестване за проникване до интегрирано тестване на сигурността на ниво компания. Burp Suite се предлага в три варианта: Community (безплатен), Professional и Enterprise. Всяко от тях е предназначено за различни нужди на потребителите - от индивидуални хакери до големи компании. Наличен е за Windows, macOS и Linux. Високо оценен заради своята поддръжка, практичност, изчерпателните си инструменти и ефективността при идентифицирането на грешки и уязвимости [10].

Спазването на посочените по-горе насоки за предотвратяване появата на уязвимости в софтуера, както и употребата на изброените инструменти за откриването им, са една добра основа за справяне с настоящи и бъдещи проблеми със софтуерната сигурност.

Заключение

Извършеният анализ на отчетите от избраните платформи за киберсигурност показва, че в последните години сред софтуерните уязвимости в компютърните системи и мрежи доминират следните типове уязвимости: cross-site scripting (XSS); инжектиране (на код, команди, SQL и др.); разкриване на чувствителна информация; неправилна конфигурация на сигурността; нарушено удостоверяване; нарушено десериализиране; нарушен контрол на достъпа.

В бързо развиващия се дигитализиран свят постоянната бдителност и адаптиране в областта на киберсигурността е от критична важност. Технологиите и заплахите в киберпространството се развиват непрекъснато, което изисква от организациите и отделните потребители да бъдат винаги нащрек и готови да адаптират своите защитни мерки. Без нужната бдителност и подготовка системите могат бързо да станат уязвими към нови видове атаки, водещи до сериозни нарушения в сигурността, загуба на данни и финансови средства. Активното следене на новите тенденции в киберсигурността и обновяването на защитните практики са ключови за поддържането на силна защита срещу кибер заплахите. Една от тези тенденции са и най-честите софтуерни уязвимости. Познаването на моментната картина на този проблем би помогнало за изготвянето на по-добри стратегии, практики и инструменти за откриването, отстраняването и предотвратяването им в бъдеще.

ЛИТЕРАТУРА

[1] Liu, M., Zhang, B., Chen, W., Zhang, X. A Survey of Exploitation and Detection Methods of XSS Vulnerabilities, in IEEE Access, vol. 7, pp. 182004-182016, 2019, doi:10.1109/ACCESS.2019.2960449.

[2] Aslan, Ö., Aktuğ, S., Ozkan-Okay, M., Yilmaz, A., Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. 2023, 12(6):1333.

[3] Baklizi, M., Atoum, I., Abdullah, N., Al-Wesabi, O. A., Otoom, A. A., Hasan, M. A.-S. (2022). A Technical Review of SQL Injection Tools and Methods: A Case Study of SQLMap. International Journal of Intelligent Systems and Applications in Engineering, 10(3), pp. 75–85.

[4] Shaneck, M. An Overview of Buffer Overflow Vulnerabilities and Internet Worms, University of Minnesota, 2003

[5] Sulatycki, R., Fernandez, E. 2015. Two threat patterns that exploit "security misconfiguration" and "sensitive data exposure" vulnerabilities. In Proceedings

of the 20th European Conference on Pattern Languages of Programs (EuroPLoP '15). Association for Computing Machinery, New York, NY, USA, Article 46, 1–11. doi:10.1145/2855321.2855368

[6] Hassan, M., Nipa, S., Akter, M., Haque, R., Deepa, F., Rahman, M., Siddiqui, M., Sharif, M.H. (2018). Broken Authentication and Session Management Vulnerability: A Case Study of Web Application. International journal of simulation: systems, science and technology, doi:10.5013/IJSSST.A.19.02.06

[7] OWASP Top 10 Vulerabilities - https://owasp.org/Top10/ - (20.01.2024)

[8] Invicti - https://www.invicti.com/ - (20.01.2024)

[9] Acunetix - https://www.acunetix.com/vulnerability-scanner/ - (20.01.2024)

[10] Burp Suite - https://portswigger.net/burp - (20.01.2024)

[11] Intruder - https://www.intruder.io/ - (20.01.2024)

[12] OpenVAS - https://www.openvas.org/ - (20.01.2024)

[13] Nexpose - https://www.rapid7.com/products/nexpose/ - (20.01.2024)

[14] Nikto - https://www.cirt.net/nikto2/ - (20.01.2024)

[15] Wireshark - https://www.wireshark.org/ - (20.01.2024)

[16] EdgeScan: 2023 Vulnerability Statistics Report, 8th Edition - https://www.edgescan.com/vulnerability-statistics-snapshot-updated-oct23/ - (20.01.2024)

[17] Denev D., Konstantinova E. Main Issues in the Protection of Information in the system of National and Corporate Security. 2020, MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 110-115.

[18] HackerOne: Hacker-Powered Security Report 2022 - https://h-isac.org/wp-content/uploads/2023/03/HackerPowered-Security-Report-2022-1.pdf - (20.01.2024)

[19] Positive technologies: Vulnerabilities on the corporate network perimeter - https://www.ptsecurity.com/upload/corporate/ww-en/analytics/vulnerabilities-corporate-networks-2020-eng.pdf - (20.01.2024)

[20] Konstantinova E., Karadocheva M., Tsankov Ts. The invisible Internet and cyber security. International scientific conference 2019, “Vasil Levski” National military university, “Artillery, aircraft defense and CIS” faculty, Shumen, 2019, ISSN 2367-7902, pp. 519-524.

[21] Simeonova I. Definition of information security as a main channel of administrative security. Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921.

ТЕХНИЧЕСКИ СРЕДСТВА В ОБУЧЕНИЕТО ПО ГЕОГРАФИЯ

Мирослав Н. Кацаров

TECHNICAL MEANS IN GEOGRAPHY TRAINING

Miroslav N. Katsarov

ABSTRACT: *Combining media and technology in the educational process supports active and engaging geography learning by providing students with many and varied opportunities to study, understand and explore geographic objects, phenomena and processes. The article reviews the most used technical means in geography education. Technical aids in teaching geography have an important role in supporting the educational process and in facilitating learning. The inclusion of modern technologies provides opportunities to increase interest in the educational process while making it more effective.*

KEYWORDS: *Geography, Training, Technical means, Technology.*

Средствата в обучението по география са разнообразни и включват традиционни, иновативни и технологични ресурси. Те подпомагат преподавателите и учениците в изучаването на предмета география, като предоставят възможности за визуализация, интерактивност и по-добро разбиране на географските обекти, явления, процеси и концепции. Традиционните учебници и учебни материали предоставят базовата географска информация и са основен ресурс в учебния процес. [1, 2, 3, 4,]

Комбинирането на средства и технологии в образователния процес подкрепя активното и ангажиращото обучение по география като предоставя на учениците много и различни възможности за изучаване, разбиране и изследване на географските обекти, явления и процеси. Техническите средства в обучението по география имат важна роля в подпомагането на образователния процес и в улесняването на ученето. Включването на съвременни технологии предоставя възможности за повишаване на интереса към обучителния процес като същевременно го прави по-ефективен.

Основни технически средства, използвани в обучението по география

Всички тези съвременни технически средства, използвани поединично или в комбинирани варианти, създават обогатена учебна среда, която стимулира

интереса и активното участие на учениците при изучаването на географията като учебен предмет (табл. 1.).

Таблица 1.

ТЕХНИЧЕСКИ СРЕДСТВА В ОБУЧЕНИЕТО ПО ГЕОГРАФИЯ				
Интерактивни дъски	Географски информационни системи (ГИС)	Виртуални екскурзии и 360°-снимки	Онлайн ресурси	Картографски софтуер и апликации
Презентационни софтуери	Учебни платформи	Виртуална реалност (VR)	Разширена реалност (AR)	Специализирани сензори и датчици

Интерактивни дъски и презентационни софтуери

Интерактивните дъски позволяват на учителите да създават динамични учебни презентации. Интерактивните дъски се използват за визуализация на географски обекти (рисунки и обяснения към тях) – планини, реки, страни и др., за интерактивни упражнения – създаване на различни задачи като учениците маркират на картата географски елементи или решават картографски задачи. Интерактивните дъски се използват и за представяне на географски данни - визуализация и анализ на статистически данни, свързани с климата, населението, стопанството и т.н. Използват се и за създаване на интерактивни презентации.

Презентационни софтуери като **PowerPoint**, **Prezi** и **Google Slides** се характеризират с визуална атрактивност – използват за създаване на образователни и визуално привлекателни и интересни материали с цел представяне на географски идеи, концепции, обекти, процеси и явления. Добавянето на интерактивни елементи към презентациите - хипервръзки към онлайн ресурси, вградени карти и графики, допълват успешно учебния материал. Налице е възможност за създаване на мултимедийни материали - интегриране на мултимедийни елементи като видео и аудио файлове, които обогатяват презентациите с допълнителна информация. Презентационните софтуери позволяват лесно споделяне и сътрудничество между ученици и учители, както и коментари и обратна връзка. Шаблоните улесняват създаването на привлекателни и добре структурирани презентации. [5, 11, 12, 17, 20]

Интерактивните дъски и презентационните софтуери са важни инструменти в съвременното образование, включително и в обучението по география. Тези технологии предоставят възможности за пълноценно ангажиране на учениците и визуализация на географските обекти, процеси, явления или концепции.

Географски информационни системи (ГИС)

ГИС позволяват на учителите и учениците да анализират и визуализират географски данни в различни контексти. Използването на ГИС може да обогати темите от учебното съдържание, свързани с картографията, изследванията на околната среда и анализа на териториалните явления. Географските

информационни системи (ГИС) представляват мощен инструмент за събиране, анализ и визуализация на географски данни. Те играят важна роля в обучението по география, предоставяйки възможности за дълбоко изследване и разбиране на пространствени връзки.

ГИС се използват в учебния процес в много аспекти: картография и визуализация - създаване на интерактивни и динамични карти, които могат да представят различни географски явления и тенденции; визуализация на сложни географски данни, което улеснява тяхното разбиране и анализ; анализ на територии и тенденции, свързани с тях - изследване на пространствени връзки и влияния, като например разпределението на населението, икономическите активности или климатичните промени; анализ на пространствените тенденции и прогнозиране на възможни бъдещи развития; теренни изследвания и приложения - използване на ГИС в теренни изследвания, където учениците могат да измерват, записват и анализират географски данни на място; създаване на приложения, които да помагат в различни сфери при реализиране на междупредметни връзки - биология, геология и др.; картографски проекти и дейности - учениците могат да създават свои собствени картографски проекти, които да включват различни теми, открития и интересни визуализации; работа в групи за решаване на географски задачи, които изискват колективно използване на ГИС; възможност за споделяне на географски данни, карти и анализи между ученици и учители; колективно изграждане на географски проекти, което стимулира сътрудничеството в учебната среда. [6, 7, 9, 21]

ГИС може да се интегрира с други технологии, като виртуална реалност или интерактивни дъски, за по-широк и иновативен образователен опит.

Географските информационни системи не само улесняват анализа на географски данни, но и насърчават учениците да развиват визуални, аналитични и пространствени умения. Те предоставят възможност за активно участие в изследването и разбирането на сложни географски явления.

Виртуални екскурзии и 360° снимки

Виртуалните екскурзии предоставят възможност за изследване на различни географски обекти и места, без да се налага физическо присъствие. 360° снимки могат да се използват за интерактивно запознаване с различни географски локации. Виртуалните екскурзии и 360-градусови снимки предоставят уникална възможност за учениците да изследват различни географски обекти и локации, без да напускат училището. Тези технологии обогатяват учебния процес и поддържат по-широко разбиране за глобалния свят.

Тези средства могат да бъдат интегрирани в обучението по география като екскурзии, свързани с природни забележителности - учениците могат да посещават национални паркове, планини, океани и други природни обекти или с исторически обекти - изследване на старинни градове, културни паметници и архитектурни съкровища от различни периоди в историята. 360° снимки – географски региони, градове и други населени места - предоставяне на учениците възможност да разглеждат 360° снимки от различни географски региони, като

сравняват климата, растителността и географските характеристики, изучаване на различни градове и населени места, анализиране на тяхната инфраструктура и уникални черти.

Тези средства се използват в образователни проекти, за проучване на конкретни географски теми, използват се активно и за осъществяване на междупредметни връзки (с биология, история, икономика). Удачно се интегрират и комбинират с виртуални уроци и с интерактивни образователни платформи.

Виртуалните екскурзии и 360° снимки подпомагат обучението по география, като предоставят визуални и имерсивни възможности за изучаване на глобалния свят. [7, 8, 13, 15, 19]

Онлайн ресурси и учебни платформи

Използването на онлайн ресурси, като текстове, статии, видео материали и интерактивни задачи, може да подкрепи самостоятелното учене. Учебните платформи, като Moodle или Google Classroom, предоставят възможности за комуникация и обмен на материали между ученици и преподаватели.

National Geographic Education предоставя безплатни учебни ресурси, интерактивни карти, уроци и видео материали, покриващи различни географски аспекти и науките за околната среда.

Google Earth for Education предоставя възможности за виртуални екскурзии, изследване на земната повърхност и създаване на интерактивни карти.

Esri GeoInquiries са кратки уроци, използващи Географски информационни системи (ГИС) за различни географски изследвания.

GeographyIQ предоставя информация за страни по света, включително статистически данни, културни аспекти и географска информация.

Geoguessr е онлайн игра, в която учениците се изправят пред предизвикателството да отгатнат местоположението на света чрез снимки от **Google Street View**.

Worldmapper предлага карти, на които са отразени различни статистически показатели като население, икономика и замърсеност.

BBC Bitesize Geography предлага онлайн ресурси и уроци, покриващи различни теми в областта на географията.

ArcGIS Online е уеб базирана платформа, която позволява на учениците да създават, споделят и анализират картографски продукти чрез Географски информационни системи (ГИС).

Google Classroom е платформа за управление на учебен процес, където учителите споделят материали, създават уроци и поддържат комуникация с учениците.

Kahoot! предоставя интерактивни игри и тестове, които учителите използват за проверка на знанията и за ангажиране на учениците.

Онлайн ресурсите и учебните платформи са важни компоненти в обучението по география, предоставяйки на учениците заобикалящи ги ресурси, визуални материали и възможности за самостоятелно учене. Използването на тези онлайн ресурси и платформи поддържа гъвкавостта и разнообразието в обучението по география, предоставяйки допълнителни ресурси и интерактивни инструменти. [6, 9, 16, 18, 22]

Картографски софтуер и апликации

Специализирани картографски софтуери като ArcGIS или QGIS позволяват на учениците да създават и анализират картографски продукти. Апликациите за мобилни устройства, които предоставят интерактивни карти и географски игри, могат да бъдат полезни за обучението.

ArcGIS Desktop е професионален Географски информационен софтуер, предназначен за анализ, визуализация и създаване на картографски продукти.

QGIS (Quantum GIS) е безплатен и отворен код ГИС софтуер, който предоставя широк спектър от функции за създаване и редактиране на карти.

Google Earth позволява на потребителите да изследват земята в триизмерно издание, разглеждайки различни обекти по целия свят.

Mapbox предлага картографски услуги и инструменти за създаване на интерактивни карти и вграждането им в уеб приложения.

Carto е онлайн платформа за картография, която позволява лесно създаване и споделяне на интерактивни карти.

OpenStreetMap е отворена карта, която позволява на потребителите да добавят, редактират и използват географска информация от цял свят.

MapMaker Interactive е инструмент на National Geographic, който позволява на потребителите да създават свои собствени карти с различни теми.

WorldMap е платформа, където потребителите могат да създават, споделят и изследват картографски данни.

Картографският софтуер и апликациите са важни инструменти в обучението по география, позволявайки на учениците и учителите да работят с географски данни, да създават карти и да изследват пространствени връзки. Тези инструменти предоставят разнообразни възможности за изучаване и създаване на карти, което обогатява и разнообразява обучението по география и подпомага визуализацията и разбирането на пространствените концепции. [16, 19]

Виртуална реалност (VR) и разширена реалност (AR)

VR предоставя възможност за имерсивно обучение, където учениците могат да посещават виртуални локации и да изследват географски обекти като част от учебния процес - виртуалните екскурзии в различни части на света позволяват на учениците да изучават географски и културни аспекти на различни

региони, виртуалните лаборатории, където учениците провеждат експерименти, свързани с географията.

AR може да бъде използвана за създаване на интерактивни карти, когато учениците се възползват от добавени в реалната среда визуални елементи и информация. AR може да допълва учебните материали с визуални елементи и допълнителни информационни слоеве, които улесняват разбирането на географски концепции. Учениците могат да използват AR при изучаването на околната среда, като разглеждат различни географски елементи в реално време.

Използването на VR и AR стимулира интереса на учениците, като прави обучението по-интерактивно. Тези технологии предоставят възможност за визуализация на географски данни и концепции в по-реалистична форма. VR и AR могат да бъдат настроени за индивидуално обучение, позволявайки на учениците се обучават в собствено темпо – възможност за индивидуализация на учебния процес. [10, 14, 17]

Използването на VR и AR в обучението по география обогатява учебния процес, правейки го по-забавен, интерактивен и ефективен, като същевременно насърчава интереса към географското познание.

Специализирани сензори и датчици

Специализираните сензори и датчици са важни компоненти в областта на географията, тъй като те предоставят възможности за събиране на различни видове географски данни. Тези данни могат да бъдат използвани за изследване и анализ на пространствени явления и тенденции.

Глобални позиционни системи (GPS). GPS сензорите предоставят точни географски координати и данни за движение, които могат да бъдат използвани за картографиране, навигация и изследване на терен.

Топографски сензори. Тези сензори могат да измерват различни параметри, като височина на местността, наклони и релеф, което е полезно за изследване на географските характеристики на различни региони.

Метеорологични сензори. Сензорите за измерване на метеорологични параметри, като температура, влажност, атмосферно налягане и вятър, предоставят важна информация за климата и околната среда на дадена територия.

Сензори за измерване на качеството на въздуха. Тези сензори могат да измерват концентрации на различни замърсители във въздуха, което е полезно за анализа на качеството на въздуха на определена територия или място.

Сензори за измерване на водни параметри. Сензорите за измерване на водни параметри като температура, pH и концентрации на различни вещества са полезни за мониторинг на водните ресурси и водните екосистеми.

Сензори за измерване на подземни води. Тези сензори предоставят информация за нивата и качеството на подземните води, което е важно при изследване на хидрографските условия на даден регион.

Сателитни сензори. Сателитните сензори предоставят възможност за събиране на данни от високо ниво, включително снимки, термални измервания и други, които могат да бъдат използвани за картиране и мониторинг на глобални географски явления.

Сензори за земетресения. Тези сензори се използват за регистрация на сеизмични активности и измерване на земетресения, което е важно при изучаването на тектоничната активност на определени региони.

Специализираните сензори и датчици предоставят ценни данни, които могат да бъдат използвани за детайлно изследване на географски характеристики и процеси в различни области на науката за земята и географията.

Използването на сензори и датчици обогатява и разнообразява учебния процес, като например измерване на климатични параметри или изучаване на характеристики на дадена територия.

Техническите средства, когато се интегрират ефективно в обучението по география, помагат не само за усвояване на конкретни факти, но и за развиване на критическо мислене, проблемно решаване и умения за обработка на информация, които са от съществено значение в днешния свят. [10, 13, 14, 15]

ЛИТЕРАТУРА

[1] Вълкова, В., Николов, И. Използване на виртуална реалност и интерактивни карти в обучението по география. В: Сб. доклади от Национална конференция "Образователни технологии". 2019

[2] Дерменджиева, С. Обучението по география. Методически анализи и интерпретации. В. Търново, Издателство "ИТИ", 2022, 332 с. ISBN 978-619-7602-22-7 COBISS.BG-ID – 52682248. 2022

[3] Димитрова, Ц. Педагогически аспекти на използването на географските информационни системи в училище. Списание "Образование и информатика", 9, 38-43. 2017

[4] Смрикаров А., Атанасов, В. и кол. Ролята на иновационните образователни технологии и дидактически модели за адаптиране на образователната система към дигиталното поколение. 2016, стр. 85, ISBN 978-954-712-697-8

[5] Тенева, Д., Тенев, И. Интегриране на технологии в обучението по география в степените на обучение. В: Сб. доклади от Националната конференция "Младите учени в науката – стъпка към успешното общество". 2017

[6] Тодоров, С. Използване на мобилните технологии в училищно обучение по география. Списание "Образование и информатика", 11, 32-36. 2018

[7] Христов Х., Цанков Ц. Използване на системата e-Learning Shell в обучението по инженерните дисциплини. Научна конференция на Факултета по технически науки, Шумен, 2009/2010, ISSN 1311-834X.

[8] Христова, М., Николов, С. Съвременни технологии в обучението по география. В: Сб. доклади от Национална научна конференция "Образование и наука – заедно към нови върхове". 2018

[9] Цанков Ц. Разпространение на електронни книги. Сп. „Автоматика и информатика“, год. L, № 3, София, 2017, ISSN 0861-7562, с. 35-38.

[10] Цанков Ц. С., Диманова Д. В. Компютърна дидактична програма за код на Хеминг. Годишник на ШУ „Епископ К. Преславски“, Шумен, 2016, ISSN 1311-834X

[11] Atanasov V., Ivanova A. A framework for evaluation of web-based learning content. International Journal on Information Technologies and Security, No. 4 (vol. 14), 2022, pp. 13-24

[12] Barker, M., Gump, S. E. The use of augmented reality in geography education. Journal of Geography, 117(6), 246-254. 2018

[13] Bednarz, R., Kemp, K. K. Using Geographic Information Systems (GIS) in the Classroom: A Reflective Practice. Journal of Geography, 118(1), 11-22. 2019

[14] Hammond, T. C., & Howard, E. A. Using Mobile Devices and Apps to Enhance Geography Education. Journal of Geography, 116(2), 49-57. 2017

[15] Harris, L. M., Castle, S. (2016). Exploring the Potential of Geographic Information Systems (GIS) in K-12 Education: A national survey. Journal of Geography, 115(4), 146-155. 2016

[16] Kolb, L. J. Enhancing geography education with virtual reality technology. Journal of Geography, 117(3), 119-129. 2018

[17] Lambert, A. M. Learning geography with technology: Evidence from a field-based study of geography educators. Journal of Geography, 115(2), 60-67. 2016

[18] Mayer, J. D., & Szilagyi, J. T. The Role of Mobile Technology in Geography Education: A US Case Study. Journal of Geography, 115(1), 31-40. 2016

[19] Molnár, G., & Kovács, G. The Role of Interactive Whiteboards in Geography Education. In Proceedings of the International Conference on Education and E-Learning (ICEEL 2017).

[20] Tsankov Ts., Konstantinova E. Computer didactic tool for network addressing and routing. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 70, June 2020, ISSN 2367-5721, pp. 54-61.

[21] Tsankov Ts., Konstantinova E. Priceless Microsoft products that we will part with forever. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 70, June 2020, ISSN 2367-5721, pp. 62-70.

[22] Tsankov Ts., Konstantinova E. Protection against illegal distribution of digitalized books. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 71, July 2020, ISSN 2367-5721, pp. 108-118.

CHALLENGES FOR ENTERPRISES IN THE DESIGN AND CONSTRUCTION OF SPUR GEAR REDUCERS

Mariela L. Ivanova

ABSTRACT: *The article explores contemporary computer tools for design of reduction gear. The article is fully adapted to the need for knowledge and skills in the future work of engineers in machine engineering.*

KEYWORDS: *Reduction gear, CAD software, Geometric design, Computer modeling.*

1. Introduction

The design of the gear including: specifying the type of contacting gears, determining their geometric parameters and performing the strength and kinematic calculations is largely determined by their purpose and the specific requirements placed on them. The existence and use of state-of-the-art CAD/CAM systems allows automation of the processes related to modeling and manufacturing gears. This is a basic prerequisite for creating new gears (including - modeling, designing, testing, documenting, manufacturing) and optimizing existing ones. The report highlights the advantages of using CAD/CAM systems for design, reflects the modeling of conjugated gears and outlines the options for their design.

2. Applicability of CAD / CAM / CAE systems in gear design.

Automated design systems occupy an extraordinary place among computer applications, as they are industrial technologies that directly affect material production.

The application of modern CAD/CAM systems is used for three-dimensional modeling of individual parts of machines and machines with a large number of high-complexity units from which the graphic part of the design documentation is drawn - drawings (CAD); for engineering calculations and analyzes (CAA); for rapid prototyping (Rapid Prototyping-RP); for Technological Preparation of Production (CAP); for the preparation of CNM control programs for the production of CAMs and for complete management of a company's design and engineering data (PDM) and documents (EDM) [1].

Strength and kinematic gears calculations using CAD systems.

Strength and kinematic calculations for gears in the gearbox using CAD systems are performed automatically when certain output parameter values are set. In this case, the final results necessary for the construction of gears are immediately displayed. There are two possibilities:

1. When designing standard gears - cylindrical, conical and worm gears. CAD products of medium and high class (AutoCAD, TopSolid, SolidWorks, CATIA) perform automatic calculations and generate the corresponding gear. The model thus obtained can be embedded directly into the structure and can be modified many times

depending on the strength, kinematic, structural and aesthetic requirements placed on it.

2. When designing non-standard gears - a program is developed for their strength-geometric calculation (Mathcad, MATLAB, Excel, etc.) or the loads are set directly on the model, with the initial results being returned again in a user-friendly manner.

Motion simulation using modules in CAD / CAM / CAE systems.

For simulation of the movements, the combined operation of the friction gears in the gearbox is reproduced and the movements in the gear mechanism are simulated, from where the normal operation is monitored and the corresponding boundaries of jamming, collisions, gaps, etc. are made.

Production technology.

The appropriately used CAM product directly generates from the gear models programs for making the respective NC machine (erosion, machining center, etc.) with the right choice of cutting tools (for rough and clean workmanship) and with the necessary cutting modes. The process of simulation is simulated and the resulting surfaces are analyzed.

Modeling of conjugated gears.

Geometric CAD modeling of gears can be done in three ways. To a large extent, the choice of option is determined by whether they are standardized or not, ie. whether they are set in CAD programs and their applications and allow the CAD systems used to make this modeling.

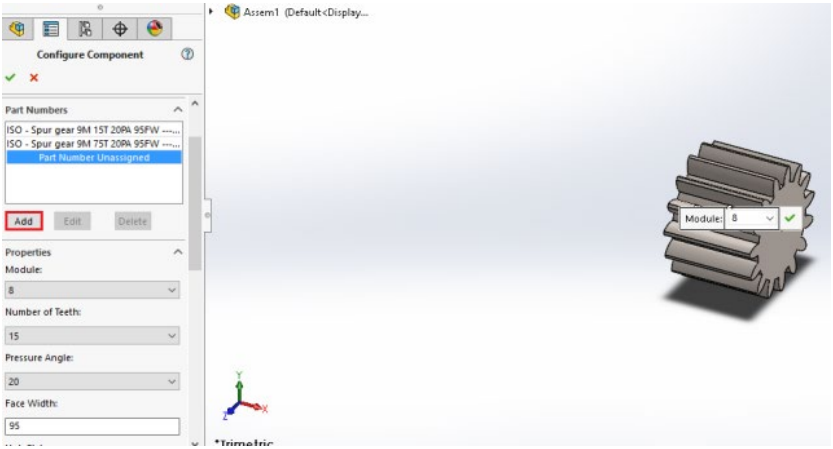


Fig. 1. *Geometric parameters of standard gears, set in CAD programs*

Modeling of conjugated gears directly from the CAD synthesis

Such modeling is possible with full compatibility of the CAD products used. It exchanges data without loss of information, whereby the resulting analytical dependencies and graphically visualized surfaces from one CAD system are transferred

to another and the solid models of the synthesized gears are generated. This is especially applicable to non-standard gears. Interestingly, the standard models set up in the CAD systems on which the desired gears are generated are obtained in this way.

Modeling Standard Gears

For modeling standard gears, the embedded CAD applications are used. In order to obtain the model of the desired gear the necessary geometric parameters (Fig.1) and force loads are set for it. Calculation is performed automatically, output results are calculated and gears are generated. If necessary, they can be replaced by changing their parameters, depending on the load and kinematics variation and depending on the design and construction features desired. Figure 2 shows models of standard gears obtained with the SolidWorks CAD product [4].

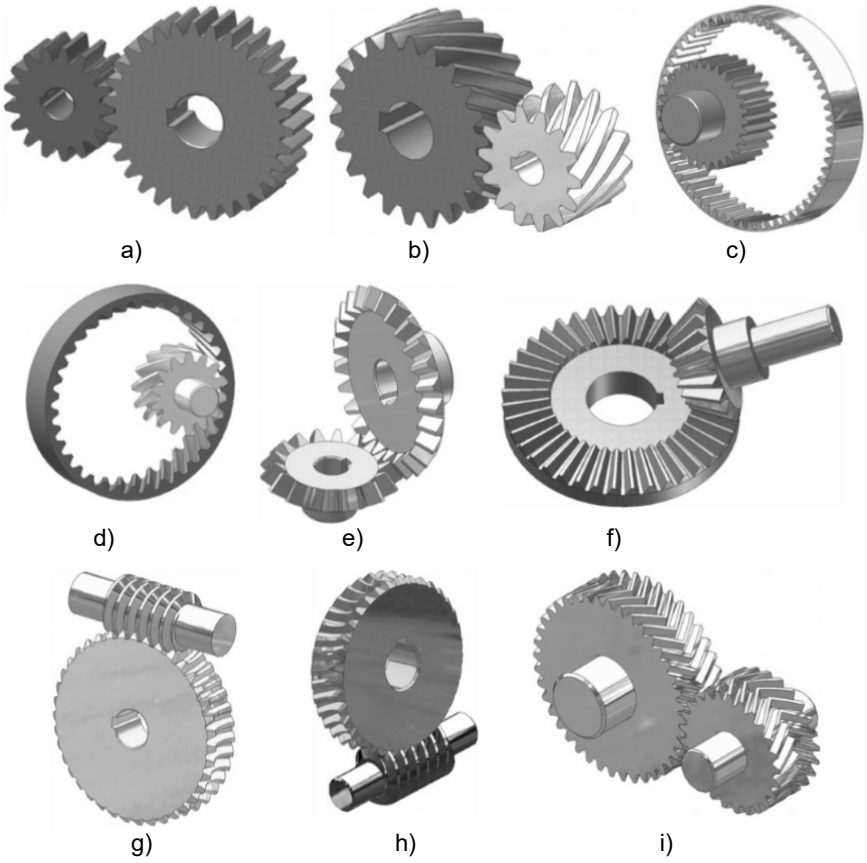


Fig. 2. *CAD models of standard gears.*

(a) Cylindrical toothed gear with external engagement with straight involute teeth;
(b) Cylindrical toothed gear with external engagement with inclined involute teeth;
(c) Cylindrical gear with internally engaged gear makes involuntary teeth;
(d) Cylindrical toothed gear with internal engagement with inclined involute teeth;
(e) Conical gear with orthogonal axes of rotation;
(f) Conical gear with non-rotary axes of rotation;
(g) Worm gear with a single-worm gear;
(h) Worm gear with three-way worm gear;
(i) Shaft gear.

3. Calculation and modeling of the one-gear reducer elements

The report presents an example for calculation, design and simulation of single gear reducer with straight toothed cylindrical gears. The steps for modeling and the sequence of their implementation are set out below. Each of the steps in the calculation and modeling can be performed in more than one way, depending on the constructor's decision.

The gearbox that is considered in the example is a one-stage with cylindrical gears with straight teeth. Its housing consists of two parts: a base and a lid that are separated from a plane passing through the axis of the shafts. The calculation is mainly based on the technical calculation guide "Calculation and Design of Machine Elements [2]".

3.1. Determination of the gear ratio of the gearbox (i).

To determine the gear ratio of a gearbox, the following factors are taken into account: the mutual arrangement of the two shafts, the magnitude and the torque transmitted (Mb), the speed of rotation, the mass limit and the overall dimensions of the components, if any [2].

A basic principle for the choice of the gear ratio for straight teeth is $i \leq 8 \div 10$.

3.2. Defining the shaft revolutions.

The input shaft speeds are dependent on the gear ratio [2]:

$$n1 = n2.i \quad (1)$$

3.3. Selecting the material for the gears.

The primary material for gear manufacturing is steel while allowing gears to be made from cast iron for low loads. The choice of steel depends on the conditions and mode of operation of the gear unit as well as on the lubrication. For gears with low revolutions up to 100 min-1, it is assumed that the hardness of the material does not matter. Dental gears with speeds above 100 min-1 necessarily work in a lubricated condition and calculate the contact strength and hardness of the teeth for the selected material.

If the load is accompanied by strikes or vibrations, additional calculations for core toughness are required. For average loads, quality carbon steel of the following brands is used: pg.35, pg.40, pg.45, pg.50.

For heavy loads and vibrations for the manufacturing of the gears steel alloy is used. The most used brands are: 40х, 40хн, ст.35хгс

The obligatory hardness of the teeth in Brinell hardness standard is ≤ 350.

Small gears are manufactured together with the corresponding shaft.

3.4. Determination of the admissible bending tension in the gear.

The permissible bending stress with regards to material fatigue is mainly determined by a symmetrical tooth-change formula in both directions [2]:

$$(2)\ [\sigma]_{от}=\frac{\sigma-1}{[n].K\sigma}.k.ц.от\ [MPa]$$

Where σ-1 is the fatigue boundary of the material under a symmetrical load cycle. The fatigue boundary can be determined by an approximate method or when calculating the type of steel [2].

$$(3)\ \sigma\text{-}1 = 0.22\ (\sigma\beta + \sigma s) +50$$

- [n] is a safety factor when calculating double wheels;
- (Ks) represents an effective stress concentration ratio;
- Kc - bending factor taking into account the number of bending cycles;

Bending stresses are calculated for each sprocket.

3.5. Calculation of gears

The forces that load the working gears create material stress that is proportional to the incoming torque that is set on condition. The tension in the teeth of the gears is not constant in place and time and is unevenly distributed along the teeth because of the inconsistency between the axes of the gears, therefore the gears are calculated by considering the required bending stresses.

3.6. Calculate the normal module.

The normal module is calculated using the formula [2].

$$(4)\ m\geq C_2.\frac{\sqrt[3]{Mв.10.Кк.Кд}}{Z1.\ \Psi m.Y.[\sigma].10^6}$$

Where C2 is the ratio of the gear type;

- Mb is torque, which is set by condition;
- Kk represents the concentration of the load;
- Kd is the coefficient that takes into account the conditions of dynamism, ie it takes into account the dynamic forces that arise from the rotation of the gears due to inaccuracies in their construction and engagement;
- Z1 - number of teeth of the sprocket;
- Ψm - coefficient that measures the length of the tooth relative to the module;
- Y - factor that takes into account the shape of the tooth;
- [σ] - permissible bending stress for the wheel.

3.7. Determining the basic parameters of the cylindrical gear.

The number of teeth of the leading sprocket (Z2) is determined by the following:

$$(5)\ Z2 = Z1.i$$

— The wheelbase (A) is determined by the formula:

$$(6)\ A=\frac{Z2+Z1}{2}.m$$

— The diameter of the circumference of the guide gear is determined by the formula:

$$(7)\ Дд=Z1.m[mm]$$

— The outer diameter of the spur gear is determined by the formula:

$$(8)\ Дк=m.(Z1+2)$$

— The length of the tooth of the guide wheel (b) is a function of the following parameters:

$$(9)\ b=\Psi m\ .m+5$$

In the same way, the parameters of the spur gear of the single gear gearbox with straight teeth are also calculated.

3.8. Calculation of the drive shaft.

The drive shaft of the gearbox is calculated for bending and spraying simultaneously:

$$(10)\ [\sigma]_{or}=\frac{Mor}{Wor}=\frac{32Mor}{\Pi.d^3}\leq[\sigma]_{or}$$

Where:

— Mor be a bending moment;

— [b] f is the flexural tension allowed;

Wor is a resistance moment.

3. 9. Calculate the diameter of the drive shaft.

The diameter of the drive shaft is determined by the formula [2]:

$$(11)\ d1\geq\sqrt[3]{\frac{Mor}{0{,}1\ .[\sigma]or}}$$

3.10. Calculation of the driven shaft.

The bending moment of the driven shaft is determined by the following formula:

$$(12)\ Mor=Mв=9554.\frac{N}{n}[N.m]$$

Where:

— N is transmitted power

— n are the revolutions of the driven gear

The diameter of the shaft is calculated using the following formula [2]:

$$(13)\ d2\geq\sqrt[3]{\frac{Mor}{0{,}1\ .[\sigma]or}}$$

Calculated shaft diameters are also bearing diameters and are the minimum shaft diameters. The diameters of the bearing necks are configured in accordance with the selected bearings.

3.11. Calculation and selecting bearings.

The calculation of the bearings is performed for dynamic load carrying capacity, and this is done consecutively for the drive and driven shaft of the formula:

$$(14)\ C=\frac{td}{fn\ .ft}.p[kN]$$

Where:

— ft is the dynamic load factor;

— fn is the rate of rotation rate;

— the force P is assumed to have a value half the set deadpoint (Mv).

— After strong and kinematic calculations, the three-dimensional modeling of the one-stage gearbox with straight teeth cylindrical gears follows.

The three-dimensional modeling of a machined workpiece using CAD systems is done in the following sequence [5]:

— the detail is analyzed and a decision is made for its separation of elementary structural elements that can be created with the system used;

— determine the element to be used for base;

— a procedure for creating the structural elements is adopted;

— choosing the ways of constructing the structural elements;

— construct the structural elements in the adopted order, applying the respective constructional operations (fig.3);

— review and correction of the elements created to implement the adopted modeling strategy.

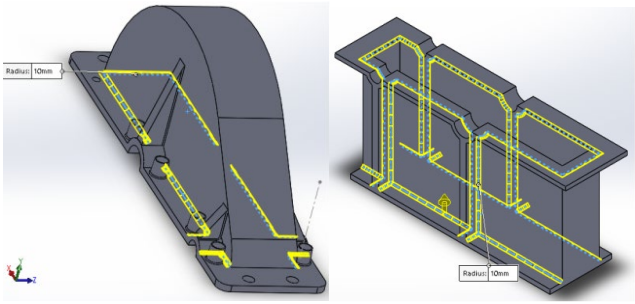


Fig. 3. *Three-dimensional hull and bonnet design.*

Machine parts for rotation motion bearings can be selected from the integrated software libraries or downloaded directly from the bearing manufacturer's web site (Figure 4).

The engineering automation product used for this purpose SolidWorks has a library of over 700,000 standard elements, supports a number of international drafting standards, and allows users to create details and documents using digital prototypes [4].

In automated design, two types of assembled units can be created by the standard:

— assembled units consisting of details only;

— assembled units containing details and other assembled units.

Once the components have been deployed in the mechanism file, they have to be assembled. When assembling the components, their degrees of freedom are restricted. There are six possibilities for movement of a solid in space - three translational displacements in the direction of the coordinate axes and three rotational movements around the coordinate axes. Components are assembled using links.

They enable the individual parts to be positioned from the assembled unit in strict accordance with each other (Fig. 5).

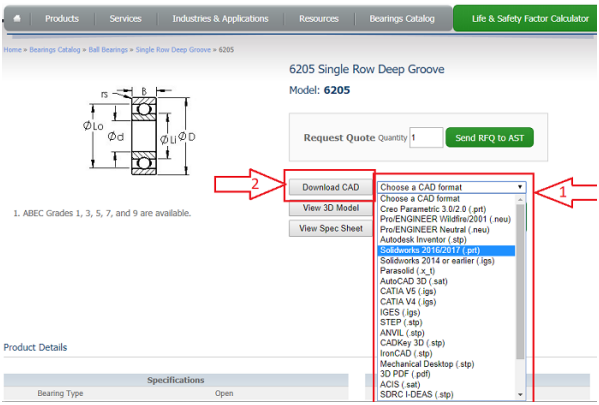


Fig. 4. *Selection and dimensioning of standard machine elements.*

4. Assembling an assembled mechanism and drawings creation.

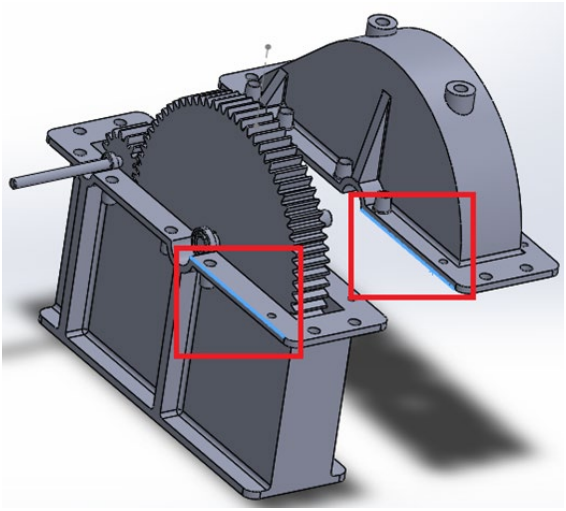


Fig. 5. *Fixating components with the assembled unit.*

Creating a drawing from a 3D model is limited to generating projections based on three-dimensional patterns, accompanied by appropriate dimensions, roughness, geometric tolerances, technical requirements, and more.

Drawings and 3D models are interconnected documents, ie. changes in the detail model or cranial unit also changes the corresponding drawings. It is also possible via changing the dimensions in the drawing to change the patterns. The drawing files must always be accompanied by the appropriate model files. Drawings are saved in separate files with the appropriate extension, depending on the CAD workflow used. The drawing file may contain one or more drawing sheets, and at one time only one of them is active.

Creating a drawing includes:

— selection of the drawing sheet format, frame and table with the basic inscription;

— Graphical environment setting - Design method (European or American position [4]), default scale, symbols for marking views, sections and technological bases, ways to represent basic elements of the drawing (lines, dimensions, hatching, geometric allowances, inscriptions, etc.);

— Compose the drawing by creating views and cuts, sizing, inscriptions, and more. (Fig. 6);

— fill in the table with the basic inscription;

— print the drawing of a peripheral device.

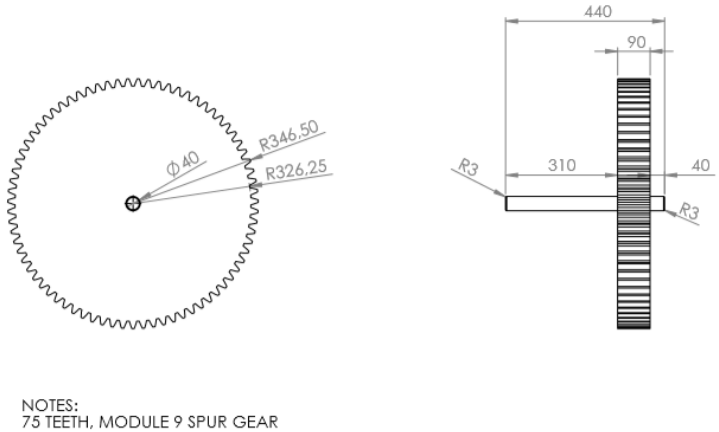


Fig. 6. *Composing a drawing in a graphic environment.*

5. Production engineering technology

Cutting of the gears can be done on a CNC machine with a profiled cutting tool according to the copying method where the tool moves along an approximate curve approaching the contour of the cross-section of the teeth cut.

The gears of the gearbox modeled in the report can be manufactured a machine with CNC control. For this purpose, it is necessary to generate a program from a suitably

chosen CAM system. Regardless of the type of CAM system used the modeling models used by the CAD systems are used to compile the control programs. The solid geometry automatically recognizes the different geometric elements. The information they receive is used to select the necessary processing tools. The tool trays generated by the CAM system are in association with the original CAD model, and when editing the 3D geometry, the trajectories are automatically changed. The CAM system simulates and verifies the tool path and removal of the material from the model, with the tool, holder, workpiece, and gripping and gripping devices included in the simulation and realistically present the processing process.

6. Conclusion.

In the report was presented a sequence for calculation and geometrically modeling gears using CAD systems and outlines the ways in which they are machined.

A rationale for using CAD/CAM/CAE systems has been made, and their advantages have been identified in the design of gears in gear units.

REFERENCES

[1] Банков Б., Имплементиране и тенденции за използване на композитни материали в областта на военното производство - Научна конференция "Научните изследвания и инвестициите в технологични иновации - решаващ фактор за отбраната и сигурността", Пловдив Хемус 2020, с. I-139 - I-146, ISSN 1312-2916;

[2] Antonov S.I., Izsledvane na prilozhenieto na CAD/CAM/CAE sistemite i tehnologiite za barzo prototipirane pri proektiraneto na komponenti na tehnicheskite sistemi, Shumen, 2021g., ISBN 978-619-7531-31-2;

[3] Brunet P, Hoffmann C, Roller D, CAD Tools and Algorithms for Product Design, Springer-Verlag Berlin Heidelberg, 2000, ISBN 978-3-642-08548-2;

[4] Petrova T., Petrov Z., Visualization of Objects in Computer Tomography, 21st International Symposium INFOTEH-JAHORINA (INFOTEH), 2022, pp. 1-4, ISBN 978-166543778-3 doi: 10.1109/INFOTEH53737.2022.9751325.

[5] Antonov S.I, Mariela Ivanova, “Studying the application of CAD/CAM/CAE systems in the design of components for personal ballistic protection equipment”, Journal Scientific and Applied Research, Vol. 25 No. 1, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, (2023), ISSN 1314-6289 (Print), ISSN; 2815-4622 (Online), DOI: https://doi.org/10.46687/jsar.v25i1

[6] Stamen I. Antonov, Conuy G. Conev, 3D printing in industry,Proceedings of International Scientific Conference - ”Defense Technologies” DefTech 2020, “Faculty of Artillery, Air Defense and Communication and Information Systems”, Shumen, pp 201 – 205, ISSN 2367-7902

CAD/CAM/CAE SYSTEMS AND ARTIFICIAL INTELLIGENCE TO HELP DESIGN COMPONENTS FOR PERSONAL BALLISTIC PROTECTION EQUIPMENT

Stamen I. Antonov

ABSTRACT: *The article analyzes the possibilities of information systems for mechanical engineering, working with artificial intelligence in the processes of 3D modeling, manipulation and testing of components included in the means of individual ballistic protection.*

KEYWORDS: *Applications for mechanical engineering, Artificial intelligence, 3D model, Engineering analysis, Means of personal ballistic protection.*

1. Introduction

The purpose of this scientific article is to study the modern applications that widely use artificial intelligence in computer design with the aim of subsequent construction and production of characteristic elements of the composition of the means of individual ballistic protection. Emphasis is placed on the conceptual design stage as the i-creative stage of product development and as a stage of the design process aimed at developing an idea, concept or general conceptual framework for a future design of a concrete product or component. This stage allows the definition of basic design principles, themes and strategies before more detailed design development begins.

An assessment of the possibilities of new information technologies for additional automation of the process of design, simulation and prototyping of components of the means of individual ballistic protection is presented. The possibilities for shortening the time from the idea to the realization of the product, flexibility in the changes of the market and the requirements of the users are analyzed.

2. Analysis of information systems supporting decision-making in the conceptual design phase of the construction of individual ballistic protection components.

Current realities require manufacturing enterprises to be increasingly dependent on information technology. At the beginning of the 21st century, their role in management is getting bigger and bigger. Economic realities also determine the need to reassess intangible assets and especially information technology. Although from a formal point of view, on the one hand, information technologies (such as means - computers, systems for collecting, processing and presenting information) are material assets, on the other hand, as an idea, as an innovation and continuous evaluation and a source of ideas for improvement of business processes they are an intangible asset [4]. From an economic point of view, information technology can be seen as means of

production that can replace labor. As their value declines, they replace labor that has historically been of increasing value. Therefore, in a microeconomic aspect, information technology should lead to a reduction in the number of middle managers and employees, since in reality they replace them [7]. They can reduce operating costs.

In the modern conditions of fierce competition on the market, success is on the side of those who are able to design their products faster and more accurately, determine the optimal production technology and ensure maximum quality (CAD/CAM/CAE systems are at the heart of it).

This is a safe and unique way to achieve the required quality, while simultaneously reducing production costs. The main part of the work of creating the project is done by computer programs, and the speed and accuracy are many times higher than what traditional technologies can offer. In this way, creating drawings, calculating loads, predicting the behavior of materials and everything else that accompanies the production process is easy and absolutely reliable [2].

On the other hand, the rapid spread of artificial intelligence (AI) has already led to radical changes in certain industries such as global e-commerce [1]. Although the ideas and some fundamental techniques of artificial intelligence arose a long time ago, today, as a result of accumulated computing capacity, communication potential and big data, the world is facing transformations that are far more comprehensive than the technological revolution of the last century. Change does not occur at the same speed in different sectors due to varying degrees of readiness of AI technologies for implementation, insufficient readiness to accept and implement the technologies, especially if substantial financial investments are required [3]. It is noted that the changes are most dynamic in countries with high-tech economies and a high level of computer skills of citizens. But daily news shows that artificial intelligence, as a key development tool, is entering many sectors and aspects of life, and, albeit slowly, is becoming a catalyst for digital transformation. Research in the field of artificial intelligence is highly specialized and divided into several subfields. These directions arise around solving specific tasks, and there are often subdivisions and differences in the approach to building artificial intelligence, as well as the use of completely different technical means. Common to most subfields of AI research are tasks such as the ability to reason, learn and improve AI through learning, perception, planning, communication, and also the ability to move and control the movement of AI objects such as cars, drones appliances and others. Taking into account these common facts, this article will analyze how artificial intelligence integrated in automated control systems (CAD/CAM/CAE) contributes to the higher accuracy and efficiency in the design and construction of equipment for military personnel, and in particular elements for individual high quality ballistic protection of all types for the needs of both military formations, police units, prison security services and private security companies [6]. They are usually required to be manufactured with high-quality materials, including aramids (Kevlar, Tvaron), high-strength polyethylenes (Dynima, Spectra) and hybrids. It is also important that they have the minimum weight with a high degree of protection and can possibly be worn comfortably under the shirt or jacket or openly over the clothing (uniform). There is a wide range of personal ballistic protection including [5]:

— Development of special and unconventional ballistic systems;

— Manufacturing a full range of body armor configurations, including concealed carry, open, women's, VIP, aquatic, tactical, military and specialty models;

— Light and specialized (heavy) suits for demining;

— Bulletproof plates, shields, bags and blankets;

— Ballistic helmets.

Due to the rich and diverse range of means for individual ballistic protection, it is quite natural that the process of managing their life cycle should be maximally automated [2]. Thus, the need for systematic use of computer technology at all stages of the design is satisfied, with a scientifically based distribution of functions between the designer and the computer. This means that the designer must perform the tasks that for now do not lend themselves to formalization (tasks of a creative nature and tasks with extremely high variability of solutions), and the computer (the information system) - routine tasks related to design and verification calculations, rendering of results, compilation and management of documentation, etc., which can be formalized and amenable to algorithmization.

From the given definition, it can be seen that the limit beyond which automated design begins is relative and changes continuously with the development of mathematics, computer technology and design theory in the relevant technical field.

That is why at this stage, and especially in the design of the means of individual ballistic protection, the best organization of the automated design is achieved by the use of automated design systems (CAD or CAD/CAM/CAE systems). In them, mathematical methods and computer technology serve as the basis for the systematization of the "design" process on a common methodological, informational and technical basis.

3. Importance of artificial intelligence in the design and construction of individual ballistic protection components.

Manufacturers and developers of virtually any type of product or service face the constant challenge of adapting to changing technologies.

In an ever digitizing world, CAD/CAM systems play a central role in transforming ideas into real products. From simple 2D drawings to complex 3D models, CAD/CAM software has contributed to improving efficiency, accuracy and productivity in various industries.

There are several main current trends in the CAD/CAM field. Perhaps the development of cloud technologies should be put in the first place, which give a different level of communication and collaboration to engineers, and to all other specialists and managers in the company.

Cloud-based CAD/CAM enables engineers to share and collaborate on projects and create simulations from any device and location, without the need for

expensive hardware and software installations. Cloud software also offers scalability and flexibility, as well as the ability to access higher computing power, for example for complex and large-scale simulations and tests.

Generative design and additive manufacturing (3D printing) are two other important trends in the field that often turn out to be interconnected. Generative design is an approach that uses algorithms and rules to generate and explore multiple design solutions that meet certain criteria and constraints [3]. It can help engineers discover optimal and innovative design solutions by considering various factors such as functionality, performance, cost, sustainability, aesthetics, etc [5]. Last but not least, generative design can also help reduce the time and complexity of the design process and increase the variety and quality of products, something that is especially important in today's fast-paced and digitized world.

Additive manufacturing is a process in which products are built layer by layer based on digital models, using specific materials and techniques. This approach makes it possible to create complex and customized products that would otherwise be difficult or even impossible with traditional manufacturing methods. Last but not least, 3D printing can speed up testing and validation of design and simulation results by rapidly prototyping in small batches.

Other important trends essential to the development of CAD/CAM systems can be listed such as virtual reality and augmented reality, as well as the rapidly developing simulation and analysis tools that allow engineers to perform virtual tests, predict the behavior of the individual elements and components of the means of personal ballistic protection under different conditions and to optimize their design and construction already at the beginning of the development process, reducing the need for physical prototypes.

As can be expected, the AI wave has not passed the CAD/CAM/CAE sector either. This is another important trend, as AI multiplies the capabilities of engineers, accumulating good practices from their daily experience. This is especially important now and even more so in the future when industries will lack millions of engineers.

Artificial intelligence and machine learning can help automate and optimize design and simulation-related tasks, such as generating and evaluating design alternatives, detecting and correcting errors, predicting and preventing failures, and improving productivity and quality. These technologies can also enable engineers to learn from data and feedback and adapt and improve their design and simulation models and methods over time.

Good examples of the use of AI in CAD applications in the modeling of components such as armor plates, combat helmets, etc. are the tools of the Design Assistant functionality in the 3DEXPERIENCE platform, which uses built-in machine learning algorithms to offer assistance to the engineer in his design workflow for the items in question. They are designed to automate time-consuming and often repetitive tasks [7].

The Sketch Helper tool, for example, can help an engineer predict what is being sketched and quickly duplicate selected elements in multiple locations that have similar characteristics. If, say, multiple holes need to be added to a bracket, only one can be placed and the system will add the others.

Said generative design is an iterative engineering process that produces optimized 3D models using AI software and cloud computing creates a set of designs based on predefined constraints in terms of weight, volume, materials, etc. Essentially, it produces iterations of 3D models from one or more software based on accumulated experience. The engineer first introduces constraints and limits to achieve a specific result and details the forces and loads that the product must withstand. It also introduces details of the materials that will be used to create the elements that make up the PPE and information about their manufacturing process, be it CNC machining, 3D printing, etc.

The more variables and information the user provides to the software, the more designs the AI can generate. More information also means AI will be able to produce better and more highly optimized designs. Modern generative design tools can produce thousands of designs in a very short time, especially if they also use the power of cloud computing.

It is important to note that generative design does not replace engineers or designers. Rather, it is a tool that is used to improve and accelerate the design process. Design generation software only works if it has high-quality data it can use to create designs. Once the designs are generated by the AI software, then the engineer or designer must select the one that best meets the stated objectives.

The facts thus presented lead to the conclusion that artificial intelligence (AI) plays an important role in the design and construction of means of personal ballistic protection (eg bulletproof vests, helmets and other protective elements). Here are some of the ways AI can be used in this process:

Data analysis and simulations: The use of AI allows engineers to analyze large amounts of data from previous incidents, tests and simulations of various impact scenarios and bullet trajectories. This helps determine the most effective materials and designs for the protective elements.

Material and design optimization: AI can be used to optimize the material structure and design of protective elements to achieve maximum protection with minimum weight and restrictions on the wearer's freedom of movement.

Predicting vulnerabilities and needs: AI can be used to predict potential vulnerabilities in already existing security systems and to identify needs for improvements.

Creating autonomous adaptive defense systems: In the future, AI can be used to create autonomous ballistic defense systems that can dynamically respond to different types of threats in real time.

Testing and validation: Artificial intelligence can be used for simulations and virtual testing of different variants of protective elements, reducing the need for physical prototypes and speeding up the development process.

All of these aspects help improve the effectiveness and reliability of individual ballistic protection, providing better protection to military, police, and other professionals at risk from gunfire and ballistic threats.

4. Conclusions

Artificial Intelligence (AI) is integrated into CAD (Computer-Aided Design), CAM (Computer-Aided Manufacturing) and CAE (Computer-Aided Engineering) systems in several ways:

4.1. Design and Manufacturing Automation: AI can be used to automate some of the core tasks in CAD/CAM/CAE systems. For example, AI can analyze and interpret geometric shapes and processes, which facilitates and accelerates the process of designing and manufacturing the means of individual ballistic protection.

4.2. Generative design and optimization: Artificial intelligence can be used to generate alternative designs and optimize existing ones. This includes the use of machine learning algorithms that analyze a large amount of data and offer optimal solutions for specific designs of bulletproof vests, helmets and other protective elements.

4.3. Predicting manufacturing processes and material properties: AI can be used to predict various manufacturing processes and material properties, which is essential for optimizing manufacturing processes and the quality of end products.

4.4. Design and Manufacturing Cost and Time Analysis: Artificial Intelligence can be used to analyze the cost and time required to design and manufacture a product. This helps engineers make better decisions about the manufacturing process and optimize their resources.

4.5. Quality control and traceability: AI can be used to control the quality of manufactured products and ensure traceability of the entire production process.

These are just some of the ways in which artificial intelligence can be integrated into CAD/CAM/CAE systems. This integration helps to increase the efficiency, accuracy and innovation of the design and manufacture of the means of individual ballistic protection to meet the requirements of the specific security environment.

REFERENCES

[1] Банков Б. Имплементиране и тенденции за използване на композитни материали в областта на военното производство - Научна конференция "Научните изследвания и инвестициите в технологични иновации -

решаващ фактор за отбраната и сигурността", Пловдив Хемус 2020, с. I-139 - I-146, ISSN 1312-2916;

[2] Банков Б. Изследване на възможностите за използване на технологии за 3D печат в логистичното осигуряване - Научна конференция „Логистиката и обществените системи" - 2023 г. Велико Търново, с. 215 - 224, ISSN 2738-8042;

[3] Банков Б. Изследване на движението на проектил на боеприпас 7.62x54 във водна среда - Научна конференция „Актуални проблеми на сигурността", Велико Търново 2023 г, с.1511 - 1516, ISSN 2367-7473, 26-27 Октомври

[4] Antonov S.I. Izsledvane na prilozhenieto na CAD/CAM/CAE sistemite i tehnologiite za barzo prototipirane pri proektiraneto na komponenti na tehnicheskite sistemi, Shumen, 2021g., ISBN 978-619-7531-31-2;

[5] Antonov S.I., Ivanova M.L. "Studying the application of CAD/CAM/CAE systems in the design of components for personal ballistic protection equipment", Journal Scientific and Applied Research, Vol. 25 No. 1, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, (2023), ISSN 1314-6289 (Print), ISSN; 2815-4622 (Online), DOI: https://doi.org/10.46687/jsar.v25i1

[6] Brunet P, Hoffmann C, Roller D. CAD Tools and Algorithms for Product Design, Springer-Verlag Berlin Heidelberg, 2000, ISBN 978-3-642-08548-2;

[7] Petrova T., Petrov Z. Visualization of Objects in Computer Tomography, 21st International Symposium INFOTEH-JAHORINA (INFOTEH), 2022, pp. 1-4, ISBN 978-166543778-3 doi: 10.1109/INFOTEH53737.2022.9751325.

CHALLENGES FOR DESIGNING PERSONAL BALLISTIC PROTECTION EQUIPMENT

Stamen I. Antonov, Mariela L. Ivanova

ABSTRACT: *The article presents the prospects for the design of certain elements of the means of individual ballistic protection using software tools for 3D visualization of details and mechanisms, in terms of designing their preliminary models, as well as their operation and engineering analysis. Particular attention is paid to determining and modeling the construction of the individual elements of the means of protection from firearms with the help of information systems for the automation of engineering work.*

KEYWORDS: *Model, Ballistic protection, Inge visualization.*

1. Introduction

Designing items for personal ballistic protection requires attention to several key aspects, including materials, construction, and functionality. The general steps and factors to consider are as follows:

Task requirements (limitations):

This includes determining the level of protection that is required for the particular task. This can vary depending on potential threats such as firearms, sharp objects, etc.

Materials:

This step involves selecting the appropriate materials to provide the required protection. Popular body armor materials include Kevlar, aramid fiber, ceramic plates, high molecular weight polyethylene (UHMWPE), and more.

Construction:

Designing the layers of the protective element to provide an optimal combination of flexibility, lightness and protection. Different materials can be combined to achieve the desired characteristics.

Coverage:

A waterproof or fireproof coating can be added for added protection and comfort.

Ergonomics and comfort:

This means carefully designing the shape and distribution of materials to ensure optimal mobility and comfort for the wearer.

Testing and Certification:

Testing personal ballistic protection equipment in accordance with protection standards (for example, NIJ body armor standards in the US) and obtaining a certificate that guarantees compliance with protection requirements.

Production:

Development of a manufacturing process to enable mass production of high quality components for protection against firearms or cold weapons.

Support and updates:

It takes into account the need for regular maintenance and, if possible, the ability to update the body armor against new technologies and threats.

2. Perspectives on the design of the construction of means of individual ballistic protection.

Designing the structure of body armor elements with CAD software (automated engineering applications) involves several steps that are performed by an engineer or designer. The main steps that could be included in this process are the following:

Defining requirements:

— identification of the level of protection that the body armor should provide;
— definition of the areas to be covered by the bulletproof vest;
— definition of the materials to be used.

Data Collection:

— extraction of the standards for body armor and their requirements;
— collection of data on preferred materials and their properties.
— selection of CAD/CAM/CAE software:
— selection of an appropriate information system (product) that supports 3D modeling and engineering analyses.

Create a 3D model:

— using CAD software to create a 3D model of the bulletproof vest (or individual ballistic protection element);
— inclusion of all details and requirements, as well as precise measurement of dimensions.

Analyzes and simulations:

— performing engineering analyzes and simulations to verify the effectiveness of the body armor;
— analyzing materials for their impact and penetration properties.

Optimization:

— performing optimizations based on the results of analyzes and simulations;
— work on improving the design for better protection and comfort.

Documentation:

— creation of technical documentation, including drawings, specifications and other relevant production data.

Testing and Validation:

— testing the body armor prototypes for design validation;
— redesign if necessary based on test results.

Production:

— preparation of the production process for mass production, if necessary.

After sales management:

— monitoring of the produced bulletproof vests (elements for individual ballistic protection) to ensure their quality and performance in accordance with the requirements.

Design automation as an independent scientific field has emerged in the last two decades. The process of creating this direction, developing a theory and summarizing the obtained practical results continues even now.

The purpose of the automation of design and construction activity is to increase the productivity of engineering work and the quality of products, to reduce material costs and to shorten design terms, without increasing the number of engineering and technical personnel.

Design automation means the systematic use of computer technology at all stages of design with a scientifically based division of functions between the designer and the computer. This means that the designer must perform the tasks that for now do not lend themselves to formalization (tasks of a creative nature and tasks with extremely high variability of solutions), and the computer - routine tasks related to design and verification calculations, display of results, compilation and documentation management, etc., which can be formalized.

Nowadays, the best organization of automated design is achieved by using automated design systems (CAD or CAD/CAM/CAE systems). In them, mathematical methods and computer technology serve as the basis for the systematization of the "design" process on a common methodological, informational and technical basis.

The process of designing the elements for individual ballistic protection takes place as a complex process of abstract thinking (creative process), which requires knowledge of sufficient information about the designed object and its related fields.

According to existing standards, design is a process in which a description of an object that does not yet exist is drawn up. This process occurs when there is a design brief, which is the primary description of the site and the legal document to start the design. The process itself consists in repeatedly transforming and supplementing the primary description, removing its errors, optimizing (rationalizing) the features of the object in a consistent presentation of descriptions of the object in different forms (text, tabular, graphic, etc.).

The design result is a final description of the object in the form of a complete set of documentation for material reproduction of the object under certain production conditions.

In the design process, intermediate descriptions of the object are created, which define either the end of the design or the paths for its continuation. These descriptions are called design decisions, and design can be seen as a purposeful sequence of actions related to making design decisions.

From the point of view of informatics, design can be considered as an information process, in which primary information about the designed object, knowledge in the relevant field, past and similar experience are transformed into source information - the documentation of the new object with a specified level of detail.

Undoubtedly, the best form of organization of automated design, creation of 3D models and visualization of the behavior of characteristic elements of personal protective equipment are systems for automated design and production, called CAD/CAM/CAE (Computer Aided Dising/Computer Aided Manufacturing/ Computer Aided Engineering). Figure 1 presents a conditional algorithmization of the process "Construction of a component of means of individual ballistic protection", detailing the implementation of the CAD geometric model in the CAE and CAM modules, respectively, for a detailed engineering analysis for checking the fulfillment of tasks (requirements) and for manufacturing process design. During the engineering analysis, the limitations of the specified materials, dimensions and weight of the elements, as well as their direct purpose, are taken into account, and during the design of the production process, the available tooling equipment and the real capabilities of the production assembly line are determined. At each stage of the construction design, it is possible (and sometimes necessary) to change the design (geometry) through the CAD modules.

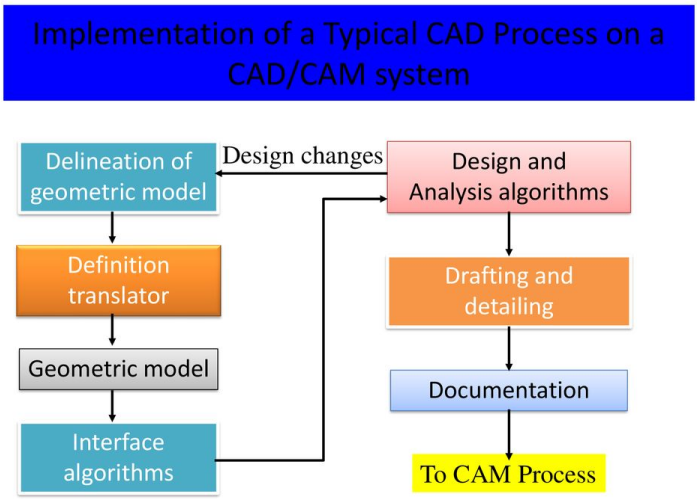


Fig. 1. *Connections between modules of automated design and engineering systems*

CAD (Computer-Aided Design):

In CAD systems, engineers and designers create 2D and 3D models of products or components.

These models include details on shape, dimensions, materials and other characteristics.CAM (Computer-Aided Manufacturing):

CAM systems convert CAD models into instructions for machines and manufacturing processes.

Cut routes, material handling programs, toolpaths and other parametric analyzes are generated on the CAD models to evaluate various aspects of the product.

They include analyzes of stresses, heat transfer, dynamics and other engineering aspects.

The general idea is that CAD, CAM and CAE systems work together to provide a complete solution for digital design, manufacturing and engineering analysis. CAD creates the designs, CAM translates them into manufacturing instructions, and CAE performs analyzes that help design and refine the product (fig. 2).

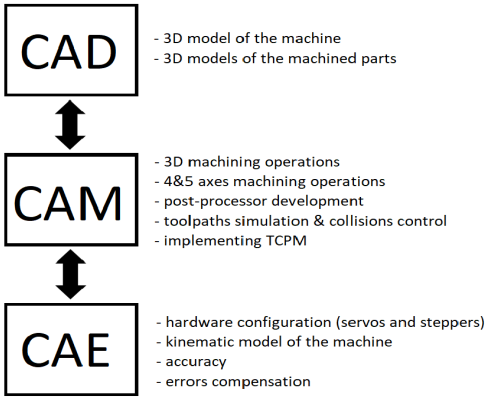


Fig. 2. *CAD/CAM/CAE integration process*

Of course, the joint operation of the individual modules of fig. 2 is not without problems and inconsistencies that must be resolved in the work process.

A key issue in this case includes the questions, which data does the CAD-engineer need and which data is transferred to the computer-aided engineering (CAE) department? Additionally, what are the requirements of simulation processes? Which parameters are created in CAD and transferred to computer-aided manufacturing (CAM) processes and which additional information is needed there? In an exemplary design process of weld points, the CAD model deals with many different structural and geometry-related parameters (e.g. ID, coordinates, connected parts, spot diameter…). For simulation topics, the CAE process needs specific information, e.g. material, coordinates, diameter, etc. Finally, the CAM process also needs a lot of information in

addition to the aforementioned parameters, such as orientation and surface normals, consideration of space requirements of welding robots, and material parameters.

The main issue is how is it possible to transfer connection technology data from the CADenvironment to the CAE-environment? Which file format is best suited for this transfer? How is it possible to guarantee that the transmitted information is received in the CAE-system? Having stated that, every discipline requires various information to fulfill its development tasks. This variety of values must be collected and can be bunched together in a comprehensive data model or in a database structure. The idea of a unified data model shall be seized up in a way that it is possible to be used in all areas of application. In this context, the presented data model is based on an optimized process to decrease development costs and guarantee reduced development time in total.

The goal is to create a data model that incorporates the issues already mentioned and that optimizes the process of exchanging data between different areas in the development process. The data model it should be applicable to all currently used CAx-systems and tools within the development environment of various OEMs. (CAx системите включват Computer Aided Design (CAD), Computer Aided Manufacturing (CAM) и Computer Aided Engineering (CAE).) The focus of the current approach is on the connection technology of the construction of elements for individual ballistic protection from many materials /composites (fig. 3).

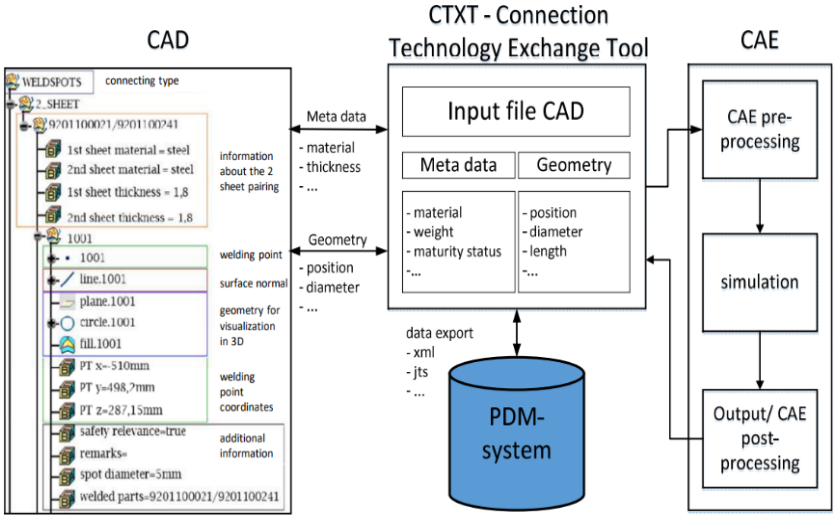


Fig. 3. *General data model layout for connection technology*

3D models of individual ballistic protection components offer numerous advantages over conventional 2D images and text, especially when it comes to

visualizing complex sculptural forms and concepts. The practice has proven many benefits, some of the key ones being:

Spatial representation (fig. 4):

3D models provide a third dimension not available in 2D images and text. This allows for a more realistic and accurate representation of objects, machines, structures and processes that have a three-dimensional nature and complex sculpture.

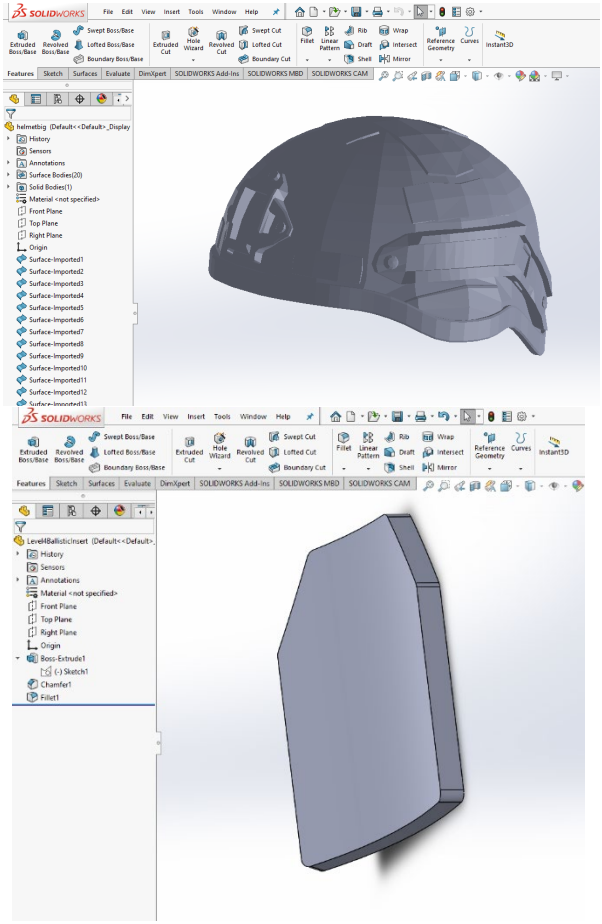


Fig.4. *3D models of battle helmet and armor plate (SolidWorks)*

Interactivity:

Virtual models can be manipulated and viewed in real time. This allows builders to rotate, zoom in and out of models to view and manipulate the details and

aspects that interest them most. This interactivity allows for better understanding and gives more opportunities.

Better visualization of complex concepts:

Complex mechanical, engineering, and scientific concepts can be difficult to understand through text and 2D images alone. 3D models of the components of personal ballistic protection means allow potential users to understand the interactions and dependencies between different elements in a clearer and more intuitive way.

Simulations and Virtual Experiments:

3D models of PPE components allow users to perform simulations and virtual experiments that are not possible with text or 2D images. This is particularly useful when simulating in a virtual environment the behavior of the various elements when struck or hit (Fig. 5).

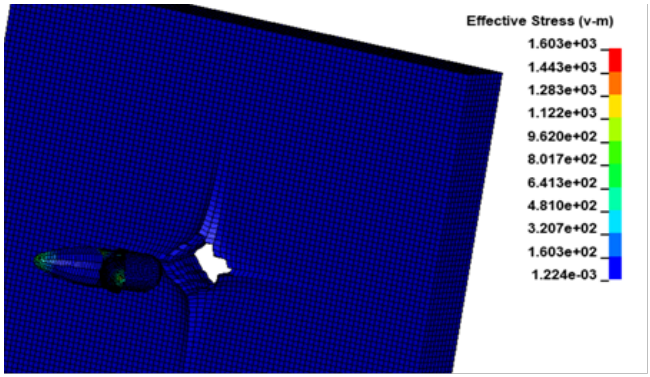


Fig. 5. *Input Data and Generate Results in Virtual Engineering (CAE), General Purpose Multiphysics Simulation Software Package (LS-DYNA)*

As it becomes clear, modern automated design systems make it possible, at a very early stage of design, to predict what will be the behavior of the final product, in this case the means of individual ballistic protection, also according to the expected final results, to select types of materials, in order to finally satisfy the requirements. All this is done in a virtual environment with a minimum expenditure of resources and labor, with extensive use of the opportunities for collective work of automated engineering applications, thereby achieving full optimization of the parameters of the final product, as well as a significant reduction in its cost.

3. Conclusion.

The design of the components that make up personal ballistic protection means is a complex engineering process that requires the combination of different materials, technologies and designs to achieve maximum protection with minimum impact on the wearer. Modern engineering automation applications provide solutions for each of the stages, namely: structural requirements analysis, material selection, structural design,

ballistic design, test and evaluation, engineering optimization, manufacturing and ergonomics. Also due to the increasing requirements for durability, ergonomics and cost in the design and production of elements for individual ballistic protection, automation is more important than ever design, simulation and manufacturing processes. This automation results in significant speeding up production development and can also increase process reliability, along with minimizing errors of a subjective nature. It can be mentioned that increasing automation in development requires optimization of the data exchange process, an example in the field of multidisciplinary development of virtual test technology to verify that a component meets requirements. A possible way to optimize the process of information exchange is provided by the implementation of unified data model. This data model represents an effective leverage point for intelligent integration of knowledge-based design methods and design automation.

REFERENCES

[1] Банков Б. Имплементиране и тенденции за използване на композитни материали в областта на военното производство - Научна конференция "Научните изследвания и инвестициите в технологични иновации - решаващ фактор за отбраната и сигурността", Пловдив Хемус 2020, с. I-139 - I-146, ISSN 1312-2916;

[2] Банков Б. Изследване на възможностите за използване на технологии за 3D печат в логистичното осигуряване - Научна конференция „Логистиката и обществените системи" - 2023 г. Велико Търново, с. 215 - 224, ISSN 2738-8042;

[3] Банков Б. Изследване на движението на проектил на боеприпас 7.62х54 във водна среда - Научна конференция „Актуални проблеми на сигурността", Велико Търново 2023 г, с.1511 - 1516, ISSN 2367-7473, 26-27 Октомври

[4] Antonov S.I., Izsledvane na prilozhenieto na CAD/CAM/CAE sistemite i tehnologiite za barzo prototipirane pri proektiraneto na komponenti na tehnicheskite sistemi, Shumen, 2021g., ISBN 978-619-7531-31-2;

[5] Brunet P, Hoffmann C, Roller D, CAD Tools and Algorithms for Product Design, Springer-Verlag Berlin Heidelberg, 2000, ISBN 978-3-642-08548-2;

[6] Petrova T., Petrov Z., Visualization of Objects in Computer Tomography, 21st International Symposium INFOTEH-JAHORINA (INFOTEH), 2022, pp. 1-4, ISBN 978-166543778-3 doi: 10.1109/INFOTEH53737.2022.9751325.

[7] Stamen I. Antonov, Mariela Ivanova, "Studying the application of CAD/CAM/CAE systems in the design of components for personal ballistic protection equipment", Journal Scientific and Applied Research, Vol. 25 No. 1, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, (2023), ISSN 1314-6289 (Print), ISSN; 2815-4622 (Online), DOI: https://doi.org/10.46687/jsar.v25i1

NEW APPROACHES TO STUDENT EDUCATION WITH 3D VISUALIZATION OF ELEMENTS OF TECHNICAL SYSTEMS

Mariela L. Ivanova

ABSTRACT: *The article presents the prospects for training students using software tools for 3D visualization of details and mechanisms, in terms of studying both their device and their operation and engineering analysis.*

KEYWORDS: *Model, Visualization, Learning.*

1. Introduction

The introduction of 3D visualization in the education of students specializing in the device of mechanisms and machines can have several important advantages and possible benefits:

— *Better understanding of concepts:* 3D visualization can help students perceive and understand complex mechanical concepts more easily by providing them with the ability to see and manipulate virtual models of machines and mechanisms [5].

— *Enhanced learning:* Interactive 3D models of components under study can make learning more fun and engaging, which can stimulate students' interest and motivation for better learning.

— *Real scenarios for problem solving:* With the help of 3D visualization generated using appropriate software packages, students can face real scenarios and challenges in the design and analysis of mechanisms, which can better prepare them for their future work .

— *Knowledge sharing and communication:* 3D visualization provides a tool for better knowledge sharing and communication between students and faculty, allowing for easier explanation and illustration of mechanical concepts.

— *Relevance:* Technological advancements in the mechanical engineering and engineering industry include the use of 3D modeling and virtual reality. Introducing 3D visualization into education can prepare students for current technologies and methods they will encounter in their future careers.

— *Facilitates the study of complex technical systems:* Technical systems can be extremely complex. 3D visualization can help students understand the interactions between parts and components better by visualizing movements, stresses, and other important aspects.

2. Why are 3D models of the studied mechanisms useful in the learning process?

3D models of learning components offer numerous advantages over conventional 2D images and text, especially when it comes to education and

visualization of complex mechanisms and concepts. The practice has proven many benefits, some of the key ones being [2]:

Spatial representation:

3D models provide a third dimension not available in 2D images and text. This allows for a more realistic and accurate representation of objects, machines, structures and processes that have a three-dimensional nature and complex sculpting.

Interactivity:

Virtual models can be manipulated and viewed in real time. This allows student learners to rotate, zoom in and out of the models to examine the details and aspects that interest them most. This interactivity engages them and allows for better understanding.

Better visualization of complex concepts:

Complex mechanical, engineering, and scientific concepts can be difficult to understand through text and 2D images alone. 3D models allow students and learners to see the interactions and dependencies between different elements in a clearer and more intuitive way.

Simulations and Virtual Experiments:

3D models allow users to perform simulations and virtual experiments that are not possible with text or 2D images. This is particularly useful for learning in fields such as mechanical engineering where different scenarios and outcomes need to be explored [6].

Better memorization and understanding:

The visual and spatial information provided by virtual prototypes can help learners remember and understand concepts more easily and for longer. This is especially important when teaching complex and abstract topics.

Knowledge sharing:

3D models can be easily shared and used for educational purposes through the Internet, virtual learning platforms and applications. This allows students to have and provide access to important information and lessons from anywhere in the world.

3. Preparation of 3D models for training in the device of complex mechanisms

Preparing the virtual prototypes (models) for learning requires several steps and processes to ensure that the models are suitable for educational purposes and that students can use them effectively for maximum benefit. The main steps in the preparation of the three-dimensional models are [1]:

Clearly define the goal:

Clear goals and requirements are set for what needs to be achieved with the 3D models. What exactly should be taught or illustrated? What concepts or processes should be presented?

Collect data sources:

At the beginning of the process, it is necessary to collect all data sources that will help in creating the 3D model. This may include drawings, photographs, scans or other visual materials.

Choosing the right software:

Creating 3D models requires specialized 3D modeling software, such as SolidWorks, TopSolid, Blender, Autodesk Maya, 3ds Max, or another similar tool.

Choose the software that is implemented in the educational process and that is available for the relevant educational institution (university, institute).

Create the base model:

The basic 3D structure is created, starting with the basic shapes and details of the mechanism under study. This can be done by modeling from scratch or by importing existing models. Existing models can be adapted to meet specific educational needs. This may include adding additional details, texturing, or dimensional modifications.

Search online resources and check licenses:

There are many online resources where free or paid 3D models can be found. For example, SketchUp 3D Warehouse, TurboSquid, CGTrader, and Blend Swap are good sources for ready-made models. These resources offer a variety of objects, components, and mechanisms[4]. In the event that ready-made models from online resources will be used, it is necessary to understand the licenses and rules of use. It is especially important that there is an opportunity to use the specific models in the educational context[3].

Adding details and textures:

Gradually, all the necessary details are added to the learning mechanism model, including textures, colors and materials. This will make the model more realistic and attractive for training.

Model optimization:

The model should be maximally adapted and optimized for educational purposes. This includes reducing the number of annotations to ensure fast loading and use of the model, especially in interactive learning.

Testing and fixes:

The model is tested in a virtual environment to ensure that all details are correct and that the components function and interact correctly. If errors and problems appear, they are fixed in the testing stage.

Export and storage:

The model is exported in a format suitable for the study and stored in a secure location so that it can be easily accessed by students during both tutor-led exercises and independent work.

Documentation and instructions:

It is desirable to provide documentation and instructions for using the 3D model so that users can understand how to use it for training and get maximum benefits.

Integration in the educational environment:

Finally, in order to have the effect of the previous actions, the 3D model is integrated into the educational process by being included in the learning (didactic) materials, virtual learning platforms or educational applications.

4. Examples of successful use of 3D models for training in the device of complex mechanisms

As noted, building 3D training models of complex mechanisms can be very useful for acquiring knowledge about the device, operation, and quality diagnostics of machines [1].

Below are some successful examples of creating 3D visualization in student learning:

Automotive Conventional Engine:

— 3D visualization of the main characteristics determining the engine parameters: cylinder volume, number of cylinders, engine revolutions, maximum power, maximum torque, etc.;

— 3D model of the engine with animations that show how each part of it works in different operating modes (Fig.1).

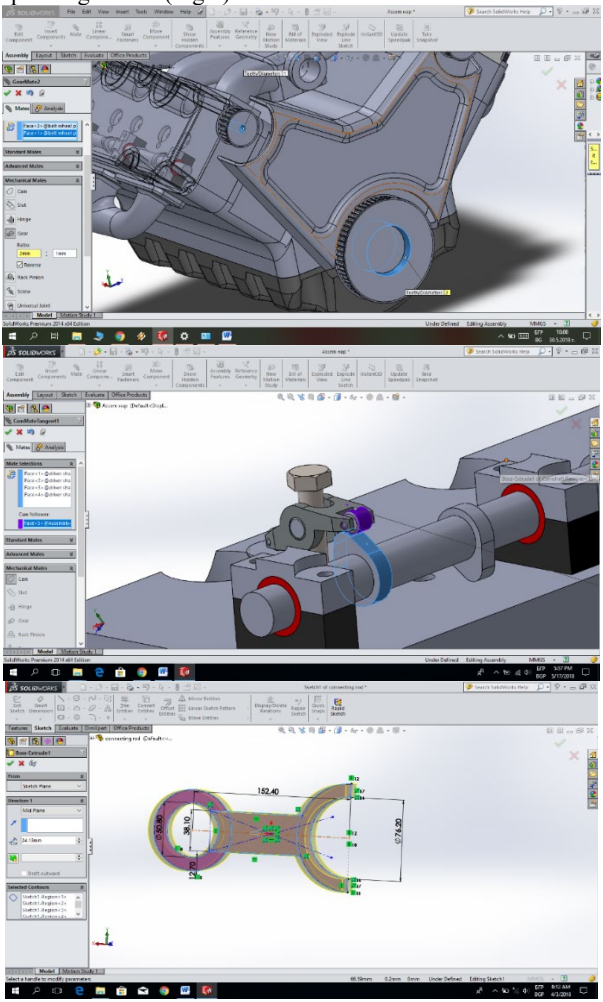


Fig. 1. *Models of components of a conventional car engine, to help the learning process to better clarify the operation of individual parts and mechanisms. (Solid Works, Dassault Systèmes)*

Robotic arm:

— Table of data for the lengths and angular positions of each arm segment;

— 3D model of the robotic arm that can rotate and fold according to the set values from the table. Built using specialized mechanical engineering software, a 3D model of a robotic arm provides a visual representation of how the different degrees of freedom move under different commands. The accompanying table may contain information about the angular values of the arm joints (Fig.2).

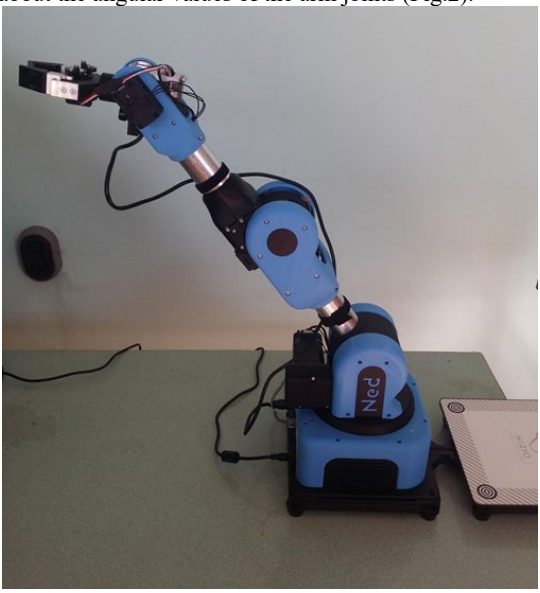


Fig. 2. *Robotic arm Niryo - 6-axis collaborative robot based on open-source technologies designed for Education, Vocational Training and Research.*

Car suspension:

— Tabular data on suspension parameters: type of suspension (for example, independent or dependent), type of shock absorbers, camber angles, etc.;

— 3D model of the car suspension that can be visualized in real time by changing all parameters.

Pneumatic production system:

— Data table for air pressure, air flow rate, diameter of pipes and valves, etc.;

— 3D model of the pneumatic system that demonstrates how the components move and interact and under different conditions.

Mechanical Engineering:

— Stress state of materials, by designing a 3D model of the structure of a specific material (e.g. metal or alloy) and visualizing how the stress and strains are distributed across it under different loads. Data generated in a tabular model can contain stress and strain information under various conditions.

These specific examples of the use of pre-created digital models can be implemented in the learning process to visualize and facilitate the understanding of complex mechanisms and concepts in different fields of knowledge.

5. Conclusion

The combination of 3D visualization with traditional teaching methods can be extremely useful for the development of students' competences and knowledge in the field of the device of mechanisms and machines. Proven by practice, 3D models provide a richer, more detailed and interactive educational experience that can enhance learning and understanding of complex topics and concepts. They are particularly useful in device knowledge, diagnostics and machine learning disciplines where visualization and interactivity are essential. Creating quality 3D training models takes time and effort, but can provide valuable visual resources for educational purposes.

REFERENCES

[1] Antonov S.I., Izsledvane na prilozhenieto na CAD/CAM/CAE sistemite i tehnologiite za barzo prototipirane pri proektiraneto na komponenti na tehnicheskite sistemi, Shumen, 2021g., ISBN 978-619-7531-31-2;

[2] Antonov S., Ivanova M, "Studying the application of CAD/CAM/CAE systems in the design of components for personal ballistic protection equipment", Journal Scientific and Applied Research, Vol. 25 No. 1, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, (2023), ISSN 1314-6289 (Print), ISSN; 2815-4622 (Online), DOI: https://doi.org/10.46687/jsar.v25i1;

[3] Antonov S., Some peculiarities of the working process of 3d printers and the software to support them, Proceedings of International Scientific Conference - "Defense Technologies" DefTech 2023, "Faculty of Artillery, Air Defense and Communication and Information Systems", Shumen, ISSN 2367-7902

[4] Bankov B., Izsledvane na vazmozhnostite za izpolzvane na tehnologii za 3D pechat v logistichnoto osiguryavane - Nauchna konferentsia „Logistikata i obshtestvenite sistemi" - 2023 g. Veliko Tarnovo, s. 215 - 224, ISSN 2738-8042;

[5] Brunet P, Hoffmann C, Roller D, CAD Tools and Algorithms for Product Design, Springer-Verlag Berlin Heidelberg, 2000, ISBN 978-3-642-08548-2;

[6] Petrova T., Petrov Z., Visualization of Objects in Computer Tomography, 21st International Symposium INFOTEH-JAHORINA (INFOTEH), 2022, pp. 1-4, ISBN 978-166543778-3 doi: 10.1109/INFOTEH53737.2022.9751325.

QUALITY MANAGEMENT METHODS AND TOOLS

Stamen I. Antonov

ABSTRACT: *The article analyzes the methods and means of quality management, in the aspect that the efforts made by the organizations to improve the quality of the products produced or the services performed are profitable in terms of financial results and customer satisfaction.*

KEYWORDS: *Quality, Measurement, Methods, Indicators.*

1. Introduction

Modern research shows that efforts made by organizations to improve the quality of products produced or services performed are profitable in terms of financial results and customer satisfaction. Therefore, quality and its management are perceived as an essential part of the organizations' business. Measures to improve and maintain a high standard of products/services are included in the strategic and operational plans.

2. Quality as a definition of an indicator for the full use of products/services by users

According to the standards of the International Organization for Standardization ISO/ is understood as "the extent to which the set of inherent characteristics satisfy the requirements". As a requirement is defined as "a stated need or expectation, which is usually implied or mandatory".

According to the standards of the International Organization for Standardization ISO/ is understood as "the extent to which the set of inherent characteristics satisfy the requirements". As a requirement is defined as "a stated need or expectation, which is usually implied or mandatory" [2].

According to the ISO 9000:2000 standard, it is defined as "...coordinated activities to direct and control an organization with respect to quality". In order to manage this process, a quality policy is developed, defining the goals and activities for their implementation, planning, management, ensuring, improving and maintaining quality. A special role in this activity is assigned to the management, which approves the quality policy and works for its implementation [3].

The development of the quality concept goes through the following stages:

First stage /until the 70s of the 20th century/. During this stage, there is a quality control department in the enterprises. The inspection is carried out on certain intermediate points of the production cycle and on the final product. The cost of maintaining this department and scrapping unfit produce is high. In many cases, products do not meet customer requirements.

Second stage. During this stage, the acceptable level of quality indicator is used to assess quality levels. It is calculated by the permissible number of defects of a certain number of production units /as a rule of 100/. During this period, the need to develop methods that ensure the quality of customers increases.

Third stage. During this stage, the emphasis is on the contribution of each participant in the production process. With his professionalism, he directly or indirectly influences the quality of the product/service. This implies the involvement of the staff in the measures to improve the quality of the products.

Fourth stage /70-80s/. It is characterized by the development and adoption of standards that guarantee quality in advance. The predominant place is occupied by the ISO 9000:2000 standards, ensuring quality and its management.

Fifth stage /after the 80s/. During this stage, the approach for total quality management /HERE/ is adopted, i.e. involving the entire organization in quality improvement processes.

The various models applied in the practice of organizations are also related to the development of the concept of quality management [1]:

A. The Deming model. In it, quality is tied to the management and improvement of the entire organization. On this basis, he builds a plan of 14 concepts and creates his famous cycle for implementing quality improvement: plan - do check - act /using statistical models/.

B. Juran's model /also known as Juran's trilogy/.

— quality planning: i.e. creating products that meet customer needs;

— quality control: i.e. comparing and evaluating quality against objectives. quality improvement: development of projects, infrastructure for quality improvement, training and motivation of participants in these projects.

C. Figenbaum model. According to him, the quality management system consists of a number of subsystems connected on the "input-output" principle. They enable internal quality control performed by a dedicated quality department.

D. Ishikawa model. The main principles laid down in it are:

— priority of quality over profit and its realization at all management levels;

— continuous training of the staff in order to reveal and develop abilities;

— forming a long-term orientation towards users;

— assessment of weaknesses and strengths in the quality activity;

— transition to a total quality management system in the organization.

E. Imei's model /KAIZEN improvement/. Each employee in the organization of their workplace affects the quality of production through innovation, improvement and maintenance.

F. Modern quality management approaches cover all processes from design to product realization. Everyone must be involved in improving the quality of the organization's products, processes and systems.

3. The planning and quality control process

Quality management is seen as a process consisting of separate steps:

Planning. In this step, it should be determined what we are trying to achieve by changing the process - we need to determine the duration of the process, how to achieve the intended goal, what information we have, what additional data needs to be collected and how it will be process the results etc.

Implementation. This is where the planned in the first step is realized. The planned activities and processes are put into practice. If new ideas are to be used for the implementation of the process, a small-scale experiment should be carried out. In case these ideas succeed, they are introduced on a large scale and thus success is achieved.

Observing the effect. In the third step, the processes are observed and measured, compared with the planned and the results are recorded. After the project has already been successfully implemented, it is necessary to determine whether the expected result has been achieved.

Study the result. Based on the results achieved, it is checked whether the preliminary goals have been reached and the targeted actions to be taken afterwards in order to continuously improve the performance of the process by restarting the cycle. Where the result is positive, the manner in which the improvement was achieved must be disclosed. This method can be used to eliminate problems when the need arises. However, when the result is negative, an analysis must be carried out so that the mistakes made are not repeated again.

Repetition of step 1. Based on the favorable results achieved, a new company action plan should be developed again.

Repetition of step 2. The developed new plan is again tested on a small scale and then on a large scale. As it turns out, the cycle begins to repeat itself.

4. Methods for measuring quality indicators

Depending on the method of obtaining the information on the numerical values of the quality indicators, there are the following methods that are applicable in production and industry:

— *organoleptic (sensory)* - they are hedonic (the pleasure that a given product evokes in the user is assessed); analytical (specially selected assessors characterize the product in order to obtain its quality assessment).

Sensory analysis methods:

Sensory methods - a series of specialized behavioral techniques with different types of effects and Sensory analysis provides an assessment of the quality of food products using the human senses, without taking into account their influence on each

other: vision (color, appearance), smell (smell, aroma), taste + tactile sensations (crunchiness), sensation (touch) and muscle sensitivity (texture), hearing (sound).

The conditions for conducting the sensory analysis are: infrastructure of the laboratory; lighting in the laboratory; working environment; materials for conducting the assessment.

Requirements for the participants in the analysis: they are called evaluators; depending on knowledge and experience, there are inexperienced and trained assessors, experts, specialized experts; to check the sensitivity of the senses of the participants in these requirements, standardized methods have been developed - to assess the sensitivity of the senses for taste, smell, smell, sight, touch, sensitivity for surface sensation.

It is important that they are expressed in an appropriate digital form, with the main analytical methods being differential and descriptive.

Differentials establish a detectable difference in the intensity of the quality marks being evaluated or any other quality difference between the compared samples. Includes "triangle" method, "duo-trio" method for comparing pairs.

Descriptives are standardized studies of ordinary processes of spontaneous description. It includes the development of lists (check list) that covers properties, indicators, concepts, terms and other descriptors or descriptors; selection of a method for indicating the degree of intensity of the perceived components of the relevant sensory means (taste, smell) through scales 0-5 or 0-10 with the corresponding verbal equivalent for each point of the scale or so-called points.

Sensory profiles – the results of each descriptor of the different products can be presented graphically; a visual representation is obtained from the profiles.

The purpose of the procedure for carrying out the sensory analysis is to specify the connections and dependencies of the individual stages of the preparation, implementation and reporting of the results.

The method of presentation of the results is coding of the results, and the order of presentation is specified in advance.

— *instrumental methods* – technical means, equipment, reagents, etc. are used. subject to compliance with strictly defined conditions and application of relevant work methods. They enable a very accurate and objective characterization of the property being investigated. Types of chemical, physical, microbiological, etc. These methods are standardized because they are fast (current, practical, not used in an arbitration dispute - for this purpose the standardized arbitration basic methods are used), classical (basic, arbitral, reference).

— *expert* - are based on the opinion of a group of experts and are applied when the use of technical means of measurement is impossible or unjustified. Advantages: it allows to give an accurate and reproducible assessment of the subject and the error of the result is commensurate with the error of the instrumental methods. Disadvantage: subjectivity, limited use, high costs, etc.

— *sociological methods* - collecting and analyzing opinions of actual or presumed users of a given product through surveys, interviews, voting, organizing conferences, exhibitions, etc.

— *experimental operation* – follows the behavior of the product under specific conditions of use, when it is impossible or difficult to reproduce the process in laboratory conditions. Example: repairability, durability, failure-free, storability, defect-free.

— *computational* - use theoretical or empirical (experimental) dependencies to determine the numerical values of given indicators by other means, the value of which is known. Example: density, volume, mass.

5. Conclusion

Tools alone do not determine the quality of work. There must be the necessary know-how, motivation and knowledge of employees about what is expected from their implementation. In quality management, many modern methods based on the system approach have been used in practice. Their development today is particularly dynamic. These methods can be applied at different stages of the product life cycle. They have developed in world practice in recent years, although the principles underlying any of them have been known for a long time.

REFERENCES

[1] Мениджмънт - ценности, комуникации и промяна – М. Христова, М. Мирчев, Н. Миронова, УИ "Стопанство", София, 2004г.;

[2] Съвременни управленски практики – II том, Д. Минчева, София, 2004г.;

[3] Управление на качеството-книга наръчник – Нако Стефанов, Христо Радев, Ивелин Бурев, Труд и право, София, 2004г., ISBN: 9546080969;

[4] www.club9000.org (Бюлетин за актуална информация в областта на качеството);

[5] https://www.iso.org/home.html;

[6] www.efqm.org (Вътрешна електронна страница на Европейската фондация за управление на качеството).

METHODS FOR DETECTING AND ANALYZING DEFECTS AND THEIR CAUSES

Stamen I. Antonov

ABSTRACT: *The article analyzes the known methods and means of quality management, accepting the hypothesis that efforts made by organizations to improve the quality of manufactured products or provided services are profitable from the point of view of financial results and customer satisfaction. Some of the known and applicable methods for detecting and analyzing defects and the reasons for their occurrence are analyzed.*

KEYWORDS: *Analysis, Measurement, Methods.*

1. Introduction

To solve quality problems, many different tools are used - methods and means, which can be summarized with the term "quality engineering". Depending on their complexity and scope of application, they can be considered at three levels:

1. Philosophy, principles and concepts of quality management.
2. Quality management methods.
3. Quality management tools.

The article discusses the most frequently used methods and tools for quality management.

Quality management methods are complex in nature. With their help, quality problems can be solved comprehensively. The methods can be applied independently or in combination - complex methods. Usually, the methods are a collection of different elementary means. Depending on their application, the methods are divided into "off-line" - preliminary, preventive, before production and "on-line" - operational, production.

2. Defect detection and analysis methods

A. Pareto Diagram or ABC Analysis

The analysis is named after the Italian economist Vilfredo Pareto, who discovered the law of disproportionate causes, according to which only a small part of the problems causes a significant part of the effect. This method is used to analyze the concentration of one variable - a dependent variable such as total sales, materials, usage value, etc. compared to another independent variable such as number of products, number of customers to determine some dependencies and management priorities [5]. According to this law, approximately 80% of the effect is the result of 20% of the causes.

Pareto analysis is done for:

Phenomena - identification of the most important problems, for example, the volume of defects, losses from defective production, sales volume, the most common errors, accidents, etc.;

Causes - what are the main reasons for the occurrence of a given phenomenon, in order to take measures to eliminate them. They can be: personnel /age, qualification/, raw material /supplier, batch, composition, etc./.

The practical use of the analysis is related to the construction of diagrams or nomograms. The diagram /Pareto diagram/ is built in different versions - of the absolute and accumulated frequencies. It is a type of frequency distribution.

A significant improvement in quality can be achieved by analyzing the causes through new Pareto diagrams /stratification/ after identifying the phenomena.

The concentration curve usually shows a typical trend which is suitable for determining the classes A, B and C, which are arbitrarily defined. Class A quite often corresponds to 70-80% of the dependent variable. On class C – less than 5% [3]. The Pareto analysis is easily performed and through it the objects /class A/ to which improvement actions should be taken are determined.

The application areas of Pareto analysis are diverse and this method has found wide application in many organizations around the world. After determining the significant problems from the Pareto diagram for each problem, an Ishikawa causal diagram is developed.

B. Cause and Effect Diagram

When there is not a clear enough idea of the factors influencing the behavior of the research object, but it is possible to determine the goal, an appropriate method of analysis is the well-known "Ishikawa-diagram" or "Fishbone Diagram" in the theory of quality management. "Cause and Effect Diagram". With the help of the diagram, the main factors affecting the achievement of the specified goal are discovered in a logical way. The possible causes that influence the problem are arranged in a hierarchical structure. The main categories in it most often correspond to the factors influencing the process - man, machine, material, method, control /the famous 5 M/ [7]. To each of them are added reasons from lower levels. The diagram consists of a central axis that points to the goal and branches that reflect the listed group causes. In these branches, the search process continues until the set goals are achieved. The following steps are used to solve the problem and build the diagram:

1. Defining the problem /effect/;
2. Determination of the root causes of the problem, recorded as branches of the central line;
3. Determination of the sub-causes for each cause / the ramifications of the main branches/;
4. Arranging the causes depending on the degree of their influence on the problem;
5. Making decisions about corrective actions.

3. Method FMEA /Failure Mode and Effect Analisis/ - probability of errors and analysis of their influence

The FMEA method is based on the assessment of the risk of potential errors and the detection of the causes related to the proposed solution to the problem or to the preparation of the developed process. By means of this method and with the help of a team of experts in the given field, potential risks can be detected, and by ranking them, a sequence of activities necessary to prevent them can be determined. It is used in quality assurance and management at the stage of design, implementation and operation of products and processes.

The FMEA method was developed in the early 1960s and was developed as a quality assurance method for AROLLO - NASA projects. After that, it was successively applied in aircraft construction /1965/, in nuclear power plants /1975/ and at the end of the 70s it was introduced in the company FORD-USA. In a series of FORD company standards, after which it is widely used in the automotive industry. In Germany, the FMEA method was introduced as DIN 25448 from 1980 [4]. The technical committee TK N56 on reliability of the International Electrotechnical Commission MEK /IEC/ adopted the standard IEC 812. It describes the procedures for analyzing the type of failures and their consequences / FMEA/ and their criticality /FMECA/.

A. Essence of the method

The FMEA method is gaining increasing application in the quality assurance of systems, structures and processes. The analysis is carried out on the basis of sequential detection of possible defects, assessment of the risk of their admission and determination of a sequence of preventive measures for their non-admission.

The risk of errors is expressed by the value of the priority risk number RPZ, determined by multiplying the three scores A, B and E. The same are chosen from 1 to 10. The RPZ is obtained in the interval 1 to 1000 and determines in what proportion the errors or causes are for mistakes, one against the other. The popular A, B and E rating scales were developed for the needs of the automotive industry. It is also embedded in the quality management system of leading automobile companies such as "Ford", "General Motors" and "Chrysler" - QS-9000.

The determination of the risk /RPZ/ is the most responsible stage for ranking the degree of importance of each of the considered errors. The most commonly used scales retain the expert analysis of the method. The priority of solving tasks is determined depending on the value of RPZ.

The effectiveness of this method largely depends on determining the values of the individual grades /A, B, E/ from 1 to 10 depending on their impact on the problem being solved. Errors with a risk score of A or E>8 require further follow-up. Those rated B>8 are a security risk and should be taken into consideration. Also, an E<3 score, in case it is not associated with a security risk, should be critically observed because it may be an indication of an existing opportunity for improvement, as the error will eventually be detected by the applied test measures, it can also be avoided through appropriate measures.

B. Analysis and Risk Assessment of Processes with FMEA

The application of the FMEA method in process design and management has specific features. It is necessary to accumulate certain experience and hold discussions about the methodology for building the analysis, determining the evaluation factors and the values of the risk numbers in the individual areas of industry and services.

There are many uncertainties associated with risk determination. In order to correctly determine the numerical values of the A, B and E ratings, the causes of the risk and its consequences must be precisely formulated.

Process FMEA, also called production FMEA, is also applied in production planning. It builds on the results of the FMEA of the structure. A design FMEA error caused by the manufacturing process is assumed to be a process FMEA error. It is therefore the task of a process FMEA to examine each process for suitability to produce the required product properties. To the FMEA of the process belong all the errors that may occur in the production of the product and the appropriate measures for their detection and elimination [1, 2].

In the EU880b Guidelines of the company FORD for process management it is said: "Measures and processes must be future-oriented so that they are fit to avoid mistakes".

The FMEA method is a systematic method. Its implementation achieves:

1. Clear formulation of the purpose of the research;
2. Presentation of information about the method in one basic document; preservation of the mutual relationship between the individual elements of the analysis, observing the logical sequence "cause-effect-measures";
3. A simple and clear scale used in ranking the priorities;
4. Personal responsibility for the effectiveness of the activities carried out within the planned period.

The FMEA method is characterized by universality of use. With its preventive nature, it is particularly suitable for limiting the adverse effects of environmental catastrophes. At the modern stage of industrial development, it is increasingly used in quality assurance and management at the stage of design, production and operation of products and services.

4. Method QFD /Quality Function Deployment/ - development of the quality function

The QFD method /house of quality/ is a strong modern method for strategic quality management. It is user-oriented, which is why many organizations are implementing it today. It is a multi-level planning tool for conscious quality planning.

The concept of the method was developed by the Japanese scientist Yoji Akao and applied for the first time in the shipyard of Mitsubishi Heavy Industries in the city of Kobe - Japan and by the company "Toyota", which further developed it and with its successful application won many supporters of the method all over the world [6].

Today, the method finds application in electronics, mechanical engineering, construction, agricultural machinery, infrastructure of residential areas, insurance, health care, ecology and other industries.

The QFD method is a planning and communication system, with the help of which all the possibilities of the organization are coordinated to achieve its goals.

Quality planning with QFD means the "Voice of the customer" - the external requirements, to be translated into the "Language of the company" - internal instructions for the processes and tests.

The main goal when applying the method is to realize the incorporation of user requirements into the product through flexible, efficient and fast design. The design stage is the first step in interpreting the user's needs in such a way that the final product best matches their requirements. The ability to account for market quality at the design stage is essential for better product definition and development documentation.

In this way, the efficiency of the project is increased from the very beginning, the number of necessary corrections in it and the total design time are sharply reduced.

Reduction of design time is achieved by grading objectives, documenting and implementing more effective communications. By implementing QFD, costs and the need for rework are drastically reduced.

QFD is a means of transforming the needs and expectations of users into relevant concrete actions on the part of the company.

In order to be able to realize the implementation of the QFD method / building the house of quality /, it is necessary to start with research towards the users and subsequently to analyze their interaction with the constructive requirements. Without knowing the users themselves, the analysis of their desires is impossible. They can be divided, for example, into "very useful" and "ordinary". The very useful form the bulk of sales. So they are our "main" users. Marketers believe that every user is important. The opinion of employees from the sales, claims, service, etc. departments should not be ignored. of the company itself. They work directly with consumers. Workers also have a say in the quality of the products they produce. All of them also talk to their relatives about this issue. Although these "internal customers" are called "secondary" by some authors, they also generate ideas.

Identifying consumer wants is a daunting task. It is desirable that the team developing the method retain the phrases they used in stating their requirements. These verbal information must be converted into design schemes and most often have a numerical expression.

Customer requirements can relate to the functionality of the product, can be naturally understood /basic/ and can also belong to those that cause their admiration for it. One must also initialize those that are negotiated, and the other non-negotiated ones that the client naturally expects.

Ignorance of consumer preferences and in-depth studies of their evaluation criteria can lead to incorrect formulation of requirements, which are an important element in the planning of quality and competitive products.

After performing a fit-for-purpose analysis, the team must systematize the accumulated information. It is desirable that the final results of the study be presented in an appropriate form. Various forms of the "House of Quality" type have been used in practice.

Quality planning with QFD.

In recent years, the QFD method has been used not only in product definition. It is a basis for planning processes and tests.

Achieving good final results requires its application in the successive phases of the product life cycle;

Product quality planning – translating the most important user requirements into critical product quality indicators;

Assembled unit quality planning – translating critical product quality indicators into critical assembled unit quality indicators;

Part quality planning – translating the critical quality indicators of the assembled units into critical quality indicators of the parts;

Process planning with QFD – process structure development and optimization; discovering the goals of the processes and their severity; translating critical detail quality metrics into critical process management metrics;

Test Process Planning – Translating critical part quality metrics into critical quality test metrics. Processing and Test Guidelines – Translating critical process and quality test metrics into work and test guidelines.

QFD – benefits:

1. Client-oriented planning;
2. Translation of customer requirements;
3. Documented quality planning;
4. Improvement of products and services;
5. Systematic approach when presenting the information;
6. Transparency of the design process;
7. Review documentation of planning results;
8. Effectively uses information about competitive products;
9. Reduction of misunderstandings;
10. Timely recognition of weak points and critical areas;
11. Fewer changes during production;
12. Reduction of product design time;
13. Scientific transfer in similar projects;
14. Allocates resources according to priority;
15. Easier reaching the targeted costs and greater transparency of costs;
16. Reduction of auxiliary and production costs;
17. Reduction of warranty costs;

18. Basis for decision-making when conducting strategic planning;
19. Improvement of communications;
20. Structures existing information and acquired experience;
21. Develops the skills to work in a team;
22. Transfers quality requirements from customers to staff;
23. Creates necessary communication between departments;
24. Easy to perceive.

QFD – Disadvantages:

1. Big waste of time for learning and applying the method at the beginning;
2. The evaluation of the results in the individual phases is difficult;
3. The impact becomes visible only when applying the product method;
4. If the design of the product is advanced, major changes in the product are possible only conditionally.

5. Conclusion

The considered methods contain only a part of the whole variety of methods and tools that find application in quality control, management and improvement. At the modern stage of intense competition, there is a diverse application of quality management methods - FTA Fault Tree Analysis - for reliability analysis and engineering, Taguchi methodology for planning of experiment /DoE/ and value and quality engineering and others. Each of the methods used has a certain advantage in its application at different stages of the product implementation. Its choice depends on the problems and the set goals.

REFERENCES

[1] Arabadzhieva-Kalcheva N., Tsankov Ts. Failure Modes and Effects Analysis – FMEA. Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 58-62.

[2] Menidzhmant - tsennosti, komunikatsii i promyana – M. Hristova, M. Mirchev, N. Mironova, UI "Stopanstvo", Sofia, 2004g.;

[3] Savremenni upravlenski praktiki – II tom, D. Mincheva, Sofia, 2004g.;

[4] Upravlenie na kachestvoto-kniga narachnik – Nako Stefanov, Hristo Radev, Ivelin Burev, Trud i pravo, Sofia, 2004g., ISBN: 9546080969;

[5] www.club9000.org (Byuletin za aktualna informatsia v oblastta na kachestvoto);

[6] https://www.iso.org/home.html;

[7] www.efqm.org (Vatreshna elektronna stranitsa na Evropeyskata fondatsia za upravlenie na kachestvoto).

ГОДИШНИК

НА ШУМЕНСКИЯ УНИВЕРСИТЕТ

„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Т. XIII Е

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

Университетско издателство

„Епископ Константин Преславски“

Шумен, 2023

ISSN 1314-8818 (print)

ISSN 2815-4703 (online)