

ГОДИШНИК

НА ШУМЕНСКИЯ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Т. XIV Е 2024

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

ANNUAL

OF KONSTANTIN PRES LAVSKY
UNIVERSITY OF SHUMEN

Vol. XIV E 2024

FACULTY OF TECHNICAL SCIENCES



Университетско издателство
„Епископ Константин Преславски“

Шумен



ISSN: 1314-8818 (print)

ISSN: 2815-4703 (online)

DOI: <https://doi.org/10.46687/AN24FTN>

ГОДИШНИК
НА ШУМЕНСКИЯ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“
Т. XIV Е 2024

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

ANNUAL
OF KONSTANTIN PRES LAVSKY
UNIVERSITY OF SHUMEN
Vol. XIV E 2024

FACULTY OF TECHNICAL SCIENCES

Университетско издателство
„Епископ Константин Преславски“

Настоящият годишник съдържа статии за 2024 г. от
Факултета по технически науки

РЕДАКЦИОННА КОЛЕГИЯ

проф. д-р инж. Събин Иванов Иванов
доц. д-р инж. Андрей Илиев Богданов
доц. д-р Здравко Юриев Кузманов
доц. д-р инж. Евгени Гришев Стойков
доц. д-р инж. Доника Величкова Диманова
доц. д-р инж. Тихомир Спирдонов Трифонов
доц. д-р Йорданка Ивайлова Янкова-Йорданова
акад. проф. д-р инж. Цветослав Станиславов Цанков

Годишникът излиза от печат през февруари 2025 година.

© Университетско издателство „Епископ Константин Преславски“

ISSN: 1314-8818 (print)

ISSN: 2815-4703 (online)

DOI: <https://doi.org/10.46687/AN24FTN>

СЪДЪРЖАНИЕ

ФОТОГРАФСКА РЪЧНА СКИЦА – ПРИЛОЖЕНИЕ В ГЕОДЕЗИЧЕСКОТО ЗАСНЕМАНЕ И КАРТОГРАФИРАНЕ НА СЛОЖНИ ОБЕКТИ, Иван Д. Иванов	5
БЛОКЧЕЙН ТЕХНОЛОГИЯ В УПРАВЛЕНИЕТО НА ВЕРИГАТА ЗА ДОСТАВКИ: ТЕКУЩИ ПРИЛОЖЕНИЯ И БЪДЕЩИ ПЕРСПЕКТИВИ, Николай Х. Йорданов	11
ДИГИТАЛНИ ТЕХНОЛОГИИ В УПРАВЛЕНИЕТО НА ВЕРИГИТЕ ЗА ДОСТАВКИ, Николай Х. Йорданов	22
СПЕЦИФИКИ И ПРЕДИЗВИКАТЕЛСТВАТА В СЪВРЕМЕННАТА КИБЕРСРЕДА, Валентина С. Хорозова	35
ПАРАЗИТНИ ЕЛЕКТРОМАГНИТНИ ИЗЛЪЧВАНИЯ И ПРОБЛЕМЪТ ЗАЩИТА НА ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ, Атанас И. Начев, Иванка Г. Павлова	46
ОЦЕНКА НА ЕФЕКТИВНОСТТА НА КОМУНИКАЦИОНЕН КАНАЛ С ОТЧИТАНЕ НА НАДЕЖДНОСТТА НА РЕАЛИЗИРАЩИТЕ ГО СРЕДСТВА, Атанас И. Начев	52
МОДЕЛ НА ЕФЕКТИВНОСТТА НА СИСТЕМА ЗА ИНФОРМАЦИОННО ОСИГУРЯВАНЕ НА ЗАЩИТАТА НА ОБЕКТИ ОТ КРИТИЧНАТА ИНФРАСТРУКТУРА, Атанас И. Начев	59
ВЛИЯНИЕ НА ТЕЖКОТОВАРНИЯ ТРАФИК ВЪРХУ ПЪТНАТА ИНФРАСТРУКТУРА И ЕКОЛОГИЧНА УСТОЙЧИВОСТ, Даниел Р. Денев, Александра П. Дочева	63
АНАЛИЗ НА МРЕЖОВ ТРАФИК И ПОДОБРЯВАНЕ НА СИГУРНОСТТА С WIRESHARK И CISCO PACKET TRACER, Цветослав С. Цанков, Илкер А. Хатиб	74
СЪЩНОСТ И ОСНОВНИ КОНЦЕПЦИИ ЗА КОРПОРАТИВНА СИГУРНОСТ, Десислава Д. Георгиева	82
СИГУРНОСТ И УЯЗВИМОСТИ В ТЕХНОЛОГИЯТА ZIGBEE, Даниел Р. Денев, Емили К. Димитрова	92
ОЦЕНКА ТЕХНИЧЕСКОТО СЪСТОЯНИЕ НА ЖИРОСКОПИЧНИ ИЗМЕРВАТЕЛНИ СРЕДСТВА, Андрей И. Богданов	98
ВНЕДРЯВАНЕ НА ИНТЕЛИГЕНТНИ КОМУТАТОРИ И ТЕХНОЛОГИИ В КОМУНИКАЦИОННИТЕ МРЕЖИ, Цветослав С. Цанков, Александра П. Дочева	103
СЪЗДАВАНЕ НА ЛОКАЛНА МРЕЖА С ИЗКУСТВЕН ИНТЕЛЕКТ, Стефан М. Казаков	111
ПОЛИГОННИ ИЗПИТВАНИЯ НА ПРОМЯНАТА НА БАЛИСТИЧНИТЕ ХАРАКТЕРИСТИКИ НА БОЕПРИПАСИ С ИЗМЕНЕНА ФОРМА НА ПРОЕКТИЛА ПРИ ДВИЖЕНИЕТО МУ ВЪВ ВЪЗДУХА И	

ПРЕМИНАВАНЕТО МУ ПРЕЗ СРЕДИ С РАЗЛИЧНА ПЛЪТНОСТ, Росен Н. Лазаров	115
КИБЕРРАЗУЗНАВАНЕ И ИНТЕГРИРАНИ РЕШЕНИЯ ЗА КИБЕРСИГУРНОСТ, Даниел Р. Денев, Илкер А. Хатиб.....	121
ЛОГИСТИЧНА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ПОТОЦИТЕ ОТ ЗАЯВКИ С ПРОГРАМА RHP SIMPLEX, Анатоли Ж. Стоянов	129
ВЛИЯНИЕТО НА ESG ВЪРХУ ЛОГИСТИЧНИЯ СЕКТОР И УСТОЙЧИВОТО РАЗВИТИЕ, Ива Б. Такова, Даниел Р. Денев.....	136
ИЗСЛЕДВАНЕ НА ЕДНОФАЗЕН СТАТИЧЕН ЕЛЕКТРОМЕР, Васил Б. Иванов	146
ТЕХНОЛОГИЧНИ ТЕНДЕНЦИИ И ЕФЕКТИВНО РАЗВИТИЕ НА СЪВРЕМЕННИ ОТОПЛИТЕЛНИ СИСТЕМИ, Милен С. Давидков, Даниел Р. Денев.....	162
КЛАСИФИКАЦИЯ В МАШИННОТО ОБУЧЕНИЕ. КЛАСИФИКАЦИОННИ МОДЕЛИ. МЕТОДИ И МЕТРИКИ ЗА ОЦЕНКА, Мая П. Тодорова	171
ДИЗАЙН НА МОБИЛНО ПРИЛОЖЕНИЕ ЗА ANDROID, ПОДПОМАГАЩО САМООБУЧЕНИЕТО ПО ТЕХНИЧЕСКИ НАУКИ, Стела Д. Минчева	178
ПРИЧИННО-СЛЕДСТВЕН АНАЛИЗ КАТО МЕТОД ЗА УПРАВЛЕНИЕ НА РИСКА, Нели А. Арабаджиева-Калчева, Цветослав С. Цанков, Мая П. Тодорова	184
ЕДИН ПОДХОД ЗА ПОДПОМАГАНЕ РАЗРАБОТВАНЕТО НА WEB ПРИЛОЖЕНИЯ ЧРЕЗ КОГНИТИВНА МАШИНА, Валентин Т. Атанасов.....	189
ИЗСЛЕДВАНЕ НА ВЗАИМОДЕЙСТВИЕТО НА ПОТРЕБИТЕЛИТЕ СЪС СЕНЗОРЕН ЕКРАН, Стела Д. Минчева	195
УВЕЛИЧАВАНЕ НА ОБЕМА ГОТОВА ПРОДУКЦИЯ ЧРЕЗ ВНЕДРЯВАНЕ НА НОВИ ТЕХНОЛОГИИ, Петя К. Велчева-Тодорова	201
ИНТЕЛИГЕНТНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА РЕСУРСИТЕ В КОМПЮТЪРНИТЕ МРЕЖИ, Силвия Х. Николова, Цветослав С. Цанков	210
АСПЕКТИ НА БЕЗПИЛОТНИ ЛЕТАТЕЛНИ АПАРАТИ, Владислава С. Георгиева, Никола П. Петров	221
ВРЪЗКА МЕЖДУ ПРИРОДНИТЕ БЕДСТВИЯ И ЕКОКАТАСТРОФИТЕ СЪС ЗАОБИКАЛЯЩАТА НИ СРЕДА, Весела Р. Петрова	226
ПРОБЛЕМИ В РАЗВИТИЕТО НА АВТОМОБИЛНИЯ ТРАНСПОРТ В ЕВРОПЕЙСКИЯ СЪЮЗ, Силвия Х. Николова, Ива Б. Такова	233
ИЗПОЛЗВАНЕ НА МОБИЛНИ УСТРОЙСТВА ЗА РАЗПОЗНАВАНЕ И НАБЛЮДЕНИЕ В РЕАЛНО ВРЕМЕ, Даниел Р. Денев, Екатерина М. Христова	243
EXPERIMENTAL DETERMINATION OF THE MAXIMUM SIGHT LENGTH TO THE MOST DISTANT BRIDGE PIERS FROM THE SHORES. CALCULATION OF THE ANGULAR SETTING OUT ACCURACY, Ani A. Stefanova	251

ФОТОГРАФСКА РЪЧНА СКИЦА – ПРИЛОЖЕНИЕ В ГЕОДЕЗИЧЕСКОТО ЗАСНЕМАНЕ И КАРТОГРАФИРАНЕ НА СЛОЖНИ ОБЕКТИ

Иван Д. Иванов

PHOTOGRAPHIC HAND SKETCH – APPLICATION IN GEODESIC SURVEYING AND CARTOGRAPHY OF COMPLEX OBJECTS

Ivan D. Ivanov

ABSTRACT: *In the past, keeping a hand sketch was one of the main activities in conducting geodetic surveying and mapping of various objects. It is no coincidence that the most experienced surveyor in the surveying team was usually chosen for its proper keeping and development. In addition to depicting the objects, their type and characteristics on an approximate scale, the hand sketch should also depict the connections between the objects, respectively the characteristic detailed points.*

KEYWORDS: *hand sketching, mapping, geodetic surveying*

DOI: <https://doi.org/10.46687/YT24IVI>

1. Въведение

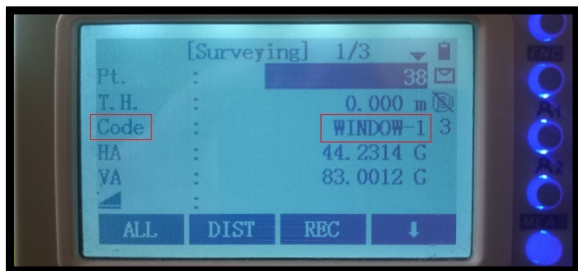
Използването на ръчна скица се свързва основно с провеждане на преки геодезически измервания, характерни за технологиите от миналия век. С напредване на технологиите, въвеждането на нови методи за събиране на геопространствена информация и внедряването на вътрешна памет в измервателните устройства, ролята на ръчната скица в геодезическото заснемане и картографиране се измени значително. Нещо повече, в много от съвременните задачи, особено в тези с по-малък обем и сложност, ръчната скица изцяло или частично може да липсва.

Ръчната скица изпълнява няколко основни роли, измежду които:

- Указва характеристика в съответствие с номерацията на подробните точки;
- Представя немащабно конфигурацията на обектите, предмет на геодезическо заснемане и картографиране;
- Отразява връзките между отделните подробни точки и картографираните обекти.

Първата роля може успешно да бъде заменена чрез въвеждането на кодова система, с която разполага всеки съвременен инструмент. Кодовата система представлява индивидуална характеристика под формата на текст на отделните подробни точки, получени в резултат на геодезическото заснемане, съответно картографиране на обектите [Фиг.1]. Съвременните софтуери предлагат различни

варианти за използването и въвеждането им като създаване на кодови групи, работни съкращения, въвеждане чрез гласови команди и др.



Фиг. 1. Въвеждане на кодове в тотална станция

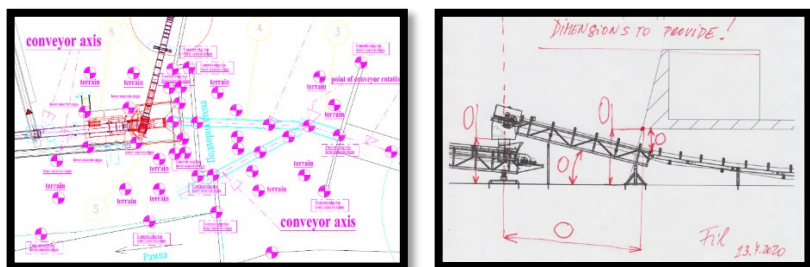
2. Изложение

В съвременното геодезическо заснемане и картографиране на обекти се „внедри“ един нов способ за водене на ръчни скици. Чрез наличната и свободна географска информация от различни приложения и сайтове се изготвя „подложка“ за изработването на ръчна скица, която частично представя конфигурацията на обектите, предмет на геодезическо заснемане и картографиране. Този подход е подходящ при планово картографиране на не сложни обекти като ефектът е по-бързо изготвяне на ръчната скица и по-правилно разпределяне на обектите (по-действителна конфигурация). Обикновено така събраната информация се използва и обработва от геодезиста, изготвил ръчната скица.

Понякога в практиката се налага да се заснемат по-сложни обекти, различни от типичните обекти като сгради, прилежащ терен, благоустройство, комуникации и др. Обикновено това са сложни технически съоръжения, конструкции на различни нива и др., заснемането и картографирането на които се свързва със специфични изисквания. Тези изисквания обикновено се формулират в задание, което се изготвя от различни специалисти като това налага оформянето на крайния продукт в съответствие с по нататъшното му директно интердисциплинарно използване [2]. При така въведени предварителни условия е добре да бъдат внимателно обмислени преди да бъдат използвани комерсиалните методи за геодезическо заснемане и картографиране като лазерно сканиране и фотограмметрия, които генерират голям обем от пространствени данни във формат, който доста често е неподходящ за интердисциплинарно използване без да бъдат допълнително обработени [4, 5]. Друго характерно условие, което е редно да се прецени, е изискванията за абсолютна точност и точност в конфигурацията на заснетите или картографирани обекти като това поставя под условие и в постижимата точност чрез използване на GNSS технологията [6, 8].

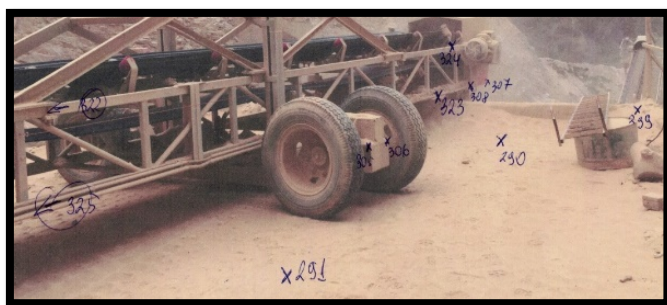
Друга особеност при заснемане на подобен тип обекти, е визуалния контакт и дискусиата относно характерни елементи от сложния обект, които трябва да бъдат заснети и представени в подходящ формат. Понякога проектантът

на техническото съоръжение няма възможност да го посети на място и изготвя задание по наличен опорен, генерален или кадастрален план, което може да доведе до пропуски при заснемането [Фиг. 2]. От друга страна като инженер-геодезисти, ние доста често нямаме необходимата строителна или технологична компетентия да интерпретираме правилно заснетия обект или характерна част от него.



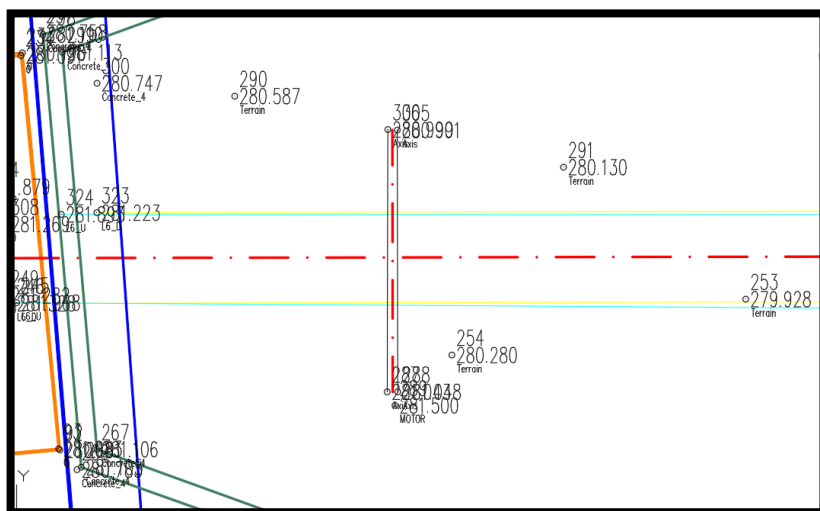
Фиг. 2. Задание за заснемане на характерни точки от стационарна роторна трошачка. С лилаво от проектанта са указани целеви характерни точки, предмет на заснемането

За решаване не гореспоменатите проблеми може да използваме подход, идентичен с изготвянето на ръчна скица като за основа използваме фотографски снимки. За изготвянето им е редно да бъде извършен предварителен обход на обекта и характерните места да бъдат надлежно фотографирани с цел при провеждане на геодезическото заснемане и картографиране, местата на характерните подробни точки да бъдат отбелязвани директно върху изображението [Фиг. 3]. Разбира се има възможност на място след направа на фотоснимките местата да се бележат върху дигитално устройство (таблет, телефон) без да се разпечатват, но практиката показва, че това забавя и затруднява процеса, а от друга страна поставя в риск самите мобилни устройства.



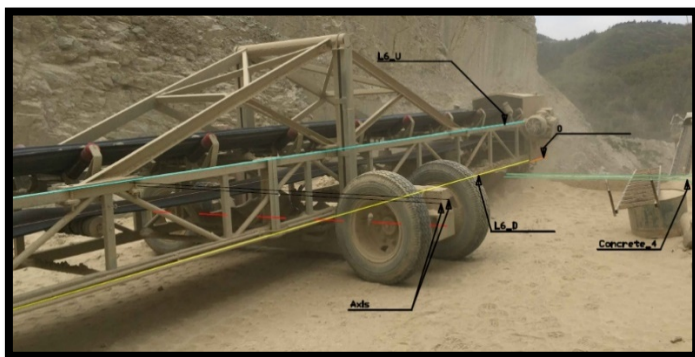
Фиг. 3. Изготвяне на ръчна скица върху фотографска снимка.

При изчертаване на чертежа (3D модела) следва да се познават добре отделните примитиви, както и възможните ограничения при някои специфични обекти (например TIN моделите) [3, 7]. Пространствената информация следва да бъде обработена по начин, който да бъде достъпен за други специалисти. Това трябва да бъде обсъдено с последващите ползватели на цифровия модел с оглед на това, че някои специфични за геодезическите дейности обекти като повърхнини, работни точки, 3D линии и др., може да останат недостъпни за ползвателите поради различните софтуери и характерните добавки към тях [Фиг. 4]. Препоръчват се използването на простите примитиви без сложни блокови елементи като някои характерни в заданието елементи (например определяне на някаква ос) следва да бъдат построени след изчертаване на характерни заснети елементи.



Фиг. 4. Частични резултати от заснемане в CAD среда. Осите (червените линии) са построени на база заснети характерни обекти/елементи от съоръжението

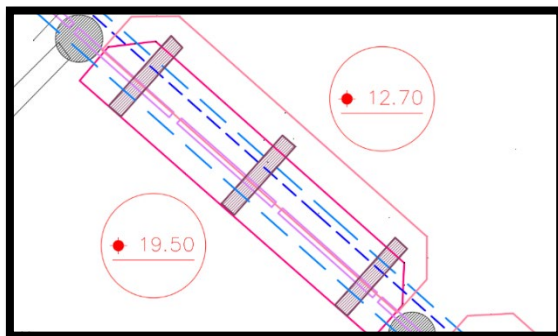
За да се внесе допълнителна яснота върху изготвеното геодезическо заснемане или картографиране, може след като изготвим цифровия модел на обекта, да направим пояснителни изображения чрез предварително изготвените фотоснимки, послужили като основа за ръчни скици. За целта чрез редактор за изображения или в CAD среда чрез вмъкване на изображението (препоръчва се втория вариант) нанасяме върху изображението линиите и обектите от изготвения цифров модел (3D модел) [Фиг. 5-7]. Това е особено полезно с цел уточняване на характерни детайли и оценка на това дали задачата е изпълнена коректно, особено ако проектанта на съоръжение е лишен от възможността да присъства на обекта.



Фиг. 5. Пояснително изображение



Фиг. 6. Пояснително изображение - пример от заснет обект на различни нива



Фиг. 7. Частични резултати от заснемане в CAD среда

3. Заключение

Настоящата статия разглежда възможността за използване на фотоснимки като основа за изготвяне на ръчни скици. Акцентите, поставени в статията, могат да послужат като напътствие при изготвяне на този вид специфична дейност с цел постигане на оптимални и икономически обосновани резултати при заснемане на сложни обекти. Чрез така предложения подход успешно се представят немасшабно конфигурацията на обектите, предмет на геодезическо заснемане и картографиране като същевременно се отразяват връзките между отделните подробни точки и картографираните обекти, което е предпоставка за изготвяне на коректен цифров модел, съобразен със спецификата на конкретното задание.

ЛИТЕРАТУРА

- [1] Маждраков М., Иванова Ил. Геодезия. 2014. Шумен, Издателство на ШУ „Епископ Константин Преславски“.
- [2] Милев Г., Милев И. Приложна геодезия Част 1, Инженерна геодезия. Книга 1.1. Основи, системи и технологии в инженерната геодезия. Съюз на геодезистите и земеустроителите в България, София 2017, ISBN 978-619-90732-2-3.
- [3] Стойков Е., Горов С. Същност и предназначение на CAD системите. Хардуер и софтуер на CAD системата. 2022 г. MATTEX 2022: Сборник научни трудове. Том 2. Шумен: Университетско издателство „Епископ Константин Преславски“, стр. 253-257, ISSN 1314-3921.
- [4] Янчев К. Оценка точността на създаване на 3D модели и топографски планове. 2022 г. MATTEX 2022: Сборник научни трудове. Том 2. Шумен: Университетско издателство „Епископ Константин Преславски“, стр. 223-225, ISSN 1314-3921.
- [5] Янчев К., Кирилова К. Наземно лазерно сканиране. 2022г. MATTEX 2022: Сборник научни трудове. Том 2. Шумен: Университетско издателство „Епископ Константин Преславски“, стр. 226-230, ISSN 1314-3921.
- [6] Dobrev S. GNSS technology for research of deformations of hydrotechnical installations. Journal scientific and applied research, vol. 27, 2024, p. 30-36, ISSN 1314-6289.
- [7] Ivanov S. Spatial data models. Journal scientific and applied research, vol. 20, 2021, p. 40-46, ISSN 1314-6289.
- [8] Stoykov E. Methodology for surveying and tracing of objects by using GNSS. Annual of Konstantin Preslavsky university of Shumen, vol. IX E, 2019, p. 21-24, ISSN 1311-834X.

БЛОКЧЕЙН ТЕХНОЛОГИЯ В УПРАВЛЕНИЕТО НА ВЕРИГАТА ЗА ДОСТАВКИ: ТЕКУЩИ ПРИЛОЖЕНИЯ И БЪДЕЩИ ПЕРСПЕКТИВИ

Николай Х. Йорданов

BLOCKCHAIN TECHNOLOGIES IN SUPPLY CHAIN MANAGEMENT: CURRENT APPLICATIONS AND FUTURE PROSPECTS

Nikolay H. Yordanov

ABSTRACT: *The supply chain is one of the use cases where blockchain has proven to be a powerful technology, enabling increased transparency, traceability, and security. However, as acknowledged by many who consider scalability, high costs, and data privacy among the key technical challenges today, this paper explores the benefits that supply chain implementation can bring, as well as its architecture. The presented examples include e-commerce and logistics, where fraud can be reduced while operational efficiency is improved through the use of blockchain technology. The research also discusses sharding solutions and Layer 2 approaches that address scalability issues without compromising security or providing unnecessary information for other research areas. It has been found that the use of blockchain technology in supply chain management is highly beneficial. However, the technical and regulatory challenges to successful adoption push industry stakeholders to address them. This, far from being fully resolved without commonly articulated goals, requires standardization efforts aimed at fostering innovations capable of driving transformative changes in global supply chains, empowered by unlocking the full potential offered by distributed ledger technology (DLT) such as blockchains.*

KEYWORDS: *blockchain technology, applications, supply chain management*

DOI: <https://doi.org/10.46687/YT24NHY>

Въведение

Управлението на веригата за доставки е основна грижа в корпоративните стратегии на повечето фирми в условията на бърза глобализация. Традиционните отношения на доставките обаче много често са пренаситени с дужина играчи, невидими за информация. Като цяло: те често създават различни проблеми като неефективност, изоставяне на данни — много висок риск от измами & Veronica М ефективно възпрепятства оперативната ефективност, също застрашава качеството на продукта и удовлетвореността на клиентите, да не говорим за корпоративния имидж. По този начин подобряването на прозрачността, ефективността и

сигурността в системата на веригата за доставки стана жизненоважно за организациите. Наистина, управлението на веригата за доставки съвсем наскоро се очерта като най-плодородното поле за практическо приложение и приемане на блокчейн технология [1, 2, 3]. Самите характеристики в основата на блокчейн системата (децентрализация плюс неизменност и проследимост) я правят приложима при решаването на проблемите, атакуващи веригите за доставки, и тези, които са критични. Например чрез блокчейн технологията информацията за всяка бизнес сделка или транзакция, свързана с всеки транзитен артикул, се записва постоянно в публични регистри в реално време. Това може да насърчи проверката на информацията сред участващите страни, да повиши прозрачността и да премахне проблемите с доверието или проблемите с асиметрията на информацията [4]. Вграждането на интелигентни договори в тези блокчейн системи би улеснило автоматичното изпълнение на договорни задължения и прехвърляне на средства вместо ръчни процеси; следователно се постига оперативна ефективност, за да се спестят разходи чрез намаляване на намесата на посредниците [5].

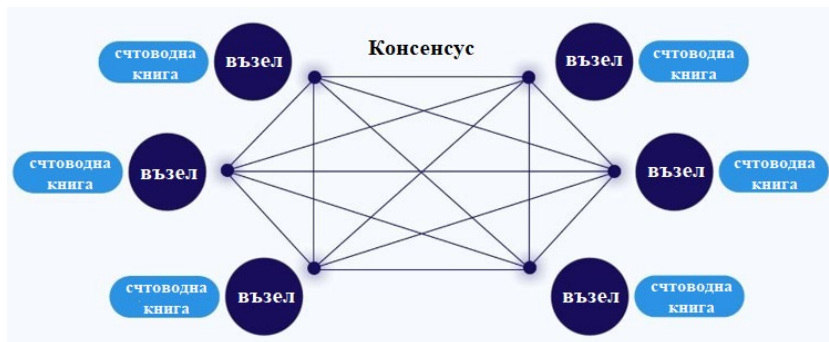
Има оскъдна подробна литература за приложението на блокчейн технологията за управление на веригата за доставки. Настоящият документ се опитва да запълни тази празнина чрез подробен преглед на литературата, анализ на казуси от реалния свят и ключови предизвикателства и ограничения в приложенията на блокчейн технологията в управлението на веригата за доставки. Насоките за развитие също бяха предложени, като се вземе предвид интегрирането на блокчейн с други нововъзникващи технологии и потенциала за широко внедряване от един сектор в друг. По този начин се надяваме, че прегледът ще допринесе за текущите разговори относно прилагането на блокчейн (или други подобни технологии) за подобряване на глобализираното управление на веригата за доставки.

Преглед на блокчейн технологията

Основи на блокчейн технологията

Състои се от свързани блокове, всеки от които съдържа криптографския хеш на предишния блок, клеймо за време и данни за транзакция [3]. Този дизайн гарантира, че сигурността, прозрачността и неизменността се изпълняват в цялата мрежа [3]. Всяка транзакция се потвърждава чрез консенсусния механизъм; така че става трудно да се променят предишни записи, което от своя страна изгражда доверие в разпределените системи [3]. Структурата на Blockchain не е просто просто съхранение на данни, а споделено доверие между множество страни, за да се гарантира прозрачност плюс сигурност с високи рискове от подправяне (Фигура 1) [1]. Блокчейн е революционна децентрализирана система за цифрови книги за записване на транзакции в обширна мрежа от компютри. Обикновено се сравнява с централизирана база данни на един сървър. Базата данни е сигурно защитена с помощта на свързани камери и няколко защитни резета, но това ниво на сигурност не може да се сравни с блокчейн от подобно естество. Тази база данни се различава по един начин от нормалните бази данни, които биха копирали всяка дейност, която се е случила с нея. Номерът с блокчейна е, че той се

самопроверява. По-нататък, когато някой направи каквото и да е запис в мрежата, той отнема предишния запис и друга важна информация, за да реши сложен математически проблем. И накрая, това е много сигурно, защото лицето, което променя, трябва да промени всички копия едновременно. Това се прави с помощта на механизъм за гласуване от всички лица, използващи мрежата [1,2]



Фиг. 1. Структура на блокчейн [1]

Децентрализирано - това е една от неговите основи. Вместо да работи с един централен орган, блокчейн работи в разпределена мрежа: всеки участник (наричан възел) има пълно копие на книгата. Последствията от тази децентрализация: шансовете за отделни точки на повреда са сведени до минимум; сигурността също е повишена. По този начин Blockchain е по-устойчив на атаки и системни повреди поради този силен модел на сигурност, където процъфтява.

Освен това разпределени, как различните страни постигат консенсус относно това кои транзакции са валидни и как могат да бъдат добавени и – и най-важното – как остава устойчив; с извършване на доказателство за работа, което е решаване на сложни пъзели с помощта на изчислителна мощност и доказателство за залог, което гласи, че участниците трябва да потвърдят транзакциите в зависимост от броя монети, които притежават, са само няколко от по-често срещаните методи за постигане на консенсус. Има алтернативен метод за постигане на споразумение, предоставен от Byzantine Fault Tolerance, в случай че има дефектни или злонамерени възли. Всички възли в системата трябва първо да изпълнят изглед, така че новите транзакции да станат приложими за изгледи за текущото състояние на книгата преди целостта. Той е надежден и целостта му е запазена.

Друга важна характеристика на блокчейна е неизменността. Това е концепцията, че информацията, добавена към блокчейна, не може да бъде променяна. Поне не без промяна на всички по-късни блокове - което го прави неосъществимо без изчислителни ресурси извън осъществимостта без консенсус от мрежата. Доверието се основава на този вид неизменност на информацията. И се поддържа подходяща надеждност на данните - много необходима в системи с висока нужда от сигурност и високо ниво на точност като управление на веригата за доставки. И тогава идва основата на интелигентните договори. Интелигентните

договори са основно линии на кодово споразумение между купувач и продавач. Той автоматично самоизпълнява и налага условията от само себе си или автоматично действа, след като са договорени в предварителен момент или е изпълнено конкретно условие (без необходимост от човешко действие, когато е свързано с условия), в който случай процесите ще бъдат рационализирани, посредниците ще вече не са необходими и ефективността ще се увеличи. Интелигентните договори обикновено се считат за един от първите положителни аспекти на блокчейн, тъй като те осигуряват начин за премахване на човешка грешка или оперативни забавяния и в същото време гарантират прозрачност и отчетност.

Характеристики и предимства на блокчейн за веригата за доставки

Прозрачността и неизменността са основните характеристики, които превръщат същата технология на блокчейн в много постижими цели за повишена производителност на веригите за доставки [6]. При наблюдение в реално време на продуктите и частите, измамите или грешките във веригата на доставки могат да бъдат ограничени и продуктите ще бъдат автентични [6]. Това може да бъде напълно автоматизирано чрез интелигентни договори, като се гарантира, че всеки етап от веригата за доставки се движи едновременно и незабавно работи за изграждане на доверие между доставчици, производители и потребители — особено в международна търговска среда. С блокчейн технологията непроменимият запис на транзакциите помага да се идентифицират всякакви несъответствия или проблеми много по-бързо. Той осигурява сигурен и прозрачен начин за проверка откъде идват стоките, как се движат и при какви условия — което прави индустриите, които се нуждаят от значително количество проследимост и отчетност, невероятно полезни [7].

Други важни характеристики на блокчейн технологията, които я правят много изгодна за работа в управлението на веригата за доставки, включват прозрачност плюс възможност за проследяване. Това високо ниво на проследимост позволява да се водят прозрачни записи, тъй като доказателствата за всякакво темпериране на информация могат да бъдат проследени във веригата на доставки. Освен това такива прозрачни записи драстично намаляват рисковете от измами, тъй като проследимостта на такива нива предоставя на компаниите (и техните клиенти) сертифицирана информация за мястото, времето и условията на производство на даден продукт. В съответствие с това компаниите могат да проследят информацията за продукта обратно до самия произход до крайния потребител. Това от своя страна им помага да имат по-добра видимост върху веригата си за доставки и своевременно уведомяване за всякакви нередности или проблеми [8].

Сигурността е друго ключово предимство на блокчейн технологията в управлението на веригата за доставки. Децентрализацията по природа на блокчейна, съчетана с усъвършенстваните криптографски техники, гарантира, че всички чувствителни данни, свързани със сигурността, се записват и предават сигурно в мрежата. Това допълнително подобрява защитата на важна информация за веригата за доставки: специфика на сделката, кои са доставчиците и откъде идват продуктите. С гаранцията за защита на данните направо от всеки етап от

веригата за доставки без влизане за неотризирано подправяне - което е главоболие за традиционните системи за верига за доставки и причината за честите изтичания на данни - е сведено до минимум.

Друг голям успех в подобряването на ефективността е прилагането на блокчейн технологията. Когато се използва във веригата за доставки, блокчейн може автоматично да изпълнява различни процеси, използвайки интелигентни договори, от изпълнението на поръчки до прехвърлянето на плащания. Автоматично изпълняваните процеси избягват намесата на посредниците, като елиминират закъсненията, дължащи се на човешка намеса, и намаляват честотата на човешките грешки. В резултат на това фирмите са в състояние да постигнат по-подредени операции в управлението на ресурсите, като както и по-бърза обработка на транзакции, към по-ефективно управление на веригата за доставки. Потенциалът за намаляване на разходите е друго много привлекателно предимство на блокчейна. Премахването на посредниците и автоматизирането на няколко процеса чрез интелигентни договори позволяват драстично намаляване на оперативните разходи, типични за традиционното управление на веригата за доставки. Фирмите са самодостатъчни при проверката на транзакциите или изпълнението на договорите, което намалява свързаните с тях административни разходи и ускорява времето за транзакцията. Такава технология, която се използва за намаляване на разходите и подобряване на разпределението на ресурсите, би била удобна за оптимизиране на веригата за доставки и повишаване на рентабилността на компаниите, които се интересуват от това.

Случай на използване на блокчейн във веригата за доставки

Следователно бързото развитие на сектора на електронната търговия доведе до навлизането на блокчейн технологията в преследване на по-голяма прозрачност при изкореняването на фалшиви продукти — по-специално при трансграничната онлайн търговия. Традиционните данни по веригата на доставки са много висок риск — особено за международни транзакции, където забавянето на данните и несъответствието на данните водят до привличане на фалшиви продукти. Споменатите предизвикателства се обслужват ефективно от децентрализирана книга, която се изпълнява от блокчейн технологията, за да позволи всички движения на продукт да бъдат постоянно записвани в различни сектори. Освен това Alibaba внедри блокчейн технологията бързо за проследяване на източниците и потвърждаване на автентичността на продуктите, продавани на нейната платформа. Това се прави, като на всеки елемент се дава нещо, което може да се опише като цифров еквивалент на паспорт. Това, което се случва, е, че тези файлове са криптирани и добавени към блокчейна, впоследствие може да бъде достъпен чрез сканиране на QR кода; това го прави защитен от подправяне и лесно достъпен. Това от своя страна повишава доверието на потребителите чрез автентичността на продукта и позволява на марките да намалят рисковете от фалшиви продукти [9].

Друг начин, по който блокчейн технологията осигурява прозрачност, е чрез поддържане на неизменни записи на транзакциите. Това е от огромно

значение в области като луксозни артикули и фармацевтични продукти, където въпросът за автентичността е всичко. Компании като Provenance и IBM Food Trust използват блокчейн за проследяване на източника на продукти с висока стойност, за да ги направят истински, като по този начин намаляват нивата на фалшиви продукти. Например Произходът проследява луксозните стоки от производството до покупката: това позволява на купувача да провери историята на продукта във всяка връзка във веригата за доставки [9,10].

Blockchain помага за стандартизиране на данните, споделяни между трансгранични платформи за електронна търговия, като улеснява по-унифициран и надежден поток от информация. Това подобрява осъществимостта на трансграничните транзакции чрез намаляване на количеството фалшиви стоки. За платформи, които са се зели да улеснят трансграничната търговия с намеренията да имат голям обхват на клиента, техните усилия могат да бъдат възпрепятствани от огромните ресурси, необходими за създаване на съвместими системи за обмен на данни [10].

Той революционизира проследяването на стоки, предотвратяването на измами и процесите на плащане в логистиката и транспорта. Сред ключовите предшественици, участващи в прилагането на блокчейн решения за осигуряване на прозрачност и проследяване в реално време във веригите за доставки, са големи компании като DHL и Maersk. Едно от основните главоболия в операциите, свързани с логистиката, е липсата в реално време на информация за проследяване на движението на стоки. Данните, които са под ръка, когато заинтересованите страни поискат, обикновено не са данни за местоположението за повечето наследени логистични системи. Въведете blockchain, технологията, която съхранява данни за доставка в децентрализирана книга. Информацията се споделя с всички упълномощени страни, т.е. изпращачи, получатели и превозвачи. И децентрализирано: така че данните са неизменни и надеждни.

Помислете за DHL — той разработи заедно с Accenture базиран на блокчейн прототип за сериализиране на продукти, който позволява проследяване на фармацевтични продукти от един етап на веригата за доставки до друг. Той гарантира, че тези продукти са оригинални и значително намалява риска фалшиви лекарства да намерят път към пазара. Чрез вграждане на запис на всяка транзакция и движение на продукта в своята товарителница, DHL позволява пълно незабавно проследяване на всички дейности при поискване по канали, видими както никога досега.

Има и платформата TradeLens на Maersk (разработена с IBM) — ядрото на това е базирано на блокчейн решение за глобална логистика. А) TradeLens позволява информацията да тече от единия до другия край на приложението напълно открито В) даде възможност на всички участници в логистичната линия да имат достъп в реално време към данни за всяка пратка. По този начин се отбелязва много голямо подобрене в това какви решения се стигат и ресурсите, които се разпределят по този начин — тъй като засегнатите страни могат да предприемат действия по-ефективно по отношение на закъснения или прекъсвания, наред с други логистични проблеми — въз основа на този капацитет.

Блокчейн системата за фактуриране на DHL автоматично генерира и валидира фактури. Няма човешка грешка и процесът се ускорява Плащанията са

грешка при това ускоряване на обработката. Той гарантира, че цялата „тези“ информация за плащанията е достъпна за всички участващи страни. Може да е конкретното, което минимизира шанса за разногласия и измами [9].

Предизвикателства и ограничения

Въпреки че за блокчейн технологията всъщност съществува голям брой възможности в управлението на веригата за доставки, редица от най-важните предизвикателства трябва да бъдат преодоляни, за да се улесни внедряването и в крайна сметка да се приеме по-широко разгръщане. Едно от най-критичните предизвикателства, възпрепятстващи иновативната блокчейн технология, е свързано с нейната мащабируемост [11]. Колкото по-голям е обемът на транзакциите, толкова по-бавна и по-ресурсоемка е блокчейн системата – особено в широкомащабните глобални вериги за доставки. Това е резултат от изискването за постигане на консенсус за съгласие относно транзакциите, добавени наскоро в множеството възли в мрежата, което води до забавяне на тяхната обработка. Например, в области, свързани с логистика, обработващи милиони ежедневни пратки във всяка блокова верига с ограничена мащабируемост, скоростта на операциите значително ще се забави [12]. Според Rejeb et al., този ефект на тясното място представлява основна пречка за генерализирането на използването на блокчейн в няколко индустрии – включително логистичните и транспортните сектори – въпреки възможностите за проследяване в реално време, предлагани от платформи като TradeLens. Остава голямо предизвикателство да се мащабират тези системи върху милиони транзакции, които се извършват по целия свят всеки ден [12].

Освен това, основно препятствие е много скъпото внедряване, свързано с иницирането на система, базирана на блокчейн. Това включва, в самото начало, много големи инвестиции, свързани с интегрирането на блокчейн със съществуващи системи за управление на веригата за доставки, които са налице, инфраструктури, предназначени да бъдат приписани, и обучение на работната сила за ефективно и ефикасно използване на технологията. Това идва в допълнение към поддръжката, техническата поддръжка и системните надстройки, които редовно предстоят към компонентите на разходите [13]. Другото е, че големите компании могат да поемат разходите за приемане на блокчейн, тъй като DHL и Maersk са два основни логистични примера предвид техните финансови възможности. По-конкретно, в повечето случаи разходите са много високи за малките и средните компании да възприемат блокчейн технологията. Следователно повечето малки и средни фирми намират за много трудно да понесат тежестта на тази инвестиция само поради една от основните бариери, които излизат от обхвата на ограничените масови индустриални решения в управлението на веригата за доставки - финансовият аспект. Това се очертава като една от основните бариери, тъй като малките и средните предприятия намират за много трудно да поемат тежестта на тази инвестиция само поради масовия ѝ обхват в различни индустрии като едно от основните решения в управлението на веригата за доставки, базирано на едно от основните бариери — неговият финансов аспект.

Освен това самата технология на блокчейните е изправена пред някои правни и регулаторни проблеми, особено когато е децентрализирана и в трансгранична среда. Blockchain е световен, така че трябва да отговаря на много различни правни системи и регулаторни изисквания, които значително варират в различните страни [14]. Например, ако DHL внедри блокчейн във фармацевтичните вериги за доставка, това ще се свърже с логистичните разпоредби, а също и със законите за съответствие в здравеопазването, които са различни в различните региони. Отнемащото време и предизвикателно приважване в съответствие трябва да отговаря на множество (често противоречиви) закони, подлагайки допълнителна бариера пред фирмите, желаещи да внедрят блокчейн в международен мащаб. Както Rejeb et al. казва, това изисква корекции на тъкането, които от своя страна могат да доведат до забавяния или трудности при интегрирането с наследени системи [12].

Във веригата на доставки поверителността на данните остава един от най-предизвикателните въпроси за решаване. Въпреки че прозрачността на блокчейн е силна страна, понякога тя може да противоречи на необходимостта от ултра защита на много чувствителна информация. За индустрии като луксозни стоки, фармацевтичната промишленост, висококачествена електроника и много други, защитата на клиентските данни, както и частната информация за доставчиците, е много чувствителна. Това е приоритет, като го пазите абсолютно поверителен. Начинът, по който блокчейн създава прозрачност, прави всички подробности за транзакции известни на всички участници в мрежата. Може да е показателно в детайли неща, които по-късно са източници на нарушения по въпроси, свързани с поверителността. Реджеб и др. заяви, че необходимостта от прозрачност при съвместяването на операциите по веригата на доставки със строгите изисквания за поверителност на данните е един от най-предизвикателните аспекти за компаниите, желаещи да внедрят блокчейн.

Решения

Управлението на веригата за доставки чрез блокчейн технологията е ужасно обещаващо, но все още е много обезсърчено – в момента се появяват редица иновативни решения за справяне с тези проблеми. Основно внимание е насочено към скалируемостта на блокчейн мрежите, поради което се заемат някои повишени или голям брой транзакции в глобалната верига за доставки. Sharding и Layer 2 протоколи са например примери за такива решения. Когато при шардинга това изпълнение блокчейн мрежата се разпада на по-малки парчета, което прави всеки шард отговорен за обработката само на част от общите транзакции, като по този начин се намалява изцяло тежестта върху нея и значително се увеличава чрез поставяне:), което я прави по-машабируема като цяло, следователно подходяща за високи обемни среди като логистика. В допълнение, Lightning Network принадлежи към редица решения от ниво 2, които помагат за принудителното извеждане на малки транзакции извън веригата, като същевременно поддържат техния запис във веригата, отчетен в основната блокчейн: докато не бъдат затворени. Това обаче измества тежестта на машабируемостта от самата първична мрежа и в резултат на това описаните иновации могат да гарантират, че блоковите

вериги могат да мащабират своята производителност, за да управляват широкомащабни вериги за доставки, като същевременно запазват ефективността си.

Решенията за шардинг и Layer 2 не само поставят нови предизвикателства, като увеличаване на сложността на поддържането на консенсус или потенциални уязвимости в транзакции извън веригата, но също така са много силни обещания за предоставяне на начини за справяне с проблема с мащабируемостта. Понататъшните изследвания се препоръчват основно да се съсредоточат върху подобряването на този компромис между мащабируемост и сигурност, за да се даде възможност транзакциите извън веригата да бъдат безопасни, но и надеждни. По-усъвършенстваните механизми за консенсус и посоката на усилията за намаляване на потреблението на енергия за PoW също биха могли да направят много, за да направят блокчейн решенията по-устойчиви в дългосрочен план. Другото голямо предизвикателство са високите разходи, свързани с внедряването на блокчейн. Разработването на система, базирана на блокчейн, често означава големи инвестиции на капитал в началния етап: придобиване на инфраструктура, интегрирането ѝ със съществуващите системи на веригата за доставки и обучение на служителите. Въпреки това, с въвеждането на платформите Blockchain като услуга (BaaS) от облачни доставчици като IBM, Microsoft Azure и Amazon Web Services, компаниите успяха да бъдат икономически ефективни в подхода си за приемане на тази технология. С тези услуги компаниите могат да вземат предвидително изградени инфраструктури за своя блокчейн без тежка инвестиция в изграждането им от нулата, което предполага големи капиталови разходи. Освен това блокчейн решенията с отворен код като Hyperledger или Ethereum позволяват на фирмите да приспособят своите решения за намаляване на разходите за разработка, като същевременно използват този вид платформи, особено малките средни предприятия (МСП).

Законово и регулаторно съответствие: това също се очертава като предизвикателство след прилагането на блокчейн технологията в трансграничните вериги за доставки. Тъй като стандартните блокчейн мрежи се натрупват в много страни, всяка със собствена правна система и разпоредби за зареждане. Опитите за спазване на разпокъсана правна среда могат да представляват трудност в дейността по спазване. И все пак фирмите трябва, за да се справят с тези предизвикателства, трябва да се ангажират в това, което е ранно сътрудничество с местните регулатори, така че техните приложения на блокчейн да отговарят на специфичните закони и правила на мястото, където работят. Участието на такива фирми в международни инициативи за определяне на стандарти може да помогне за оформянето на глобалния регулаторен пейзаж за блокчейн, намалявайки правната несигурност, която в резултат възпрепятства гладките трансгранични операции. Поверителността на данните обаче е голяма работа, тъй като просто технологията поддържа отвореност и неизменност. Във вертикали като фармацевтика или продукти на високо ниво, където предприятията използват изключително критични данни, трябва да се внедри криптиране на данни в покой. Това местоположение трябва да постигне този баланс между прозрачност и поверителност. Едно от онези много практически решения, които прилагат доказателства с нулево знание (ZKPs) - това е

криптографска техника, при която едната страна може да докаже на другата, че знае някаква информация, и заедно с ZKPs с анонимизирани части отгоре на това, доставката членовете на веригата ще могат да удостоверяват транзакции, без да разкриват подробности, които той би трябвало да знае от първа ръка и по този начин пренебрегвайки поверителността на клиента, но все пак запазвайки необходимо ниво на прозрачност и за двамата, които заслужават нещо: Друг начин може да бъде използването на разрешени блокчейни, където само проверени участници ще получат достъп до някои много разумни подробности, докато останалата част ще бъде достатъчно отворена по начин, затварящ се от мястото, където има значение.

В заключение, проблемите с мащабируемостта, разходите, съответствието с нормативните изисквания и поверителността на данните може да измъчват блокчейн, но няколко иновативни решения могат да помогнат за смекчаване на тези предизвикателства. Някои прагматични подходи, които гарантират пътя към препятствия като шардинг, протоколи от слой 2, платформи BaaS и доказателства с нулево знание, биха направили блокчейн още по-жизнеспособен за внедряване в управлението на веригата за доставки. След успешното справяне с предизвикателствата, свързани с всеки такъв аспект, компаниите ще бъдат в състояние да отключат пълните предимства на блокчейн технологията. Това води до начин, който се отличава с повече прозрачност, ефективност и сигурност в глобалните вериги за доставки.

Заключение

В статията се разглежда текущото състояние, предизвикателствата и бъдещето на блокчейн технологията в управлението на веригата за доставки. Неговият децентрализиран, неизменен и проследим характер предлага значителна подкрепа за подобряване на прозрачността, ефективността и сигурността на веригата за доставки.

Мащабируемостта е проблем поради потенциала блокчейн мрежите да се забавят с големи обеми на транзакции. И все пак иновации като шардинг и протоколи от слой 2 подобряват капацитета за обработка. Тези решения увеличават пропускателната способност чрез разпределяне на натоварванията за обработка на транзакции, което е от полза за логистичните среди с голям обем. Разходите за внедряване са високи и включват инфраструктура, интеграция и обучение. Появата на BaaS платформи обаче позволява по-рентабилно приемане чрез предоставяне на готова блокчейн инфраструктура, като по този начин намалява първоначалните капиталови разходи. Поверителността на данните и спазването на регулаторните изисквания също поставят предизвикателства в трансграничните вериги за доставки поради различните правни условия. Ранното ангажиране с регулаторите и участието в глобалното определяне на стандарти е от съществено значение за справяне с тези сложности.

Въпреки тези препятствия, бъдещето на блокчейн в управлението на веригата за доставки е обещаващо. С развитието на технологията и разработването на иновативни решения блокчейнът е готов да играе по-критична

роля, подобрявайки управлението на веригата за доставки чрез повишена прозрачност, ефективност и сигурност.

ЛИТЕРАТУРА

- [1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. URL: <https://bitcoin.org/bitcoin.pdf>, 4(2), 15.
- [2] Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. Ethereum project yellow paper, 151, 1-32.
- [3] Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. IBM Research.
- [4] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security & Privacy*, 13(2), 35-43. <https://doi.org/10.1109/MSP.2015.45>
- [5] Szabo, N. (1997). The idea of smart contracts. Nick Szabo's Essays, Papers, and Concise Tutorials. <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- [6] Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80-89. <https://doi.org/10.1016/j.ijinfomgt.2017.12.005>
- [7] Casino, F., Dasaklis, T.K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and Informatics*, 36, 55-81. <https://doi.org/10.1016/j.tele.2018.11.006>
- [8] Kim, H.M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management*, 25(1), 18-27. <https://doi.org/10.1002/isaf.1424>
- [9] Apte, S., & Petrovsky, N. (2016). Will blockchain technology revolutionize healthcare? *Blockchain in Healthcare Today*. <https://doi.org/10.30953/bhty.v1.8>
- [10] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557-564). <https://doi.org/10.1109/BigDataCongress.2017.85>
- [11] Kouhizadeh, M., & Sarkis, J. (2018). Blockchain practices, potentials, and challenges: A focus on healthcare supply chain. *The International Journal of Logistics Management*, 29(2), 533-555. <https://doi.org/10.1108/IJLM-03-2018-0065>
- [12] Rejeb A, Rejeb K, Simske S, et al. (2021) Blockchain technologies in logistics and supply chain management: a bibliometric review. *Logistics*, 5(4): 72.
- [13] Casino, F., Dasaklis, T.K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55-81. <https://doi.org/10.1016/j.tele.2018.11.006>
- [14] Agarwal S. (2018) Blockchain technology in supply chain and logistics. Massachusetts Institute of Technology

ДИГИТАЛНИ ТЕХНОЛОГИИ В УПРАВЛЕНИЕТО НА БЕРИГИТЕ ЗА ДОСТАВКИ

Николай Х. Йорданов

DIGITAL TECHNOLOGIES IN SUPPLY CHAIN MANAGEMENT

Nikolay H. Yordanov

ABSTRACT: *With the rise of Industry 4.0, new technologies are opening up opportunities for business transformation. These technologies are reshaping supply chains and driving new ways of creating value. However, not all companies have embraced this path of digitalization due to significant investment costs, risking falling behind. This article analyzes three key areas of digital technology development and their impact on supply chain transformation, including the emergence of closed-loop systems as a foundation for the circular economy. The article provides practical examples of supply chain digitalization, along with its socio-economic and environmental effects. It is demonstrated that the creation of a shared information space for all participants and the transformation of the supply chain into an ecosystem have the most significant impact on supply chains.*

KEYWORDS: *digital technologies, digital transformation, digital economy, digital supply chain, circular economy, closed loop supply chain, digital ecosystem*

DOI: <https://doi.org/10.46687/YT24NIK>

Въведение: Принос на цифровите технологии

Невъзможно е да се отрече, че дигиталните технологии промениха фундаментално поведението на потребителите, фирмените дейности и взаимоотношенията между всички елементи на икономиката. Така мобилният интернет доведе до манталитета „винаги онлайн“ и свръхсвързаността на хората, компаниите и машините в цифровата икономика. Социалните мрежи натрупват голям обем информация за всичките си потребители. Изкуственият интелект осигурява алгоритмично вземане на решения и автоматизирано управление на процесите. Технологиията BigData позволява да се обработват големи количества структурирани и неструктурирани данни и прогнозни анализи, които прехвърлят сложни данни и знания на всички. Членовете на екосистемата правят човешката реалност почти излишна. Интернет на нещата дава възможност за дистанционно управление на процесите и системите на участниците и надеждността на транзакциите.

Интересното е, че дигиталните технологии както повлияха на операциите, така и ускориха разработването и внедряването на недигитални иновации, като

нанотехнологии, когнитивни технологии, автономни автомобили, генно инженерство, съхранение на енергия, 3D печат, нови производствени материали, нови начини за нефт и газ проучване и добив и възобновяема енергия.

Например, количеството енергия, генерирано от слънчеви и вятърни източници, зависи от метеорологичните условия и може да варира понякога, причинявайки излишък или дефицит на енергия. Интелигентните мрежи осигуряват взаимодействие между производителите, потребителите на електроенергия и мрежовите регулаторни системи. Подобно на интернет, интелигентната мрежа включва контролери, компютри, автоматични процеси и цифрови технологии, работещи в унисон с производственото оборудване. Основната функция на интелигентната мрежа е да осигури цифров отговор на бързо променящото се търсене на електроенергия и да го приведе в съответствие с предлагането.

Въпреки големия потенциал, цифровите технологии не се прилагат във всички компании в еднаква степен и имат различни нива на ефективност поради различни нива на развитие и привеждане в съответствие. Това се демонстрира в *hype cycle*, който се разработва от Gartner всяка година. Така през 2019 г. основните тенденции и движещи сили зад промените в операциите и бизнес моделите са представени от блокчейн, квантово изчисление, разширен анализ и изкуствен интелект [1].

В същото време на фирмено ниво се наблюдава следната динамика. Според проучване на 4600 бизнес лидери от 42 държави, проведено от компанията Dell, има пет отделни области, в които компанията инвестира в дигитална трансформация: киберсигурност, интернет на нещата, мулти-облачна среда, изкуствен интелект, подход, ориентиран към компютрите [2].

Изследването е фокусирано, първо, върху анализа и класификацията на приложението на цифровите технологии, като се фокусира върху тяхното въздействие върху трансформацията на веригите за доставки; второ, относно идентифицирането на централните фактори за цифровизацията на веригите за доставки, с използването на казуси от затворени вериги за доставки; трето, за идентифициране на доминиращите тенденции в развитието на веригите за доставки и превръщането им в екосистеми, които координират действията на всички техни участници и елементи.

ДИГИТАЛИЗИРАНЕ НА ВЕРИГАТА ЗА ДОСТАВКИ

Бизнес моделите на някои компании (напр. Google, Amazon, Alibaba, Airbnb, Uber) са основно изградени върху цифрови технологии. Други компании, независимо дали съществуват от пет, десет, двадесет или дори сто години, са принудени да трансформират и възприемат цифровите технологии, за да се конкурират. Този процес има различни имена като дигитализация, цифровизация или цифрова трансформация. Сега ще бъдат дефинирани подробно тези термини.

Дигитализацията е процес на създаване на цифрови версии на аналогови/физически неща като хартиени документи, микрофилмови изображения, снимки, звуци и др. По този начин той просто преобразува нещо нецифрово (други примери включват сигнали, здравни досиета, данни за

местоположение, лични карти и т.н.) в цифров формат, който след това може да се използва от изчислителна система за множество възможни цели [3].

В резултат на това получаваме непрекъснати информационни потоци в цифров вид, което води до ускоряване и подобряване на точността на операциите и намаляване на необходимия персонал. Дигитализацията създава почвата за автоматизация и дигитализация на операциите. Дигитализацията означава добавяне на цифровост към взаимодействията, комуникациите, бизнес функциите и бизнес моделите, което често води до комбинация от цифрово и физическо, като например многоканално обслужване на клиенти, интегриран маркетинг или интелигентно производство с комбинация от автономни, полуавтономни и ръчни операции [3].

По този начин цифровизацията е подобряване на функциите и бизнес процесите с цифрови технологии и цифрови данни. Основата на дигиталните процеси е използването на подробни анализи за управление на фирмените операции. Можем да говорим за дигитализация на производството или дигитализация на маркетинга, което означава, че много функции и операции ще се извършват автоматично без човешко участие. Дигитализацията поставя основите за преход към дигитален бизнес. Дигиталната трансформация е преход към дигитален бизнес: сложна трансформация на бизнес дейности, процеси, модели и компетенции на служителите за пълно използване на цифровите възможности. Много често дигиталната трансформация води до появата на нови пазари, нови потребители и нов бизнес. Подробно изследване на етапите на дигиталната трансформация е представено в [3].

Най-общо казано, цифровизацията и цифровата трансформация са насочени към постигане на следните цели:

- Използване на информация в цифров вид
- Сензорно взаимодействие с устройства
- Управление на клиентския опит
- Осигуряване на киберсигурност
- Автоматизация на операциите и вземането на решения
- Използване на външни и вътрешни социални мрежи

Дигиталната верига за доставки (DSC) е интелигентен, ориентиран към стойността, ефективен процес за генериране на нови форми на приходи и бизнес стойност за организациите и използване на нови подходи с нови технологични и аналитични методи. DSC не се отнася до това дали стоките и услугите са цифрови или физически; става въпрос за това как процесите по веригата на доставки се управляват с голямо разнообразие от иновативни технологии, напр. безпилотни летателни апарати, облачни изчисления и интернет на нещата, из между други [4].

Можем също да намерим дефиниция на Supply Chain 4.0 като приложение на Интернет на нещата, използването на усъвършенствана роботика и приложението на усъвършенствания анализ на Big Data в управлението на веригата за доставки: поставяйте сензори във всичко, създавайте мрежи навсякъде, автоматизирайте всичко и анализирайте всичко, за да подобрите значително производителността и удовлетвореността на клиентите [5].

Използването на цифрови технологии води до положителни икономически ефекти, като икономия на суровини и енергийни ресурси, поради

рационализиране на производството и потреблението, както и до перспектива за рехабилитация и възстановяване на околната среда. Всичко това допринася за формирането на нов модел на икономика, който се нарича кръгова икономика. Това е икономика, основана на процеси на реконструкция, оптимизация и пестене на ресурси, улеснени от цифрови технологии, която постига безотпадно производство и потребление, устойчив икономически растеж и социално-икономическа и екологична ефективност. Ключовата концепция на кръговата икономика е развитието на затворен цикъл и устойчиви вериги за доставки.

Устойчивите или зелени вериги за доставки означават, че принципите на устойчив екологичен и икономически растеж са внедрени в традиционна верига за доставки. Изборът на доставчици, проектирането на продукта, производството, съглобяването, дистрибуцията, устойчивата употреба, потреблението и изхвърлянето са предмет на тези изисквания. По този начин кръговата икономика и затворените вериги за доставки извеждат компаниите на ново ниво на иновации и конкурентоспособност, генерират нови източници на приходи и позволяват създаването на стойност в цялата верига на доставки.

В една кръгова икономика дигитализацията на веригата за доставки е насочена към предоставяне на необходимата информация за важни елементи и бизнес процеси, за тесни места и прекъсвания, както и за опции за оптимизиране на ключови показатели за ефективно използване на ресурсите и намаляване на разходите за постигане на социални, икономически и екологични цели. Дигиталните технологии спомагат за създаването на иновативни вериги за доставки, като вземат предвид жизнения цикъл на продукта, неговото въздействие върху околната среда, не само в производствения процес, но и при употреба, като същевременно оптимизират разходите и минимизират отрицателните ефекти от производството и потреблението.

ДИГИТАЛНИ ТЕХНОЛОГИИ В УПРАВЛЕНИЕТО НА ВЕРИГИТЕ ЗА ДОСТАВКИ

При оптимизирането на веригата за доставки се използва широк набор от инструменти с различна сложност и цена, например софтуерни продукти за ефективно проектиране на веригата за доставки, осигуряващи системна интеграция, като SAP, Oracle и т.н. Управлението на веригата за доставки традиционно прилага сценарийно и симулационно моделиране, изследване на операциите, производство и контрол на инвентара.

Ясно е, че най-голяма ефективност се постига чрез съвместното прилагане на цифрови и информационни системи. Например, електронните доставки и автоматизираното търсене на доставчици са инструменти, които използват цифрови технологии и интернет приложения в комбинация с ERP системи, които позволяват автоматизиране както на вътрешни, така и на глобални бизнес процеси. Специалистите по доставки по целия свят могат лесно да споделят информация, за да опростят процеса и да спестят време и пари без отрицателно въздействие върху качеството и стандартите на продукта.

Разнообразието от технологии може да се групира в три големи области: технологии за анализ на данни и визуализация; технологии за автоматизация на

операциите и управление на оборудването; технологии, осигуряващи комуникация между участниците във веригата за доставки (таблица 1).

Ще бъде разгледано как технологиите се използват във веригите за доставки със затворен цикъл, като се фокусираме върху директните и обратните потоци на материали, компоненти и стоки. Тези процеси, включително дейностите, свързани с продукта или неговата следпродажбена поддръжка, с цел оптимизиране, подобряване на ефективността на обслужването, намаляване на разходите и спестяване на екологични ресурси, са известни като обратна логистика[10].

Таблица 1. Цифрови технологии в SCM, съставена от автора с използването [6, 7, 8, 9]

Цел	Функции	Информационни и автоматизирани системи и технологии	Цифрови технологии
Анализ и визуализация на данни	Навигация на бизнес процеси, унифициране на данни от електронни каталози, интеграция на информационни системи, мониторинг на веригата за доставки, планиране в реално време на дейността на предприятието, администриране на продуктови данни и събития, обработка на данни, прогнозиране анализи	SCOR, ISO и CALS- стандарти, ERP, PIM, SCEN, TMS, SCMo, Фабрично планиране в реално време	Големи данни, изкуствен интелект, облачни изчисления и съхранение, квантови изчисления, S&OP платформи, интелигентен склад, носими устройства
Комуникация между участниците във веригата за доставки	Автоматизирано търсене на доставчици, електронни поръчки, напр - търговия, синхронизация на процесите по веригата за доставки, прозрачност на веригата за доставки, комуникация между елементите на веригата за доставки	CRM, SRM, CSRP, AMS, Single Window, EDI, EANC 0M, EDIFACT, digital signature	Автоматизирано електронно снабдяване, многоканално интелигентно решение за изпълнение, блокчейн, маркетинг в социалните медии, обратна връзка, социални мрежи, индустриален облак
Автоматизация на процеси и управление на активи	Гъвкава автоматизация на производството, дигитални производствени процеси, дигитално качество на продукта, дигитален обратен инженеринг, виртуални аналози за физически продукти/продукт йон	Роботи, автоматични производствени линии, WMS, гъвкава фабрична автоматизация, RFID	Цифрови близнаци, 3D-уплътнение, сензори, превозни средства без шофьор, смесена и разширена реалност, индустриален IoT, адитивно производство g, интелигентен роботи

Основната цел е ефективно генериране, събиране, съхраняване и анализиране на информация за всеки дизайн и състав на продукта, специфика на употреба, местоположение, възможности за разглобяване, различни начини за рециклиране и т.н. Всичко това е необходимо за създаване на множество жизнени цикли на продукта в по-късните етапи след първоначална употреба. Преди това липсата на актуална информация във всички части на веригата не позволяваше ефективни затворени вериги за доставки, но сега разпространението на цифровите технологии гарантира развитието на затворения жизнен цикъл на продукта.

По този начин киберфизичните системи позволяват достъп до информация за продуктите във всички етапи на производство и употреба, въздействието върху околната среда на всички процеси и обработката на продукта. Това намалява информационната асиметрия, тъй като производителите разкриват информация за компонентите и материалите на продуктите, докато употребата на продукта от потребителите също се наблюдава.

Сензори проследяват в реално време точното местоположение на продукта в края на употребата му. Анализът на големи данни се прехвърля към компании, които използват използвани продукти като основни производствени ресурси.

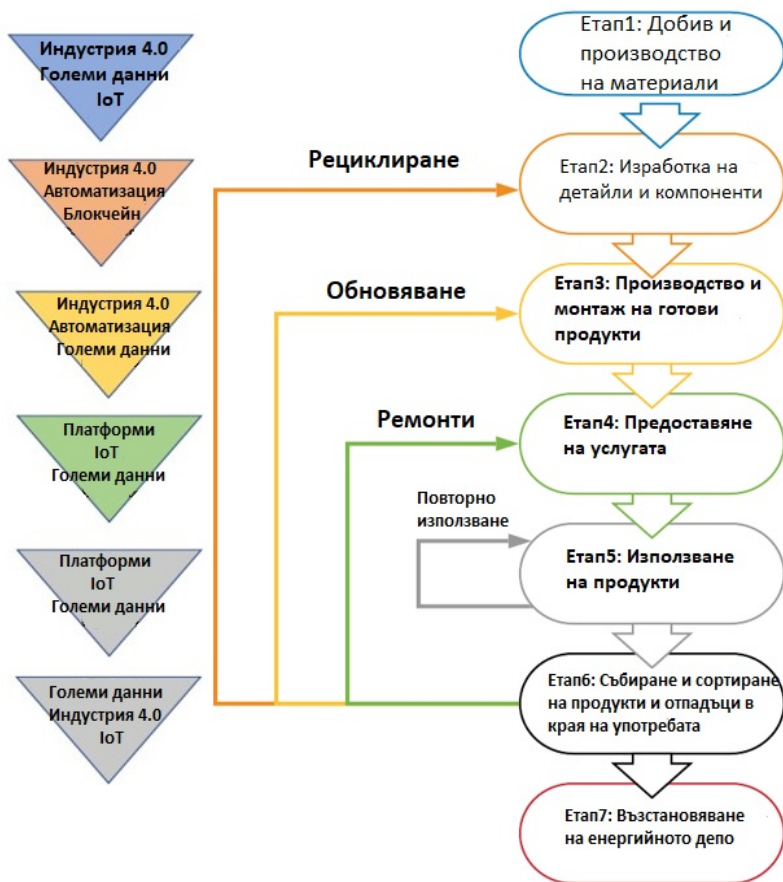
Оптимизирането на търсенето и предлагането на първични ресурси според количествата отпадъци и рециклируеми материали е революционизирано с дигиталните платформи, които формират пазарите за използвани продукти, с прилагане на IoT сензори. Тези сензори предоставят данни за състава на продуктите и показват възможностите за тяхното по-нататъшно приложение. В резултат на това рециклираните ресурси стават по-евтини и по-конкурентни в сравнение с първичните ресурси и материали. По този начин се появяват цифрови пазари за рециклиране на продукти и отпадъци.

Ключови процеси, консолидиращи продукти, компоненти, материали и ресурси в рамките на веригата за доставки, позволяват удължаване на жизнения цикъл на продукта чрез повторна употреба, ремонт и обновяване на използван продукт за постигане на качеството на нов продукт или спестяване на ресурси чрез обработка и екструдирание на нови материали, енергия и торове.

Трябва да се отбележи, че цифровите технологии имат различна степен на приложимост за отделните процеси, генериращи обратни потоци. Фигура 1 представя жизнения цикъл на продукта във фази: от извличането на суровини и енергийни ресурси, необходими за производството, до изхвърлянето му в края на употребата. Всеки процес в обратния поток връща продукта на определен етап от жизнения цикъл, напр. повторната обработка връща материалния поток към Етап2 - Производство на детайли и компоненти.

Тук процесите на генериране на енергия чрез изгаряне на отпадъци и тяхното обезвреждане не участват в затворените вериги за доставки, тъй като те не са предназначени да запазват ресурси във веригата за доставки и следователно трябва да бъдат сведени до минимум.

Етап 1. Потреблението и използването на първични материали е сведено до минимум от технологиите на Industry 4.0, като водещият е 3D-принтирането, което не само позволява персонализиране на продуктите и намаляване на потреблението, но също така и рециклирането на 3D отпадъците и превръщането им обратно в използвана нишка .



Фиг. 1. Цифрови технологии, поддържащи обратни материални потоци в затворена верига на доставки. Съставено от автора въз основа на [11,12,13,14,15,16]

Етап 2. Производството на елементи и компоненти включва избор на материали, които са най-подходящи за бъдещо рециклиране, включително биоразградими. Освен това всеки продукт с екологичен дизайн трябва да има дълъг жизнен цикъл и, когато е приложимо, възможност за ремонт или обновяване. Големи данни и високопроизводителни изчисления, автоматизация на търсенето на доставчици и цифрови близнаци предоставят широк набор от възможности за напредък в екодизайна.

Етап 3. Продуктите са проектирани да позволяват бъдещо автоматизирано разглобяване с минимален ръчен труд. Особено внимание се обръща на

етикетирането и сертифицирането на отделните артикули за бъдещо рециклиране. Така Michelin монтира сензори директно в своите гуми, за да позволи наблюдение на гумите в реално време. Когато се достигнат критични нива на износване, превозните средства се извикват във фабриката за възстановяване на гумите, като разходите за реконструкция са около половината от цената на суровините, необходими за производството на нов продукт [17].

Етап 4. Активно се развива предлагането на услуги и стоки за временно ползване като алтернатива на собствеността върху стоките. Масовата персонализация надделява над масовата стандартизация, а постоянното подобряване на продуктите за изискванията на клиентите се осъществява чрез обратна връзка и системи за прогнозен анализ. Например компанията Hello Tractor от Нигерия използва мобилна технология, за да предостави на 250 000 дребни фермери достъп до трактори в удобно време, подобрявайки тяхната хранителна сигурност и оптимизирайки разходите. Вместо да закупи и поддържа трактора, фермер го взема под наем. В допълнение, тракторите са оборудвани с M2M технология за споделяне на информация за превозното средство и неговата ефективност, което от своя страна увеличава максимално използването му и удължава живота на трактора [18].

Етап 5. В процеса на употреба продуктите се контролират от производителите и когато са изчерпани, повредени или остарели, се изхвърлят ефективно по най-екологичния начин. Използването на технологии за автоматизация и прогнозни анализи е изключително актуално на този етап. Така робот за разглобяване на Apple iPhone има 29 ръце и е в състояние да разложи използван iPhone за 11 секунди и да раздели компонентите му на полезни материали. Към днешна дата Apple е извлякла 61 милиона паунда материали, които могат да бъдат използвани в бъдещи продукти, включително 2204 паунда злато на стойност 40 милиона долара [19].

Етап 6. Събирането и сортирането на отпадъци и използвани продукти е много ефективно с IoT, платформи за обратна връзка и Big Data. Мониторингът на местоположението, качеството и собствеността върху продукта, както и определянето на участниците, отговорни за изхвърлянето, са изключително важни. Например в САЩ базираната в облак платформа за анализ на големи данни Rubicon свързва производителите на отпадъци с мрежа от независими превозвачи на отпадъци в 50 американски и канадски щата, както и в 18 други държави. Това осигурява по-високи нива на рециклиране, персонализиран подход за повторно използване на отпадъците, оптимизирани транспортни маршрути и подробен анализ на данните за отпадъците.

Тенденцията на глобалната цифровизация доведе до появата на затворени вериги за доставки и до развитието на фундаментално нов модел на кръгова икономика, основан на принципа „вземи-направи-използвай повторно“ [20]. Днес кръговата икономика е основата за постигане на целите за устойчиво развитие на SDG9 (устойчива индустриализация) и SDG12 (устойчиво производство и потребление). По този начин цифровата кръгова икономика се характеризира с безотпадно производство и потребление, минимални използвани материали за произведена единица и трансформиране на търговски и лични отпадъци в полезен ресурс за по-нататъчно използване.

Верига за доставки като екосистема

Както виждаме, концепцията за управление на веригата за доставки е непрекъсната координация на действията на участниците с цел организиране на логистични процеси и намаляване на разходите, времето и рисковете, свързани с движението на материали по цялата верига на доставки. В ерата преди дигитализацията координацията на участниците се извършваше от централна компания и се основаваше на използването на информационни системи (ERP, CRM, SRM, WMS и др.). Най-предизвикателните пречки за гладкото взаимодействие между елементите на веригата за доставки бяха:

- различни, често несъвместими информационни системи на страните
- прекъснати комуникационни и маркетингови канали (телефон, поща, факс, електронна поща, електронни документи, лични контакти)
- липса на редовен обмен на информация не само между отделни субекти, но и между различни отдели в рамките на една и съща компания.

Цифровите технологии предлагат ефективни решения на тези проблеми чрез създаване на общо цифрово пространство за различните участници във веригата за доставки. Сред тях клиенти и доставчици, транспортни и логистични компании, търговци на едро, дребно, дистрибутори, складове, както и финансови и консултантски фирми. Непрекъснатият достъп на участниците до актуална информация определя всички характеристики на веригата за доставки.

От миналия век насам са правени различни опити за изграждане на общо информационно пространство. За тази цел едно от първите общи информационни пространства, Single Window, беше създадено от компании, работещи в пристанището на Феликстоу (Обединеното кралство) през 1984 г. Основната причина за неефективността на пристанището бяха потоците от хартиени документи: времето за митническа обработка на пристигащите кораби в пристанището надвишава пет дни. Заинтересованите страни в пристанището (корабни линии и агенти, спедитори и брокери, митнически и държавни органи) инвестираха в развитието на системата на пристанищната общност с електронните документни потоци между участниците във веригата за доставки за пристигащи корабни товари. В резултат на това времето, прекарано в пристанищната обработка на товарите, беше намалено до шест часа и се подобри прозрачността и ефективността на логистичните процеси, което привлече нови инвестиции в транспортната индустрия. По-късно системата на един прозорец беше внедрена на много други големи гранични контролно-пропускателни пунктове (пристанища и летища), а стандартите за електронни документи (EDI и EDIFACT) бяха регистрирани съгласно ISO [21].

По-късно такива системи привлякоха интерес от страна на международни организации, особено работещи в областта на митническия и граничен контрол. През 2008 г. стартира програмата на ЕС за среда на един прозорец за митниците, като по този начин се създаде правна рамка за замяна на документацията с електронни комуникации на граничните контролно-пропускателни пунктове – инициатива, която все още остава важен елемент от международната търговия [22]. В Русия също е въведена система на едно гише за Федералната митническа служба и до 2016 г. над 99% от митническите декларации за внесени и изнесени

стоки са подадени по електронен път. Порталът за обществени услуги на страната също се основава на подхода на един прозорец.

По този начин развиващите се екосистеми са важна тенденция в управлението на веригата за доставки. Популярната концепция за екосистемата е взета от биологията и приложена към икономиката и управлението от J. F. Moore през 1993 г. Той дефинира бизнес екосистемата като гъвкава структура, състояща се от хора и фирми, взаимодействащи помежду си, за да създават и споделят ценности в системата [23].

Екосистема, използваща потенциала на участниците, създава нови възможности за създаване на нови продукти, услуги и повишаване на удовлетвореността на клиентите. Една екосистема може да включва участници във веригата за доставки, партньорски компании, потребители и дори конкуренти. В цифровата икономика екосистемите се основават на цифрови технологии и включват не само компании и хора, но и обекти и устройства, поради което се наричат цифрови екосистеми. Обикновено екосистемите са подкрепени от цифрови платформи.

Много известни производствени компании създават екосистеми от участници във веригата за доставки. Например Bosch се е заел да създаде свързана логистична система и да свърже всички електронни компоненти чрез Интернет на нещата [24]. За да се осигури бърз отговор на промените, беше решено да се създаде гъвкава екосистема за компанията и доставчиците. Компанията ръководи консорциум от немски производители за разработване на стандарти за автоматизирано производство и Industry 4.0. Като следваща стъпка компанията възнамерява да свърже своите интелигентни фабрики чрез интернет, което ще им позволи да се адаптират автономно към престоя на оборудването и към колебанията в предлагането и търсенето на материали. Така в цифровата екосистема се формира динамична верига на доставки от доставчика на суровини до крайния потребител.

Компанията Volkswagen, в сътрудничество с Amazon Web Services, създава цифрова екосистема, която ще комбинира данни в реално време от 122 завода, машини и системи, за да оптимизира вътрешните системи и процеси [25]. Следващата стъпка е създаването на индустриалния облак на Volkswagen и интегрирането на 30 000 места за доставка, собственост на 1500 доставчици и партньори на компанията в единна система. Това ще даде възможност да се идентифицират всички тесни места и да се оптимизира веригата за доставки. Основната концепция за новия индустриален облак на Volkswagen е отворена индустриална платформа, която производствените, логистичните и търговските партньори на компанията могат да използват в бъдеще. Тази цифрова екосистема се основава на облачна технология, ИТ сигурност, усъвършенствани анализи и индустриалния интернет на нещата.

По този начин веригите за доставки се трансформират в екосистеми, координирани от централна платформа, която непрекъснато натрупва и обработва данни за взаимодействията на хора, процеси и устройства в екосистемата. Те от своя страна формират нова логика за движение на материалните потоци в една екосистема. Координацията в рамките на веригата за доставки става все по-гъвкава и динамична, като по този начин надхвърля границите между отделните

предприятия и води до понятието „разширена фирма“ и динамична верига за доставки.

Платформа, хостваща екосистема, е в състояние да натрупва данни не само за материалните потоци и запасите, но и за репутацията на доставчиците, оценена чрез задълбочен анализ на техните дейности. Такава информация се използва в подкрепа на тактическо и стратегическо сътрудничество и решения за сключване на договори.

Веригите за доставки се развиват в цифрови екосистеми, базирани на платформа, което води до появата на мрежови ефекти, тъй като подобрената координация между членовете на екосистемата и по-доброто управление на репутацията привличат още по-добри и по-надеждни доставчици, което води до по-устойчива екосистема [26].

Доскоро веригите за доставки бяха предимно системи, в които участниците са тясно свързани чрез договорни отношения. Въпреки това, тъй като веригите за доставки преминават през цифрова трансформация, ще станем свидетели на по-гъвкави процеси, нови бизнес модели и екосистеми за доставки, улеснени от мрежовите ефекти.

Заклучение

Според прогнозите около 50% от най-големите компании в списъка Fortune Global 500 ще бъдат изместени от иновативни дигитални предприятия през следващите десет години.

Това означава, че дигиталните технологии имат огромен потенциал за промяна на очакванията на потребителите, операциите и комуникационните процеси, формите и характеристиките на веригите за доставки и накрая за трансформиране на всякакви икономически системи.

Промените ще настъпят чрез по-широка и по-задълбочена автоматизация на процесите, използване на по-сложни усъвършенствани анализи и преминаване от линейни вериги за доставки към цифрови платформи и екосистеми за доставки.

ЛИТЕРАТУРА

- [1] Gartner Top 10 Strategic Technology Trends for 2019 URL: <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/> (reference date: 29.06.2024)
- [2] Top 5 technology investments that will drive digital transformation URL: <https://www.techrepublic.com/article/top-5-technology-investments-that-will-drive-digital-transformation/> (reference date: 29.06.2024)
- [3] Digitization, digitalization and digital transformation: the differences URL: <https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption/> (reference date: 29.06.2024)
- [4] Digital Supply Chain: Literature review and a proposed framework for future research URL: <https://www.sciencedirect.com/science/journal/01663615> (reference date: 29.06.2024)

- [5] Supply Chain 4.0 – the next-generation digital supply chain, 2016 URL: <https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-40--the-next-generation-digital-supply-chain> (reference date: 29.06.2024)
- [6] Pagoropoulos, A., Pigosso, D. C. A., & McAloone, T. C. (2017). The emergent role of digital technologies in the Circular Economy: A review. *Procedia CIRP*, 64, 19 – 24. <https://doi.org/10.1016/j.procir.2017.02.047>
- [7] Bressanelli G, Adrodegari F, Perona M, Saccani N. Exploring How Usage Focused Business Models Enable Circular Economy through Digital Technologies. *Sustainability* 2018; 10:639. doi:10.3390/su10030639.
- [8] Salminen V, Ruohomaa H, Kantola J. Digitalization and big data supporting responsible business co-evolution. *Adv. Intell. Syst. Comput.*, vol. 498, Springer, Cham; 2017, p. 1055–67. doi:10.1007/978-3-319-42070-7_96.
- [9] Bressanelli G, Adrodegari F, Perona M, Saccani N. The role of digital technologies to overcome Circular Economy challenges in PSS Business Models: an exploratory case study / *Procedia CIRP* 73 (2018) 216–221
- [10] Gailen V. What is Reverse Logistics? / Gailen Vick // URL: <http://www.reverselogisticstrends.com/reverselogistics.php> (reference date: 29.06.2024)
- [11] Circular economy, your digital path. How digital enables the transformation into the sustainable circular economy/ White paper Scientific Community. Thought Leadership Atos URL: <https://atos.net/wp-content/uploads/2019/02/atos-circular-economy-white-paper.pdf> (reference date: 29.06.2024)
- [12] Ghisellini P, Cialani C, Ulgiati S. A review on circular economy: the expected transition to a balanced interplay of environmental and economic systems. *J Clean Prod* 2016; 114:11–32. doi:10.1016/j.jclepro.2015.09.007.
- [13] Ardolino M, Rapaccini M, Saccani N, Gaiardelli P, Crespi G, Ruggeri C. The role of digital technologies for the service transformation of industrial companies. *Int J Prod Res* 2017; 7543:1–17. doi:10.1080/00207543.2017.1324224.
- [14] R.Pardo, J.P Schweitzer (2018): ‘A long-term strategy for a European circular economy – setting the course for success’, Policy Paper produced for the Think2030 project, Brussels, November 2018
- [15] Neligan A. Digitalization as Enabler Towards a Sustainable Circular Economy in Germany/ *Inter-economics* 2018, p. 101-106 doi: 10.1007/s10272-018-0729-4
- [16] Ellen MacArthur Foundation. Towards the circular economy; Ellen MacArthur Foundation: UK, 2013.
- [17] Reinventing the wheel: Why smart tyres give the IoT real grip URL: <https://internetofbusiness.com/reinventing-the-wheel-smart-tyres-and-the-iot/> (reference date: 29.06.2024)
- [18] Hello tractor URL: <https://www.hellotractor.com/about-us/> (reference date: 29.06.2022)

- [19] Apple unveils 29-armed robot designed to disassemble old iPhones URL: <https://www.extremetech.com/mobile/225337-apple-unveils-29-armed-robot-designed-to-disassemble-old-iphones> (reference date: 29.06.2024)
- [20] Ellen MacArthur Foundation. Intelligent Assets: Unlocking the Circular Economy Potential. Ellen MacArthur Found, 2016.
- [21] Alan Long. Port Community systems. World customs journal, Vol.3, N1, 2009 URL: <https://pdfs.semanticscholar.org/93a7/e67f0520ca23f71eb73f2dfb93724f191724.pdf> (reference date: 29.06.2024)
- [22] The EU Single Window environment for customs URL: https://ec.europa.eu/taxation_customs/general-information-customs/electronic-customs/eu-single-window-environment-for-customs_en (reference date: 29.06.2024)
- [23] J.F.Moore. Predators and Prey. Harvard Business Review, 1993 May- Jun; 71(3): 75-86.
- [24] Volkswagen and Amazon Web Services to develop Industrial Cloud URL: <https://www.volkswagen-newsroom.com/en/press-releases/volkswagen-and-amazon-web-services-to-develop-industrial-cloud-4780> (reference date: 29.06.2024)
- [25] Always on board you're your freight is on the move. Bosch connected logistics. URL: <https://www.boschservicesolutions.com/monitoring/connected-logistics/> (reference date: 14.07.2024)
- [26] The future of supply chains as networked ecosystems. <https://platformed.info/the-future-of-supply-chains-as-networked-ecosystems/> (reference date: 14.07.2024)

СПЕЦИФИКИ И ПРЕДИЗВИКАТЕЛСТВАТА В СЪВРЕМЕННАТА КИБЕРСРЕДА

Валентина С. Хорозова

SPECIFICITIES AND CHALLENGES IN THE MODERN CYBERENVIRONMENT

Valentina S. Horozova

ABSTRACT: *The article is dedicated to the study of the main specifics and challenges of the modern cyber environment. A special place is devoted to clarifying the role and importance of social media and social networks in the context of security. For this purpose, a comparison was made on key indicators regarding the two concepts. The current trend of using fake news and disinformation as manipulative techniques in cyberspace is clarified. Next, the focus shifts to cybercrime, which is accepted as an immanent feature of modern reality. The current appearance of the modern criminal is presented. Special attention is paid to the various ways and channels for preparing and committing crimes in the cyber environment. The main conclusion drawn after the analysis of the topic is that training is the main tool for increasing internet literacy, respectively security.*

KEYWORDS: *security, cyber security, challenge, cybercrime, cyber environment*

DOI: <https://doi.org/10.46687/YT24HRZ>

Въведение

Съвременният динамичен свят характеризира с глобална киберобвързаност. Същата достигна своя пиков момент по време на пандемията от Ковид -19 и продължава устойчиво да се развива и днес. Така оформилата се тенденция към преминаване на общуване, пазаруване, забавление, бизнес, политика, дипломация, разузнаване, образователен процес в киберпространството продължава под различни форми и днес. Почти всички дейности, процеси и услуги намериха своя кибереквивалент, а някои дори и своя директен киберзаместител в киберпространството. Веднъж зародила се тази тенденция, в обозримо бъдеще трудно ще намери алтернатива. Успоредно с това, в киберпространството се създават благоприятни условия и най-разнообразни предпоставки за подготовка, извършване и дори модификация на различни по вид, мащаб, големина, форма и проявление киберпрестъпления. Това на свой ред поставя сериозни предизвикателства пред гарантиране на сигурността в различните й форми и на различните й нива. Поддържането на съвременната сигурност-глобална, национална, корпоративна, лична до голяма степен зависи от възможностите, ресурсите, познанията, специалистите и технологиите, с които

разполага системата за сигурност и обществен ред в борбата и противодействието на различните по вид киберрискове, заплахи и атаки.

Специфики на съвременната киберсреда

Дигитализацията е една от най-големите социални промени на XXI век. Тя кардинално трансформира формите, начините и методите, чрез който е възможно да се създава, обменя и разпространява информацията. В резултат общуването/комуникацията успешно преодолява национални и географски граници, покорява религиозни, езикови, политически, възрастови бариери. По този начин всеки човек получава възможност да бъде участник/съучастник в социалните процеси в обществото, в което живее, получава възможност да бъде и генератор на промяна, която желае.

Събитията от последните години разшириха облика и гамата от дейности и процеси, които имат пряко роля, значение и влияние върху осигуряването и поддържането на сигурността. Показател за това е, факта, че в почти всички съвременни стратегически документи и анализи на национално, международно и на корпоративно ниво, киберсигурността се окачествява като важен елемент от системата за сигурност, а на места се оценява дори и като ключов. Още през 2014 година ставаме свидетели на официализирането и признаването на киберпространството за петото бойно поле, в което могат да се извършват операции срещу националните интереси, териториалната цялост, конституционно установения ред на страните – членки на НАТО (Декларацията от срещата на върха в Уелс през 2014 г.) В същия документ, киберсигурността се определя и превръща в основна задача на колективната защита на страните членки на Алианса.¹

Това създава сериозни предизвикателства пред вече съществуващите мерки, изградените защиты и противодействия. Същите трябва да бъдат адаптирани навреме/успоредно към новите реалности продиктувани от иновативните открития и достижения на Индустрия 4.0 и Индустрия 5.0.

На следващо място, спецификите на киберсредата създадоха възможности:

- за анонимност;
- за лесен пренос на данни и информация в различни форми, вид и обем;
- за комуникация в реално време до различни точки на света, с различни участници, почти без никакви ограничения и почти без никакви забавяния или с минимални такива;
- за перманентност в създаването и използването на фалшиви самоличности с разнообразни подривни и престъпни цели;
- за формиране и целенасочено използване на цели организирани общности от хора с фалшиви самоличности с прикрити намерения, умисъл и план;
- за глобални манипулационни процеси;

¹ Allied Joint Doctrine for Land Operations (AJP-3.2 Edition A). NSO, 2016.

- за хибридни предизвикателства, рискове и заплахи;
- за превес/приоритизиране на дезинформационни действия и организирани мащабни, дезинформационни кампании;
- за психологически операции за влияние;
- за киберразузнавателна дейност.

Социалните мрежи и платформите за видео споделяне са основно място за изразяване и публично споделяне на чувства, на лични позиции и мнения относно събития, явления, процеси от всякакво естество. Редно е да отбележим, че те превръщат във водещ фактор в глобалната сцена. Все по-засилващата се мощ на социалните медии и мрежи, тяхната роля и значение в глобален аспект, безспорно ги определя като т.нар. пета власт, която по своята сила, влияние, потребители и информация далеч надминава четвъртата власт, а именно традиционните медии.²

Вл. Иванов изтъква, че „днес интернет придава стойностите на бъдещето, чрез хилядите си автори.“³ Тоест, киберпространството ще конструира бъдещето, поради факта, че владее настоящето и знае за миналото много повече от всеки друг.

Съгласно актуалните изследвания в световен мащаб, социалните медии продължават да бъдат най-предпочитаната платформа⁴, а интернет пространството се оформя като първи избор на онлайн потребителите при търсене на информация.⁵

С оглед темата, целесъобразно е да изясним основните различия и допирни точки между термините социални медии и социални мрежи. Въпреки че на пръв поглед двете понятия изглеждат взаимнозаменяеми и често се употребяват като синоними, те имат различни случаи на приложение, цел, аудитории, комуникационен стил, както е видно от табл. 1.

Социалните медии и мрежи се затвърждават като сериозен източник на киберпредизвикателства, рискове, заплахи за сигурността, на дестабилизиращи и дебалансиращи процеси със значителен отзвук в обществото с национален и с международен ефект. Тази тенденция се запазва и дори и усилюва, поради факта, че те съчетават от една страна характеристиките и архитектурата на мрежовите структури, от друга – свободата, глобализиращия ефект и особеностите на

² Методиева Ц., "Заплахи в интернет. Фишинг и финансово муле.", Международна научна конференция „Киберсигурността в информационното общество“, НВУ „Васил Левски“, Факултет „Артилерия, ПВО и КИС“ - гр. Шумен, 20-21 Април 2017 г., ISBN 978-954-9681-82-6, с. 157- 160.

³ Иванов. Вл. Българите, Том 2, издателство Хистореон, 2023, година, ISBN 9786199113561, стр. 7

⁴https://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 05.10.2024 г.

⁵https://www.gwi.com/bookdemo?utm_source=kepios&utm_medium=referral&utm_campaign=2023+Kepios+Global+Audiences посетен на 05.03.2024 г.

киберсредата, заедно с многообразието от своите потребители и информацията, която притежават. Социалните мрежи и мрежи се отличават с:

- лесно поддаваща се и нагаждаща се на промени структура;
- възможност за самоорганизация отвътре и отдолу;
- цялостна устойчивост при промени в средата;
- опростена организираност, без тромавост и изключителна сложност;
- хоризонтална конструкция на връзки и отношения;
- преобладаващи се самоструктуриращи се и самоконтролиращи се

единици (мрежи);

- малък брой нива на управление и йерархична подчиненост;
- целево ориентирани и планирани стратегии;
- многообразие на варианти на изграждане и поддържане на връзки и

свързаност;

- свобода на елементите;
- бързи възможности за сътрудничество.

Таблица 1. Сравнение между социалните мрежи и социалните медии⁶

	Социални мрежи	Социални медии
По дефиниция/определение	са свързани с това коя е вашата аудитория и какви са вашите отношения с нея;	включва информацията и съдържанието, които всъщност споделяте
Основната цел	Обсъждане и изграждане на връзки	Маркетинг
Стил на комуникация	включва двупосочна комуникация	основно доставя съобщение до голяма аудитория
Целева аудитория	конкретна аудитория/ съобразно броя на хората в групата	Възможно е и да няма конкретна целева аудитория
Навременни реакции	подобрява навременните отговори, тъй като включва директна комуникация	може да няма навременни отговори, тъй като не е напълно интерактивен

⁶ <https://avada.io/blog/social-networking-vs-social-media/> - посетен на 10.11.2024 г

Социалните медии устойчиво се утвърдиха като неоспорим фактор в глобалната сцена. Те са сред едни от основните канали за създаване, споделя и разпространение на актуална информация от различен вид и естество-включително политическа, икономическа, социална, радикална, а в последно време и военна. Новините вече се раждат в интернет и социалните медии. Дори и традиционните медии, в своите предавания и новинарски емисии, ползват информация, която е представена и споделена първо в социалните медии. Почти всички световни лидери и важни/ключови фигури имат специален публичен профил, които се ползва/служи като основно средство и канал за официални изказвания, за изявления по различни теми, за заявяване и отстояване на позиции, за поздравителни адреси и т.н. Всичко това ги превръща в благоприятна среда за разпространение на всякакви данни и информация, включително и манипулативни такава. Възможността за ежесекундното ѝ създаване и почти светкавичното ѝ разпространяване и лесно манипулиране в киберпространството, заслужено превръщат *информацията в оръжие*. (съгласно резолюция на Парламентарната асамблея на НАТО от 2017 г.) Тя, заедно с интернет технологиите, дават/осигуряват все по-голяма прозрачност и публичност/гласност на крайни мнения и настроения, на фалшиви новини.

Дезинформацията, фалшивите новини, създаването и наслагването на полюсни настроения, радикални нагласи сред потребителите на социалните медии, са само част от широката гама/палитра на хибридни предизвикателства, рискове и заплахи, които се раждат именно в киберпространството. Манипулативният процес лесно може да бъде прикрит, да бъде замаскиран зад фалшиви профили, тайни, скрити самоличности, чужди имена, фалшиви снимки. По този начин лесно се ражда т.нар. невидим враг. Враг, който може напълно спонтанно или планирано и целенасочено да предизвика промяна в общата нагласа сред обществото, да провокира и режисира създаването и ескалацията на силно дестабилизиращи процеси, както във виртуална, така и в реална среда, да генерира нарушаване на обществения ред, създаване на масови протестни действия, хулигански прояви, агресия и други. Тези особености на социалните медии, превръщат/дават възможност на всеки техен потребител да стане не просто наблюдател, а участник или дори генератор на различни по вид и сила обществените процеси.⁷

В този смисъл заблудата в интернет може да се породи не са само от чисто случайно поднесена погрешна информация, а може да бъде продукт на целенасочени, предварително обмислени и преднамерени действия и дори на цели стратегии.

Социалните медии и мрежи са основен генератор на нови идеологии, на насаждане на полюсни настроения сред обществата, на разделение и противопоставяне сред нации, държави, етноси.

⁷ Dimanova, D., Kuzmanov, Z., Risk management in information security, Conference proceedings MATTEX 2018. Information, Technical and Economical Problems of Security Systems, October 2018, Shumen, ISSN: 1314-3921, vol. 2, part. 1, pp. 139-145.

Социалните медии и мрежи преплетени с дезинформацията, манипулираното и целенасочено разпространение на фалшивите новини, се превръщат в съвременната реалност както за най-малките им потребители, така и за възрастните такива.

Тези факти, сами по себе си са достатъчна предпоставка за засилването/зараждането на новия вид предизвикателства и нов вид престъпност.

Без аналог в историята на човечеството, киберпрестъпността бързо се оформя като предпочитан метод на престъпния контингент- от дребни нарушители, през организирани престъпни групи, до трансгранична престъпност.

Киберпрестъпността – съвременната реалност

Дигитализацията, интернет свързаността, разнообразието от социални медии и мрежи, скоростта на информационните канали и лесния достъп до тях, предоставят възможност на всеки техен потребител да бъде свидетел, провокатор, а не в редки случаи дори съучастник или директен извършител на различни по вид неправомерни действия.

Самото киберпространство се превърна в благоприятна среда и примамлива възможност както за подготовка, така и за извършване на различни по характер, тежест форма, сложност, престъпления.

В съвременния свят киберпрестъпленията се превърнаха в ежедневна, дори в ежечасна практика. Причините затова са много. Сред тях безспорно се нарежда фактът, че глобалната икономика продължава да се развива устойчиво върху и чрез киберекосистема. Само по себе си това е достатъчно основание както държавни институции, така и частни такива, и всеки един потребител, да бъдат изложени на риск от различни видове атаки и предизвикателства, които стават възможни по най-разнообразни начини и канали. Водещите сред тях са:

- интернет;
- киберпространството;
- разнообразието от онлайн сайтове;
- различни приложения и платформи;
- профили в социалните мрежи;
- фалшивите профили;
- фалшиви примамливи предложения;
- социални медии;
- различна по вид и форма споделена информация- снимка, видео, излъчване на живо;
- разпространение на фалшива и манипулативна информация;
- зловредни софтуери и приложения- съгласно официални проучвания от IBM⁸ и Devry University⁹ по последни данни съществуват повече от един

⁸ <https://www.ibm.com/reports/data-breach> - посетен на 15.11.2024 година

⁹ <https://www.devry.edu/> - посетен на 10.10.2024 година

милиард програми за зловреден софтуер и повече от половин милион (560 000) нови такива се откриват всеки ден. Най-често срещаните сред тях са троянски коне(вид зловреден софтуер, който се маскира като легитимен код или софтуер, които съставляват 58% от целия компютърен зловреден софтуер);

- разнообразни психологични похвати, чрез които се търси директно провокиране и влияние върху психиката на бъдещата жертва, което предлога почти автоматична реакция(пример е социалното инженерство);

- фишинг- вид кибератака, при която се изпращат фалшиви електронни съобщения с цел да се измамят потребителите да предоставят лична информация. Съгласно официалните доклади за Интернет престъпления на Федералното бюро за разследване, фишингът запазва челна позиция сред публично докладваните киберпрестъпления както за 2022, така и за 2023 година. Тези данни се потвърждават от редица други официални източници. Съгласно техните данни, броят на фишинг атаките се е увеличил с 34% през 2021 г. и според APWG 2022 г. е била рекордна година с повече от 4,7 милиона фишинг атаки.

- **DDoS атаки- разпределена атака за отказ от услуга**
- **Бот мрежа – група от злонамерени компютри, които са заразени със зловреден софтуер, който ги контролира отдалечено;**
- **Спам акаунти и други.**

Въпреки, че киберпрестъпленията са безспорен феномен и неизменна част от ежедневната киберреалност, не съществува единно общоприето тълкуване на термина. Почти във всички нормативни актове, стратегически документи и правилници, основно се поставя акцент върху киберсигурността, нейните елементи, системи, както и различните механизми за противодействие на киберпрестъпността в различните ѝ проявления.

Според Cambridge dictionary киберпрестъпността представлява престъпления или незаконна дейност, които се извършват с помощта на интернет.

¹⁰

Merriam-Webster dictionary приема киберпрестъпността като вид престъпната дейност (като измама, кражба или разпространение на детска порнография), която се извършва с помощта на компютър, по-специално за осъществяване на незаконен достъп, предаване или манипулиране на данни.¹¹

¹⁰ <https://dictionary.cambridge.org/dictionary/english/cybercrime> - посетен на 08.09.2024 г

¹¹ <https://www.merriam-webster.com/dictionary/cybercrime> - посетен на 08.09.2024 г

Според Oxford dictionary киберпрестъпността е такъв вид престъпление, което се извършва с помощта на интернет. Като пример са посочени кражба на нечи лични или банкови данни или чрез заразяване на компютъра им с вирус.¹² За сведение, термина киберпрестъпност липсва в Българския тълковен речник¹³, в Закона за киберсигурност.

Съгласно Актуализираната Национална стратегия за киберсигурност „Киберустойчива България 2023“, киберпрестъпността (ЕС) обхваща традиционни престъпления (например измами, фалшифициране и кражба на самоличност), престъпления, свързани със съдържанието (напр. онлайн разпространение на детска порнография или подбуждане към расова омраза), и престъпления, които са възможни само при компютри и информационни системи (например атаки срещу информационни системи, предизвикване на отказ на услуга и зловреден софтуер).¹⁴

В последно време станавме свидетели на все по-честата употреба на термини производни с представка кибер. Например киберсигурност, киберриск, киберзаплаха, киберразузнаване, киберотбрана, киберполиция, кибердипломация, киберинформация, киберпрестъпление, киберпрестъпник и т.н. Първоначално иновативна по характер, тази тенденция плавно се оформя като трайна, с ясна перспектива да продължава. Представката кибер носи със себе си всички специфики и особености на киберпространството. Така всяко производна дума придобива рязко нови параметри, нови цели, нови задачи, ново значение и ново поле на приложение и изисква нов тип управление.

Всичко това промени облика на съвременния престъпник. Киберсредата е неготово е основното или спомагателно местопроизшествие. Киберпрестъпникът има много лица. Той може да бъде:

- хакер – лице, което има специални/специфични компютърни познания, с помощта, на които извършва неоторизиран достъп до данни с подривна цел;
- онлайн хищник- лице, което може да определим като преследвач онлайн. Най-често хищниците умишлено създават множество фалшиви профили и идентичности. Чрез тях предварително проучват жертвите си чрез профилите им в социалните мрежи и демонстрират привидно същите интереси и предпочитания като тях. Той се възползва от други лица (най-често деца) в интернет.
- вълк единак;

12

<https://www.oxfordlearnersdictionaries.com/definition/english/cybercrime?q=cybercrime> - посетен на 08.09.2024 г

¹³<https://rechnik.chitanka.info/w/%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%8A%D0%BF%D0%BD%D0%BE%D1%81%D1%82> - посетен на 10.09.2024 г

¹⁴ Актуализираната Национална стратегия за киберсигурност „Киберустойчива България 2023“,

- непълнолетен, проявяващ агресия и недоволство чрез кибертормоз, киберизнудване и/или чрез острия език на омразата;

- непълнолетен (и несамо) прибегващ към т. нар. секстинг(етимологията на термина идва от думите „секс“ и „текстинг“ (в превод от английски език - писане на съобщения) и означава размяна на съобщения, снимки или клипове със сексуално съдържание между двама партньори)¹⁵. В нередки случай, размяната се извършва между непълнолетни лица и след това споделения материал се използва като основа за изнудване и/или директно разпространение в социалните мрежи, в затворени групи, което води до поредното киберпредизвикателство - увредена онлайн репутация;

- педофил, който търсят своите жертви в социалните мрежи. Чрез използването най-често на фалшив профил или присвоен чужд такъв, едни от тях се опитват да достигнат до снимки и видеоматериали с деца, а други - директно търсят контакт с набелязаната жертва. Статистиката от последните години, показва/разкрива, че именно социалните мрежи и киберсвързаността откриват изцяло нов път и поле на този вид жестоки престъпления. Друга важна последица е снижаване на възрастовата граница и интереса към деца между 3 – 6 годишна възраст.¹⁶

- извършител на сексуални престъпления и онлайн насилие;
- разпространяващ порнографски материали;
- крадец на самоличности;
- кибертерорист;
- лице извършващо радикализация през интернет и социалните мрежи;
- **финансово муле**- най-често лице, което е склонено да участва в прехвърляне на незаконно придобити финансови средства между различни банкови сметки, често в различни държави, като за тази дейност получава комисионна. В нередки случай, финансовите мулета не подозират, че са привлечени в тази схема;

- **лице извършващо романтична измама, с цел финансова облага;**
- **и други.**

Киберпрестъпленията са едно от множеството видове предизвикателства, които дебнат онлайн потребителите днес. Но дори и тази скромна извадка може да послужи като показател как технологичния напредък, интернет свързаността и социалните мрежи, наред с положителните си аспекти, създават разнообразни деструктивни възможности, нови пътища и шансове за високотехнологични престъпления.

¹⁵ <https://www.safenet.bg/sexting/> - посетен на 14.10.2024 година

¹⁶ <https://www.safenet.bg/pedofili/> - посетен на 15.10.2024 година

Заклучение

Задълбоченото изследване на спецификите и предизвикателствата в киберсредата може да разкрие състоянието на националните и международни системи за киберсигурност, нивото на киберкултура на отделния онлайн потребител и неговата киберхигиена. От там, може да се направят изводи и препоръки как да бъдат актуализирани системите за сигурност, как да се неутрализират вече идентифицираните пропуски. Налага се изводът, че обучението е главен инструмент за повишаване на интернет грамотността както за мениджърите на киберспециалистите отговорни за мрежите, така и за целия състав в институциите.

ЛИТЕРАТУРА

- [1] Актуализираната Национална стратегия за киберсигурност „Киберустойчива България 2023“, приета с решение № 301 на Министерския съвет от 02.04.2021 г.
- [2] Методиева Ц., "Заплахи в интернет. Фишинг и финансово муле.", Международна научна конференция „Киберсигурността в информационното общество“, НВУ „Васил Левски“, Факултет „Артилерия, ПВО и КИС“ - гр. Шумен, 20-21 Април 2017 г., ISBN 978-954-9681-82-6, с. 157- 160.
- [3] Закона за киберсигурност, Обн. ДВ. бр. 94 от 13 Ноември 2018г., изм. и доп. ДВ. бр. 85 от 2 Октомври 2020 г.
- [4] Иванов. Вл. Българите, Том 2, издателство Хистореон, 2022, година, ISBN 9786199113561,
- [5] Официален доклад за Интернет престъпления на Федералното бюро за разследване за 2022 г.
- [6] Официален доклад за Интернет престъпления на Федералното бюро за разследване за 2023 г.
- [7] Allied Joint Doctrine for Land Operations (AJP-3.2 Edition A). NSO, 2016.
- [8] Dimanova, D., Kuzmanov, Z., Risk management in information security, Conference proceedings MATTEX 2018. Information, Technical and Economical Problems of Security Systems, October 2018, Shumen, ISSN: 1314-3921, vol. 2, part. 1, pp. 139-145.
- [9] <https://avada.io/blog/social-networking-vs-social-media/>
- [10] 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.
- [11] <https://dictionary.cambridge.org/dictionary/english/cybercrime> - посетен на 08.02.2024 г.
- [12] <https://nordvpn.com/cybersecurity/glossary/cybersecurity-ecosystem/>

- [13] <https://rechnik.chitanka.info/w/%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%8A%D0%BF%D0%BD%D0%BE%D1%81%D1%82>
- [14] <https://rechnik.chitanka.info/w/%D0%BF%D1%80%D0%B5%D0%B4%D0%B8%D0%B7%D0%B2%D0%B8%D0%BA%D0%B0%D1%82%D0%B5%D0%BB%D1%81%D1%82%D0%B2%D0%BE>
- [15] <https://strategyofsecurity.com/cybersecurity-ecosystem/>
- [16] <https://www.devry.edu/>
- [17] https://www.gwi.com/bookdemo?utm_source=kepios&utm_medium=referral&utm_campaign=2023+Kepios+Global+Audiences
- [18] <https://www.ibm.com/reports/data-breach>
- [19] <https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx>
- [20] <https://www.merriam-webster.com/dictionary/cybercrime>
- [21] <https://www.oxfordlearnersdictionaries.com/definition/english/cybercrime?q=cybercrime>
- [22] <https://www.safenet.bg/pedofili/>
- [23] <https://www.safenet.bg/sexting/>

ПАРАЗИТНИ ЕЛЕКТРОМАГНИТНИ ИЗЛЪЧВАНИЯ И ПРОБЛЕМЪТ ЗАЩИТА НА ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ

Атанас И. Начев, Иванка Г. Павлова

PARASITIC ELECTROMAGNETIC EMISSIONS AND THE PROBLEM OF INFORMATION PROTECTION IN COMPUTER SYSTEMS

Atanas I. Nachev, Ivanka G. Pavlova

ABSTRACT: *The article examines a specific problem – the possibility of hidden unauthorized access to information in computer systems, networks, etc. by intercepting and analyzing emerging parasitic electromagnetic radiation and parasitic electromotive voltages. The reasons for the appearance of these phenomena and the possibilities for extracting information from them are examined.*

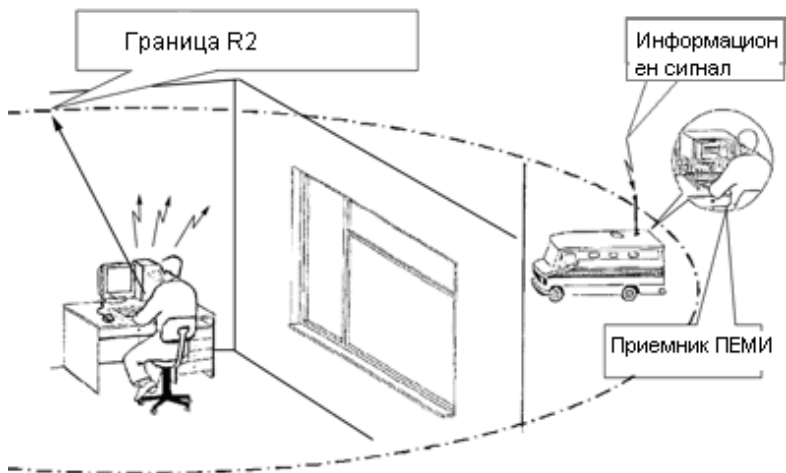
KEYWORDS: *information protection, parasitic electromagnetic radiation, parasitic electromotive force, unauthorized information access*

DOI: <https://doi.org/10.46687/YT24NIP>

При работа на електронните средства в тях протичат променливи електрически токове, което е съпроводено с излъчване в околното пространство на електромагнитна енергия, която се разпространява под формата на електромагнитни вълни. Тези вълни са известни [1, 2, 3, 4, 5] като паразитни електромагнитни вълни (ПЕМВ). Голяма част от протичащите токовете във веригите на електронните устройства, като персонални микрокомпютри, комуникационно оборудване и пр., и по съответните проводници и кабели на телекомуникационните и компютърни мрежи, носят информация. Поради това и електромагнитните вълни, които те възбуждат също са информационно носещи. С прехващането на тези излъчвания и в резултат на техния анализ може да се получи информация както за обработваните, така и за предаваните данни (фиг. 1).

Паразитни електромагнитни излъчвания при работа на компютърните системи възникват при:

- запис и четене на информацията в/от оперативната памет;
- извеждане на информацията на екран;
- въвеждане на данни посредством клавиатура;
- запис на информация на магнитни носители;
- четене на информация от магнитни носители,
- предаване на информация в обхвата на локална мрежа и по комуникационните системи;
- извеждане на информацията на печат.



Фиг. 1.

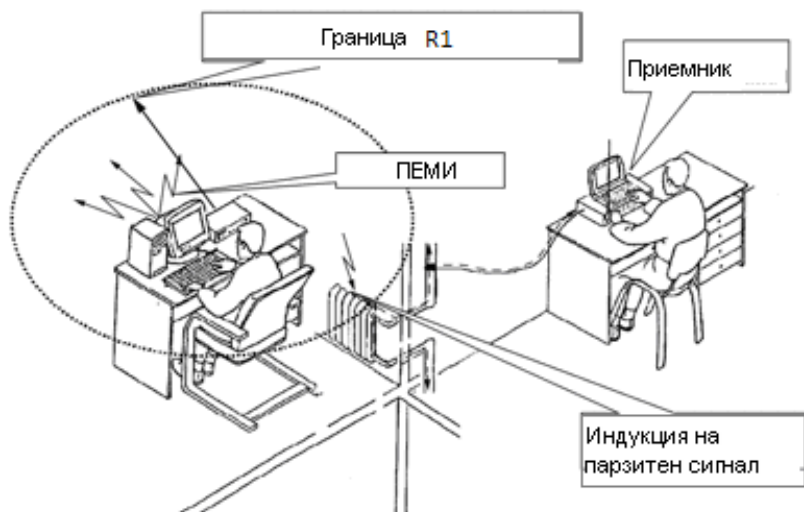
Паразитните електромагнитни излъчвания, които се създават от персоналните компютри и сървъри се характеризират с широк честотен спектър, заемащ полосата от десетки килохерци до един и повече гигахерци. Основната част от информационната им съставляваща се намира в честотната лента 300 – 600 MHz, но в редица случаи се разпростира до 1 GHz, понякога и повече. Честотната лента 300 –600 MHz е в диапазона на телевизионния обхват. Поради това често информацията от ПЕМИ от монитора на персонален компютър може да се възпроизведе и с аналогов телевизор, понякога дори и без доработки в него. При изменение на схемата на телевизора, като се доработи така, че да може да се регулира системата му за вертикална и хоризонтална синхронизация приемането на информацията от монитора на компютъра става още по-лесно.

Процесите на формиране на паразитни електромагнитни излъчвания могат да се усилят с използване на високочестотно активиране, осъществявано чрез облъчване на съответните електронни средства или на помещенията в които са разположени с мощни синусоидални радиосигнали. За целта се използват високочестотни генератори с остронасочени антени. В резултат на това в нелинейните елементи на електронните средства възникват модулирани високочестотни сигнали, които се излъчват в околното пространство и се разпространяват в него във вид на паразитни амплитудно модулирани радиовълни. Те могат да се използват за неоторизиран информационен достъп.

Прихващането на информацията въз основа на възникващите в процеса на работа на компютърните системи паразитни електромагнитни излъчвания може да се осъществи с използване на специални за целта радиоприемни устройства, разположени като правило извън контролираната зона на обекта. Качеството на

откриване на сигнала се определя чрез параметрите вероятност P_0 за правилно откриване на сигнала и вероятност $P_{лт}$ за лъжлива тревога. За надеждно приемане на информацията е необходимо $P_0 = 0,7 - 0,9$, и $P_{лт} \leq 10^{-3}$. Пространството в което е възможно да се прихванат паразитните електромагнитни излъчвания и на тяхна основа да се осъществи неоторизиран информационен достъп се нарича зона 2 (R_2) – фиг. 1. Нейните пространствени размери се определят при изследване на създаваните от съответните технически средства паразитни електромагнитни излъчвания, в това число и в различни условия на тяхното използване.

Електромагнитните излъчвания, които възникват при работа на компютърните системи и други електронни средства индуцират в захранващата мрежа, в телефонните линии, в тръбите на водопроводните и отоплителни инсталации, в заземителните уредби и пр. електродвижещи напрежения, които когато са възбудени от информационно носещи токове са също информационно носещи. Индуцираните електродвижещи напрежения са известни като паразитни електродвижещи напрежения (ПЕДН). Това позволява чрез прехващане и анализ на тези ПЕДН също да се осъществи неоторизиран информационен достъп (фиг. 2). По този начин се образуват електрически канали за изтичане на информация.



Фиг. 2.

Конкретните причини за възникване на електрически канал за неоторизиран информационен достъп могат да бъдат:

— Наличие на галванична връзка между веригите на електронните средства и странични проводници и токопроводящи среди.

— Индуциране от ПЕМИ на електродвижещи напрежения в електрическата силова инсталация.

— Индуциране от ПЕМИ на електродвижещи напрежения в заземяващите вериги.

— Индуциране от ПЕМИ на електродвижещи напрежения в телефонните линии.

Индуциране на от ПЕМИ на електродвижещи напрежения в тръбите на ВиК и отоплителните инсталации и в други токопроводящи среди.

Индуцирането на токове и напрежения в токопроводящите елементи на ВиК, отоплителните и пр. инсталации (фиг. 2) се обуславя от паразитните електромагнитни излъчвания, които възникват при работата на компютърните системи и другите електронни средства и от капацитетните и индуктивни връзки между тези елементи. Паразитен антенен ефект може да се появи от съсредоточени и разпределени „случайни антени“.

Съсредоточените „случайни антени“ представляват конкретни технически средства, например системен блок на персонален компютър, монитор, свързани към токопроводяща линия, излизаща извън предела на охраняемата зона.

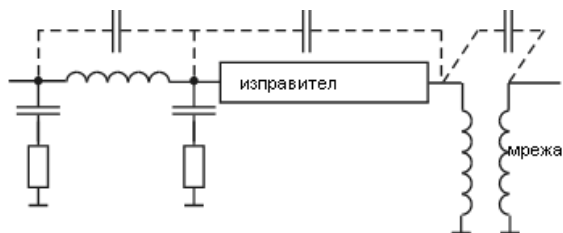
Към разпределените случайни антени се отнасят елементи с разпределени параметри, като кабели, проводници метални тръби и др. Големината на индуцираните в тях електродвижещи напрежения зависи не само от мощността на сигнала, но и от разстоянието до излъчвателя на паразитни електромагнитни излъчвания и тази част от дължината им, която е подложена на електромагнитно въздействие. При разпространяване на сигналите в случайните антени те постепенно затихват. Степента на затихване може да се определи като се имат предвид електрическите характеристики на съответната електро проводяща среда.

Пространството около техническите средства, които излъчват паразитни електромагнитни излъчвания, в пределите на което информационният сигнал в съсредоточените и разпределени случайни антени превишава допустимите нива се нарича зона едно (зона r_1). За всяка електронна апаратура тази зона се определя експериментално.

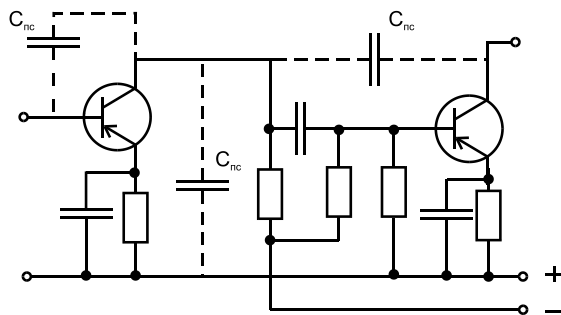
Индуцирането на информационни сигнали в електрозахранващите вериги е възможно при наличие на вътрешни паразитни капацитетни и/или индуктивни връзки в захранващия блок на компютърните системи и на другите електронни средства (фиг. 3)

Паразитни връзки са налични не единствено в захранващите блокове, но и в схемите на другите елементи на електронните средства (фиг. 4). Тези паразитни връзки също са източник на информационно носещи електродвижещи напрежения и токове в захранващата мрежа.

Паразитни електродвижещи напрежения в проводниците на мрежата възникват под въздействие на разпространяващите се в околната среда паразитни електромагнитни излъчвания.



Фиг. 3.



Фиг. 4.

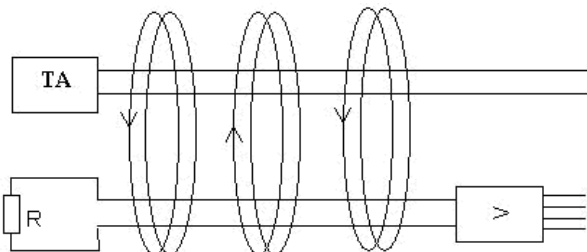
При въздействието на паразитните електромагнитни излъчвания върху проводниците на електрозахранващата мрежа, в телефонните линии, в кабелите на локалните компютърни мрежи и на други слаботокови инсталации в тях се индуцират паразитни електродвижещи напрежения, които носят информацията, съдържаща се в ПЕМИ.

Паразитни информационни напрежения и токове се индуцират и в проводниците от заземителната инсталация. Заземяването представлява устройство, което се състои от заземителни проводници, които свързват заземителя с електронни и електрически устройства и прибори. Заземителят представлява заземен проводник, група проводници или заземено проводящо тяло или група тела, намиращи се в непосредствен контакт с почвата.

Освен заземителните проводници, които служат за непосредствено свързване на съответните електронни средства с веригата за заземяване галваническа връзка с земята могат да имат и различни проводници, които са извън контролираната зона. Такива могат да са нулевите проводници на електрозахранващата мрежа, екраните на различните кабели, металните тръби от ВиК и отоплителните инсталации, металната арматура на железобетонните конструкции и др. Всички те образуват разпределена мрежа за заземяване, в която могат да се индуцират информационни сигнали. Освен това в почвата около заземените устройства възниква електромагнитно поле, което също е източник на информация.

Прехващането на информацията в токозахранващата инсталация, в проводниците на телефонните линии, в електрозаземителните проводници, в тръбите на ВиК и отоплителните тръби и пр. се извършва чрез непосредствено, галванично подключение на съответна електронна апаратура (фиг. 2).

При протичане на информационно носещи променливи токове през телефонните се генерират информационно носещи електромагнитни полета. Тези електромагнитни полета се разпространяват в околното пространство във вид на електромагнитни вълни и могат да бъдат прехванати и анализирани с помощта на съответна радиоелектронна апаратура–фиг. 5.



Фиг. 5.

От изложеното следва, че работата на компютърните системи, мрежи и други електронни устройства се съпровожда с възникване на паразитни електромагнитни излъчвания и паразитни електродвижещи напрежения. Съществена част от тях носят в себе си информация за обработваните и обменяни данни. Това налага предприемане на съответни технически и организационни мерки за ограничаване възможностите за осъществяване на скрит, неотризиран достъп с използване на тези канали.

ЛИТЕРАТУРА

- [1] Information: A Very Short Introduction. Luciano Floridi. //Oxford University Press, 2010.
- [2] Беджев Б. Технически средства в системата на националната сигурност. Университетско издателство „Епископ Константин Преславски“, Шумен, 2006.
- [3] Белов Л.А., Богачев В.М., Благовещенский М.В. и др. Устройства генерирания и формирания радиосигналов. Радио и связь, Москва, 1994.
- [4] Домарев В.В. Безопасности информационных технологий. DiaSoft, Москва, Санкт Петербург, Киев, 2002.
- [5] Начев А. Технически средства и системи за защита на информацията. София, „За буквите. О‘писменех“, 2014.

ОЦЕНКА НА ЕФЕКТИВНОСТТА НА КОМУНИКАЦИОНЕН КАНАЛ С ОТЧИТАНЕ НА НАДЕЖДНОСТТА НА РЕАЛИЗИРАЩИТЕ ГО СРЕДСТВА

Атанас И. Начев

ASSESSMENT OF THE EFFICIENCY OF A COMMUNICATION CHANNEL TAKING INTO ACCOUNT THE RELIABILITY OF ITS IMPLEMENTING MEANS

Atanas I. Nachev

ABSTRACT: *The article proposes a method for determining and assessing the effectiveness of the functioning of a communication channel, considering the reliability characteristics of its implementing means.*

KEYWORDS: *information channel, reliability, functional reliability, message*

DOI: <https://doi.org/10.46687/YT24AIN>

Един от основните проблеми при проектирането и експлоатацията на комуникационните системи е свързан с определяне на тяхната ефективност. Общеизвестен факт е [1, 2, 3, 4], че ефективността в случая е пряко свързана с функционалната надеждност на средствата за осъществяване на информационен обмен. Подход за определяне на тази функционална надеждност се предлага в настоящото изложение при следните условия:

Нека по комуникационен канал се осъществява предаване на m различни по характер (тип) съобщения. Общото количество съобщения, предавани за времето $T_{цф}$ на функциониране (цикъл на функциониране) е равно на n .

Количеството съобщения от i -ти тип, $i = \overline{1, m}$, които подлежат за предаване за времето $T_{цф}$ представляват случайна величина с поасонов закон на разпределение с интензивност λ_i , $i = \overline{1, m}$. Времето τ_i за предаване на i -то, $i = \overline{1, m}$, съобщение е случайна величина с експоненциален закон на разпределение с интензивност μ_i : $\lambda_i : \mu_i = \frac{1}{\mu_i}$.

По време на предаване на съобщенията каналът е подложено на въздействие на кратковременни прекъсвания (сбоеве), количеството на които за времето $T_{цф}$ е случайна величина с поасонов закон на разпределение с параметър

λ_c . Продължителността на сбоеките τ_c е случайна величина с експоненциален закон на разпределение с параметър μ_c , т. е. $\tau_c = 1/\mu_c$.

В указаните условия е необходимо да се определи средната продължителност на предаване на съобщенията с отчитане на дефинираните смущаващи въздействия, при условие, че времената за предаване на отделните съобщения без възникване на сбоеките са съизмерими.

При така дефинираната постановка количеството n_i съобщения от i – ти тип, $i = \overline{1, m}$, които се предават за времето $T_{\text{цф}}$ е

$$n_i = \lambda_i T_{\text{цф}} \quad (1)$$

Средната продължителност $\bar{t}$ на изпълнение на една заявка ще е:

$$\bar{t} = \frac{n_1 \tau_1 + n_2 \tau_2 + n_3 \tau_3 + \dots + n_m \tau_m}{n} = \frac{1}{n} \sum_{i=1}^m n_i \tau_i. \quad (2)$$

Тъй като $p_i = \frac{n_i}{n}$ е вероятността за постъпване за предаване на i – ти тип съобщение, $i = \overline{1, m}$, то (2) може да запишем като:

$$\bar{t} = \sum_{i=1}^m p_i \tau_i = \sum_{i=1}^m \frac{p_i}{\mu_i} \quad (3)$$

Съгласно условието $p_i = 1 - e^{-\lambda_i T_{\text{цф}}}$ и тогава

$$\bar{t} = \sum_{i=1}^m \frac{[1 - \exp(-\lambda_i T_{\text{цф}})]}{\mu_i}$$

В такъв случай средното време T_3 за цикъла на функциониране $T_{\text{цф}}$ за което информационният канал е ангажиран с предаване постъпили съобщения ще се определи като:

$$T_3 = n \bar{t} = n \sum_{i=1}^m \frac{[1 - \exp(-\lambda_i T_{\text{цф}})]}{\mu_i}. \quad (4)$$

Ще обозначим чрез $\Lambda = \sum_{i=1}^m \lambda_i$ интензивността на постъпване на съобщенията за предаване по канала. Но е вярно и съотношението $\Lambda = \frac{n}{T_{\text{цф}}}$.
Тогава:

$$n = \Lambda T_{\text{цф}}.$$

В такъв случай (4) ще запишем като:

$$T_3 = \Lambda T_{\text{цф}} \sum_{i=1}^m \frac{[1 - \exp(-\lambda_i T_{\text{цф}})]}{\mu_i}. \quad (5)$$

За времето предаване на едно съобщение каналът е подложено на въздействието на кратковременни прекъсвания. В резултат на това средното време за предаване ще се увеличи. Ще обозначим това време с $\bar{t}$.

$$\bar{t} = \bar{t} + \theta. \quad (6)$$

За времето $\bar{t}$ ще възникнат η кратковременни прекъсвания:

$$\eta = \lambda_c \bar{t}. \quad (7)$$

При всяко прекъсване на процеса на предаване на съобщението се извършва повторното му предаване след самовъзстановяване на канала. Това се извършва за времето $\tau_c = 1/\mu_c$. В резултат времето $\bar{t}$ ще се увеличи със случайната величина θ :

$$\theta = \eta \left(\bar{t} + \tau_c \right) = \eta \left(\bar{t} + \frac{1}{\mu_c} \right). \quad (8)$$

Предвид на (7) изразът (8) ще получи вида:

$$\theta = \lambda_c \bar{t} \left(\bar{t} + \frac{1}{\mu_c} \right). \quad (9)$$

Тогава

$$\bar{t} = \bar{t} + \lambda_c \bar{t} \left(\bar{t} + \frac{1}{\mu_c} \right). \quad (10)$$

Ще разгледаме случай, когато след самотстраняването на възникналото кратковременно прекъсване процесът на предаване на съобщението процес продължава не отначало, а от момента на прекъсването му. Тогава в условията на разглеждания случай средното време за предаване на съобщението ще съдържа времето $\bar{t}$, плюс $\eta = \lambda_c \bar{t}$ и

продължителност $\tau_c = 1/\mu_c$ на кратковременното прекъсване, т.е.:

$$\bar{t} = \bar{t} + \lambda_c \bar{t} \tau_c = \bar{t} + \lambda_c \frac{\bar{t}}{\mu_c}$$

След съответно преобразование ще имаме:

$$\bar{t} = \bar{t} \left(1 + \frac{\lambda_c}{\mu_c} \right). \quad (11)$$

В табл.1 са представени значенията на $\bar{t}$ и относителното увеличаване на времето за изпълнение на информационния процес $\Delta \bar{t}$ при различни значения на продължителността $\tau_c = 1/\mu_c$ на кратковременните прекъсвания.

$$\bar{t} = 60 S; \lambda_c 0,01 \text{ 1/S}$$

Таблица 1

τ_c [S]	$\bar{t}$ [S]	$\Delta \bar{t}$ %
1	60,6	1
5	63,0	5
10	66,0	10
15	69,0	15
20	72,0	20

С оглед на практическата реализация на разгледаната дисциплина на предаване на съобщения същите се разделя на участъци. В края на изпълнението на всеки един от тези участъци се извършва проверка на правилността на предаването му. При наличие на несъответствие поради възникнали кратковременни прекъсвания съответния участък се предава отново. Доказано е [2], че оптимално решение от гледна точка на времето на предаване на съобщенията се получава при разделянето им на R равни участъка. В този случай средното време $\bar{T}$ на предаване ще се определи като:

$$\bar{T} = \frac{R}{\lambda_c} \left\{ \left[\exp \left(\lambda_c \frac{\bar{t}}{R} + \tau_p \right) - 1 \right] \right\}, \quad (12)$$

където τ_p е времето за проверка на правилността на предаване на един участък от съобщението.

В табл. 2 са приведени стойностите на $\bar{T}$ при $\bar{t} = 60 S$; $\lambda_c = 0,01$ $1/S$; $\tau_p = 1 S$ и различни значения на времето за проверка τ_p .

$$\bar{t} = 60 S; \lambda_c 0,01 \text{ } 1/S$$

Таблица 2

R	$\bar{T}$ [S]	$\Delta \bar{t} \%$
2	72,60	21
3	70,01	16,83
4	69,40	15,66
5	69,41	15,68
6	69,70	16,17
10	72,50	20,80

Оптималната стойност R_{opt} на броя на участъците се определи по формулата [2]:

$$R_{opt} = \bar{t} \sqrt{\frac{\lambda_c}{2\tau_p}} \quad (13)$$

За условията на разглеждания и представен в табл. 2 пример оптималната стойност на количеството участъци е $R_{opt} = 4$. Както се вижда от представените резултати при стойности на $R \neq 4$ времето $\bar{T}$ расте спрямо това за при $R = 4$, което има минималната стойност 69,40 S , която е с 15,66 % по голяма от $\bar{t} = 60 S$.

Изразът (13) се основава на минимизиране на допълнителното време, необходимо за определяне на грешки при предаване на съответните участъци на съобщението, като не се отчита самата продължителност на това време. А то може да окаже съществено влияние на стойността на R_{opt} , особено когато t_c има стойности, съизмерими или по-големи от τ_p , което е и най-често срещания се случай в практиката. Това налага търсене и на друго решение.

Времето за предаване на съобщение ще се определи от времето $\bar{t}$ и от допълнителното време θ , добавяно поради необходимост от изпълнение на алгоритми за детайлен анализ на открити грешки по отношение на съответните участъци. В случая въз основа на (11) ще имаме:

$$t^* = \bar{t} \left(1 + \frac{\lambda_c}{\mu_c} \right) \quad (14)$$

Като се вземе предвид времето τ_p за анализ всеки един участък на съобщението за правилност на предаването му, изразът (14) ще добие вида:

$$t^* = \left(\bar{t} + R \tau_p \right) \left(1 + \frac{\lambda_c}{\mu_c} \right) \quad (15)$$

Интензивността на изпълнение на анализа наличието на грешки τ_c се определя от продължителността на изпълнение на този алгоритъм и от времето θ , необходимо за анализ съответния участък, в който е открита грешка. Тогава (15) ще запишем като:

$$t^* = \left(\bar{t} + R \tau_p \right) \left[1 + \lambda_c \left(\frac{1}{\mu_c} + \frac{\bar{t}}{R} \right) \right] \quad (16)$$

Ще определим чрез $\frac{dt^*}{dR} = 0$ броя на участъците R_{opt} , при който времето t^* на предаване на съобщението с отчитане на влиянието на времето за анализ на открити грешки е минимално.

$$\frac{dt^*}{dR} = R^2 \left(\tau_p + \frac{\lambda_c \tau_p}{\mu_c} \right) - \lambda_c \tau_p \quad (17)$$

След като приравним (17) на нула

$$R^2 \left(\tau_p + \frac{\lambda_c \tau_p}{\mu_c} \right) - \lambda_c \tau_p = 0 \quad (18)$$

и решим уравнение (18) спрямо R ще получим следния израз, даващ значението на R_{opt} :

$$R_{opt} = \bar{t} \sqrt{\frac{\lambda_c \mu_c}{\tau_p (\lambda_c + \mu_c)}} \quad (19)$$

Изразът (19) позволява при определяне на R_{opt} да се отчетат всички времеви параметри, които имат отношение към процеса на предаване на съобщението.

ЛИТЕРАТУРА

- [1] Начев А. И. Надеждност на програмното осигуряване. Шумен, Университетско издателство „Епископ Константин Преславски“, 2017.
- [2] Начев А. И. Информационни процеси в компютърните мрежи в условия на реална надеждност. София, Военно издателство, 2001.
- [3] Начев А. И. Общосистемно проектиране на автоматизирани системи за управление. София, За буквите, О‘писменех, 2014.
- [4] Репкин В. Ф., Лернер В. Ю., Шубс М. Н., Персиков А. С., Сидоров Л. А. Основы надежности и эксплуатации радиолокационного вооружения. КВИРТУ, Киев, 1963.

МОДЕЛ НА ЕФЕКТИВНОСТТА НА СИСТЕМА ЗА ИНФОРМАЦИОННО ОСИГУРЯВАНЕ НА ЗАЩИТАТА НА ОБЕКТИ ОТ КРИТИЧНАТА ИНФРАСТРУКТУРА

Атанас И. Начев

MODEL OF THE EFFICIENCY OF A SYSTEM FOR INFORMATION ASSURANCE OF THE PROTECTION OF CRITICAL INFRASTRUCTURE OBJECTS

Atanas I. Nachev

ABSTRACT: *The article proposes a method based on a mathematical model developed for the purpose for determining and assessing the effectiveness of information assurance of critical infrastructure objects. A characteristic feature of the method is its invariance.*

KEYWORDS: *critical infrastructure, information assurance, management, protection of critical infrastructure*

DOI: <https://doi.org/10.46687/YT24ANA>

Характерна особеност на системите за информационно осигуряване на обектите от критичната инфраструктура е, че те могат да се намират в няколко работни състояния, което е свързано с това, че при отказ на отделни техни елементи в преобладаващите случаи не се предизвиква отказ на системата като цяло, а само нарушаване в една или друга степен на качеството им на функциониране. Тази особеност, характерна за почти всички информационни системи, в това число и за системите, които са обект на настоящото разглеждане е наложило въвеждането [1, 2, 3] на критерий като функционална надеждност и ефективност с отчитане на посочената специфика. Ще разгледаме това при следната теоретична постановка:

Нека система за информационно осигуряване на обект от критичната инфраструктура (по-нататък просто системи за информационно осигуряване) реализира n информационни (управленски) задачи. Ще дефинираме следното определение:

Определение: Под функционална надеждност по отношение изпълнението на i -та, $i = \overline{1, n}$, задача се разбира вероятността $P_{\phi i}$, че системата която я реализира е в състояние да я изпълни в даден момент t .

Функционалната надеждност на системите за информационно осигуряване по отношение на решаването на всички n информационни задачи се задава чрез матрицата

$$P_{\phi} = \{P_{\phi i}\}, i = \overline{1, n}, \quad (1)$$

която може да се представи в следния табличен вид (табл. 1):

Таблица 1

Индекс (номер) i на реализираната задача	1	2	3	...	n
Вероятност $P_{\phi i}$ за решаването на съответната задача	$P_{\phi 1}$	$P_{\phi 2}$	$P_{\phi 3}$	...	$P_{\phi n}$

Нека i – та, $i = \overline{1, n}$, задача се изпълнява от M_i технически средства на системата, като за зададен цикъл на функциониране $T_{\text{цф}}$ тя се реализира N_i пъти. При всяко изпълнение на i – та задача, j – то устройство реализира своите функции за време $t_{i,j}$. Сумарната продължителност $T_{i,j}$ на работа на това устройство за времето $T_{\text{цф}}$ с решаване на i – та задача ще бъде:

$$T_{i,j} = N_i t_{i,j}. \quad (2)$$

Вероятността $p_j(T_{i,j})$ за безотказна работа на j – то устройство при изпълнение на i – та задача за времето на функциониране $T_{\text{цф}}$ на от системата за информационно осигуряване е:

$$p_j(T_{i,j}) = p_{a,j}(T_{i,j}) p_{p,j}(T_{i,j}), \quad (3)$$

където $p_{a,j}(T_{i,j})$ е вероятността за безотказна работа на апаратната част на j – то устройство, а $p_{p,j}(T_{i,j})$ на софтуера му, изпълняван за решаване на i – та задача в продължение на сумарното време $T_{i,j}$.

Нека $K_{\Gamma j}$ е коефициентът на готовност на j – то устройство на системата за информационно осигуряване. Тогава за цикъла $T_{\text{цф}}$ на функциониране на тази система вероятността $P_{\phi i}$ за решаване на i – та задача ще се определи, като

$$P_{\phi i} = \prod_{j=1}^{M_i} K_{\Gamma j} p_j(T_{i,j}). \quad (4)$$

Ще обозначим чрез λ_j интензивността на възникване на откази на j – то устройство. Ако $\lambda_{a,j}$ е интензивността на откази на апаратната му част, а $\lambda_{p,j}$

интензивността на откази на реализираните от него програми и при условие, че $\lambda_{aj} = const$ и $\lambda_{pj} = const$, то

$$p_{aj} = \exp(-\lambda_{aj} T_{ij}), \quad (5)$$

$$p_{pj} = \exp(-\lambda_{pj} T_{ij}). \quad (6)$$

Тогава (4) ще приеме вида:

$$P_{\phi i} = \prod_{j=1}^{M_i} K_{Tj} \exp(-\lambda_{aj} T_{ij}) \exp(\lambda_{pj} T_{ij}) \quad (7)$$

Ако обработката на информацията се извършва от един централен възел, който за сумарното времето T_i от цикъла $T_{\phi i}$ на функциониране е ангажиран с решаването на i – та задача, изразът (7) ще добие вида:

$$P_{\phi i} = K_{\Gamma 0} P_0(T_i) \prod_{j=1}^{M_i} K_{Tj} \exp(-\lambda_{aj} T_{ij}) \exp(\lambda_{pj} T_{ij}), \quad (8)$$

където $K_{\Gamma 0}$ е коефициент на готовност, а $P_0(T_i)$ -вероятност за безотказна работа на централния възел за времето T_i , K_{Tj} -на готовност на j – то устройство, T_{ij} – сумарна продължителност на работа на j – то устройство от състава на системата за информационно осигуряване за решаване на i – та задача за времето $T_{\phi i}$ на функциониране.

Ще обозначим чрез E_{0i} ефективността от работата на системата за информационно осигуряване с решаването на i – та задача за времето $T_{\phi i}$. Тогава реалната ефективност E_i от решаването на тази задача, с отчитане на надеждността на системата ще се определи, като:

$$E_i = P_{\phi i} E_{0i}. \quad (9)$$

Ако всички задачи, решавани от системата за информационно осигуряване са с еднаква тежест (важност за управлявания обект) общата ефективност от работата ѝ ще е:

$$E = \sum_{i=1}^n E_i. \quad (10)$$

Ще въведем термина коефициент K_e на ефективно използване на системата за информационно осигуряване на обект от критичната инфраструктура, под който ще разбираме:

$$K_e = \frac{E}{\sum_{i=1}^n E_{0i}} \cdot 100\% \quad (11)$$

За случай на безотказна работа на средствата на системата $K_e = 100\%$.

Като правило различните задачи, решавани от системата за информационно осигуряване в процеса на управление на съответния обект са с различна важност. Това може да оценим чрез коефициента α_i , $i = \overline{1, n}$ на значимост на i -та задача, $\sum_{i=1}^n \alpha_i = 1$. Тогава (10) ще има вида:

$$E = \sum_{i=1}^n \alpha_i E_i \quad (12)$$

Коефициентът на ефективност в такъв случай ще се определи, като:

$$K_e = \frac{\sum_{i=1}^n \alpha_i E_i}{\sum_{i=1}^n \alpha_i E_{0i}} \cdot 100\% \quad (13)$$

Разгледаният подход за определяне на ефективността на системите за информационно осигуряване на защитата на обектите от критичната инфраструктура, както се вижда от изложеното, се характеризира с висока степен на инвариантност. Това позволява използването му и по отношение на други системи за обработка на информация.

ЛИТЕРАТУРА

- [1] Начев А. И. Информационни процеси в компютърните мрежи в условия на реална надеждност. София, Военно издателство, 2001.
- [2] Начев А. И. Надеждност на въоръжението. Методи за определяне на надеждността на примера на електронните средства и системи въоръжение, София, Българска академия на науките, Институт по металознание, съоръжения и технологии „Академик Ангел Балевски“ с център по хидро- и аеродинамика, 2014.
- [3] Ушаков И. Жива ли още теория надежности. e-journal “Reliability: Theory&Applications”, No 1, Vol. 2, March 2007.

ВЛИЯНИЕ НА ТЕЖКОТОВАРНИЯ ТРАФИК ВЪРХУ ПЪТНАТА ИНФРАСТРУКТУРА И ЕКОЛОГИЧНА УСТОЙЧИВОСТ

Даниел Р. Денев, Александра П. Дочева

IMPACT OF HEAVY FREIGHT TRAFFIC ON ROAD INFRASTRUCTURE AND ENVIRONMENTAL SUSTAINABILITY

Daniel R. Denev, Aleksandra P. Docheva

ABSTRACT: Heavy freight traffic significantly affects road infrastructure and environmental sustainability, especially in transit-intensive regions like Bulgaria. Frequent road maintenance, safety risks, and increased emissions highlight the challenges associated with heavy vehicles. This paper explores sustainable solutions, such as implementing Ro-La transport, modernizing railway infrastructure, and adopting eco-friendly technologies. The integration of these approaches aims to reduce road wear, enhance safety, and minimize environmental impact. Lessons from countries like Switzerland demonstrate the effectiveness of innovative transportation strategies. This study emphasizes the need for strategic investments and collaboration to achieve a resilient and sustainable transport system in Bulgaria.

KEYWORDS: environmental sustainability, heavy freight traffic, road infrastructure, Ro-La transport, transportation optimization

DOI: <https://doi.org/10.46687/YT24ALX>

Введение

Тежкотоварният трафик е основен компонент на транспортната система, но същевременно представлява сериозно предизвикателство за пътната инфраструктура и околната среда. В България, интензивният транзитен трафик натоварва пътищата и води до значителни разходи за поддръжка, както и до повишен риск от пътнотранспортни произшествия. Ограничената транспортна инфраструктура и екологичните предизвикателства изискват иновативни подходи за оптимизация. Изследването на алтернативни решения, като комбинирания транспорт и въвеждането на екологични технологии, предоставя възможности за намаляване на негативното въздействие и повишаване на ефективността на транспортния сектор.

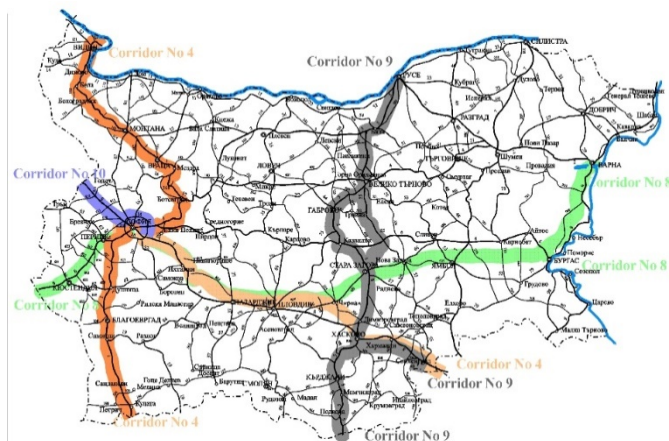
Влияние на тежкотоварния трафик върху пътната инфраструктура и възможности за оптимизация

Тежкотоварните автомобили, преминаващи през българските пътища, причиняват сериозно износване и повреди на пътната настилка. Това явление е

особено изразено по пътищата от републиканската пътна мрежа, които често не са проектирани за интензивния трафик и тежките товари. Резултатът е необходимостта от чести ремонти, което увеличава разходите за поддръжка на пътната инфраструктура и поставя финансово бреме върху държавния и местния бюджет.

Ограничаването на видимостта и безопасността за останалите участници в движението е друг значим проблем, причинен от големите размери на товарните автомобили. Леките автомобили често са принудени да се движат зад тежкотоварни превозни средства поради невъзможността за изпреварване, особено по тесни пътища и планински участъци. Това води до образуването на дълги колони, увеличава времето за пътуване и повишава стреса на водачите.

Рискът от тежки катастрофи също е значителен, особено в участъци с остри завои, стръмни наклони и неблагоприятни метеорологични условия. При инциденти с тежкотоварни автомобили последствията често са фатални за другите участници в движението, а материалните щети могат да бъдат значителни. Тези фактори поставят въпроса за безопасността на движението като приоритет.



Фиг. 1. Терминали за комбиниран транспорт и свързването на различни транспортни мрежи в България

За да се намали натоварването върху инфраструктурата, е необходимо да се развият алтернативи като комбинирания транспорт Ro-La. Този подход включва използването на железопътни платформи за превоз на товарни автомобили, което би намалило както пътния трафик, така и износването на пътищата. Железопътният транспорт е по-устойчив от екологична и икономическа гледна точка, тъй като позволява транспортиране на големи обеми товари с минимално въздействие върху пътната мрежа. Освен това, използването

на Ro-La платформите може да облекчи трафика по ключови коридори и да намали времето за пътуване чрез избягване на задръстванията.

Развитието на Ro-La превозите изисква инвестиции в модернизацията на железопътната инфраструктура, включително изграждане на терминали за качване и сваляне на товарните автомобили. Тези терминали трябва да бъдат стратегически разположени в близост до основните транспортни коридори, за да осигурят безпроблемен преход между автомобилния и железопътния транспорт. Освен това, е необходимо да се стандартизират платформите и вагоните, така че да отговарят на нуждите на съвременните товарни автомобили.

Пример за успешното прилагане на този подход е Швейцария, където Ro-La транспортът е интегриран като част от националната транспортна стратегия. В България подобна инициатива може да бъде подпомогната от Европейския съюз, като се използват средства от фондовете за развитие на транспортната инфраструктура. Това ще даде възможност не само за намаляване на натоварването върху пътищата, но и за подобряване на екологичната устойчивост на транспорта в региона.

Екологични предизвикателства и решения в товарния транспорт

Изгарянето на дизелово гориво от товарните автомобили води до значително натоварване върху околната среда. Това се изразява в повишаване на емисиите на въглероден диоксид, фини прахови частици и други замърсители, които имат вредно въздействие върху здравето на населението и околната среда. Пътищата в Република България, през които преминават значителни обеми транзитен трафик, са основен източник на тези замърсявания.

Проблемът се задълбочава поради особеностите на релефа и инфраструктурата в страната. Наклоните, завоите и липсата на адекватни магистрални трасета водят до честа смяна на режимите на двигателите на товарните автомобили, което значително увеличава разхода на гориво и вредните емисии. Това създава предпоставки за опасности на пътя, образуване на задръствания и увеличаване на екологичния отпечатък.

За справяне с този проблем е необходимо разработването и прилагането на интегриран подход, който включва следните мерки:

- Пренасочване на транзитния трафик към железопътния транспорт – Използването на комбинирания Ro-La превози би намалило значително вредните емисии и износването на пътната инфраструктура. Пример за успешна реализация на този подход е Швейцария, където този тип транспорт е широко използван.

- Инвестиции в инфраструктура и интермодални терминали – Развитието на железопътната инфраструктура и създаването на интермодални терминали ще улесни прехода между различните видове транспорт, като същевременно ще намали разходите и времето за доставка.

- Стимулиране на алтернативни горива и електрически превозни средства – Въвеждането на електрически товарни автомобили и хибридни технологии,

както и увеличаване на дела на биогоривата, ще допринесат за дългосрочно намаляване на въглеродния отпечатък.

— Внедряване на интелигентни транспортни системи – Тези системи могат да оптимизират маршрутите, да намалят задръстванията и да подпомогнат икономичното управление на транспортните средства.

— Обучение на водачите и обществени кампании – Насърчаването на екологично и икономично шофиране може да намали разхода на гориво и вредните емисии.

— Политики за ограничаване на замърсяването – Включват рехабилитация и модернизация на съществуващите пътни мрежи, както и фискални стимули за компании, използващи екологични транспортни решения.

Прилагането на тези мерки ще изисква стратегически инвестиции, съвместни усилия между държавни институции, транспортни компании и обществото, както и подкрепа от Европейския съюз. Намаляването на вредните емисии и подобряването на транспортната инфраструктура ще имат дългосрочен положителен ефект както върху околната среда, така и върху качеството на живот на населението.

Възможности и предимства на Ro-La транспорта в България

Ro-La транспортът е иновативно решение за справяне с екологичните и инфраструктурните предизвикателства, свързани с транзитния товарен транспорт. Този подход се основава на прехвърляне на товарните автомобили върху железопътни платформи, което носи редица ползи за околната среда, икономиката и обществото.

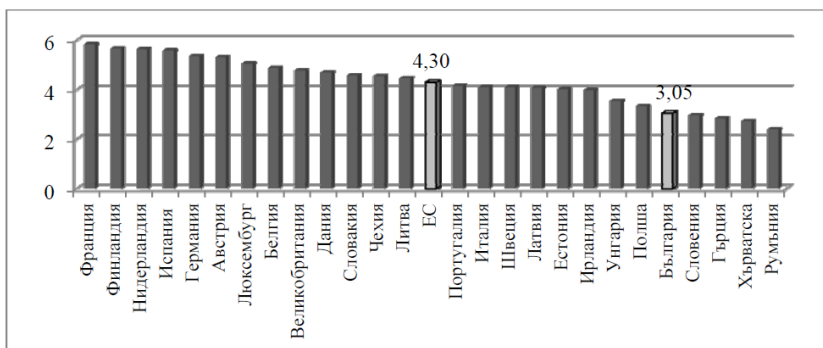
България е сред страните с особено интензивен транзитен трафик, тъй като през нея преминават четири паневропейски транспортни коридора. Това създава значителен натиск върху пътната инфраструктура, особено в участъци с тесни и планински маршрути. Постоянното движение на тежкотоварни автомобили води до редица проблеми – повишено замърсяване на въздуха, чести повреди на пътната настилка и увеличен риск от пътно-транспортни произшествия. В същото време, дългото чакане на граничните пунктове допълнително утежнява трафика и води до излишни разходи за гориво и емисии.

Швейцария е добър пример за успешно прилагане на Ro-La транспорт. В тази страна е въведена система, която позволява товарните автомобили да преминават през територията ѝ с минимално натоварване върху пътната инфраструктура. Чрез инициативата RAlpin, която осигурява транспортиране на около 100 000 товарни автомобила годишно, Швейцария спестява приблизително 30 000 тона CO₂ годишно.

Ефективността на Ro-La транспорт в България би могла да се увеличи чрез изграждане на специализирани терминали и модернизиране на железопътната инфраструктура. Според изследванията, икономическата рентабилност за превозвачите е значителна. Например, разходите за железопътен превоз на един товарен автомобил са с около 30% по-ниски в сравнение с транспорт по пътищата, ако се вземат предвид спестените такси, гориво и време. Инвестициите в

комбинирани транспортни системи могат да бъдат подкрепени от европейски програми като „Хоризонт Европа“ и „CEF Transport“. [1, 3]

За да се ускори развитието на Ro-La транспорт в България, е необходимо рационално планиране на терминали, които да отговарят на международните стандарти. Използването на унифицирани железопътни платформи и ефективно разпределение на ресурсите ще гарантира по-висока товароносимост и гъвкавост на системата. Важно е също така да се осигури интеграция между различните видове транспорт, което ще спомогне за намаляване на вредните емисии и ще увеличи привлекателността на железопътния транспорт за логистичните компании. Ro-La транспортът предоставя уникална възможност за България да намали екологичния си отпечатък и да модернизира транспортния си сектор. Чрез инвестиции в инфраструктура и внедряване на иновации страната може да постигне по-устойчиво и конкурентоспособно транспортно бъдеще, което ще бъде от полза както за икономиката, така и за околната среда.



Фиг. 2. Оценка на железопътния транспорт на България спрямо други държави

Въпреки предизвикателствата, свързани с първоначалните инвестиции и координацията между различните заинтересовани страни, внедряването на Ro-La транспорт може да донесе дългосрочни ползи за региона. Съчетаването на технологични иновации с активна държавна подкрепа ще улесни адаптацията на системата и ще насърчи използването ѝ от транспортния сектор. Създаването на пилотни проекти за Ro-La транспорт в ключови транспортни коридори, съчетани с стимули за превозвачите, може да послужи като основа за изграждането на устойчива и интегрирана транспортна мрежа. Това би утвърдило България като лидер в екологичния транспорт в региона и като предпочитан партньор в логистиката на европейско ниво. Допълнително, популяризирането на Ro-La транспорт сред местните и международни превозвачи чрез информационни кампании и финансови облекчения може значително да ускори прехода към този устойчив модел. Подобна инициатива би подобрила свързаността на България с останалите европейски държави, превръщайки я в ключов хъб за екологично чист товарен транспорт.

Таблица 1. Оценка ключови проблеми

Проблем	Засегнат регион	Причини	Ефект върху транспорта	Възможни решения
Недостатъчно финансиране	Национално	Липса на бюджет	Забавени проекти	Държавно и частно партньорство
Лоша поддръжка	Северозападна България	Стари пътища, липса на ремонти	Риск за безопасност	План за регулярна поддръжка
Задръствания	София, Пловдив, Варна	Липса на обходни пътища	Загуба на време и гориво	Инвестиране в обходни пътища
Слаба ЖП мрежа	Национално	Остаряла техника	Ниска скорост на пътуване	Реконструкция на ЖП линии

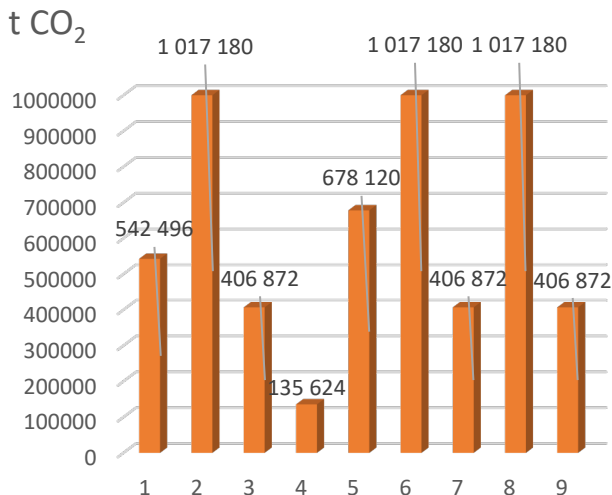
Мерки за подобряване на транзитния транспорт

За постигане на устойчиво управление на транзитния транспорт в България е необходимо прилагането на комплексен подход, включващ следните мерки:

— Разработване на национална стратегия за комбинирани превози, включително Ro-La транспорт – Интегрирането на различни видове транспорт е ключово за повишаване на ефективността и намаляване на екологичния отпечатък. Разработването на национална стратегия за комбинирани превози, включително Ro-La транспорт (превоз на камиони чрез железопътен транспорт), ще допринесе за оптимизиране на логистичните вериги и намаляване на задръстванията по пътищата. [7]

— Модернизация на железопътната инфраструктура и изграждане на нови терминали – Инвестициите в железопътната инфраструктура са от съществено значение за подобряване на скоростта, безопасността и надеждността на превозите. Изграждането на нови интермодални терминали ще улесни прехвърлянето на товари между различни видове транспорт, повишавайки ефективността на цялата система. [5]

— Въвеждане на строги екологични стандарти за товарните автомобили – Прилагането на по-строги екологични стандарти за товарните автомобили ще намали емисиите на вредни вещества и ще подобри качеството на въздуха. Това може да включва изисквания за използване на по-екологични горива, редовни технически прегледи и стимули за обновяване на автопарка с по-екологични превозни средства.



Фиг. 3. Сумарно намаление в тонове на CO₂ или съответния му косвен еквивалент

— Насърчаване на инвестиции в технологии за намаляване на емисиите и повишаване на енергийната ефективност – Подкрепата за внедряване на нови технологии, като електрически или хибридни двигатели, системи за управление на енергопотреблението и аеродинамични подобрения, ще спомогне за намаляване на емисиите и повишаване на енергийната ефективност в транспортния сектор. Това може да бъде постигнато чрез данъчни облекчения, субсидии или публично-частни партньорства. [2, 4]

— Подобряване на управлението на транспортната система – Ефективното управление на транспортната система изисква координация между различните видове транспорт и оптимизация на транспортните потоци. Въвеждането на интелигентни транспортни системи (ITS) може да подпомогне управлението на трафика, намаляване на задръстванията и повишаване на безопасността на пътя.

— Повишаване на безопасността и сигурността на транспортната система – Прилагането на мерки за повишаване на безопасността, като подобряване на инфраструктурата, обучение на водачите и стриктен контрол върху спазването на правилата за движение, е от съществено значение за намаляване на пътнотранспортните произшествия и повишаване на доверието в транспортната система. [9]

— Ограничаване на негативното въздействие на транспорта върху околната среда и здравето на хората – Наред с намаляването на емисиите, е важно да се предприемат мерки за намаляване на шума, вибрациите и други негативни въздействия на транспорта върху околната среда и здравето на населението. Това може да включва изграждане на шумоизолиращи бариери, залесяване около

транспортни коридори и насърчаване на използването на по-тихи превозни средства.

— Осигуряване на качествен и достъпен транспорт във всички райони на страната – Равномерното развитие на транспортната инфраструктура и услуги в различните региони на страната е от съществено значение за социалната и икономическа кохезия. Това включва подобряване на достъпа до транспорт в селските и отдалечените райони, както и осигуряване на достъпност за хора с увреждания. [8]



Фиг. 4. Възможности за подобряване качеството на транспортната инфраструктура в България

— Ефективно поддържане, модернизация и развитие на транспортната инфраструктура – Редовната поддръжка и модернизация на съществуващата инфраструктура, както и стратегическото планиране на нови проекти, са ключови за осигуряване на надеждна и ефективна транспортна система. Това включва инвестиции в пътища, железопътни линии, пристанища и летища, съобразени с бъдещите нужди и тенденции в транспорта. [6]

— Интегриране на българската транспортна система в европейската – Хармонизирането на стандартите, процедурите и инфраструктурата с тези на Европейския съюз ще улесни международния транспорт и ще повиши конкурентоспособността на българските транспортни оператори. Това включва

участие в трансевропейските транспортни мрежи (TEN-T) и прилагане на европейските регулации и добри практики.

Прилагането на тези мерки ще допринесе за устойчиво развитие на транзитния транспорт в България, повишаване на ефективността и конкурентоспособността на транспортния сектор, както и за опазване на околната сред

Пример 1: Да се оцени влиянието на тежкотоварния трафик върху износването на пътя

Задача: Да се изчисли натоварването върху пътната настилка и вероятното износване въз основа на броя на преминаващите тежкотоварни превозни средства и тяхното тегло.

Данни:

Брой тежкотоварни превозни средства на ден (N): 1,000.

Средно тегло на едно превозно средство (W): 25 тона.

Коефициент на натоварване спрямо стандартна ос (F): 4 (тежкотоварно превозно средство причинява 4 пъти повече износване от стандартна ос).

Период на анализ (T): 1 година (365 дни).

Износването на пътната настилка се измерва с **еквивалентни стандартни оси (ESAL)**, които се изчисляват по формулата:

$$ESAL = N \times F \times T \quad (1)$$

Изчисление:

Да се открие общото натоварване на еквивалентни стандартни оси годишно

$$ESAL = 1,000 \times 4 \times 365 = 1,460,000 \quad (2)$$

Резултат:

Годишното натоварване на пътната настилка от тежкотоварния трафик е 1,460,000 еквивалентни стандартни оси.

Пример 2: Да се извърши оценка на екологично въздействие:

Данни:

Средно изразходвано гориво от тежкотоварно превозно средство на 100 км: 30 литра.

Среден пробег на едно превозно средство на ден: 300 км.

Емисионен фактор за CO_2 (EF): 2.64 кг CO_2 на литър дизел.

Общото количество емисии CO_2 се изчислява като:

$$\text{Общо } CO_2 = N \times \text{разход гориво (литри)} \times EF \times T \quad (3)$$

$$\text{Общо } CO_2 = 1,000 \times \frac{300}{100} \times 30 \times 2,64 \times 365 \quad (4)$$

$$\text{Общо } CO_2 = 1,000 \times 30 \times 2,64 \times 365 = 86,868,000 \text{ кг годишно (5)}$$

Резултат:

Тежкотоварният трафик генерира 86,868 тона CO_2 за една година.

Заклучение

Тежкотоварният трафик оказва съществено влияние върху инфраструктурата, безопасността и екологичната устойчивост на България. Оптимизирането на този сектор чрез внедряване на Ro-La транспорт, модернизация на железопътната инфраструктура и насърчаване на екологични технологии може значително да намали натоварването върху пътищата и да подобри качеството на живот. Примерите от страни като Швейцария показват, че успешното прилагане на иновации в транспорта е възможно чрез стратегически инвестиции и ефективно управление. Реализирането на тези мерки ще допринесе за постигане на устойчиво и конкурентоспособно развитие на транспортната система в България.

Тежкотоварният трафик не само увеличава разходите за поддръжка на пътната инфраструктура, но също така допринася за повишена аварийност и замърсяване на въздуха, особено в градските и индустриалните райони. Въвеждането на интелигентни системи за управление на трафика, включително контрол на маршрути и ограничения за тежкотоварни превозни средства в определени зони, би могло да намали риска от инциденти и да подобри ефективността на транспортната мрежа. Същевременно, стимулирането на комбинирани транспортни решения, като Ro-La и интермодален транспорт, ще облекчи натиска върху пътната инфраструктура, насочвайки по-голямата част от тежкотоварния трафик към железопътната система.

Екологичната устойчивост също трябва да заеме водещо място в развитието на транспортния сектор. Освен внедряването на по-екологични превозни средства, насърчаването на технологии като електрификация и използване на възобновяеми енергийни източници би намалило емисиите на парникови газове. Допълнителна подкрепа под формата на данъчни облекчения за компании, които инвестират в зелени технологии и оптимизация на товарния транспорт, ще подпомогне екологичния преход. Чрез интеграцията на тези подходи България може да постигне балансирано развитие, което отговаря на съвременните екологични и икономически изисквания.

ЛИТЕРАТУРА

- [1] Желязкова Д. Устойчиво развитие на транспортната система на България. Economics 21, D. A. Tsenov Academy of Economics, Svishtov, Bulgaria, issue 2 Year 20, pp. 80-132.
- [2] Цанков Ц., Янкова-Йорданова Й. Намалване на последствията от транзитно преминаващите товарни автомобили по пътищата на Република

България. Седма международна научна конференция „Техника. Технологии. Образование. Сигурност“, Велико Търново, 2019, ISSN 2535-0315, с. 83-85.

- [3] Цветкова С. Политика за устойчиво развитие на автомобилния транспорт. Управление и устойчиво развитие 4/2017.
- [4] Цветкова С. Устойчиво развитие на обществения транспорт на град София. Управление и устойчиво развитие 5/2018.
- [5] Янкова-Йорданова Й., Цанков Ц. Необходимостта от намаляване на неблагоприятните последици за околната среда при транзитен превоз на товари. Седма международна научна конференция „Техника. Технологии. Образование. Сигурност“, Велико Търново, 2019, ISSN 2535-0315, с. 110-112.
- [6] Tsankov Ts. Possibilities for the use of road trains on pan-European transport corridors. KNOWLEDGE – International Journal Scientific Papers, Vol. 63.3, Institute of Knowledge Management, Skopje, 2024, ISSN 2545-4439, pp. 303-309.
- [7] https://www.mtc.government.bg/bg/category/312/analiz-na-sistemata-za-obschestven-transport-i-pregled-na-neynata-normativna-uredba?utm_source=chatgpt.com
- [8] https://www.mtc.government.bg/sites/default/files/transport_strategy_2020_last_r.pdf?utm_source=chatgpt.com
- [9] <https://www.mtc.government.bg/bg/category/42/integrirana-transportna-strategiya-v-perioda-do-2030-g>

АНАЛИЗ НА МРЕЖОВ ТРАФИК И ПОДОБРЯВАНЕ НА СИГУРНОСТТА С WIRESHARK И CISCO PACKET TRACER

Цветослав С. Цанков, Илкер А. Хатиб

ANALYSE NETWORK TRAFFIC AND IMPROVE SECURITY WITH WIRESHARK AND CISCO PACKET TRACER

Tsvetoslav S. Tsankov, Ilker A. Hatib

ABSTRACT: *Today's networks are the backbone of any modern organization, and their security is paramount. To ensure stability and protection against growing threats, it is necessary to use effective analysis and optimization tools. In this context, Wireshark and Cisco Packet Tracer are powerful allies. Wireshark provides the ability to analyse network traffic in detail in a real-world environment, while Cisco Packet Tracer allows simulation of various network scenarios for testing and training. The purpose of this report is to explore how these two tools can be used together to improve network security and performance, as well as to diagnose and prevent potential problems.*

KEYWORDS: *Wireshark, Cisco Packet Tracer, optimization, security*

DOI: <https://doi.org/10.46687/YT24CEC>

1. Въведение

Днешните мрежи изискват надеждни инструменти за диагностика и сигурност, за да се справят с нарастващите заплахи и да осигурят оптимална производителност. Wireshark и Cisco Packet Tracer са два ключови инструмента, които могат да се използват съвместно за анализ на мрежовия трафик и подобряване на защитата[1]. Wireshark предоставя детайлен анализ на пакети в реална среда, което е изключително полезно за засичане на аномалии и диагностика на проблеми. С възможности като филтриране на трафик, анализ на протоколи и декриптиране на SSL/TLS, инструментът е незаменим за откриване на заплахи като DDoS атаки или неоторизиран достъп.

От своя страна, Cisco Packet Tracer позволява симулация на мрежови топологии и конфигурации, включително тестване на защитни мерки като VLAN сегментация и ACL (Access Control Lists). Той е ценен инструмент за обучение и тестване на стратегии за сигурност без риск за реалните мрежи.

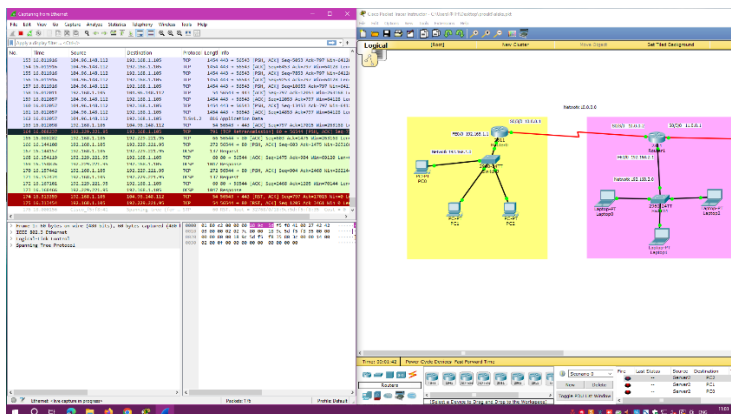
Комбинирането на Wireshark и Cisco Packet Tracer позволява проектиране и тестване на мрежови архитектури, анализ на уязвимости и разработване на ефективни мерки за защита [2]. Този интегриран подход помага на организациите да откриват потенциални заплахи, да оптимизират производителността на

мрежата и да изграждат по-сигурни инфраструктури [5]. Така Wireshark и Cisco Packet Tracer се утвърждават като мощни инструменти за проактивно управление на мрежовата сигурност и диагностика.

2. Основни характеристики на софтуерните инструменти Wireshark и Cisco Packet Tracer

Wireshark

Wireshark е един от най-разпространените инструменти за анализ на мрежовия трафик. Неговата основна сила е в способността му да предоставя детайлна информация за всеки пакет, преминаващ през мрежата [7]. Това го прави особено полезен за разследване на проблеми с производителността и за откриване на потенциални заплахи. Сред основните предимства на Wireshark е възможността да се филтрира трафикът според различни критерии, като IP адрес, протокол или порт. Освен това инструментът позволява анализ на криптирани връзки, ако разполагаме с необходимите сертификати. Тази функционалност го прави особено полезен за мрежови инженери, които искат да идентифицират необичайни поведения, като неоторизиран достъп или атаки.



Фиг. 1. Софтуерни инструменти Wireshark и Cisco Packet Tracer

Cisco Packet Tracer

Cisco Packet Tracer, от друга страна, е симулационен инструмент, който се използва за изграждане и тестване на мрежови архитектури. Той е особено подходящ за обучение и подготовка, както и за тестване на нови конфигурации, без да се засягат реалните мрежи. Едно от ключовите му предимства е възможността да се симулират сложни мрежови топологии, което позволява предварително тестване на настройки като VLAN, маршрутизация и политики за сигурност. Например, ACL (Access Control Lists) могат да бъдат конфигурирани и тествани в Packet Tracer, за да се провери тяхната ефективност срещу специфични видове трафик.

3. Анализ на мрежовия трафик с Wireshark

Wireshark е основен инструмент за всеки специалист по мрежова сигурност и диагностика. Неговата способност да предоставя детайлна информация за всички пакети в мрежата го прави незаменим при идентифициране на проблеми и потенциални заплахи. [8]

Една от ключовите функции на Wireshark е възможността да филтрира трафика по конкретни критерии. Например, ако има съмнение за DDoS атака, специалистът може да филтрира трафика за специфични Z-wave пакети и да анализира източниците на тези заявки. Това помага за локализиране на проблема и за предприемане на конкретни мерки. [9]

Друга важна функция е декриптирането на криптиран трафик, когато са налични сертификати. Това е особено полезно за анализ на Zigbee връзки и идентифициране на потенциални опити за компрометиране на данните. Достъпът до съдържанието на криптирани пакети помага за установяване на необичайни активности или уязвимости, свързани с неправилна конфигурация на криптографски протоколи. [3, 4]

Wireshark в мрежовата диагностика

Wireshark не е просто инструмент за пасивно наблюдение на мрежовия трафик – той предоставя мощни аналитични възможности. Специалистите могат да използват софтуера за:

- Идентифициране на забавяния в мрежата: Чрез анализ на време закъснения между пакетите и проследяване на маршрута им.

- Проследяване на грешки в комуникацията: Откриване на дублирани пакети, липсващи ACK съобщения или неправилно затваряне на TCP сесии.

- Откриване на злонамерена активност: Като подозрителни DNS заявки, аномални портове или необичайно голямо количество входящи/изходящи пакети от определен IP адрес.

Обучение и практическо приложение

Wireshark е ценен не само за професионалистите, но и за начинаещите в областта на мрежовата сигурност. Лесният за разбиране интерфейс и широката документация позволяват бързо овладяване на основните функции. Чрез практическа работа с различни видове трафик – от HTTP и FTP до по-сложни протоколи като SIP или SMB – потребителите могат да придобият ценни умения за работа с мрежи.

Wireshark е инструмент, който непрекъснато се развива, добавяйки поддръжка за нови протоколи и функции. Това го прави съвместим с модерните мрежови среди, включително виртуализирани инфраструктури и облачни услуги. Съчетанието от мощност, гъвкавост и лесна достъпност го прави незаменим избор за всеки, който работи в областта на мрежите. Wireshark доставя и запис на времето между пристигането на последователни пакети, което може да се използва за анализ на натоварване по следната формула:

$$\text{Inter} - \text{PacketTime} = \text{Arrival of Packet Time} (n + 1) - \text{Arrival of Packet Time} (n) \quad (1)$$

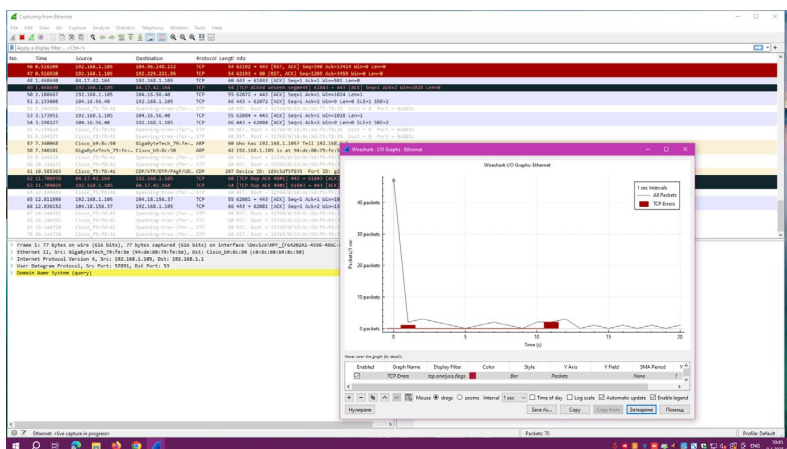
Пример:

Ако пакет 1 пристигне в 10:00:01.500, а пакет 2 в 10:00:01.520:

$$\text{Inter} - \text{PacketTime} = 10:00:01.520 - 10:00:01.500 = 0.020 \text{секунди (20 ms)} \quad (2)$$

Таблица 1. Измерено закъснение при предаване на данни чрез Wireshark

Тип пакет	Източник (IP)	Дестинация (IP)	Време на заявка (ms)	Време на отговор (ms)	Закъснение (ms)
HTTP Request	192.168.1.2	192.168.1.11	100	150	50
Z-wave Echo	192.168.1.5	8.8.8.4	200	270	70
DNS Query	192.168.1.3	8.8.4.4	320	300	20
Zigbee Data	192.168.1.4	192.168.1.20	500	650	150
TCP SYN	192.168.1.7	192.168.1.12	800	900	100



Фиг. 2. Работа в софтуерен инструмент Wireshark

4. Оптимизация и защита чрез Cisco Packet Tracer

Cisco Packet Tracer е идеалният инструмент за симулиране на различни мрежови сценарии и тестване на стратегии за сигурност. Чрез него мрежовите инженери могат да проектират мрежи, да настройват политики за достъп и да симулират потенциални атаки, за да видят как ще реагират системите. Една от

най-важните му функционалности е тестването на QoS (Quality of Service). Това позволява оптимизиране на мрежовата производителност, като се дава приоритет на критичния трафик, например VoIP или видео конференции. [6]

Cisco Packet Tracer също така позволява симулация на атаки като ARP spoofing, за да се провери ефективността на защитните мерки. Например, настройката на VLAN сегментация може да бъде тествана, за да се види как мрежата ще ограничи разпространението на заплахата. Cisco Packet Tracer е изключително полезен не само за професионалисти, но и за студенти, които изучават мрежови технологии. С негова помощ те могат да изградят практически умения, като създават и настройват сложни мрежови топологии в напълно безопасна виртуална среда. Софтуерът предлага визуално интуитивен интерфейс, който прави процеса на обучение и експериментиране лесен и достъпен, дори за начинаещи. Освен това, Cisco Packet Tracer поддържа разнообразие от устройства и протоколи, което позволява на потребителите да симулират реални мрежови условия. Инструментът включва функции като IoT (Internet of Things) симулации, което го прави подходящ за модерните предизвикателства в мрежовия свят. Независимо дали става дума за създаване на мащабни корпоративни мрежи или изследване на малки домашни конфигурации, Packet Tracer осигурява пълна гъвкавост и безкрайни възможности за тестване и обучение. [10]

Таблица 2. Сравнение между симулирани атаки и защитни мерки в Cisco Packet Tracer

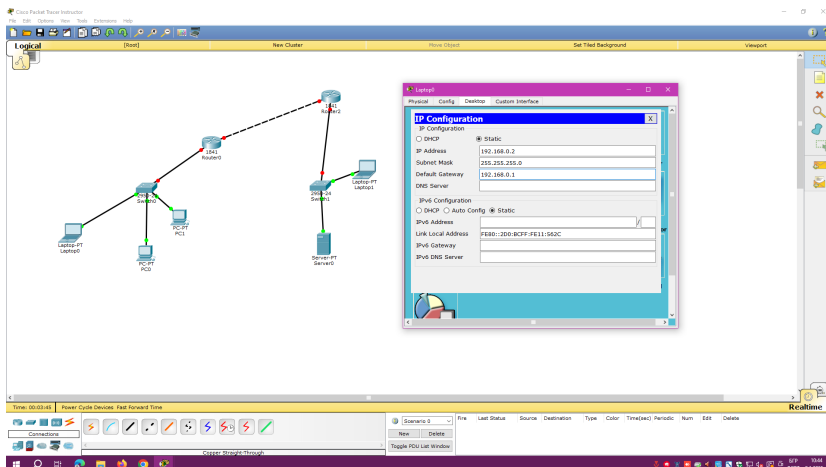
Атака	Описание	Възможна защита
ARP spoofing	Подправяне на ARP таблиците	Настройка на статични ARP записи, VLAN
DoS (Denial of Service)	Претоварване на мрежовите ресурси	Мониторинг и ограничаване на трафика
Man-in-the-Middle	Подслушване на комуникацията	Използване на криптирани протоколи
Brute Force	Неправомерно гадаене на пароли	Ограничения за опити за вход

5. Съвместно използване на Wireshark и Cisco Packet Tracer

Комбинирането на Wireshark и Cisco Packet Tracer предоставя уникална възможност за задълбочен анализ и тестване. Чрез симулиране на реални сценарии в Cisco Packet Tracer и последващ анализ на трафика с Wireshark, специалистите могат да разработят ефективни стратегии за защита.

Пример: В случай на подозрение за ARP spoofing, атаката може да бъде симулирана в Packet Tracer, като се използват виртуални устройства за имитация на злонамерен трафик. След това трафикът се улавя с помощта на Wireshark, където се анализират пакети в реално време, за да се идентифицират аномалии като дублиращи се MAC адреси или неправомерни заявки. Инженерът може да разгледа ARP таблицата на устройствата в мрежата, за да открие фалшивите IP

адреси и тяхното свързване с неподходящи MAC адреси. След установяване на заплахата могат да се приложат различни мерки за защита. Например, активирането на динамично ARP инспектиране (DAI) върху свичовете помага за филтриране на невалидни ARP пакети. Освен това, конфигурирането на защитени портове на ключови устройства в мрежата ограничава възможностите за неправомерни манипулации. Тази симулация дава възможност не само за тестване на ефективността на защитните механизми, но и за идентифициране на слабости в текущата конфигурация.



Фиг. 3. Работа в софтуерен инструмент Cisco Packet Tracer

Подобен подход не само подобрява мрежовата сигурност, но и служи като ценен инструмент за обучение на екипи. Чрез възпроизвеждане на реални атаки в контролирана среда, администраторите и инженерите придобиват умения за бързо разпознаване на инциденти и прилагане на адекватни защитни мерки в реални ситуации. Това значително повишава тяхната готовност за реагиране при киберзаплахи.

6. Заключение

Wireshark и Cisco Packet Tracer представляват мощен tandem от инструменти, които, когато се използват в съчетание, предоставят изключителни възможности за повишаване на мрежовата сигурност, ефективност и устойчивост на системите. Wireshark, като водещ инструмент за анализ на мрежовия трафик, осигурява детайлен поглед върху пакетите данни, позволявайки на специалистите да идентифицират аномалии, уязвимости и потенциални заплахи. От друга страна, Cisco Packet Tracer предоставя интерактивна среда за симулиране на мрежови топологии, експериментирание с различни сценарии и тестване на стратегии за защита, без да се изисква физически хардуер. Съвместното използване на тези инструменти създава уникална възможност за интегриран подход към мрежовото

управление. Докато Wireshark помага за диагностициране на проблеми и задълбочен анализ в реално време, Cisco Packet Tracer позволява проактивно моделиране на заплахи и разработване на решения. Тази комбинация не само улеснява откриването и разрешаването на текущи проблеми, но също така позволява симулация и тестване на бъдещи сценарии, което е от съществено значение за подготовката срещу нововъзникващи киберзаплахи. Освен това, тези инструменти играят ключова роля в образованието и обучението на мрежови специалисти. Те предоставят безопасна и контролирана среда, в която потребителите могат да развиват уменията си, да експериментират с нови технологии и да оценяват ефективността на различни методи за защита. Тази практическа насоченост е особено ценна в контекста на динамичното развитие на мрежовите технологии и нарастващия брой заплахи в киберпространството.

Таблица 3. *Процес за симулация на ARP spoofing и прилагане на защитни мерки*

Стъпка	Описание	Инструменти/Мерки
1. Симулация на атака	Създаване на сценарий с фалшив ARP трафик в Packet Tracer.	Packet Tracer: Настройка на злонамерен хост
2. Улавяне на трафика	Заснемане и анализ на мрежовите пакети за идентифициране на подозрителна активност	Wireshark: Анализ на дублирани MAC/IP адреси
3. Проверка на ARP таблица	Преглед на ARP таблицата на устройствата за невалидни записи.	CLI: show arp команда
4. Идентифициране на проблема	Определяне на източника на фалшиви ARP записи и засегнатите устройства.	Wireshark/ARP таблица
5. Прилагане на мерки	Конфигурация на защитни механизми като DAI и защитени портове.	DAI: Динамично ARP инспектиране Port Security: Ограничение на MAC адреси
6. Тестване на мерките	Ресимулация на атака за потвърждение на ефективността на защитата.	Packet Tracer/CLI: Проверка на трафика
7. Обучение на екипите	Провеждане на симулации за запознаване на екипа с процедурите за откриване и реакция.	Packet Tracer: Реални сценарии

Интеграцията на Wireshark и Cisco Packet Tracer не само подпомага управлението на сложни мрежови инфраструктури, но също така насърчава иновации и повишава готовността на мрежовите специалисти да се справят с

предизвикателствата на съвременната мрежова сигурност. Тази синергия между анализ и симулация може да бъде основа за по-сигурни и ефективни мрежи в бъдеще.

ЛИТЕРАТУРА

- [1] Denev D., Konstantinova E., Ismail T., Cybersecurity – International and National Dimensions, 2019, Cadet-Students Scientific Conference, Collection of Papers, National Military University „Vasil Levski“, Veliko Tarnovo, ISSN 2367-7481, pp. 300-310.
- [2] Denev D., Konstantinova E., Main Issues in the Protection of Information in the system of National and Corporate Security, 2020, Conference with international participation MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 110-115.
- [3] Denev D., Z-WAVE Communication for Home Automation, 2020, Conference with international participation MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 96-103.
- [4] Denev D., Terziev H., Zigbee Communication Protocols and Their use to Manage Smart Devices, 2020, Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of technical sciences, ISSN 1311-834X, pp. 83-89.
- [5] Denev D., Low Energy Real-Time Routing, 2022, Annual University Scientific Conference, Proceedings of National Military University „Vasil Levski“, Veliko Tarnovo, 2022, ISSN 2367-7481, pp. 1267-1276.
- [6] Denev D., Tsankov Ts., Communication-Based Dynamic Packet Optimization for Visual PLC Monitoring, 2022, Annual University Scientific Conference, Proceedings of National Military University „Vasil Levski“, Veliko Tarnovo, ISSN 2367-7481, pp. 1259-1266.
- [7] Denev D., Tsankov Ts., A Survey of Data Quality and Processing of Information in Innovative Smart Devices, 2022, International Conference Automatics and Informatics (ICAI) 2022, <https://ieeexplore.ieee.org/>, Varna Bulgaria, 06-08 October, ISBN 978-1-6654-7625-6 and 10.1109/ICA155857.2022.9960040
- [8] Denev D., Modeled Security in Communication Network Coding, 2022, Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, ISSN 1311-834X, pp. 153-161.
- [9] Denev D., Surveillance with Wireshark and its Use in Communication Networks, 2023, Annual of Konstantin Preslavski University of Shumen, Volume XIII E, ISSN 1314-8818, pp. 104-109.
- [10] Denev D., Tsankov Ts., Use of Cisco Packet Tracer in Evaluation of Communication Networks, 2023, XVI International Scientific Conference, Belovo, ISBN 978-5-00137-315-5 (item 1), ISBN 978-5- 00137-314-8, pp. 163-171.

СЪЩНОСТ И ОСНОВНИ КОНЦЕПЦИИ ЗА КОРПОРАТИВНА СИГУРНОСТ

Десислава Д. Георгиева

ESSENCE AND KEY CONCEPTS OF CORPORATE SECURITY

Desislava D. Georgieva

ABSTRACT: *Corporate security is a key element for the sustainable functioning of businesses, encompassing not only physical protection but also information security, intellectual property protection, and crisis management. While traditional corporate security primarily focused on local measures such as guarding and asset protection, modern corporate security incorporates strategic approaches like cybersecurity and compliance with legal requirements. The evolution of the concept of corporate security reflects global economic and technological challenges, as well as the need for integration with companies' business strategies.*

KEYWORDS: *company, corporation, corporate security, national security, concepts of corporate security*

DOI: <https://doi.org/10.46687/YT24DES>

Увод

Сигурността е категория с фундаментално значение в сферата на живота и в частност в политиката. Тя е многоизмерна и има различни нива, аспекти, обекти и субекти, поради което често се изпълва с най – разнообразно съдържание [3]. Сигурност е състояние, при което се осигурява защита на хората, обществото и околната среда от потенциални заплахи, рискове или вреди. В по-широк смисъл тя обхваща гарантирането на безопасност, стабилност и надеждност в различни сфери на живота, включително лична, обществена, икономическа, екологична и национална. Разглежда се като основна предпоставка за развитие и устойчивост на човешките дейности и системи [22].

Сигурността, като родово понятие се определя, като невъзможност да се нанесе вреда, защита на всеки човек и обкръжаващата го среда от опасности. В политически контекст терминът „сигурност“ обикновено се свързва с „защитеност“, „състояние на безопасност“ и „гарантирана надеждност“ за развитието на индивидите, обществото и държавата.

Понятието се разглежда от множество перспективи в различни научни дисциплини. В политологията и международните отношения, традиционното разбиране за сигурност често е свързано със защитата на държавния суверенитет и териториалната цялост. В социологията, политологията и психологията определенията за сигурност корелират в областта на защита на важните

необходими нужди на обществото и човека. Философията и политологията разглеждат сигурността, като определено състояние на системата. Надеждността характеризира сигурността във философията, правото, политическите науки и математиката. Само социологията и политологията разглеждат сигурността от гледна точка на развитието на системата, тоест в динамика [5].

С времето обаче концепцията за сигурност се е развила, за да обхване по-широки аспекти. Например, "човешката сигурност" се фокусира върху благосъстоянието на индивидите и обществата, включително икономическата, социалната, здравната и екологичната стабилност. Това понятие става особено актуално след края на Студената война, когато новите заплахи, като тероризъм, климатични промени и транснационални конфликти, изместват фокуса от чисто военната към неконвенционалната сигурност [12].

Системата представлява цялостна структура, съставена от взаимосвързани елементи, които функционират заедно за постигане на определени цели. Тя подчертава организацията, взаимозависимостта и целенасочеността на елементите, които образуват едно цяло [2].

Елементите в системата могат да бъдат обекти, процеси или явления, свързани чрез определени отношения, които обуславят структурата на системата. Тази структура може да бъде статична или динамична, в зависимост от взаимодействията между компонентите и външната среда. Системите често се делят на подсистеми и се описват чрез теоретични, алгебрични или топологични модели, които позволяват по-добро разбиране на тяхното функциониране и развитие.

Понятието „сигурност“ трябва да бъде разгледано във връзка с понятието „система“, като интегрирана общност от взаимосвързани елементи [6].

От такава гледна точка сигурността се определя като динамично състояние на защитеност на система, при което е гарантирано нейното съществуване и са защитени надеждно жизненоважните ѝ интереси. Затова за защита на жизненоважните интереси се отделят значителни ресурси, като само по този начин системата може да гарантира своето успешно съществуване и развитие [1].

Същинска част

Видове сигурност

Съществуват различни класификации на отделните аспекти на сигурността, т.е. на видовете сигурност. Според различни критерии сигурността се определя като национална, политическа, икономическа, социална, финансова, информационна, киберсигурност, лична, корпоративна и други [10].

— Национална сигурност:

Националната сигурност може да бъде дефинирана като състояние на защитеност на жизненоважните интереси на личността, обществото и държавата от вътрешни и външни заплахи. Тази концепция обхваща множество аспекти, включително политическата, икономическата, социалната, екологичната и военната сфера. Националната сигурност е динамична и зависи от промените във

вътрешната и международната среда, като се стреми да гарантира стабилност, ред и развитие в обществото.

Според *Стратежията за национална сигурност на Република България (2011 г.)*, националната сигурност е дефинирана като система от мерки и дейности за защита на правата, свободите, сигурността и благосъстоянието на гражданите и обществото. Основни цели са опазването на суверенитета, териториалната цялост и единството на страната, както и защитата на демократичните ценности, конституционния ред и критичната инфраструктура. Политиката за национална сигурност включва предотвратяването на рискове като природни бедствия, аварии, терористични заплахи и екологични кризи. Освен това, стратегията поставя акцент върху интеграцията на страната в ЕС и НАТО и осигуряването на енергийна, екологична и икономическа стабилност [11].

— **Политическа сигурност:**

Политическата сигурност се отнася до състоянието на стабилност и защитеност в рамките на политическата система на дадена държава или общество. Тя обхваща защитата от заплахи, които могат да подкопаят политическите институции, правата на гражданите и демократичните процеси. Основен акцент е гарантирането на законност, равенство пред закона, участие в управлението и ефективна защита на правата и свободите на хората.

Политическата сигурност също така се свързва с усилията за предотвратяване на екстремистки заплахи, авторитарни режими или политическа корупция, които биха могли да нарушат основните политически права. Тя е тясно свързана с концепцията за „свобода от страх“ в рамките на човешката сигурност, което подчертава значението на защитата на гражданите от политически репресии и насилие [12].

— **Икономическа сигурност:**

Икономическата сигурност може да се дефинира като способността на държавата да поддържа стабилност в своята икономическа система, така че да предотвратява и минимизира негативните въздействия от вътрешни и външни заплахи. Тя включва защита на критичните сектори на икономиката, осигуряване на устойчиво развитие, контрол върху инфлацията и безработицата, и управление на ресурсите за дългосрочен икономически растеж.

— **Социална сигурност:**

Социалната сигурност обхваща системи и механизми, насочени към защита и подпомагане на хората срещу социални рискове. Тя включва осигуряване на достъп до социални услуги, като пенсии, здравни грижи, помощи за безработица и социални програми за уязвими групи от населението. Основната цел на социалната сигурност е да се гарантира основен стандарт на живот и равен достъп до социални права за всички граждани, като същевременно насърчава социалната стабилност и икономическо развитие.

Според Европейската комисия и други експерти, социалната сигурност е от ключово значение за справяне с демографските и икономическите предизвикателства в съвременните общества, като в същото време служи за инструмент за намаляване на социалните неравенства и бедността [14].

— **Финансова сигурност:**

Финансовата сигурност се дефинира като състояние, при което индивиди, домакинства и институции разполагат с достатъчно ресурси и стабилност за посрещане на краткосрочни и дългосрочни финансови нужди, дори при неблагоприятни икономически условия. Тя включва способността за управление на рискове, свързани с доходите, спестяванията, инвестициите и кредитирането, както и устойчивостта на финансовите системи при икономически кризи. Финансовата сигурност играе важна роля в предотвратяването на социални и икономически неравенства и укрепването на икономическата стабилност в дадено общество [7].

— **Информационна сигурност:**

Информационната сигурност е основен елемент на националната сигурност и има за цел да защити правата на индивидите и обществото за достъп до обективна и достоверна информация. Тя включва разработването на политики, правила и процедури за сигурност, които подкрепят устойчивостта на информационното пространство срещу съвременните заплахи като дезинформация, кибератаки и информационна агресия. Информационната сигурност е не само техническо, но и стратегическо предизвикателство, свързано с гарантиране на стабилността на държавата и развитието на информационното общество [4].

— **Киберсигурност:**

Киберсигурността се отнася до практиките, процесите и технологиите, които са предназначени да защитават компютърни мрежи, системи и данни от неразрешен достъп, атаки и други заплахи. Тя обхваща защитата на информационни технологии, данни и критични инфраструктури от киберзаплахи като хакерски атаки, вируси и изтичане на информация, които могат да нанесат сериозни щети на лични данни, бизнес и национални интереси [15].

— **Лична сигурност:**

Личната сигурност обхваща защитата на индивида от различни форми на заплахи, които могат да нарушат неговото физическо, психическо или социално благосъстояние. Това включва превенция на насилие, престъпност, тероризъм и други опасности, които застрашават личния живот и имущество на гражданите. Личната сигурност е важен аспект в контекста на националната сигурност, като индивидите са основни участници в създаването на стабилна и сигурна социална среда [16].

Националната сигурност на всяка една държава е следствие от нейното икономическо състояние. Над 90 % от икономиката у нас е в ръцете на частни компании. Големите и средни фирми имат под една или друга форма структури за сигурност, които пазят техните активи. Съответно тяхната работа, оказва благоприятно или негативно влияние върху националната сигурност. Следователно, финансово-икономическата сигурност е елемент на националната сигурност. Концепцията за национална сигурност е най – общата основа, върху която се реализира връзката между икономиката и потребностите на сигурността и отбраната [8].

Икономическата система на всяко общество се състои от голям брой бизнес организации, затова успешно, пълноценно и ефективно решаване на задачите, стоящи пред икономическата сигурност на всяка държава, зависят от резултативността на тяхната дейност. Бизнес организациите осигуряват икономическата сфера на обществото, нейното възпроизводство и развитие.

Тъй като в обществото и в редица научни и образователни организации се използва общо приетият термин „корпоративна сигурност“, той може да се използва заедно с еквивалентното понятие „сигурност на бизнес организация“.

— Корпоративна сигурност

Корпоративната сигурност представлява значим ресурс за укрепване на системата на националната сигурност. За да бъде ефективна тази връзка, е необходимо компетентно и добронамерено разрешаване на конфликтите и напреженията между механизмите, осигуряващи корпоративната и националната сигурност. Множество експерти подчертават, че е невъзможно да се говори за национална сигурност, без да се отчита взаимозависимостта ѝ с корпоративната сигурност. Все по-ясно се осъзнава, че корпоративната сигурност е основен структурен елемент в цялостната архитектура на националната система за сигурност.

Съгласно търговския закон, *фирма е наименованието, под което търговецът извършва своята дейност* („упражнява занаятието си и се подписва“).

Предприятието, или както често е наричано в разговорната реч – „фирмата“ може да се дефинира като основна структурна и икономическа единица в икономиката и представлява независима система с правен статут на юридическо лице. Фирмата комбинира ресурси като труд, капитал и суровини, за да произвежда стоки или услуги за удовлетворяване на потребностите на обществото или за използване в производството. Термините „предприятие“ и „фирма“ често се използват взаимозаменяемо, въпреки че имат нюанси в значението си. Фирмата представлява стопанска, търговска или промишлена организация, която функционира в рамките на установените правни норми .

Тя функционира в рамките на определена институционална структура и използва механизми за трансфер на технологии, знания и ресурси от околната среда към производствения процес. Основната ѝ цел е да създава стойност чрез ефективно управление на процесите, което включва планиране, организиране и анализ на бизнес дейностите, като се отчита конкурентоспособността и интересите на собствениците на капитала [17].

Компания е търговско или индустриално предприятие, представляващо бизнес сдружение на предприемачи, обединени с цел извършване на стопанска дейност. Тя обикновено е по-малка по мащаб и структура в сравнение с корпорацията. Корпорацията, от своя страна, е сложна организационна и икономическа форма на бизнес комбинация, която обединява множество фирми за съвместна работа и постигане на общ резултат. Тя може да бъде сравнявана с други видове бизнес асоциации, като холдинг, тръст, синдикат, консорциум или група от компании, които работят под общо управление и цел.

Корпорацията е правен субект, създаден с цел извършване на стопанска дейност, който притежава отделна юридическа личност от своите собственици. Основната ѝ характеристика е ограничената отговорност на акционерите, които отговарят само със своите инвестиции, а не с личното си имущество. Тя функционира като независима икономическа единица, която може да сключва договори, да притежава активи и да носи отговорност за своите задължения. Корпорациите са ключови играчи в глобалната икономика, често със значително влияние върху иновациите и разпределението на ресурси.

В зависимост от целта и вида на собствениците корпорациите се наименоуват различно: еднолична корпорация; събирателна корпорация; чужда корпорация; местна корпорация; многонационална корпорация; квазикомунална корпорация; комунална корпорация; публична корпорация. Това са все лица обединени в едно дружество, което е юридическа личност. Много от корпорациите само привидно са независими и самостоятелни. Тази привидност е в зависимост от релацията държава – корпорация. Когато се анализират релациите между системата на националната сигурност и корпоративната сигурност, никога не трябва да се забравя, че е напълно възможно да възникнат противоречия между тях. Това са противоречията, които се намират между държава и корпорация.

Според Бизнес факултета на Оксфордския университет логистиката в корпорациите се основава на бизнес планиране за управление на материали, услуги, информация и капиталови потоци. Интегрирането на планирането включва все по-комплексна информация, системи за комуникация и контрол, необходими в днешната бизнес среда [19].

Корпоративната сигурност се дефинира като съвкупност от дейности, насочени към идентифициране, анализ и управление на рискове, които застрашават устойчивостта, ефективността и конкурентоспособността на организациите. Тя включва стратегически подход за защита на ресурсите, информацията и служителите на компанията чрез мерки за превенция, контрол и реакция на потенциални заплахи. Корпоративната сигурност обхваща не само физическа охрана, но и защита на интелектуална собственост, киберсигурност, управление на кризи и спазване на правни изисквания [20].

Важен аспект на корпоративната сигурност е изграждането на интегрирана система за управление, която да осигурява устойчивост и адаптивност към динамичните промени в бизнес средата. Това включва активна оценка на рисковете, минимизиране на уязвимостите и внедряване на ефективни методи за защита на интересите на организацията. Тази практика не само гарантира стабилността на организацията, но и допринася за нейното развитие и обществено доверие [18].

„Фирмената сигурност“ се определя като състояние на защитеност на компанията от външни и вътрешни заплахи, което осигурява нейното устойчиво съществуване, растеж и развитие с оптимален разход на ресурси. Тя включва комплекс от взаимосвързани дейности и мерки, насочени към защита на физическите и информационните активи, хората, финансовите средства, както и материалната и интелектуалната собственост на организацията. Важен аспект е осигуряването на условия за непрекъсваемо функциониране и постигане на

целите на фирмата чрез изграждане на подходящи механизми за охрана, разследване и предотвратяване на заплахи.

У нас понятието „фирмена сигурност“ често се ограничава до практически действия само по техническата и физическата охрана на фирмите. Има причини за това – преди всичко значително по – малкия мащаб на дейности на самите фирми, а от там и ограничените задачи на собствените фирмени системи за сигурност, ако такива са създадени. Сега за тях не е приоритет противодействието на чужди корпоративни разузнавания, свързани с кражба на научни и технологични секрети и „ноу-хау“ на наши водещи фирми [21].

Комплексното решаване на въпроса за фирмената сигурност провокира необходимостта от анализиране и на корпоративна сигурност, което означава, че обективно отделното предприятие не би могло да се предпази самостоятелно от всички елементи на риска [9].

Фирмената и корпоративната сигурност се отличават по своите цели, мащаб и подходи, въпреки че и двете концепции са свързани със защитата на ресурси и устойчивото функциониране на бизнес субекти. Основните разлики могат да се обобщят, както следва:

I. Мащаб и обхват:

— **Фирмена сигурност:** Фокусира се върху конкретна компания или предприятие. Основно се занимава с физическа охрана, информационна сигурност, защита на активите и управление на риска, специфични за дадена организация.

— **Корпоративна сигурност:** Отнася се до стратегическата защита на големи корпорации, често с многообразие от бизнес единици, глобално присъствие и сложни структури. Тук се разглеждат въпроси, като защита на критична инфраструктура и стратегически интереси, с поглед върху националната сигурност и глобалните икономически рискове.

II. Цели:

— **Фирмена сигурност:** Основната ѝ цел е оперативната защита – предотвратяване на заплахи, минимизиране на загуби и гарантиране на нормалното протичане на бизнес процесите.

— **Корпоративна сигурност:** Придобива по-стратегически характер, с акцент върху защитата на репутацията, иновациите, интелектуалната собственост и поддържането на дългосрочна устойчивост на компанията.

III. Методи и подходи:

— **Фирмена сигурност:** Използва локални мерки и процеси като охрана, контрол на достъпа и оперативен анализ на риска.

— **Корпоративна сигурност:** Разчита на координация между различни бизнес единици, стратегическо планиране, управление на сложни мрежи от доставчици и партньори, както и международно сътрудничество.

IV. Ролята в националната сигурност:

— **Фирмена сигурност:** Ориентирана към частния интерес на индивидуалните компании.

— **Корпоративна сигурност:** Счита се за критичен елемент от националната икономическа и инфраструктурна сигурност, особено когато се отнася до крупни бизнес структури, ангажирани с ключови индустрии или публични услуги.

Тези различия показват как фирмената сигурност се фокусира върху оперативни и локализирани мерки, докато корпоративната обхваща по-широк контекст, включващ стратегически и национални интереси [13].

През последните 20 години концепцията за корпоративна сигурност се е трансформирала значително в отговор на променящите се глобални, икономически и технологични предизвикателства. Преди вниманието е насочено към личната безопасност на собственика на бизнеса и имота. С течение на времето държавата започва да се занимава повече или по-малко с регулирането на икономическите процеси в страната и проблемите със сигурността преливат в равнината на икономиката.

Основни промени включват:

— **Разширяване на обхвата:** В миналото корпоративната сигурност е фокусирана главно върху физическата защита и предотвратяването на кражби или щети. Днес тя обхваща и киберсигурност, управление на данни, защита на интелектуалната собственост и съобразяване с правните и регулаторни изисквания.

— **Интеграция с бизнес стратегията:** Корпоративната сигурност вече не е отделна функция, а е интегрирана част от стратегическото управление. Това включва анализ на рисковете и планиране на реакциите при заплахи като част от дългосрочната устойчивост на организацията.

— **Технологична еволюция:** С развитието на технологиите, автоматизацията и цифровизацията, корпоративната сигурност се адаптира към новите предизвикателства, включително заплахите от киберпрестъпност и нуждата от сложни механизми за управление на информационната сигурност.

— **Международно сътрудничество:** С нарастващата глобализация компаниите все повече работят с международни партньори и прилагат стандарти като ISO 27001 за управление на сигурността, за да укрепят своите структури [18].

Заклучение

Корпоративната сигурност на предприятието“ (бизнес организацията) е състояние на защитеност на стабилното функциониране и корпоративните интереси на предприятието от потенциални и реални заплахи, постигнати чрез хармонизиране и взаимно свързване на неговите интереси в съответствие с интересите на субектите от вътрешната и външна среда.

Концепцията за корпоративна сигурност е претърпяла значителни промени през последните десетилетия, които показват нарастващата ѝ значимост

като стратегически елемент за устойчивостта и конкурентоспособността на организациите. Акцентът се е преместил от физическата защита на бизнеса към по-широкото управление на рисковете, включително киберсигурността и защита на интелектуалната собственост.

Това разширение на обхвата на корпоративната сигурност отразява технологичната еволюция, новите глобални икономически и политически рискове и необходимостта от интеграция на сигурността с дългосрочната стратегия на компанията. Въпросът за корпоративната сигурност е преминал към глобална перспектива, в която международното сътрудничество и съответствието с правни изисквания стават все по-важни. Тези промени показват как корпоративната сигурност е издигната до стратегическа функция, създаваща основата за устойчивост и конкурентоспособност на компаниите в съвременната динамична бизнес среда.

ЛИТЕРАТУРА

- [1] Асенов, Б., Теория на разузнаването и контрразузнаването. ВСУ „Черноризец Храбър“, Варна. 2008г.
- [2] Бахчеванов, Г., Система за национална сигурност.стр.346-359. В: Национална и международна сигурност
- [3] Бекярова, Н., Регионализъм. Регионална сигурност. стр.156-166. В: Национална и международна сигурност. Сборник, Военно издателство, София, 2005г., 520 стр.
- [4] Велков, С., Информационната сигурност на обществото – основа на държавната информационна политика
- [5] Зайнуллин С.Б., Сорокин Н.Д., Особенности корпоративной безопасности российских предприятий // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №6 (2017г.)
- [6] Казаков, К., Управление на системата за защита на националната сигурност. Информация и сигурност. Първо издание. София. 2016г.
- [7] Казанджиева-Йорданова, И., Доктрината too big to fail и мрежата за финансова сигурност
- [8] Митев, Бойко, Корпоративната сигурност – защита на всички активи, СЮ Media, 2011г.
- [9] Петров, А., Активна корпоративна сигурност. София, 2007г.
- [10] Слатински, Н., Измерения на сигурността, София, Издателство “Парадигма”, 2000г. стр. 20-21
- [11] https://www.me.government.bg/files/useruploads/files/nss_bul.pdf, Стратегия за национална сигурност на Република България, посетено на 20.11.2024г.
- [12] <https://institute.nvu.bg/sites/default/files/inline-files/2023-2-11-sidova.pdf>, Политическата сигурност като измерение на свободата от страх в контекста на човешката сигурност, посетено на 27.11.2024г.

- [13] <https://profisec.bg/50/firmena-sigurnost/>, Фирмена сигурност, посетено на 19.11.2024г.
- [14] https://europeanunion.europa.eu/index_bg, Вашите права на социална сигурност в България, посетено на 20.11.2024г.
- [15] <https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52021IP0286>, Резолюция на Европейския парламент от 10 юни 2021 г. относно стратегията на ЕС за киберсигурност за цифровото десетилетие (2021/2568(RSP)), посетено на 22.11.2024г.
- [16] <https://www.scientificatlas.com/article/lichnostni-vazpriyatiya-za-nesigurnost>, посетено на 22.11.2024г.
- [17] <https://ageconomy.wordpress.com/wp-content/uploads/2014/08/ikonomika-na-predpriatiето.pdf>, посетено на 24.11.2024г.
- [18] <https://geopolitica.eu/ekip/1110>, Корпоративната сигурност като елемент на системата за национална сигурност, посетено на 25.11.2024г.
- [19] <https://ebox.nbu.bg/sec16/pdf/66.pdf>, Логистика на корпоративната сигурност, посетено на 25.11.2024г.
- [20] Методиева, Ц., „Корпоративната сигурност и нейните компоненти“. Годишник на Шуменския университет „Епископ Константин Преславски“, с. 338-341, ISSN 1311-834X, 2020 г.
- [21] Методиева Ц, ”Национална и корпоративна сигурност”, НК с международно участие „МАТТЕХ 2018“, ШУ ”Епископ Константин Преславски”, 25-27 октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018
- [22] Simeonova, I., Metodieva, TS., Model for administrative security management in a municipality, Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 26, Shumen, 2024, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 93-105

СИГУРНОСТ И УЯЗВИМОСТИ В ТЕХНОЛОГИЯТА ZIGBEE

Даниел Р. Денев, Емили К. Димитрова

SECURITY AND VULNERABILITIES IN ZIGBEE TECHNOLOGY

Daniel R. Denev, Emili K. Dimitrova

ABSTRACT: *The ZigBee technology is a cornerstone of automation in smart homes due to its affordability and flexibility. However, its widespread use reveals significant security vulnerabilities, such as key distribution issues, ineffective frame counters, and susceptibility to data manipulation or eavesdropping. This paper explores these vulnerabilities and proposes an innovative architecture that replaces standard key distribution with session-specific keys, verified through cryptographic hash functions. The suggested improvements reduce the risk of network compromise and enhance device security. These measures are applicable not only to residential applications but also to industrial environments where security is crucial.*

KEYWORDS: *cryptographic hash functions, key management, network vulnerabilities, smart home security, ZigBee*

DOI: <https://doi.org/10.46687/YT24EMI>

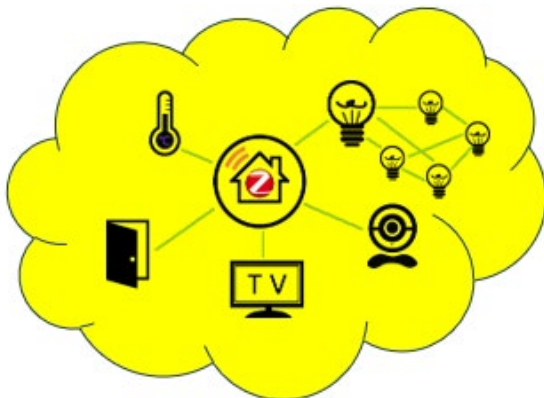
Въведение

С развитието на технологиите за автоматизация и свързаност на устройствата, технологията ZigBee се утвърди като ключов компонент в интелигентните домове. Нейната ниска цена, надеждност и гъвкавост я правят привлекателна за широк спектър от приложения. Въпреки това, широкото ѝ използване разкрива значителни уязвимости в сигурността, които могат да застрашат не само поверителността на потребителите, но и стабилността на свързаните мрежи. Разглеждането на тези уязвимости и предлагането на решения за тяхното преодоляване е от критично значение за постигането на устойчиви и защитени мрежи. Настоящият текст разглежда както общите рискове, свързани със ZigBee, така и иновативна архитектура за сигурност, която минимизира заплахите и повишава защитата на устройствата и комуникациите. [1, 10]

За да се повиши сигурността на ZigBee мрежите, е необходимо внедряването на усъвършенствани механизми за криптиране и автентикация, които да предотвратяват неоторизиран достъп и атаки от типа "човек в средата". Освен това, регулярното актуализиране на фърмуера на устройствата и мониторингът на мрежовия трафик могат да спомогнат за ранното откриване на подозрителна активност. В комбинация с добри практики за конфигурация, като например уникални идентификатори и използване на силни пароли, тези мерки

ще гарантират по-голяма устойчивост на мрежите и ще осигурят безопасна среда за интелигентните домове.

Също така, разработването на стандартизирани протоколи за сигурност и сътрудничеството между производителите на устройства могат значително да подобрят защитата на ZigBee мрежите.



Фиг. 1. *Обща представа на Zigbee мрежа*

Сигурност и уязвимости в технологията ZigBee

Интернет пространството може да бъде разделено на три основни слоя, които се различават по степента на достъпност и предназначение на съдържанието. Видимата мрежа включва публично достъпни и индексирани уебсайтове, които лесно се откриват чрез търсачки като Google и Bing. Това е най-често използваната част от интернет, но тя представлява малка част от цялото съдържание. Дълбоката мрежа обхваща страници, които не са индексирани от търсачките и са достъпни само чрез директни линкове или с използване на пароли. В нея се съдържат академични бази данни, вътрешни корпоративни системи и частни форуми. Тъмната мрежа е подмножество на дълбоката мрежа, която използва криптирани протоколи като Tor и I2P, за да осигури анонимност и защита на потребителите. Въпреки че е създадена за законни цели, тъмната мрежа често се свързва с незаконни дейности като хакерски атаки, нелегална търговия и кибершпионаж. Разделението на тези слоеве подчертава разнообразието на интернет пространството и необходимостта от подходящи технологии за сигурност и защита на данните.[4, 5]

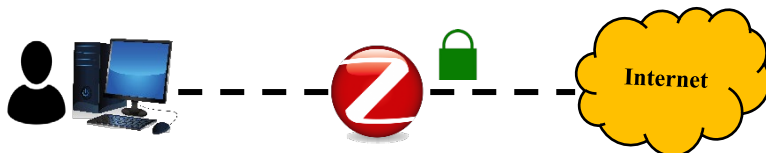
Технологията ZigBee е ключова за автоматизацията в интелигентните домове, предлагайки ниска цена и висока ефективност, но същевременно е уязвима към редица атаки, които застрашават сигурността на свързаните устройства. Основните уязвимости на ZigBee са:

- Разпределение на ключовете – Често всички устройства в мрежата споделят един и същ ключ, което означава, че компрометирането на един възел

излага на риск цялата система. За подобряване на сигурността се препоръчва използването на индивидуални идентификатори и еднократни ключове. [6]

— Брояч на кадри – Използва се за защита от атаки чрез повторение, но е недостатъчно ефективен. По-добра алтернатива са времеви етикети или произволни стойности за еднократна употреба.

— Подслушване и манипулация на данни – Нискобюджетни устройства като RZUSB могат да бъдат използвани за извличане на чувствителна информация или инжектиране на зловердни данни.



Фиг. 2. Сигурност в ZigBee мрежа

За да се противодейства на тези заплахи, е необходимо внедряване на подходящи криптографски методи, като динамични ключове и надеждни процедури за управление на сигурността. Освен това, включването на нови механизми за откриване на атаки, базирани на аномалии в поведението на устройствата, може да подобри устойчивостта на системите в интелигентните домове. Това ще осигури защита срещу различни видове атаки и ще гарантира дългосрочна сигурност и ефективност на ZigBee технологиите. [2]

Подобрена архитектура за управление на сигурността в мрежи с технология ZigBee

Предложената архитектура въвежда иновативен подход към управлението на сигурността, като заменя стандартното разпределение на ключовете с временни ключове, които са валидни само за една сесия. Този метод значително намалява риска от компрометиране на мрежата, тъй като компрометирането на един възел не предоставя достъп до останалите възли или информация в мрежата. Всеки временен ключ се генерира динамично и се използва само за определена комуникационна сесия, след което става невалиден.

За да се постигне още по-висока степен на сигурност, архитектурата включва надеждни центрове за управление, които действат като главен координиращ орган за всички устройства в мрежата. Тези центрове генерират и разпространяват временните ключове, като осигуряват тяхната уникалност и валидност само за конкретна сесия. За допълнителна защита, идентификацията на устройствата се извършва чрез хеш функции. Тези функции създават уникални подписи за всяко устройство, които не могат да бъдат подправени или манипулирани. Тази процедура елиминира риска от неоторизиран достъп и осигурява защитена комуникация.[7, 8]

Хеш функциите се използват за верификация на устройствата, като създават уникални криптографски стойности на база на идентификационните номера и временните ключове. Тази информация се проверява от надеждния

център, който потвърждава легитимността на устройството. Дори при загуба или кражба на устройство, достъпът до мрежата може да бъде бързо и ефективно прекъснат, като се нулират съществуващите ключове. [9]

Архитектурата е проектирана така, че да ограничи уязвимостите, свързани със стандартните методи за разпределение на ключове. Ключовите предимства на предложението включват:

- Елиминиране на риска от компрометиране на всички устройства чрез един компрометиран ключ.
- Динамично генериране на временни ключове за всяка сесия.
- Въвеждане на надеждни центрове за управление за координация и защита.
- Използване на криптографски хеш функции за уникална идентификация на устройствата.
- Възможност за бързо анулиране на достъпа при загуба или компрометиране на устройство.

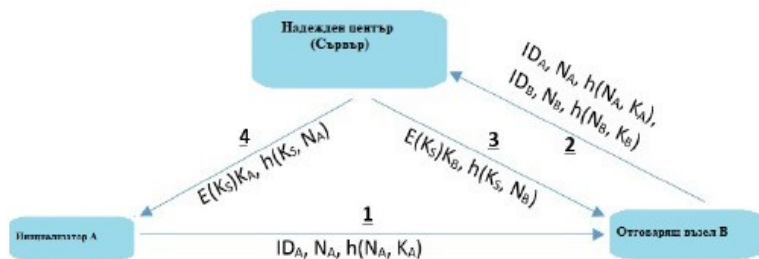
Тези подобрения правят архитектурата подходяща за използване не само в интелигентни домове, но и в индустриални приложения, където сигурността е от съществено значение. [3]

Таблица 1. *Процес на управление на ключове*

Етап	Действие	Роля на надеждния център
Генериране на ключ	Създаване на временен ключ за всяка сесия	Уникалност и валидност на ключа
Разпространение	Изпращане на временния ключ до устройствата	Координация и сигурност
Анулиране	Нулиране на ключовете при загуба или компрометиране	Бърза реакция за защита на мрежата



Фиг. 3. *Сценарий за създаване на Свързващи ключове*



Фиг. 4. Предложение за подобряване на защитата

Пример: Да се изчисли общия брой временни ключове, необходими за един месец в система с даден брой устройства

Примерни данни:

Брой устройства (N): 100.

Средна продължителност на сесията (T): 1 час.

Период за изчисление (P): 30 дни (720 часа).

$$\text{Брой ключове} = N \times \frac{P}{T} \quad (1)$$

$$\text{Брой ключове} = 100 \times \frac{720}{1} = 100 \times 720 = 72000 \quad (2)$$

Резултат:

За мрежа от 100 устройства, в която всяко устройство изисква нов временен ключ за всяка сесия с продължителност 1 час, ще са необходими 72,000 временни ключа за един месец.

Ако добавим криптографски изисквания или времето за генериране на един ключ, можем да оценим допълнително натоварването върху системата.

Заклучение

Технологията ZigBee, въпреки своите предимства, изисква специално внимание към сигурността, за да отговори на съвременните изисквания за защита. Анализът на нейните уязвимости, като разпределение на ключовете, броячите на кадри и подслушването на данни, подчертава необходимостта от внедряването на усъвършенствани решения. Предложената архитектура с временни ключове и надеждни центрове за управление осигурява значителни подобрения в защитата, като предлага динамично управление на достъпа и криптографски защити за всяко устройство. Тези подходи не само елиминират риска от компрометиране на мрежата, но и я правят подходяща за индустриални приложения, където изискванията за сигурност са още по-високи. Изграждането на такива защитени системи е ключът към постигането на устойчивост и доверие в технологиите на бъдещето.

ЛИТЕРАТУРА

- [1] Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020, ISBN: 978-1119642787.
- [2] 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.
- [3] Konstantinova E., Karadocheva M., Tsankov Ts. The invisible Internet and cyber security. International Scientific Conference 2019, “Vasil Levski” National Military University, Faculty “Artillery, Aircraft Defense and CIS”, Shumen, 2019, ISSN 2367-7902, pp. 519-524.
- [4] Konstantinova E., Tsankov Ts. Analyzing security threats in smart homes technology. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 373-378.
- [5] Lilov V., Konstantinova E., Tsankov Ts. Cyber intelligence in protecting organizations from malicious activity. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 386-392.
- [6] Microsoft Security Intelligence Report. Threat Intelligence Report, Volume 23, 2019, Microsoft Corporation.
- [7] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996, ISBN: 978-1119096726.
- [8] Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2017, ISBN: 978-0134444284.
- [9] Tor Project. The Onion Router – Technical Overview and Use Cases. Available online at www.torproject.org.
- [10] ZigBee Alliance. ZigBee Specification. ZigBee Alliance, 2021, available online at www.zigbee.org.

ОЦЕНКА ТЕХНИЧЕСКОТО СЪСТОЯНИЕ НА ЖИРОСКОПИЧНИ ИЗМЕРВАТЕЛНИ СРЕДСТВА

Андрей И. Богданов

AN ASSESSMENT OF THE GYROSCOPE MEASUREMENT SYSTEM TECHNICAL CONDITION

Andrey I. Bogdanov

ABSTRACT: *Vibration loadings occur during the work of the gyroscope measuring systems pertaining to pilotless flying machines. This is the reason for accuracy disturbance. The routine checks don't control the influence of the vibration loading, which prevents from giving real information about the measuring systems condition. Our investigation offers a method for an assessment of the gyroscope measuring systems technical conditions by the vibrations of the high-speed bearings.*

KEYWORDS: *gyroscope measuring system, vibration loading*

DOI: <https://doi.org/10.46687/YT24ABG>

Увод

Анализа на грешките и проверките извършвани на жирокопичните измервателни средства позволява да се прогнозира техническото състояние на системата за управление полета на безпилотните летателни апарати. Основен фактор влияещ върху точността на измерваните ъглови отклонения са вибрациите в окачването на чувствителния елемент (жирокопа). Те се използват като обобщен параметър, характеризиращ износването в точките на окачване и стареене на уплътнителните и смазващи вещества в лагерните групи.

Същинска част

Целта на изследването е да се предложи обобщен подход за оценка техническото състояние на жирокопични измервателни средства с изтекъл срок на техническа годност, по измереното ниво на вибрациите в точките на окачване на чувствителният елемент.

В изпълнение на поставената цел се прилагат способите за дефектация на роторни механични системи по спектъра на колебателния процес. Те се основават на факторите: вибрациите се явяват естествено явление съпътстващо работата на чувствителният елемент, а конструктивните характеристики от факта, че не е възможно да се изработи такъв вид механична система без наличието на дисипативни натоварвания [1, 2]. Това налага да се анализират тези фактори, като допустими за работата на жирокопичните измервателни средства. Промяна на техния спектър в условията на експлоатация на безпилотните летателни апарати,

води до увеличаване грешката и са източник на механични неизправности в отделните възли на уредите.

Оценката на техническото състояние на жирокопичните измервателни средства се свежда до определяне на границата на изменение на диагностичните признаци, до която уредът може да се класифицира с едно е също състояние. Практическата допустима гранична норма за такъв вид уреди е 6dB [3, 4]. Прилага се препоръка № 2372/74г. по ISO, съгласно която машините и механизмите се класифицират в шест групи. Методиката на експерименталните изследвания включва чувствителния елемент (жиродвигателя), електродвигателя на програмния механизъм и за заключване и редукторите осигуряващи движението на двата механизма

Техническото състояние на отделните механизмите се класифицират в четири класа:

- A. добро;
- B. удовлетворително;
- C. допустимо(необходим ремонт)
- D. недопустимо.

Измерванията се извършват в характерни точки в три взаимноперпендикулярни равнини.

Плътноста на вероятностите на измерените случайни величини за всеки параметър и при събитие C не излиза от интервала . Прилага се теоремата за умножение на вероятностите и се получава зависимостта [1].

$$f_u(u/C)P(C) = f_u(u)P(C/a), \quad (1)$$

където:

$$P(C/a) = \left\{ \frac{1}{2} \left[\Phi \left(\frac{u+\varepsilon}{\sigma_x} \right) - \Phi \left(\frac{u-\varepsilon}{\sigma_x} \right) \right] \right\}^n, \quad (2)$$

$$P(C) = \int_{-\infty}^{\infty} P(c/u) f_u(u) du. \quad (3)$$

Замества се с (2) и (3) в (1) и се получава:

$$f_u(u/C) = \frac{\left\{ \frac{1}{2} \left[\Phi \left(\frac{u+\varepsilon}{\sigma_x} \right) - \Phi \left(\frac{u-\varepsilon}{\sigma_x} \right) \right] \right\}^n f_u(u)}{\int_{-\infty}^{\infty} f_u(u) \left\{ \frac{1}{2} \left[\Phi \left(\frac{u+\varepsilon}{\sigma_x} \right) - \Phi \left(\frac{u-\varepsilon}{\sigma_x} \right) \right] \right\}^n du}. \quad (4)$$

Като се интегрира последния израз по u от $u - \varepsilon$ до $u + \varepsilon$ се получава търсената вероятност α_1 .

$$\alpha_1 = 1 - \frac{\int_{u-\varepsilon}^{u+\varepsilon} f_u(u) \left\{ \frac{1}{2} \left[\Phi \left(\frac{u+\varepsilon}{\sigma_x} \right) - \Phi \left(\frac{u-\varepsilon}{\sigma_x} \right) \right] \right\}^n du}{\int_{-\infty}^{\infty} f_u(u) \left\{ \frac{1}{2} \left[\Phi \left(\frac{u+\varepsilon}{\sigma_x} \right) - \Phi \left(\frac{u-\varepsilon}{\sigma_x} \right) \right] \right\}^n du} \quad (5)$$

Полученият израз позволява да се изследва вероятността α_1 да се оцени уреда като некачествен или качествен при брой изпитвания n и широчина на контролния интервал ε . За окончателен рационален избор на тези величини е

необходимо да се отчете и значението на вероятността β_1 , за това качествено уред да бъде признат за некачествен.

В приетия подход за прогнозиране на техническото състояние на жирокопичното измервателно средство е използвана класическата процедура на статистическия анализ. Обработката на получените резултати се извършва чрез пълните вероятностни характеристики на грешките с отчитане на процесите на стареене и износване. Приетия модел се базира на случайния процес от вида [1]:

$$y_i(t) = \sum_{j=0}^m a_{ij} \phi_j(t), \quad i = \overline{0, n} \quad (6)$$

където a_{ij} е случайна величина;

$\{\phi_i(t)\}_{j=0}^m$ е непрекъснато детерминирана функция на времето.

Такова решаване на задачата за прогнозиране техническото състояние на жирокопичните измервателни средства се извършва при априори известна структура на зависимостта, а свойствата на грешката при измерване $\varepsilon(t)$ се описва с помощта на вероятностното неравенство от типа:

$$P[|\varepsilon(t)| \leq \Delta t] \geq P_0, \quad t \in T_p \subset T \quad (7)$$

където Δt е зададена функция;

T_p - продължителност на интервала на наблюдение;

T е продължителността на гаранционния период за работа на жирокопичните измервателни средства.

Метод за прогнозиране техническото състояние, пригоден за използване в условията на ограниченост на изходните данни се построява на основата на минимаксното оценяване. Принципа на минимакса, т. е. разчет на най-добрия случай в сравнение с приетия в класическата статистика принцип на минимизация на средния риск позволява да се реши задачата без проверка на хипотези за стохастическите свойства на прогнозируемия процес и пълно използване на зададената изходна информация.

Оценките за техническото състояние на жирокопичните измервателни средства контролиращи програмата и стабилизацията на безпилотните летателни апарати по два канала са показани на фиг. 1 и фиг.2:

В случай, че нивата на вибрациите се намират в зона А или В за отделните механизми изграждащи жирокопичното измервателно средство може да бъде удължен срока за техническа годност. При ниво на вибрациите в зона С се препоръчва снемане от експлоатация, тъй като за тези измервателни средства не се предвижда извършване на регулировъчни и ремонтни дейности.

Заклучение

Предложената оценка дава възможност да се анализира техническото състояние на жирокопични измервателни средства с изтекъл срок на техническа годност. Предимство на предложения подход е оценката на фактическото състояние на жирокопичните измервателни средства и вземане на обосновано решение за снемане от използване по предназначение и подмяна с ново от запаса. По този начин се гарантира безопасността на техническия състав, пряко

ангажиран с експлоатацията на безпилотните летателни апарати. Резултатите от изследването могат да се използват както за оценка техническото състояние на жирокопите за направление от системата за управление полета на безпилотните летателни апарати така и при вземане на решение за удължаване срока на тяхната експлоатация.

Lv			
dB			
140		D	
130	D	C	D
120	C		C
	B		
110		B	B
100	A	A	A
90			
80			
70			
	I	II	III
60	ЖИРОКОПИЧЕН ХОРИЗОНТ		

Фиг. 1. Оценка техническото състоянието на жирокопичен хоризонт

Lv			
dB			
140		D	
130	D	C	D
120	C		C
110	B		
		B	B
100	A	A	A
90			
80			
70			
	I	II	III
60	ЖИРОКОПИЧЕН ВЕРТИКАНТ		

Фиг. 2. Оценка техническото състоянието на жирокопичен вертикант

ЛИТЕРАТУРА

- [1] Ковалев М. П., Опоры и подвесы гироскопических устройств Машиностроение, Москва, 1972.
- [2] Петренко В. Е., Башов А.И., Исследование осевой жесткости роторной системы с неидеальными подшипниками, Механика гироскопических систем, вып.2 стр. 82-89, 2013.
- [3] Минчев Н., Григоров В., Вибродиагностика на ротационни и бутални машини, Техника, София, 2008.
- [4] Derritron – Portable Vibration Analyzer, London 1998,
- [5] ISO 1925: 1990, Mechanical Vibrations – Balancing – Vocabulary
- [6] ISO 1940/2 – 1997(E) Mechanical Vibrations – Balance Quality Requirements of Rigid Rotors.

ВНЕДРЯВАНЕ НА ИНТЕЛИГЕНТНИ КОМУТАТОРИ И ТЕХНОЛОГИИ В КОМУНИКАЦИОННИТЕ МРЕЖИ

Цветослав С. Цанков, Александра П. Дочева

IMPLEMENTING SMART SWITCHES AND TECHNOLOGIES IN COMMUNICATION NETWORKS

Tsvetoslav S. Tsankov, Aleksandra P. Docheva

ABSTRACT: *With the development of communication technologies and increasing demands on network infrastructures, the implementation of intelligent switches plays a key role in optimizing network traffic, security, and manageability. Smart switches are the foundation of modern communication networks, providing advanced network traffic management, security, and optimization features. This article analyzes the role of smart switches in modern network infrastructure, their main characteristics, advantages, and challenges, as well as examples of their application.*

KEYWORDS: *switches, modern communication networks, security*

DOI: <https://doi.org/10.46687/YT24CAL>

1. Въведение

Комуникационните мрежи са гръбнакът на съвременния цифров свят, свързвайки милиарди устройства и потребители. Нарастващият обем от данни, изискванията за ниска латентност и увеличаващата се сложност на мрежите налагат използването на нови технологии като интелигентни комутатори. Традиционните мрежови комутатори вече не отговарят на изискванията на бързо развиващите се комуникационни мрежи. С нарастващия обем данни, необходимостта от ниска латентност и адаптивност доведе до развитието на интелигентни комутатори, които комбинират хардуерна производителност с напреднали софтуерни функции.

2. Интелигентни комутатори в мрежовите технологии

Интелигентните комутатори са мрежови устройства, които предлагат разширени възможности за анализ, управление и автоматизация на мрежовите процеси. Те надграждат традиционните Layer 2 и Layer 3 функции с внедряване на интелигентни алгоритми, базирани на машинно обучение и изкуствен интелект. За разлика от стандартните комутатори, които изпълняват задачи според предварително зададени правила, интелигентните комутатори могат динамично да се адаптират към променящи се мрежови условия, като предоставят в реално време решения за оптимизация на трафика, разпределение на ресурси и идентифициране на аномалии. Това ги прави изключително подходящи за сложни

мрежови среди като облачни платформи, 5G инфраструктура и IoT екосистеми. Основни техни функции са:

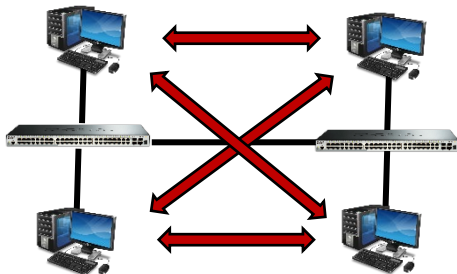
➤ **Динамично маршрутизиране:** Осигуряват ефективно управление на мрежовия трафик.

➤ **Сигурност:** Интегрирани модули за разпознаване и защита от атаки, като DDoS и зловреден софтуер. [1]

➤ **QoS (Quality of Service):** Приоритизират критичния трафик за по-добра производителност.

➤ **Мрежова виртуализация:** Поддръжка на VLAN, VXLAN и други технологии за сегментиране на трафика.

Интелигентните комутатори обединяват хардуерни и софтуерни иновации, за да осигурят максимална ефективност и сигурност. Сред ключовите функции са динамичното маршрутизиране, което позволява адаптивно насочване на трафика въз основа на текущото натоварване, както и автоматизираните механизми за мониторинг, които анализират мрежовите данни в реално време. Освен това те интегрират разширени функции за управление на качеството на услугата (QoS), които приоритизират критичния трафик, като видеоконференции и VoIP. Вградени системи за сигурност, като защитни стени и системи за откриване на проникване, позволяват на интелигентните комутатори да защитават мрежите срещу съвременни заплахи. Тези функции са поддържани от интерфейси за програмиране на приложения (API), които улесняват интеграцията с други мрежови системи и приложения.



Фиг. 1. Комутация между мултипортови устройства

3. Технологични иновации в интелигентните комутатори

С развитието на технологиите интелигентните комутатори се превръщат в ключов компонент за модернизирването на мрежовите инфраструктури. Техният напредък е тясно свързан с интеграцията на съвременни софтуерни и хардуерни решения, които позволяват по-добра адаптивност, ефективност и сигурност. Тази част от статията разглежда основните технологии, които стоят зад интелигентните комутатори, както и тяхното приложение в мрежовите среди. Чрез използването на иновации като изкуствен интелект, софтуерно дефинирани мрежи и автоматизация, тези устройства променят начина, по който се управляват и използват мрежите. [2]

➤Изкуствен интелект и машинно обучение (AI/ML)

Интелигентните комутатори използват AI/ML за предсказване на мрежови претоварвания и адаптиране към промените в реално време. Изкуственият интелект и машинното обучение играят основна роля в трансформацията на интелигентните комутатори. Те позволяват анализ в реално време на големи обеми данни, идентифициране на аномалии и прогнозиране на потенциални проблеми. Чрез внедряването на AI/ML алгоритми, комутаторите могат автоматично да адаптират мрежовите ресурси, да идентифицират неефективности и да предложат оптимални решения. Това значително подобрява производителността и минимизира времето за реакция при възникване на проблеми.

➤Софтуерно дефинирани мрежи (SDN)

Интеграцията на SDN технологии позволява централизирано управление и гъвкавост в мрежовата архитектура. Софтуерно дефинираните мрежи позволяват централизирано управление на мрежовата инфраструктура чрез отделяне на управлението от хардуера. Интелигентните комутатори, интегрирани в SDN среда, предлагат гъвкавост и възможност за динамична конфигурация на мрежовите параметри. Това означава, че администраторите могат бързо да внедряват нови услуги, да адаптират мрежовите политики и да оптимизират използването на ресурси в отговор на променящите се нужди на мрежата.

➤Автоматизация и оркестрация

Интелигентните комутатори автоматизират задачи като конфигуриране на портове, мониторинг на трафика и идентифициране на аномалии. Автоматизацията и оркестрацията са ключови за модерните мрежови инфраструктури, като значително намаляват необходимостта от ръчна намеса. Интелигентните комутатори използват автоматизирани процеси за конфигурация, наблюдение и управление на мрежата. Оркестрацията, от своя страна, позволява координиране на различни мрежови устройства и приложения, осигурявайки безпроблемно функциониране на цялата система. Това е особено важно в сложни среди като центрове за данни и облачни инфраструктури, където ефективното управление на ресурсите е от критично значение.

4. Функционални предимства на интелигентните комутатори в съвременните мрежови архитектури

Основно интелигентните комутатори предоставят ефективност на мрежата чрез която оптимизират използването на ресурси и минимизират латентността. Гъвкавостта лесно се адаптира към различни приложения като IoT, 5G и облачни услуги. Сигурността интегрира механизми за защита предотвратяващи заплахи в реално време. Дори намалянето на оперативните разходи чрез автоматизация дови до по-добро управление.

➤В корпоративни мрежи

Интелигентните комутатори играят ключова роля в корпоративните мрежи, предоставяйки възможности за управление на сложни инфраструктури. Те позволяват оптимизиране на мрежовия трафик, приоритизиране на критични приложения и засилване на сигурността чрез откриване и предотвратяване на

кибератаки. Освен това, благодарение на тяхната способност за автоматизация, те значително намаляват натоварването върху ИТ отделите. [7]

➤ В центрове за данни

В центровете за данни интелигентните комутатори се използват за управление на големи обеми от трафик и осигуряване на надеждност и мащабируемост. Те подпомагат динамичното разпределение на ресурси и минимизират латентността, като гарантират непрекъсната работа на критични приложения. Чрез интеграция с SDN решения те осигуряват централизиран контрол и по-добро използване на хардуерните ресурси. [8]

➤ В IoT и 5G мрежи

С нарастващото използване на IoT устройства и развитието на 5G мрежите интелигентните комутатори стават незаменими за осигуряване на висока производителност и сигурност. Те позволяват управление на огромен брой свързани устройства, като предоставят ниска латентност и адаптивност към променящите се условия. Тези комутатори също така осигуряват високо ниво на сигурност, което е критично за IoT екосистемите чрез Zigbee и Z-wave протоколи. [3, 4]

Таблица 1. Функционални параметри и показатели на интелигентни комутатори

Функция	Параметър	Стойност
Ефективност	Намаляване на латентността	До 50%
	Повишаване на пропускателната способност	До 30%
Гъвкавост	Поддръжка на IoT устройства	До 10,000 устройства
	Скорост на данни (5G мрежи)	До 100 Gbps
Сигурност	Разпознаване на киберзаплахи	99,9% в реално време
	Намаляване на инцидентите	До 40%
Намаляване на разходите	Намаляване на оперативните разходи	До 25%
	Повишаване на ефективността на ИТ екипа	До 35%

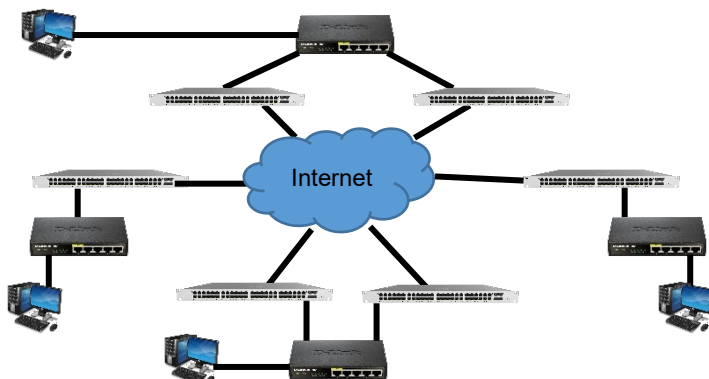
5. Внедряване на интелигентни комутатори чрез практически примери

Внедряването на интелигентни комутатори в различни мрежови инфраструктури предоставя редица предимства, като подобрена производителност, повишена сигурност и гъвкавост при управление на трафика. Тези устройства използват иновационни технологии за динамично разпределение на ресурсите и мониторинг в реално време, което е особено важно в области с високи изисквания за надеждност и ефективност. Следващите примери разглеждат конкретни приложения на интелигентни комутатори в различни индустриални сектори, като показват как тяхното внедряване води до

оптимизация на мрежовите операции и подобряване на цялостната инфраструктура.

➤ **Пример 1:** Управление на корпоративна мрежа в голяма финансова институция

Голяма финансова институция внедрява интелигентни комутатори за управление на своята мрежова инфраструктура. С помощта на тези устройства банката успява да постигне висока надеждност и оптимизация на мрежовия трафик, като приоритизира критични операции като онлайн банкиране и трансакции. Интелигентните комутатори предоставят разширени функции за мониторинг и идентифициране на киберзаплахи, като позволяват на институцията да реагира бързо на потенциални инциденти. [5]



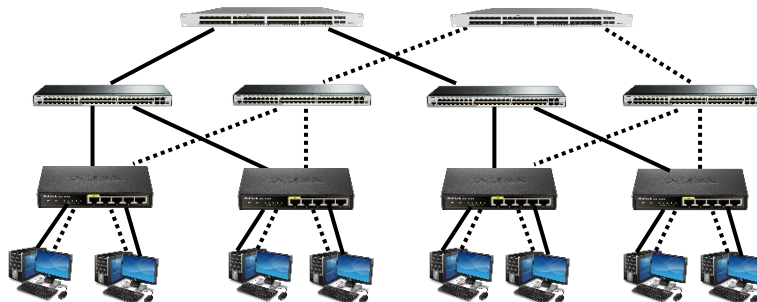
Фиг. 2. Архитектура на корпоративна мрежа с интелигентни комутатори

➤ **Пример 2:** Подобряване на производителността в център за данни

Голям доставчик на облачни услуги внедрява интелигентни комутатори в своя център за данни. Те позволяват динамично разпределение на мрежовите ресурси в зависимост от натоварването и изискванията на клиентите. Комутаторите, интегрирани със SDN решения, гарантират минимална латентност и висока производителност, като осигуряват надеждна работа на критични приложения като бази данни и виртуални машини. [6]

➤ **Пример 3:** Управление на IoT инфраструктура в интелигентен град

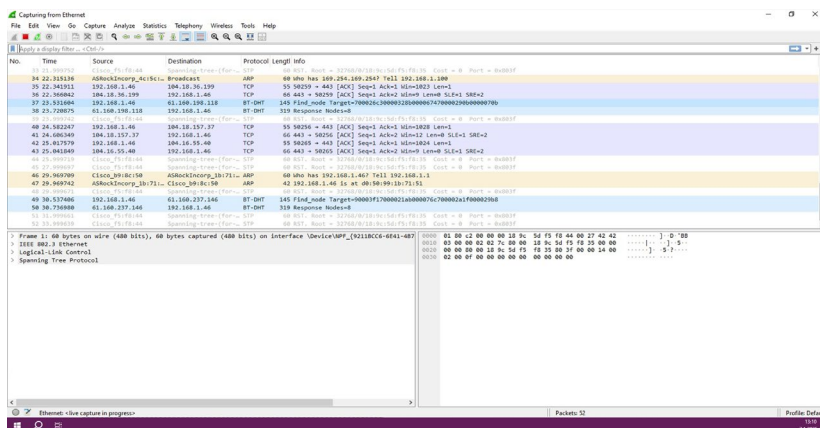
В интелигентен град, където се използват хиляди IoT устройства за управление на осветление, трафик и сигурност, интелигентните комутатори играят ключова роля. Те осигуряват ефективно управление на мрежовия трафик и сигурност, като предотвратяват неоторизиран достъп до чувствителни данни. Освен това, автоматизираните функции позволяват бърза реакция на мрежови проблеми, което допринася за непрекъснатата работа на градската инфраструктура.



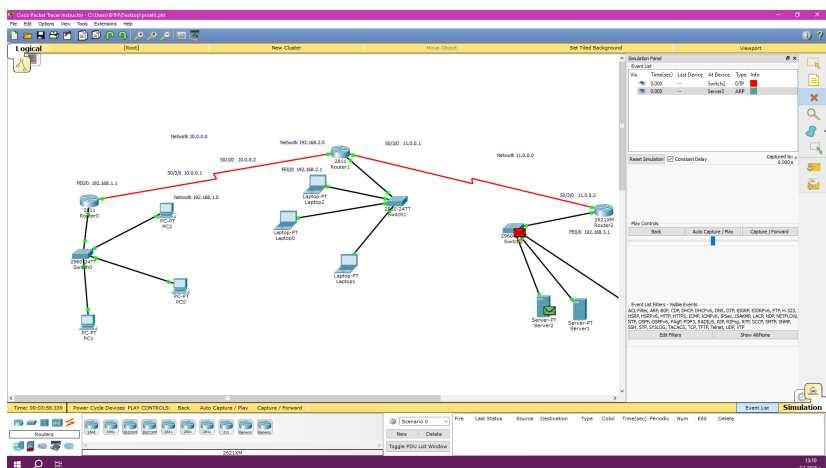
Фиг. 3. Архитектура на център за данни сформирана с интелигентни комутатори

6. Инструменти за управление и анализ на интелигентни комутатори

Интеграцията на интелигентни комутатори в съвременните мрежови архитектури предоставя значителни предимства в управляемостта, сигурността и ефективността на трафика. Чрез симулации с инструменти като Cisco Packet Tracer могат да се изследват сложни сценарии, включващи VLAN сегментация, динамично маршрутизиране и внедряване на политики за качество на услугата (QoS). В същото време Wireshark позволява детайлен анализ на мрежовите пакети, като предоставя данни за идентифициране на латентност, загуба на пакети и неправилно конфигурирани протоколи. Комбинирането на тези технологии улеснява изграждането на високопроизводителни мрежи и оптимизацията им за бъдещи натоварвания, което подчертава тяхната критична роля в мрежовото инженерство.[9, 10]



Фиг. 4. Инструмент за анализ на данни – Wireshark



Фиг. 5. Инструмент за симулация на сложни сценарии – Cisco Packet Tracer

7. Заключение

Развитието на мрежовите технологии е тясно свързано с внедряването на интелигентни комутатори, които осигуряват значителни функционални предимства в съвременните мрежови архитектури. Тези устройства не само подобряват производителността и ефективността на мрежите, но и предоставят възможности за интеграция на иновативни технологии, като автоматизация, динамично управление и анализ в реално време. С развитието на AI, SDN и автоматизацията, тяхното значение ще продължи да нараства, правейки ги неотменима част от всяка модерна мрежова архитектура. Прегледът на технологичните иновации и функционалните предимства на интелигентните комутатори показва тяхната ключова роля за оптимизацията на мрежовите процеси и адаптацията към нарастващите изисквания на дигиталната трансформация. Практическите примери за внедряване и използването на съвременни инструменти за управление и анализ потвърждават тяхната ефективност и гъвкавост. В заключение, интелигентните комутатори представляват стратегически елемент за модернизиране на мрежовите инфраструктури, като съчетават висока функционалност, надеждност и иновации. Това ги прави основен двигател за създаването на стабилни, мащабируеми и ефективни мрежови среди, подходящи за нуждите на съвременните организации.

ЛИТЕРАТУРА

- [1] Denev D., Konstantinova E., Ismail T., Cybersecurity – International and National Dimensions, 2019, Cadet-Students Scientific Conference, Collection of

- Papers, National Military University „Vasil Levski“, Veliko Tarnovo, ISSN 2367-7481, pp. 300-310.
- [2] Denev D., Konstantinova E., Main Issues in the Protection of Information in the system of National and Corporate Security, 2020, Conference with international participation MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 110-115.
 - [3] Denev D., Z-WAVE Communication for Home Automation, 2020, Conference with international participation MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 96-103.
 - [4] Denev D., Terziev H., Zigbee Communication Protocols and Their use to Manage Smart Devices, 2020, Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of technical sciences, ISSN 1311-834X, pp. 83-89.
 - [5] Denev D., Low Energy Real-Time Routing, 2022, Annual University Scientific Conference, Proceedings of National Military University „Vasil Levski“, Veliko Tarnovo, 2022, ISSN 2367-7481, pp. 1267-1276.
 - [6] Denev D., Tsankov Ts., Communication-Based Dynamic Packet Optimization for Visual PLC Monitoring, 2022, Annual University Scientific Conference, Proceedings of National Military University „Vasil Levski“, Veliko Tarnovo, ISSN 2367-7481, pp. 1259-1266.
 - [7] Denev D., Tsankov Ts., A Survey of Data Quality and Processing of Information in Innovative Smart Devices, 2022, International Conference Automatics and Informatics (ICAI) 2022, <https://ieeexplore.ieee.org/>, Varna Bulgaria, 06-08 October, ISBN 978-1-6654-7625-6 and 10.1109/ICA155857.2022.9960040
 - [8] Denev D., Modeled Security in Communication Network Coding, 2022, Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, ISSN 1311-834X, pp. 153-161.
 - [9] Denev D., Surveillance with Wireshark and its Use in Communication Networks, 2023, Annual of Konstantin Preslavski University of Shumen, Volume XIII E, ISSN 1314-8818, pp. 104-109.
 - [10] Denev D., Tsankov Ts., Use of Cisco Packet Tracer in Evaluation of Communication Networks, 2023, XVI International Scientific Conference, Belovo, ISBN 978-5-00137-315-5 (item 1), ISBN 978-5- 00137-314-8, pp. 163-171.

СЪЗДАВАНЕ НА ЛОКАЛНА МРЕЖА С ИЗКУСТВЕН ИНТЕЛЕКТ

Стефан М. Казаков

CREATE LAN WITH AI

Stefan M. Kazakov

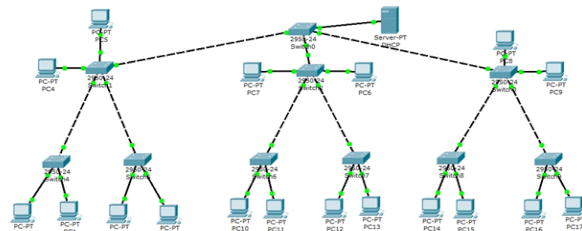
ABSTRACT: The advent of Artificial Intelligence (AI) has heralded a transformative era in technology, reshaping various sectors, including networking. This paper discusses the integration of AI in the design and management of Local Area Networks (LANs). By employing AI techniques such as machine learning, predictive analysis, and intelligent decision-making, organizations can enhance their network's efficiency, security, and scalability. It explores the fundamental concepts of LANs, the role of AI in optimizing network performance, and the implications of AI-driven LANs on organizational operations and security.

KEYWORDS: computer, LAN, network, AI, technology, design, security, integration

DOI: <https://doi.org/10.46687/YT24SMK>

Въведение

Локалните мрежи (LAN) (Фиг.1) са основни инфраструктури, които свързват компютри и устройства в рамките на ограничен географски район, като например офис сграда или предприятие. Тъй като организациите все повече разчитат на вземане на решения, базирани на данни, и взаимосвързани устройства, търсенето на ефективни, стабилни и сигурни LAN мрежи нарасна. На традиционните подходи за управление на мрежата често им липсва гъвкавостта, необходима за реагиране на динамични мрежови условия и заплахи за сигурността. Това ограничение представлява убедителен аргумент за интегрирането на AI технологии в дизайна и управлението на LAN.



Фиг. 1. Локална компютърна мрежа (LAN)

1. Разбиране на локалните мрежи.

1.1 Основни понятия и компоненти

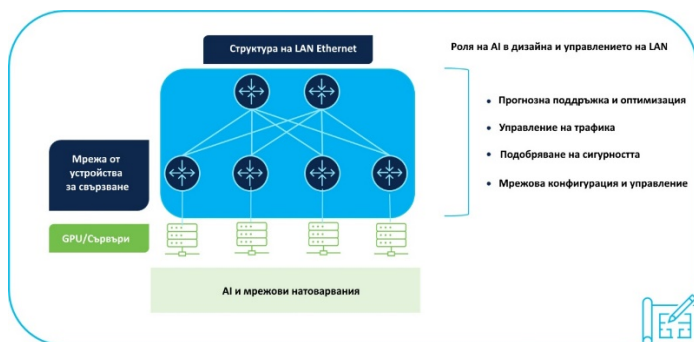
LAN е съвкупност от взаимосвързани устройства в ограничена зона. Типичните компоненти на LAN включват:

- Устройства: Компютри, принтери, сървъри и IoT устройства.
- Мрежов хардуер: комутатори, рутери, точки за достъп и окабеляване.
- Протоколи: Стандарти като Ethernet и Wi-Fi, които управляват предаването на данни.

1.2 Приложения на LAN

LAN обслужват различни цели, включително споделяне на ресурси (принтери, файлове), комуникация (имейл, незабавни съобщения) и достъп до интернет. Те са неразделна част от позволяването на сътрудничеството между потребителите и поддържането на различни бизнес приложения.

2. Роля на AI в дизайна и управлението на LAN



Фиг. 2. Интегриране на AI в управлението на LAN

Интегрирането на AI в управлението на LAN (Фиг. 2) въвежда няколко предимства и възможности, които могат да бъдат категоризирани, както следва:

2.1 Прогнозна поддръжка и оптимизация

AI алгоритмите могат да анализират исторически данни за ефективността от мрежата, за да предвидят модели на използване и потенциални повреди. Тази възможност за предвиждане позволява проактивни корекции за оптимизиране на разпределението на честотната лента и минимизиране на времето за престой.

2.2 Управление на трафика

AI може динамично да научава модели на трафик и да коригира протоколите за маршрутизиране в реално време, оптимизирайки пътищата за предаване на данни. Алгоритмите за машинно обучение могат да анализират потока от данни и да коригират настройките за качество на услугата (QoS), за да приоритизират критични приложения.

2.3 Подобряване на сигурността

Системите за сигурност, управлявани от AI, могат да откриват аномалии и потенциални заплахи в мрежовия трафик. Чрез използване на техники като системи за откриване на проникване (IDS) и поведенчески анализ, AI може да идентифицира опити за неоторизиран достъп и да реагира автоматично, като значително подобрява цялостната позиция на сигурност на LAN.

2.4 Мрежова конфигурация и управление

AI може да улесни интелигентната мрежова конфигурация чрез самооптимизиращи се алгоритми, които автоматично коригират настройките на устройството въз основа на анализ в реално време. Тази възможност намалява необходимостта от ръчна намеса и позволява по-бързо разгръщане на мрежовите ресурси.

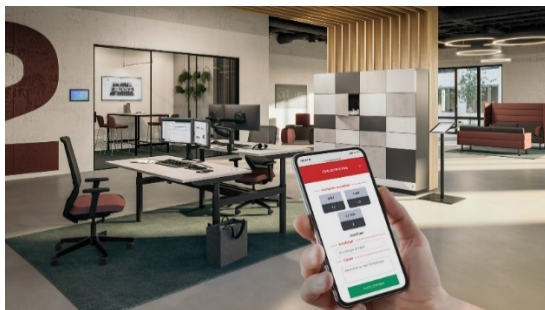
3. Казуси

3.1 Мрежово управление, подобрено с AI в корпоративна среда

Голяма корпорация внедри управлявани от изкуствен интелект решения за управление на мрежата, което доведе до 30% намаление на времето за престой на мрежата и значително подобрение в удовлетвореността на потребителите. Системата AI наблюдаваше моделите на използване на мрежата, като динамично разпределяше ресурси по време на пиковите изисквания и предоставяше предупреждения за сигурност в реално време.

3.2 Внедряване на интелигентен офис(Smart Office)

В сценарий на интелигентен офис(Фиг. 3) AI, интегриран в LAN, позволява безпроблемна комуникация между IoT устройства, оптимизира потреблението на енергия и повишава ефективността на работното място. Алгоритмите за машинно обучение коригират осветлението и HVAC системите въз основа на данни за заетостта, което води до намалени оперативни разходи.



Фиг. 3. Примерен изглед на Интелигентен офис

4. Предизвикателства и съображения

Въпреки че потенциалните ползи от интегрирането на AI в LAN системи са значителни, няколко предизвикателства трябва да бъдат разгледани:

4.1 Поверителност и сигурност на данните

Внедряването на AI в управлението на LAN поражда опасения относно сигурността и поверителността на данните. Организациите трябва да гарантират, че данните, използвани за машинно обучение, не нарушават поверителността на потребителите или регулаторните изисквания.

4.2 Сложност и цена

Първоначалните разходи и сложността на внедряването на AI технологии могат да бъдат значителни. Организациите трябва да претеглят тези фактори спрямо потенциалните дългосрочни ползи.

4.3 Липса на умения

Преходът към LAN управление, управлявано от AI, изисква квалифициран персонал, който владее както мрежовите, така и AI технологиите. Тази празнина в уменията може да представлява предизвикателство за организациите, които искат да приемат AI решения.

5. Заключение

Включването на AI в локалните мрежи представлява трансформираща възможност за организации, които търсят подобрена ефективност, сигурност и адаптивност. Чрез използване на AI за предсказуема поддръжка, управление на трафика и подобряване на сигурността, фирмите могат значително да подобрят своите LAN възможности. Въпреки това справянето с потенциални предизвикателства, свързани с поверителността на данните, разходите и уменията, ще бъде от решаващо значение за успешното внедряване. Тъй като AI технологията продължава да се развива, нейната роля в мрежите несъмнено ще се разшири, проправяйки пътя за по-интелигентни, по-устойчиви LAN инфраструктури.

ЛИТЕРАТУРА

- [1] Cisco Systems. (2021). AI and Machine Learning in Networks.
- [2] IEEE Communications Society. (2022). The Future of Local Area Networks with AI.
- [3] Gartner, Inc. (2023). Predicting Network Dynamics Using AI.
- [4] Zhang, Y., & Li, Q. (2023). AI-driven Network Security: Trends and Challenges.
- [5] Journal of Network and Computer Applications.
- [6] Kauffman, R. J., & Walden, E. A. (2022). AI for Network Management: Challenges and Opportunities. Communications of the ACM.

ПОЛИГОННИ ИЗПИТВАНИЯ НА ПРОМЯНАТА НА БАЛИСТИЧНИТЕ ХАРАКТЕРИСТИКИ НА БОЕПРИПАСИ С ИЗМЕНЕНА ФОРМА НА ПРОЕКТИЛА ПРИ ДВИЖЕНИЕТО МУ ВЪВ ВЪЗДУХА И ПРЕМИНАВАНЕТО МУ ПРЕЗ СРЕДИ С РАЗЛИЧНА ПЛЪТНОСТ

Росен Н. Лазаров

POLYGON TESTS OF THE CHANGE IN BALLISTIC CHARACTERISTICS OF AMMUNITION WITH MODIFIED PROJECTILE SHAPE DURING ITS MOVEMENT IN AIR AND PASSAGE THROUGH MEDIA OF DIFFERENT DENSITY

Rosen N. Lazarov

ABSTRACT: *When a projectile passes through environments of varying density, processes changing its energy, trajectory and integrity are observed. To determine the phenomena that occur when the bullet meets an environment of different density, it is necessary to develop a methodology that would unify the experiments of this type of tests.*

KEYWORDS: *ballistics, methodology, environments of varying density*

DOI: <https://doi.org/10.46687/YT24LZR>

Балистическите характеристики на боеприпасите с проектили с променена форма, които представляват интерес в настоящото изследване са: началната скорост на проектила, балистическият му коефициент, групираността на стрелбата и пробивното му действие при преминаването му през среди с различна плътност.

Необходимият минимален брой опитни данни, който трябва да имат групите е 13, като за по-достоверни резултати приемаме да изпълняваме по 20 опита за серия. [1]

Обект и условия на изпитването:

1.Целта на изпитването е: Изследване на влиянието на формата на проектил с променени геометрични и масови характеристики при промяна на плътността на средата, през която преминава, групираността, началната скорост и пробивното му действие при единична стрелба.

2.Предназначение и област на приложение: Методиката за изпитание е предназначена за изследване на влиянието на формата на проектил с променени геометрични и масови характеристики върху пробивното му действие, групираността и началната скорост при единична стрелба.

3.Обект на изпитването: Обект на изпитването са проектили с променени геометрични и масови характеристики на боеприпаси, калибър 7,62x39 mm и 7,62x54 mm.

4.Списък на нормативно-техническата документация:

- Наредба за условията и реда за осъществяване на дейностите, свързани с оръжията, боеприпасите, взривните вещества и пиротехническите изделия и контрола над тях във и от въоръжените сили на Република България;

- Правилник за складовете и базите за съхранение, производство, ремонт, разснарядяване и унищожаване на бойни припаси, взривни вещества и барути в БНА – МНО 1982 г.;

- Проверка боя и привеждане на стрелковото оръжие към нормален бой, Цонев Ц. Г., Богданов А. И., Шумен 2006 г.;

- Наставление по стрелково дело, Материална част на стрелковото оръжие, МНО, Военно издателство 1987 г.

5.Подготовка на бойните припаси за изпитването: Проверява се опаковката на бойните припаси. Извършва се темпериране на бойните припаси в помещение с температура – $t = 20^{\circ} \pm 2^{\circ}$, в продължение на 24 часа преди извършване на стрелбата.

6.Подготовка на оръжието за изпитването:

При изпитване на групираността и началната скорост:

- подготвя се за стрелбата станок за балистични изпитвания с балистична цев за стрелба с проектил с променени геометрични и масови характеристики на стрелбищния полигон;

- извършва се почистване на цевта;

- поставя се вертикален щит със закрепена на него мишена с размери 1,0 m височина и 1,0 m ширина, на разстояние 100 m от дулния срез на цевта;

При изпитване на пробивното действие на проектила:

- подготвя се за стрелбата станок за балистични изпитвания с балистична цев за стрелба проектил с променени геометрични и масови характеристики на стрелбищния полигон;

- извършва се почистване на цевта;

- поставя се мишена, състояща се от 12 платна, изработени от сух чамов материал с дебелина на платното 30 mm и разстояние помежду им 30 mm, на разстояние 100 m от дулния срез на цевта;

7.Подготовка на позицията и площадката за изпитването:

Мястото за провеждането на изпитването на групираност и начална скорост да осигурява:

- разполагане на щита на равна хоризонтална площадка с наклон не повече от $2\div 3^{\circ}$ на височината на очите, вертикално, без наклон встрани или назад/напред;

- разстояние на стрелбата при проверка на групираността и началната скорост на проектила – 100 m (мерено от дулния срез на цевта до щита с мишената);

- ъгъл на наклон на цевта – 0° спрямо хоризонталната равнина;

- охлаждане на цевта след произвеждане на всяка серия изстрели.

Мястото за провеждането на изпитването на рикошетното действие на проектила да осигурява:

- разполагане на мишената с дървени платна вертикално, на височината на осканалната линия на балистичната цев, като се укрепи против падане при попадения от проектилите;
- разстояние на стрелбата при проверка на пробивната сила на проектила – 100 m, (мерено от дулния срез на цевта до щита с мишената);
- ъгъл на наклон на цевта – 0° спрямо хоризонталната равнина;
- охлаждане на цевта след произвеждане на всяка серия изстрели.

8. Метеорологични условия на изпитанието чрез стрелба:

Стрелбата да се извършва при благоприятни метеорологични условия (нормални атмосферни условия) – ясно и безветрено време или в закрити стрелбища; температура на околния въздух – $15^{\circ} \div 20^{\circ}$; относителна влажност на въздуха $65 \pm 5\%$. Ако условията, при които се провежда изследването са различни, същите да бъдат записани в протокола.

Забранява се стрелбата да се извършва при влошена видимост или при скорост на вятъра повече от 5 m/s.

Описание на методите за изпитване

1. Проверка на външния вид и състоянието на опаковката на бойните припаси (извършва се преди модификацията на формата на проектилите).

Проверява се: външния вид и състояние на кутиите, наличието и правилността на маркировката.

Проверката се извършва по визуален способ в следната последователност:

- проверява се кутията - херметичното затваряне на кутията не трябва да е нарушено;
- извършва се оглед на маркировката на кутията - маркировката трябва да бъде правилна, ясна и четлива; да посочва вида и/или производствените данни на бойните припаси;
- извършва се оглед на защитното (антикорозионно) покритие (емайллак, лак) - защитното покритие трябва да бъде плътно, равномерно и без пропуски.

Допуска се:

- незначително изтриване на маркировката, но позволяващо ясно определяне на вида и/или производствените данни;
- точки от корозия на отделни участъци на места, където е нарушено защитното покритие;
- незначителни механични деформации (смачкване, огъване, хлътване) по корпуса.

Не се допуска:

- липсваща или нарушена маркировка, не позволяваща определяне вида и/или производствените данни;
- корозия с разрушаване на корпуса на кутията;
- значителни механични деформации (смачкване, огъване, хлътване) по кутията, възпрепятстващи или изключващи възможността за използване по предназначение;

- нарушаване херметичността на кутията.

2. Проверка на външния вид и състояние на бойните припаси

Проверява се:

- външния вид и състояние на бойните припаси;
- наличието и правилността на маркировката;
- Проверката се извършва по визуален способ в следната последователност:
- изваждат се бойните припаси от кутията - външната обвивка трябва да бъде

без механични повреди.

- извършва се оглед на маркировката и външната обвивка на бойните припаси - маркировката трябва да бъде правилна, ясна и четлива; да посочва вида и/или производствените данни на бойните припаси.

- извършва се оглед на защитното (антикорозионно) покритие (емайллак, лак) - защитното покритие трябва да бъде плътно, равномерно и без пропуски.

- бойните припаси се поставят в щатната опаковка - техническото състояние на бойните припаси трябва да съответства на изискванията за втора категория.

Допуска се:

- незначително изтриване на маркировката, но позволяващо ясно определяне на вида и/или производствените данни;

- незначителни надирания/изтривания /на защитното покритие;

- точки от корозия на отделни участъци от външната обвивка на места, където е нарушено защитното покритие;

- незначителни механични деформации (смачкване, огъване, хлътване) по външната обвивка;

Не се допуска:

- техническото състояние на бойните припаси да не съответства на изискванията за втора категория;

- липсваща или нарушена маркировка, не позволяваща определяне вида и/или производствените данни;

- корозия с разрушаване на външната обвивка на бойните припаси;

- значителни механични деформации (смачкване, огъване, хлътване) по корпуса, възпрепятстващи или изключващи възможността за използване по предназначение на бойните припаси;

- наличие на пукнатини по корпуса;

3. Проверка на външния вид и състоянието на оръжието

Проверява се:

- външния вид и състоянието на балистичната цев, затвора и станок за балистични изпитвания;

- сигурното закрепване на станок за балистични изпитвания към фундамента.

4. Изпитване на групираността и началната скорост

Изпитването се извършва с цел проверка за балистичните характеристики на проектилите след промяна на геометричните и масовите им характеристики.

При изпитването се контролира изменението на:

- началната скорост и скоростта на проектилите на разстояние 25m и 100 m от дулния срез на цевта;

- координатите точките на попаденията по хоризонталната и вертикалната оси на мишената;

Изпитването се извършва с по 20 изстрела с боеприпаси от всяка модификация на проектила.

Изпитването се извършва в следната последователност:

- изстрелва се една серия от 20 изстрела на единичен огън първо с фабрични боеприпаси и се определя началната скорост и скоростта на проектила на 100 m от дулния срез;

- изстрелва се по една серия от 20 изстрела на единичен огън с различните модификации проектили с променени геометрични и масови характеристики по отделна мишена и се определя началната скорост и скоростта на проектила на 25 m и 100 m от дулния срез;

- определя се групираността за всяка серия;

- след изстрелване на всяка серия се измерват величините на отклонението на центровете на пробойните на всеки проектил в мишената от координатните оси. Измерването се извършва в милиметри посредством линия. Стойностите на страничните отклонения вляво от вертикалната ос се нанасят в бланката със знак минус, а вдясно – със знак плюс. Стойностите на вертикалните отклонения под хоризонталната ос се нанасят в бланката със знак минус, а над нея – със знак плюс;

- определя се групираността за всяка серия поотделно. Измерват се стойностите на разстоянията между центровете на пробойните в хоризонталната и вертикалната равнини на двете най-отдалечени попадения в милиметри посредством линия. За стойност на групирането се приема по-голямата от измерванията.

5.Изпитване на пробивното действие

Изпитването се извършва с цел проверка на пробивното действие на проектили на фабрични патрони 7,62x39 и 7,62x54, както и на 7,62x39 след промяна на геометричните и масовите им характеристики. При изпитването се контролира броят мишенни дъски, пробити от съответния модел проектили. Установяват се по броя пробойни върху щита за съответната серия;

Изпитването се извършва с по 20 изстрела с фабрични боеприпаси и с боеприпаси, с модифициран проектил с изработен канал по оживалната частна разстояние 7 mm от върха.

Изпитването се извършва в следната последователност:

- на поставения на станок за балистични изпитвания се задава ъгъл на цевта – 0° спрямо хоризонталната равнина;

- монтира се устойчиво мишената на разстояние 100 m от дулния срез на цевта;

- върху всяка табла се поставя номериран лист, по който да бъдат снети отчети за попаденията;

- произвеждат се по една серия от по 20 изстрела на единичен огън първо с фабрични боеприпаси, а после и с групата с проектили с променени геометрични и масови характеристики. Фотографират се попаденията върху щита, след което се отчитат попаденията и се прибират листите за отчет на координатите на попаденията.

6. Обработка, анализ и оформяне на резултатите от изпитването.

Резултатите се отчитат в протокол от изпитванията, както следва:

- за резултати от началната скорост и скоростта на 25 m и 100 m от дулния срез на проектила се записват данните отчетени от апаратурата по време на стрелбата;

- броят на пробойните на всяка една отделна табла се записва след всяка серия изстрели за всяка партия и за всеки наклон на цевта.

- координатите на пробойните, отчетени по щита и групираността на серията, в хоризонталната и вертикалната равнини се изчислява за всяка серия поотделно.

За стойност на групирането се приема по-голямата от измерванията.

Стойността на групираността на серията се определя по формулата:

$$X < Y \Rightarrow D_{100} = Y; (1)$$

$$X > Y \Rightarrow D_{100} = X,$$

Където: D_{100} – стойност на групираността в mm;

$$X = X_{max} - X_{min}; (2)$$

$$Y = Y_{max} - Y_{min},$$

Където:

- X_i, Y_i , - стойност на отклонението на центровете на пробойните на всеки проектил в мишената от координатните оси преминаващи през центъра на координатната система в mm;

- X_{max}, Y_{max} – стойност на максималното отклонение на центровете на пробойните в хоризонталната и вертикалната равнини на мишената от координатната система в mm.

- X_{min}, Y_{min} – стойност на минималното отклонение на центровете на пробойните в хоризонталната и вертикалната равнини на мишената от координатната система в mm. [2]

Анализът се извършва след сравняването на резултатите, получени при експериментите за съответната модификация проектил с резултатите за фабричния и за другите модификации на проектили с променени геометрични и масови характеристики.

ЛИТЕРАТУРА

- [1] Ганев В., Лазаров Р., Димитрова Я., Банков Б. Анализ на възможностите за промяна формата на куршума на боеприпас 7,62x54 с цел намаляване на рикошетното му действие при среща с водна среда. Научна конференция „Логистиката и обществените системи“ 2023 г., ИК на НВУ „Васил Левски“ – БТ, ISSN 2738-8042, с. 181-186.
- [2] Цонев Ц., Богданов А. Проверка боя и привеждане на стрелковото оръжие към нормален бой. Шумен, 2006.

КИБЕРРАЗУЗНАВАНЕ И ИНТЕГРИРАНИ РЕШЕНИЯ ЗА КИБЕРСИГУРНОСТ

Даниел Р. Денев, Илкер А. Хатиб

CYBER INTELLIGENCE AND INTEGRATED CYBERSECURITY SOLUTIONS

Daniel R. Denev, Ilker A. Hatib

ABSTRACT: *Cybersecurity challenges in today's digital era require a holistic approach combining advanced technologies and human expertise. Cyber intelligence plays a critical role in identifying, preventing, and responding to threats by integrating data from diverse sources. Tools like Wireshark, Microsoft Defender Advanced Threat Protection (ATP), and Azure Security Center provide organizations with centralized monitoring and effective threat management. The paper emphasizes the importance of packet analysis, automation, artificial intelligence, and personnel training in enhancing organizational resilience. Key examples, such as the EternalBlue vulnerability and the WannaCry ransomware attack, illustrate the significance of proactive measures and incident response. Understanding the deep web, IoT vulnerabilities, and implementing advanced cryptographic solutions further bolster the defense against evolving cyber risks.*

KEYWORDS: *automation, cyber intelligence, cybersecurity, network packet analysis, Wireshark*

DOI: <https://doi.org/10.46687/YT24DIL>

Въведение

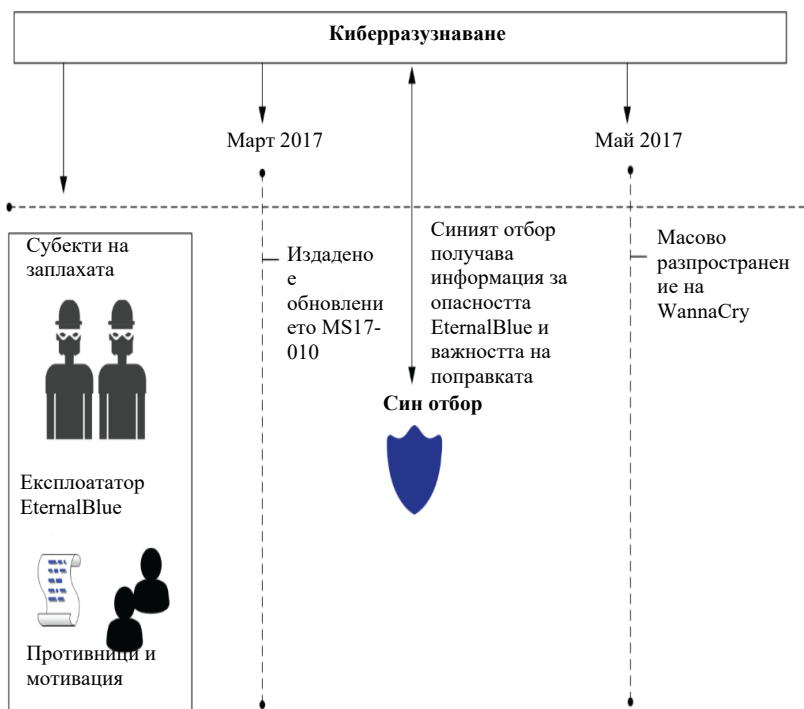
В епохата на цифровизация и бързоразвиващи се технологии, киберзаплахите се увеличават по сложност и честота, създавайки сериозни предизвикателства за сигурността на организациите. Киберразузнаването и съвременните инструменти за анализ играят ключова роля в идентифицирането, предотвратяването и реакцията на заплахи. От наблюдението на зловредни активности и анализ на мрежови пакети до използването на изкуствен интелект и човешки експертиза, ефективната киберзащита изисква комбинация от технологични и аналитични подходи. Настоящият текст изследва съвременните методи за управление на риска, подчертавайки важността на инструменти като Wireshark, Azure Security Center и Microsoft Defender ATP, както и значението на мониторинга, автоматизацията и обучението на персонала.

Съвременни заплахи в киберпространството

Киберразузнаването обединява данни от различни източници, за да осигури на организациите информация за потенциални заплахи и методи за защита.

Този аналитичен подход включва наблюдение на зловредни активности, идентифициране на уязвимости и предприемане на превантивни мерки. Сред основните противници в киберпространството са киберпрестъпниците, които търсят финансова печалба, хактивистите, мотивирани от политически или социални причини, както и държавните кибершпиони, които целят стратегическа информация от корпоративни и правителствени организации. Тяхната дейност изисква разработване на ефективни стратегии за разузнаване и сигурност.

Пример за ефективно киберразузнаване е реакцията към експлоатацията EternalBlue и рансъмуера WannaCry през 2017 г. Групата The Shadow Brokers разкри уязвимостта в протокола SMB, която Microsoft своевременно коригира с пач MS17-010. Въпреки това много организации не успяха да приложат обновлението навреме, което доведе до глобално разпространение на WannaCry и значителни загуби. Този случай демонстрира важността на бързата реакция и прилагането на превантивни мерки. Подобни атаки изискват и задълбочено разследване, включващо идентифициране на компрометирани системи, проследяване на първоначалните точки на атака и анализ на използваните методи. Инструменти като Wireshark и VPN технологии се оказват критични за проследяване и ограничаване на зловредния трафик.



Фиг. 1. Опит за предпазване от WannaCry

Особено внимание заслужава и изследването на дълбоката мрежа и Dark Web, където се извършват множество нелегални дейности. Тези пространства предоставят платформа за анонимност, която често се използва от киберпрестъпници за координация и провеждане на атаки. Инструменти като мрежата Тор дават възможност за криптирана комуникация, която трудно се проследява. Разбирането на тези мрежи и разработването на механизми за тяхното наблюдение е ключово за киберсигурността. В допълнение, технологията ZigBee, широко използвана в IoT устройства, също демонстрира уязвимости, свързани с разпределението на ключовете и защитата на комуникацията. Усъвършенствани подходи, включващи еднократни ключове и подобрени криптографски методи, могат значително да подобрят сигурността.

Киберразузнаването трябва да се разглежда не само като инструмент за информационна безопасност, а и като стратегически ресурс, подпомагащ вземането на критични решения в организациите. То е в основата на успешното справяне със заплахите и осигуряването на ефективна защита срещу бързо еволюиращите киберрискове. [1], [2]

Ролята на Wireshark в анализа на мрежови пакети и киберсигурността

Анализът на мрежови пакети е ключов инструмент за откриване на заплахи в реално време. Той осигурява детайлна информация за структурата и съдържанието на мрежовия трафик, което позволява идентифициране на аномалии, предотвратяване на атаки и оптимизация на мрежовата инфраструктура. Wireshark е водещ софтуер за мрежови анализи, широко използван от мрежови администратори и експерти по киберсигурност заради своята ефективност и богат набор от функции.[9]

Wireshark предоставя възможност за идентифициране на зловредни дейности чрез подробен анализ на мрежовия трафик. Чрез инструмента могат да се открият подозрителни модели като неоторизирани достъпи, инжектиране на зловреден код и атаки тип „човек в средата“. Например анализът на HTTP сесии позволява разкриване на необичайни заявки и взаимодействия, които могат да сигнализират за активност на злонамерен софтуер. Освен това, инструментът улеснява откриването на продължителни връзки към външни IP адреси, които често са свързани с комуникация с командни сървъри. [11]

Wireshark е изключително полезен и за оптимизация на мрежовата производителност. Софтуерът помага за диагностициране на мрежови проблеми като задръствания, висока латентност и неефективно разпределение на трафика. Чрез мониторинг на мрежовите протоколи, като TCP/IP, могат да се идентифицират настройки или конфигурации, които влияят отрицателно на ефективността. Това позволява на администраторите да предприемат корективни действия за подобряване на мрежовата работа.[4]

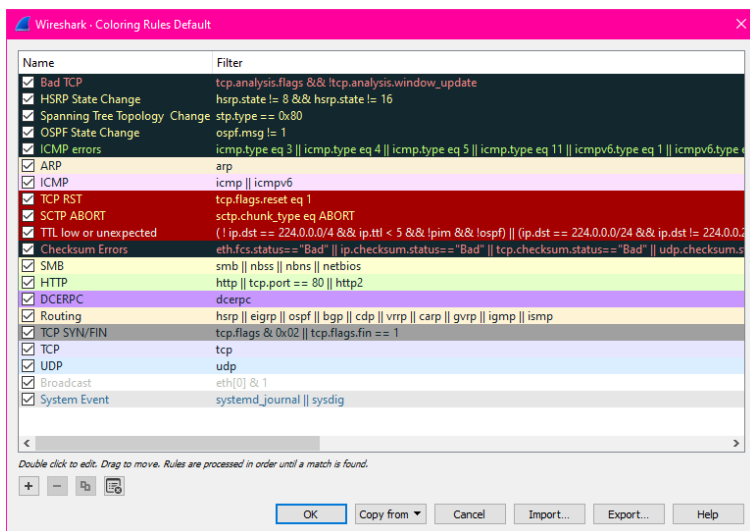
Wireshark поддържа анализ на над 1000 мрежови протокола, което го прави универсален инструмент за всякакви мрежови среди. Сред поддържаните протоколи са както традиционните TCP, UDP, HTTP и FTP, така и съвременни криптирани протоколи като TLS/SSL, използвани за сигурна комуникация.

Неговият интуитивен графичен интерфейс улеснява работата както на начинаещи, така и на опитни потребители, като предлага удобни функции за визуализация и бързо филтриране на специфични данни, например IP адреси или типове пакети.

Една от най-ценните функции на Wireshark е Stream Capture, която позволява изолиране и анализ на специфични потоци данни, като HTTP или FTP сесии. Тази възможност е особено полезна при диагностициране на проблеми с конкретни приложения или при разследване на инциденти, свързани със сигурността. Например, чрез функцията може да се проследят всички заявки и отговори между клиент и сървър в рамките на дадена HTTP сесия, което улеснява откриването на проблеми в уеб приложенията. [7]

Wireshark е незаменим и за откриване на зловреден софтуер. Софтуерът идентифицира необичайно поведение, като постоянни връзки към известни злонамерени IP адреси или трафик, характерен за ransomware или DDoS атаки. Анализът на DHCP трафика, от своя страна, помага за откриване на проблеми с IP адресирането и конфигурацията на мрежата.

Wireshark е мощен инструмент, който осигурява ефективност и гъвкавост в анализа на мрежовия трафик. Той е от съществено значение за защита срещу съвременните киберзаплахи, оптимизация на мрежовата производителност и разкриване на уязвимости в приложения и протоколи. Неговите функции го правят един от най-надеждните инструменти за мрежови анализи в съвременната киберсигурност. [5]



Фиг. 2. Софтуерен инструмент Wireshark

Пример: Да се изчисли средна скорост на трансфер на данни

За да се изчисли средната скорост на трансфер в мрежа въз основа на информацията за обема на трафика и времето, за което е записан.

Данни:

Размер на всички пакети: $TotalBytes = 50000000$ (50 MB)

Времетраене на сесията: $Time\ Duration = 120seconds$

$$СРЕДНА\ СКОРОСТ = \frac{ОБЩ\ ОБЕМ\ НА\ ДАННИТЕ}{ВРЕМЕ} \quad (1)$$

$$СРЕДНА\ СКОРОСТ = \frac{50000000\ BYTES}{120\ SECONDS} = 416,66667\ Bytes/second \quad (2)$$

За по-разбираем резултат преобразуваме в мегабайти на секунда (MB/s):

$$СРЕДНА\ СКОРОСТ = \frac{416,66667}{1,048,576} \approx 0,397\ MB/s \quad (3)$$

Резултат:

Средната скорост на трансфер на данни е 0.397 MB/s или приблизително 397 KB/s.

Интегрирани решения за управление на риска

В съвременната дигитална ера организациите са изправени пред нарастващи и все по-сложни киберзаплахи, което налага възприемането на холистичен подход към киберсигурността. Този подход комбинира усъвършенствани софтуерни инструменти с човешки анализ, за да осигури цялостна защита на информационните активи. [3]

Интегрирани софтуерни решения за киберсигурност

Инструменти като Microsoft Defender Advanced Threat Protection (ATP) и Azure Security Center предоставят на организациите възможности за централизирано наблюдение и управление на заплахите. Microsoft Defender ATP е платформа за защита на крайните точки, която предлага откриване, разследване и реагиране на напреднали заплахи. Azure Security Center, от своя страна, осигурява унифицирано управление на сигурността и разширена защита срещу заплахи в хибридни облачни среди. Тези инструменти позволяват на организациите да получат пълна видимост върху своите ИТ среди и да реагират бързо на инциденти.

Значението на човешкия анализ в киберсигурността

Въпреки напредъка на автоматизираните решения, човешкият фактор остава критичен за ефективната киберзащита. Експертите по киберсигурност прилагат своя опит и интуиция за интерпретиране на данни, идентифициране на сложни заплахи и вземане на стратегически решения. Човешкият анализ е особено важен при разпознаването на нови или непознати атаки, където автоматизираните системи може да не са достатъчно ефективни. Сътрудничеството между ИТ екипите и специалистите по сигурността, известно като SecOps, е ключово за постигане на синергия между технологиите и човешкия опит. [6]

Мониторинг на ключови параметри за осигуряване на прозрачност

За да се гарантира цялостна видимост и контрол върху системите, е необходимо постоянно наблюдение на критични параметри, включително:

- Честота на инцидентите: Анализът на броя и вида на възникващите проблеми помага за оценка на ефективността на мерките за сигурност и идентифициране на области, изискващи подобрене.

- Потребителски идентификатори: Следенето на активността на потребителите позволява откриване на неотризири достъпи и потенциални вътрешни заплахи. [10]

- Мрежови конфигурации: Редовният преглед и анализ на мрежовите настройки спомага за откриване на уязвимости и осигуряване на оптимална мрежова производителност.

- Инструменти като HikCentral предлагат централизирано наблюдение и управление на мрежови устройства, което улеснява мониторинга и подобрява реакцията при инциденти.



Фиг. 3. *Хибридна облачна среда*

Автоматизация и изкуствен интелект в киберсигурността

Внедряването на автоматизирани системи и изкуствен интелект (AI) в киберсигурността повишава ефективността на откриване и реагиране на заплахи. Автоматизацията позволява бързо обработване на големи обеми данни и изпълнение на рутинни задачи, освобождавайки експертите да се фокусират върху по-сложни анализи. AI подпомага разпознаването на модели и аномалии, които може да останат незабелязани при традиционните методи. Този подход

подобрява киберустойчивостта на организациите и намалява времето за реакция при инциденти. [8]

Обучение и осведоменост на персонала

Човешкият фактор често е най-слабата връзка в киберсигурността. Редовното обучение на служителите за разпознаване на фишинг атаки, социално инженерство и други заплахи е от съществено значение. Осведомеността и спазването на добри практики намаляват риска от инциденти, предизвикани от човешка грешка.

Таблица 1. Програми за обучение на персонал

Област на обучение	Описание	Очакван ефект
Разпознаване на фишинг атаки	Обучение за разпознаване на съмнителни имейли и линкове	Намаляване на успешните фишинг атаки
Социално инженерство	Осведомяване за методите, използвани за манипулиране на хора	Намаляване на риска от измами
Добри практики за сигурност	Указания за силни пароли, управление на достъп и други	Подобряване на общата сигурност в организацията

Заклучение

Киберсигурността в съвременния свят е не просто техническо предизвикателство, а стратегически приоритет за организациите. Холистичният подход, комбиниращ модерни технологии, автоматизация и човешка експертиза, осигурява не само защита, но и устойчивост при инциденти. Използването на инструменти като Wireshark за детайлен анализ на мрежовия трафик, Microsoft Defender ATP и Azure Security Center за централизиран мониторинг, както и обучение на персонала, са ключови за справяне със заплахите. Само чрез цялостно разбиране и интегриране на тези компоненти организациите могат да постигнат висока степен на защита срещу еволюиращите киберрискове.

ЛИТЕРАТУРА

- [1] 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.
- [2] Goodin D.NSA-leaking Shadow Brokers just dumped its most damaging release yet. Ars Technica. p. 1. Retrieved May 13, 2017.

- [3] 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.
- [4] Konstantinova E., Tsankov Ts. Analyzing security threats in smart homes technology. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 373-378.
- [5] Lilov V., Konstantinova E., Tsankov Ts. Cyber intelligence in protecting organizations from malicious activity. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 386-392.
- [6] <https://heritage-offshore.com/net-administrator/kak-da-izpolzvate-wireshark-urok/>
- [7] <https://www.microsoft.com/bg-bg/security/business/security-101/what-is-security-operations-secops>.
- [8] <https://www.microsoft.com/bg-bg/security/security-insider/intelligence-reports/microsoft-d>
- [9] <https://habr.com/ru/articles/436226/>
- [10] <https://bg.linux-console.net/?p=13572>
- [11] <https://habr.com/ru/articles/735866/>

ЛОГИСТИЧНА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ПОТОЦИТЕ ОТ ЗАЯВКИ С ПРОГРАМА PHP SIMPLEX

Анатоли Ж. Стоянов

LOGISTICS SYSTEM FOR MANAGEMENT OF REQUEST FLOWS WITH PHP SIMPLEX

Anatoli Zh. Stoyanov

ABSTRACT: *The report presents an automated method using the capabilities of the PHP Simplex program for solving multi-stage logistics tasks. The theoretical formulation of the multi-stage logistics task serving postal activities based on the simplex method of the two phases is analyzed. The application of such an approach aims to obtain optimal attachment of the flow of requests to the postal service delivery areas and costing of the entire procedure.*

KEYWORDS: *multi-stage logistics tasks, PHP Simplex, two-phase method, freight transport, optimal planning of logistics activities*

DOI: <https://doi.org/10.46687/YT24ATL>

Увод

Логистичната задача за обслужване на пощенските дейности намират широко приложение при планирането на потоците от заявки. Планирането на експедиторската дейност е изключително сложна задача, чието успешно решаване е свързано с отчитането на голям брой фактори. Един от основните принципи на планиране е принципът на оптималност, който изисква от всички възможни варианти да се избере най-добрият вариант, осигуряващ възможно най-добрите условия за развитие и най-пълно постигане на набелязаните цели. Практическото приложение на логистичната задача се свежда до разработването на оптимален план за превозите на даден пощенски продукт, т.е. до оптимално обвързване на неговите производствени и консумативни пунктове. Чрез прилагането на такъв вид технология се осигурява т.нар. оптимизиране на товарните превози. Товарният транспорт е необходимо условие за нормалното функциониране на всички отрасли на пощенските услуги. Важната роля на товарния транспорт за развитие на доставките се определя преди всичко от факта, че чрез него се осъществяват икономическите връзки между отделните отрасли и различните райони. Изследваме тези дейности в пощенските услуги, който е свързан с алгоритъма разработен на фиг. 1.

Разработеният алгоритъм ни предоставя възможността да формулираме потоците от заявки и приложим програмата PHP Simplex за всяко едно от направленията. За целта анализираме вътрешната и международна дейност за управление на потоците от заявки.



Фиг. 1. Логистични пощенски услуги

Като се има предвид, че в мащаба на пощенските услуги почти няма технология, която да не представлява част от сложна многоетапна система, може да се твърди, че решаването на многоетапни логистични задачи е в състояние да осигури възможно най-рационална организация на превозите [2].

В настоящото изследване се представя автоматизиран метод за решаване на многоетапни транспортни задачи и приложението му за получаване на оптимално прикрепване на складовете към районите на пощите и на операционните звена към складовете бази. Съвременното обслужване и логистиката са немислимо без своевременни и качествени транспортни операции. Особено важно значение има организацията на превозите на международните пощенски пратки от една страна до тяхното временно складиране. Те се определят по основните производствени единици (държави, общини, пощенски централи), намиращи се в местния район на притегляне и по характерните за района видове пратки, като международни, местни, кореспондентски и др. Обемът на товарните превози от една централа се определя, като се изхожда от размера на обема и площ на товара и разпределението по видове, както и от величината на средните количества, потребностите за нуждите на населението. Практическото приложение на многоетапните транспортни задачи е свързано с изчислителни процедури с много голям обем и поради тази причина е уместно да се използват компютърни програми, които да улеснят решаването им. Програмата PHP Simplex е специализиран софтуер за решаване на задачи на линейното оптимизиране чрез симплекс-метода на базата на метода на двете фази. В настоящата статия се илюстрира метод за решаване на многоетапни транспортни задачи с приложение на програмата PHP Simplex, който цели не само да се генерира оптималния план на превозите, но и да се автоматизира изчислителния процес [4].

Теоретична постановка

При многоетапните системи за управление на потоците от заявки и потребление се извършва транспортиране на даден продукт на няколко етапа. На първия етап продуктът се превозва от дадени изходни пунктове, в които се намират определени количества от него, до дадена първа група междинни пунктове, всеки от които може да получи определено количество продукт. На втория етап той се превозва до втора група междинни пунктове в определени количества и т.н. На последния k -ти етап продуктът се превозва от дадена $(k - 1)$ група междинни пунктове до приемателните пунктове, в които трябва да се достави този продукт в определени количества. Известни са транспортните разходи за единица продукция от всеки изходен пункт до всеки междинен пункт за всеки от етапите. Търси се оптимален план на превозите, по който сумарните транспортни разходи да са минимални [5].

В практиката широко приложение намира т.нар. двуетапна транспортна задача. Това се определя от обстоятелството, че една значителна част от пощенските пратки на различните отрасли не се придвижва непосредствено до потребителите, а преминава през междинни складови бази. Затова разгледаме теоретичната постановка на двуетапната транспортна задача. Където пощенските

центрове $A_1, A_2, \dots, A_m$ съхраняват даден продукт – колетни пратки в количества съответно $a_1, a_2, \dots, a_m$ единици. Дадени са складовете $D_1, D_2, \dots, D_p$, в които може да се съхранява този продукт, като всеки склад може да приеме съответно $d_1, d_2, \dots, d_p$ единици. От дадена пощенска централа продуктът се превозва до складовете и оттам до пунктовете на следващата – $B_1, B_2, \dots, B_n$, чийто възможности са съответно $b_1, b_2, \dots, b_n$ единици. Известни са транспортните разходи C_{ik}^1 ($i = 1, 2, \dots, m$; $k = 1, 2, \dots, p$) от всяка поща до всеки склад на

следващата централа, както и транспортните разходи C_{kj}^2 ($k = 1, 2, \dots, p$; $j = 1, 2, \dots, n$) от всеки склад до всеки потребител. Предполага се, че съществува баланс между производството и потреблението, т.е. [6]

$$\sum_{i=1}^m a_i = \sum_{j=1}^n b_j. \quad (1)$$

Задачата има смисъл, когато общият капацитет на складовете надвишава общото количество на колетните пратки, подлежаща на транспортиране, т.е.

$$\sum_{k=1}^p d_k \geq \sum_{i=1}^m a_i = \sum_{j=1}^n b_j. \quad (2)$$

Да означим с x_{ik}^1 и x_{kj}^2 неизвестните обеми на превозите съответно от всяка пощенска централа до всеки склад и от всеки склад до всеки потребител. Търсят се такива обеми на превозите, че общата сума на транспортните разходи да бъде минимална. За да се реши двуетапната транспортна задача, тя се споставя с една обикновена транспортна задача, в която складовете се разглеждат като приемателни пунктове за първия етап и изходни пунктове за втория етап. В този случай превозите се оптимизират едновременно и за двата етапа, с което се реализират допълнителни възможности за минимизиране на транспортните разходи. Тази обикновена транспортна задача (наречена M - задача) има $m + p$ отправни пункта $A_1, A_2, \dots, A_m, D_1, D_2, \dots, D_p$ и $p + n$ приемателни пункта $D_1, D_2, \dots, D_p, B_1, B_2, \dots, B_n$. Между транспортните разходи за единица продукт c_{ij} в M -задачата и транспортните разходи в двуетапната задача съществува следната връзка: $c_{ij} = c_{ik}^1$, за $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$, $k = 1, 2, \dots, p$; $c_{ij} = c_{kj}^2$, за $i = m + 1, m + 2, \dots, m + p$, $j = p + 1, p + 2, \dots, p + n$, $k = 1, 2, \dots, p$. Директни превози от A_i до B_j са невъзможни и за да не се допускат такива превози, за тях се въвеждат фиктивни транспортни разходи M , където M е достатъчно голямо положително число. Ако един и същи склад се разглежда едновременно като отправен и приемателен пункт, то съответните транспортни разходи се приемат за нула. Означавайки транспортните разходи c_{11}^1 със c_1 , т.е. $c_{11}^1 \rightarrow c_1, \dots, c_{1p}^1 \rightarrow c_h, \dots, c_{m1}^1 \rightarrow c_{r+1}, \dots, c_{mp}^1 \rightarrow c_s, c_{m+1}^1 = 0 \rightarrow c_{s+1}, c_{11}^2 \rightarrow c_{s+2}, \dots, c_{1n}^2 \rightarrow c_t, \dots, c_{m+p}^1 = 0 \rightarrow c_{v+1}, c_{p1}^2 \rightarrow c_{v+2}, \dots, c_{pn}^2 \rightarrow c_z$, а неизвестните обеми на превозите x_{11}^1 с x_1 , т.е. $x_{11}^1 \rightarrow x_1, \dots, x_{1p}^1 \rightarrow x_h, \dots, x_{m1}^1 \rightarrow x_{r+1}, \dots, x_{mp}^1 \rightarrow x_s, x_{m+1}^1 \rightarrow x_{s+1}, x_{11}^2 \rightarrow x_{s+2}, \dots, x_{1n}^2 \rightarrow x_t, \dots, x_{m+p}^1 \rightarrow x_{v+1},$

$x_{p1}^2 \rightarrow x_{v+2}, \dots, x_{pn}^2 \rightarrow x_z$, получаваме следната задача на линейното оптимиране [7]:

$$\begin{aligned} \min \{ Z = & c_1 x_1 + \dots + c_h x_h + \dots + c_{r+1} x_{r+1} + \dots + c_s x_s + 0 x_{s+1} \\ & + c_{s+2} x_{s+2} + \dots + c_t x_t + \dots + 0 x_{v+1} + c_{v+2} x_{v+2} + \dots + c_z x_z \} \\ & x_1 + \dots + x_h = a_1 \\ & x_{r+1} + \dots + x_s = a_m \\ & x_{s+1} + x_{s+2} + \dots + x_t = d_1 \\ & x_{v+1} + x_{v+2} + \dots + x_z = d_p \\ & x_1 + x_{r+1} + x_{s+1} = d_1 \\ & x_h + x_s + x_{v+1} = d_p \\ & x_{s+2} + x_{v+2} = b_1 \\ & x_t + x_z = b_n \end{aligned} \quad (3)$$

$$x_j \geq 0, \quad j = 1, \dots, h, \dots, r+1, \dots, s, s+1, s+2, \dots, t, v+1, v+2, \dots, z \quad (4)$$

Така формулираната задача може да бъде решена със симплекс-метода на двете фази. На първата фаза се решава помощната задача:

$$\begin{aligned} \min \{ V = & x_{z+1} + \dots + x_{z+m} + x_{z+m+1} + \dots + x_{z+m+p} + x_{z+m+p+1} + \dots + x_{z+m+2p} \\ & + x_{z+m+2p+1} + \dots + x_{z+m+2p+n} \} \\ & x_1 + \dots + x_h + x_z = a_1 \\ & x_{r+1} + \dots + x_s + x_{z+m} = a_m \\ & x_{s+1} + x_{s+2} + \dots + x_t = d_1 \\ & x_{v+1} + x_{v+2} + \dots + x_{z+m} = a_m \\ & x_{s+1} + x_{s+2} + \dots + x_t + x_{z+m+1} = d_1 \\ & x_{v+1} + x_{v+2} + \dots + x_{z+m+1} = d_p \\ & x_1 + x_{r+1} + x_{s+1} + x_{z+m+p+1} = d_1 \\ & x_{s+2} + x_{v+2} + x_{z+m+2p+1} = b_1 \\ & x_t + x_z + x_{z+m+2p+n} = b_n \end{aligned} \quad (5)$$

при условие $x_j \geq 0, \quad j = 1 \dots x_{r+1} \dots s_{s+1}, \quad s+2 \dots t, \quad v+2, \dots z_{z+1}, \quad z+m+1 \dots z_{z+m+p+1}$

По прием $\min V = 0$, на оптималната базисна програма на помощната задача и, когато това условие е налице, се преминава към **втора фаза** през която се решава дадената задача, като се търси:

$\min \{ Z = c_1 x_1 + \dots + c_h x_h + \dots + c_{r+1} x_{r+1} + \dots + c_s x_s + 0 x_{s+1} + c_{s+2} x_{s+2} + \dots + c_t x_t + \dots + 0 x_{v+1} + c_{v+2} x_{v+2} + \dots + c_z x_z \},$
но ограничителните условия се вземат от оптималната симплекс-таблица на помощната задача.

С програмата PHP Simplex можем да решаваме многоетапни транспортни задачи затворен и отворен модел без ограничение на размерите им. За да илюстрира приложението на разработения метод с програмата PHP Simplex разглеждаме транспортна задача в два пощенски международни района A_1 и A_2 (София и Виена). Извършва се трансфер съответно 4 и 6 тона пощенски пратки. Дадени са три склада за съхранение на кореспонденцията D_1, D_2 и D_3 с капацитет съответно равен на 7, 5 и 4 тона. От пощенските централи кореспонденцията се

превоза до складовете за съхранение, съответно B_1 , B_2 и B_3 , които имат капацитет 2, 1 и 3 тона. Разходите в лева за превоз на един тон пощенски пратки (съдържащи писма, колет и др.) между складовете са $c_{11}^1 = 13$, $c_{12}^1 = 15$, $c_{13}^1 = 12$, $c_{21}^1 = 20$, $c_{22}^1 = 8$, $c_{23}^1 = 14$, а разходите в лева за превоз на един тон между складовете и разпределителният център са $c_{11}^2 = 12$, $c_{12}^2 = 8$, $c_{13}^2 = 3$, $c_{21}^2 = 9$, $c_{22}^2 = 5$, $c_{23}^2 = 7$, $c_{31}^2 = 11$, $c_{32}^2 = 6$, $c_{33}^2 = 13$. Разработва се план за оптимално прикрепване на складовете към районите на пощите и на разпределителния склад, така че сумарните транспортни разходи да са минимални [6].

Задачата може да бъде решена като многоетапна, т.е. при едновременно разработване на оптимален план и за двата етапа, включени в системата (т.нар. M -задача). Разглежданата многоетапна транспортна задача е отворен модел, т.к. сумарната наличност на пратките 10 тона надвишава сумарната потребност на разпределителния център 7 тона. За да се сведе откритата транспортна задача към затворена непосредствено след трите склада се добавя фиктивен потребител D_4 (с потребности равни на $10 - 7 = 3$ тона и транспортни разходи $c_{14}^1 = c_{24}^1 = 0$). Получената затворена транспортна задача има 5 отправни пункта A_1, A_2, D_1, D_2, D_3 и 7 приемателни пункта $D_1, D_2, D_3, D_4, B_1, B_2, B_3$.

След като се стартира програмата се задава броя на променливите 3 и на константите 10 (брой на потребителите – складове). За да се получи оптималното решение на многоетапната транспортна задача с приложение на програмата PHP Simplex се избира вида на функцията Minimize и се въвеждат коефициентите от целевата функция и ограничителните условия, както е показано на фиг. 2 [7].

Which is the objective of the function? [Minimize]

Function: 13 X1 + 15 X2 + 12 X3 + 0 X4 + 20 X5 + 8 X6 + 14 X7 + 0 X8 + 0 X9 + 12 X10 + 8 X11 + 3 X12 + 0 X13 + 9 X14 + 5 X15 + 7 X16 + 0 X17 + 11 X18 + 6 X19 + 13 X20

Constraints:

1	X1 + 1	X2 + 1	X3 + 1	X4 + 0	X5 + 0	X6 + 0	X7 + 0	X8 + 0	X9 + 0	X10 + 0	X11 + 0	X12 + 0	X13 + 0	X14 + 0	X15 + 0	X16 + 0	X17 + 0	X18 + 0	X19 + 0	X20 = 60
0	X1 + 0	X2 + 0	X3 + 0	X4 + 1	X5 + 1	X6 + 1	X7 + 1	X8 + 0	X9 + 0	X10 + 0	X11 + 0	X12 + 0	X13 + 0	X14 + 0	X15 + 0	X16 + 0	X17 + 0	X18 + 0	X19 + 0	X20 = 80
0	X1 + 0	X2 + 0	X3 + 0	X4 + 0	X5 + 0	X6 + 0	X7 + 0	X8 + 1	X9 + 1	X10 + 1	X11 + 1	X12 + 0	X13 + 0	X14 + 0	X15 + 0	X16 + 0	X17 + 0	X18 + 0	X19 + 0	X20 = 70
0	X1 + 0	X2 + 0	X3 + 0	X4 + 0	X5 + 0	X6 + 0	X7 + 0	X8 + 0	X9 + 0	X10 + 0	X11 + 0	X12 + 0	X13 + 1	X14 + 1	X15 + 1	X16 + 0	X17 + 0	X18 + 0	X19 + 0	X20 = 50

Фиг. 2. Вид на програмата PHP Simplex

Използвайки задачата за минимизиране заменяме $\min Z = -\max(-Z)$, програмата PHP Simplex преобразува задачата за минимизиране (MINIMIZE) в задача за максимизиране (MAXIMIZE). Решението на разглежданата задача с приложение на програмата PHP Simplex се генерира в шестата симплекс-таблица на втората фаза. Методът за решаване на многоетапни транспортни задачи с

използване на PHP Simplex може успешно да се използва в практиката при планирането на товарните превози. Предимство на описания метод е, че оптималният вариант може да се получи още при самото планиране на превозите, което е от значение при практическото приложение, тъй като само тогава може да се реализира икономически ефект.

1. Получава се, че общите сумарни транспортни разходи на разглежданата задача възлизат на сума, което е с 12,73% по-малко в сравнение с общите сумарни транспортни разходи от предходни трансфери при решаване на задачата на два отделни етапа.

2. С илюстрирания автоматизиран метод за решаване на многоетапни транспортни задачи с приложение на програмата PHP Simplex могат да се решават многоетапни транспортни задачи затворен и отворен модел без ограничение на размерите им.

3. Друго предимство на илюстрирания метод с приложение на компютърната програма PHP Simplex е автоматизирането на изчислителния процес за получаване на оптималния план на превозите, осигуряващ минимални сумарни транспортни разходи при решаване на многоетапните транспортни задачи.

ЛИТЕРАТУРА

- [1] Бакалова В., Организация на транспортната дейност в отраслите на икономиката, Университетско издателство „Стопанство”, София, 2009
- [2] Бакалова В., Хр. Николова, Икономика на транспорта, Университетско издателство „Стопанство”, София, 2010
- [3] Бакалова В., Т. Минков, Прогнозиране и планиране на транспортната дейност, Издателски комплекс-УНСС, София, 2011
- [4] Василев Е., Б. Арнаудов, Проектиране развитието на транспорта, Издателски комплекс-УНСС, София, 2012
- [5] Илиева Л., Висша математика първа част, Печатна база на УНСС, София, 2001
- [6] Мутафчиев Л., Е. Василев, Икономико-математически методи и модели в транспорта, Университетско издателство „Стопанство”, София, 1999
- [7] Първанов Хр., С. Цветкова, Организация на товарния транспорт, Университетско издателство „Стопанство”, София, 2006

ВЛИЯНИЕТО НА ESG ВЪРХУ ЛОГИСТИЧНИЯ СЕКТОР И УСТОЙЧИВОТО РАЗВИТИЕ

Ива Б. Такова, Даниел Р. Денев

THE IMPACT OF ESG ON THE LOGISTICS SECTOR AND SUSTAINABLE DEVELOPMENT

Iva B. Takova, Daniel R. Denev

ABSTRACT: *The report examines the impact of ESG (Environmental, Social and Governance) factors on the logistics sector and its role in sustainable development. It analyses the importance of sustainable practices for minimizing the carbon footprint, optimizing resources and implementing environmentally efficient technologies in logistics processes. The social aspect of ESG is examined through the prism of improving working conditions, ensuring the safety of workers in the sector and implementing corporate social responsibility policies. In this context, innovative solutions for automation, digitalization and sustainable transport methods are examined, which not only improve efficiency, but also create better working conditions. From a management perspective, the report analyses the importance of transparency, ethical management and regulatory requirements that shape ESG policies in logistics. It examines good practices implemented by leading companies and their impact on competitiveness and long-term sustainability of the business. The report highlights the need to integrate ESG strategies as a key factor for developing the logistics sector in line with global environmental and social challenges.*

KEYWORDS: *transparency, radioactive materials, safe working environment, working conditions, modern business, radioactive waste*

DOI: <https://doi.org/10.46687/YT24ITK>

Въведение

В последните години темата за устойчивото развитие придобива все по-голямо значение в различни индустрии, включително логистиката. Концепцията ESG се фокусира върху екологичните, социалните и управленските фактори в бизнеса. В логистичния сектор ESG критериите играят ключова роля за намаляване на въглеродния отпечатък, подобряване на условията на труд и осигуряване на прозрачност и отговорност в управлението. Съвременният бизнес е изправен пред предизвикателството да съчетава икономически растеж с устойчиво развитие. Логистиката, като една от най-динамичните индустрии, играе съществена роля в глобалните вериги за доставки и има значително въздействие върху околната среда, обществото и икономиката. Концепцията ESG обхваща три основни аспекта:

- **Околна среда (Environmental):** влиянието на логистичните дейности върху природните ресурси и климатичните промени.

- **Социална отговорност (Social):** условията на труд, безопасността и взаимодействието с местните общности.

- **Корпоративно управление (Governance):** прозрачност, етика и ефективност в управлението на логистичните компании.

Интегрирането на ESG принципите в логистичния сектор е от съществено значение за намаляване на екологичния отпечатък, подобряване на социалните стандарти и осигуряване на дългосрочна устойчивост на бизнеса. [6, 9, 11]

ESG компоненти в логистиката

ESG компонентите в логистиката обхващат три ключови аспекта – екологичен, социален и управленски, които формират устойчивото развитие на сектора. Екологичният компонент се фокусира върху намаляването на въглеродните емисии, оптимизацията на ресурсите и внедряването на зелени технологии. Социалният аспект включва подобряване на условията на труд, безопасността на работниците и социалната отговорност на компаниите. Управленската част засяга прозрачността, етичното корпоративно управление и съответствието с регулаторните изисквания. Интегрирането на тези три елемента е от съществено значение за постигането на устойчива и ефективна логистична индустрия.

• Околна среда

Логистичният сектор оказва сериозно влияние върху околната среда поради интензивното използване на транспортни средства, складови съоръжения и природни ресурси. В отговор на нарастващите екологични предизвикателства, компаниите въвеждат ESG стратегии, насочени към намаляване на въглеродните емисии, повишаване на енергийната ефективност и устойчиво управление на отпадъците. Една от основните мерки за ограничаване на вредното въздействие върху околната среда е преминаването към по-екологични транспортни средства. Използването на електрически, водородни и природногазови превозни средства значително намалява въглеродния отпечатък на логистичните операции. Оптимизацията на маршрутите чрез интелигентни логистични системи също играе ключова роля, тъй като намалява разхода на гориво и изминатите километри. Освен това, кargo консолидирането, или групирането на товари, допринася за ефективното използване на транспортните средства и минимизира ненужните курсове. Складовите съоръжения също са важен компонент в екологичната трансформация на логистиката. Инвестициите във фотоволтаични панели, LED осветление и енергоспестяващи отоплителни и охладителни системи спомагат за повишаване на енергийната ефективност. Все по-често складовете се проектират и сертифицират по международни стандарти като LEED (Leadership in Energy and Environmental Design) и BREEAM, което гарантира намалено екологично въздействие. Автоматизацията и дигитализацията чрез роботизирани складови системи и IoT технологии

допълнително оптимизират енергийното потребление и намаляват ненужните ресурси. Ефективното управление на отпадъците е неразделна част от екологичните ESG политики в логистиката. Компаниите все по-често използват рециклируеми и биоразградими материали за опаковки, което намалява пластмасовите и картонени отпадъци. Освен това, чрез подобро прогнозиране на търсенето, фирмите могат да минимизират свръхпроизводството и разхищението на ресурси, което води до по-устойчиви логистични операции. [4]



Фиг. 1. Екологични мерки в логистиката

• Социална отговорност

Социалният аспект на ESG в логистиката засяга не само условията на труд, но и по-широкото въздействие върху обществото. Логистичната индустрия осигурява заетост на милиони хора по света, което прави социалната отговорност изключително важен фактор за устойчивото развитие на сектора. Компаниите прилагат различни мерки за подобряване на работната среда, развитие на служителите и корпоративна социална отговорност, като целта е създаването на по-етичен и социално отговорен бизнес модел. Едно от основните предизвикателства в логистичната индустрия е осигуряването на безопасни и адекватни условия на труд. В тази връзка компаниите инвестират в подобряване на работната среда, намаляване на риска от трудови инциденти и повишаване на ергономичността на работните места. Прилагането на международни стандарти като ISO 45001 за управление на здравето и безопасността на работното място гарантира по-добра защита на служителите. Особено внимание се отделя на намаляването на работния стрес, като се оптимизират графикаите на шофьорите на дълги разстояния и се създават механизми за по-добър баланс между работа и личен живот. Развитието на кадрите е друг ключов аспект в социалната

отговорност на логистичните компании. Инвестициите в обучения и квалификационни програми допринасят за повишаване на дигиталните умения на служителите и адаптацията им към новите технологии в сектора. За да задържат квалифицираните кадри, компаниите предлагат конкурентни възнаграждения, допълнителни социални придобивки и различни стимули, които мотивират персонала и повишават неговата лоялност. Корпоративната социална отговорност също заема важно място в ESG политиките на логистичния сектор. Компаниите все по-често подкрепят местни инициативи, социални каузи и благотворителни програми, насочени към подобряване на общностите, в които оперират. Освен това, те въвеждат принципи на етично снабдяване, като гарантират, че техните доставчици спазват социалните и трудови стандарти. [3]

• Управление и прозрачност

Добрата корпоративна етика и прозрачността са ключови фактори за устойчивото развитие на логистичните компании. Управлението, основано на принципите на ESG, гарантира етично бизнес поведение, отчетност пред заинтересованите страни и внедряване на иновации за по-ефективно управление. Въвеждането на антикорупционни политики, спазването на международните регулации и използването на цифрови технологии за прозрачност и ефективност са сред основните аспекти, които определят добрите управленски практики в сектора. Прозрачността и отчетността играят съществена роля за доверието между компаниите, клиентите, инвеститорите и регулаторните органи. Публикуването на ESG доклади позволява на заинтересованите страни да проследяват напредъка на организациите в постигането на устойчиви цели и ангажиментите им към екологичните, социалните и управленските стандарти.

Таблица 1. *Спазване на регулации и стандарти в логистиката*

Регулация/Стандарт	Описание
Европейска зелена сделка	Международен стандарт за намаляване на въглеродните емисии, устойчиво развитие и опазване на околната среда
Парижко споразумение	Глобален ангажимент за намаляване на глобалното затопляне чрез намаляване на въглеродните емисии
Инициатива за научно базирани цели	Инициатива за установяване на научно обосновани цели за намаляване на въглеродните емисии и устойчиво развитие

Освен това, прилагането на строги антикорупционни политики и кодекси за поведение гарантира справедлива и етична бизнес среда, минимизирайки риска от злоупотреби. Важен елемент от управлението на съвременните логистични компании е внедряването на технологични решения за повишаване на ефективността и проследимостта на процесите. Блокчейн технологиите осигуряват пълна прозрачност във веригата на доставки, като позволяват надеждно проследяване на пратките и предотвратяване на измами. Изкуственият

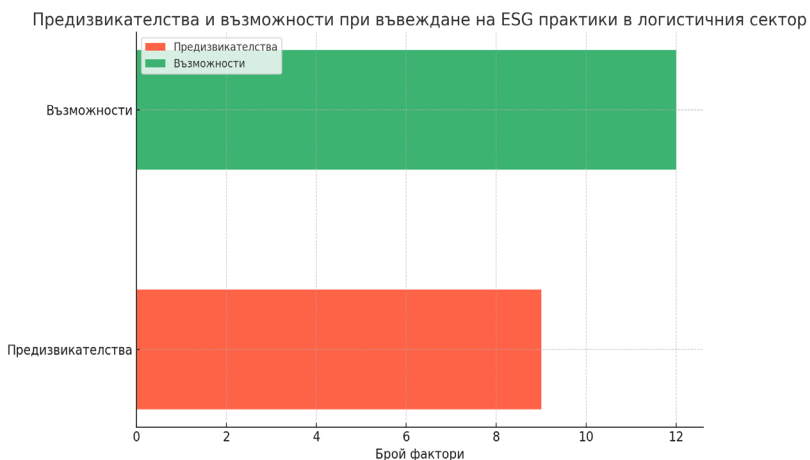
интелект и анализът на големи данни (Big Data) допринасят за оптимизиране на логистичните процеси, намаляване на разходите и подобряване на клиентското обслужване. Спазването на регулаторните изисквания също е съществен аспект на ESG управлението в логистиката. Компаниите все по-често съобразяват дейността си с международни екологични стандарти, като тези, заложиени в Европейската зелена сделка и Парижкото споразумение. [1, 5, 7]

Предизвикателства и възможности

Въведеното на ESG практики в логистичния сектор предоставя както предизвикателства, така и значителни възможности. Компаниите, които се стремят към устойчиво развитие, трябва да се справят с високи първоначални инвестиции, както и с необходимостта от технологична трансформация и обучение на персонала. Освен това, различията в регулаторните изисквания и стандарти между различните държави могат да усложнят процеса на внедряване на ESG практики. Въпреки тези трудности, съществуват редица възможности, които включват дългосрочни икономии чрез повишена енергийна ефективност, подобряване на репутацията и привличане на нови клиенти и партньори, както и достъп до зелени финансираня и субсидии, които могат да подпомогнат устойчивото развитие на логистичния сектор. [2, 8]

Предизвикателства:

- Високи първоначални инвестиции за въвеждане на ESG практики.
- Необходимост от технологична трансформация и обучение на персонала.
- Регулаторна сложност и различни стандарти в отделните държави.



Фиг. 2. *Предизвикателства и възможности при въвеждане на ESG*

Възможности:

- По-ниски дългосрочни разходи чрез енергийна ефективност и оптимизация.
- Подобрена репутация и привличане на повече клиенти и партньори.
- Достъп до зелени финансираня и субсидии за устойчиви проекти.

ESG в логистиката и управление на радиоактивни отпадъци

Екологичният аспект на логистиката, свързан с транспортирането на радиоактивни материали, поставя сериозни изисквания към безопасността и устойчивостта на процесите. Управлението на радиоактивни отпадъци изисква специални мерки за осигуряване на безопасно транспортиране и съхранение, с цел минимизиране на въздействието върху околната среда. В този контекст, намаляването на радиационното замърсяване е от съществено значение. За тази цел се използват специализирани контейнери и протоколи, които предотвратяват изтичания или замърсяване по време на транспортирането. В допълнение, съвременните ESG стандарти насърчават използването на технологии за мониторинг на радиацията, което допринася за по-доброто управление на тези рискове и осигурява безопасността на процесите.

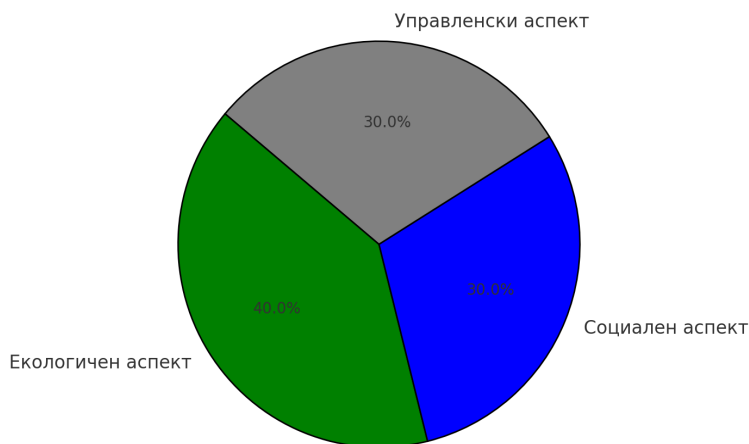
Таблица 2. *Екологичен аспект на логистиката при транспортиране на радиоактивни материали*

Мярка/Аспект	Описание
Минимизиране на радиационното замърсяване	Използване на специализирани контейнери и протоколи за предотвратяване на изтичания и замърсяване
Безопасно транспортиране и съхранение	Изпълнение на изисквания за безопасност по време на транспортиране и съхранение на радиоактивни материали
Мониторинг на радиацията	Използване на съвременни технологии за мониторинг на радиационните нива в процеса на транспортиране
Устойчивост на процесите	Процедури за управление на рискове, свързани с околната среда, за намаляване на въздействието върху природата

Социалният аспект на ESG в логистиката на опасни материали акцентира върху защита на работниците и обществото. Възможността за облъчване е реална опасност, поради което е необходима строга подготовка на персонала, включително специализирано обучение и осигуряване на лични предпазни средства. Това е от съществено значение за минимизиране на рисковете за здравето на служителите, които участват в обработката и транспортирането на радиоактивни материали. В същото време, безопасността на обществото се

гарантира чрез строгите регулации и висока степен на прозрачност в процесите, които осигуряват, че транспортирането на радиоактивни вещества няма да представлява заплаха за населението. Управленският аспект на ESG в този контекст се фокусира върху спазването на регулациите и законите. Логистичните компании трябва да следват международни и национални стандарти, включително тези на Международната агенция за атомна енергия (МААЕ) и Международната морска организация (ИМО), които определят строгите изисквания за безопасност и управление на радиоактивни материали. Освен това, компаниите трябва да поддържат висока степен на прозрачност и отчетност, като редовно докладват за своите дейности и предприетите мерки за безопасност. Това изгражда доверие сред заинтересованите страни и помага за предотвратяване на санкции и правни проблеми, като същевременно демонстрира ангажимент към устойчивото и отговорно управление на тези рискове. Съчетаването на иновации в технологиите с стриктното спазване на екологични, социални и управленски стандарти е от съществено значение за гарантиране на безопасността и устойчивото развитие в логистиката на радиоактивни материали. [5, 6, 7]

ESG в логистиката и управление на радиоактивни отпадъци

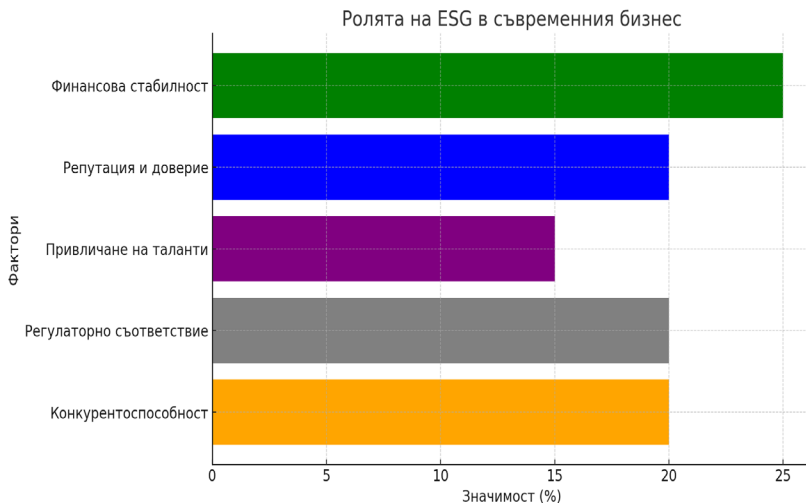


Фиг. 3. ESG в логистиката и управление на радиоактивни отпадъци

Ролята на ESG в съвременния бизнес

Концепцията за ESG играе изключително важна роля в съвременния бизнес, като съдейства за устойчивото развитие и дългосрочния успех на компаниите. Интегрирането на ESG принципите не само че носи значителни ползи за финансовите резултати, но също така укрепва репутацията и

конкурентоспособността на фирмите, като ги поставя в позиция да отговорят на нарастващите изисквания на пазара и обществото. Чрез фокус върху екологичните, социалните и управленските аспекти, предприятията могат да изградят солидна основа за стабилност, да привлекат нови възможности и да се подготвят за бъдещи предизвикателства.



Фиг. 4. Ролята на ESG в съвременния бизнес

- **Подобряване на финансовата стабилност**

ESG стратегиите могат значително да намалят разходите и да повишат оперативната ефективност. Това включва оптимизация на ресурсите чрез намаляване на енергийните и водните разходи посредством устойчиви технологии, както и по-добро управление на рисковете, което намалява въздействието на екологични и социални кризи върху бизнеса. В допълнение, компаниите, които се ангажират с ESG практики, лесно получават достъп до финансиране, тъй като инвеститори и финансови институции все повече изискват доказателства за устойчивото управление на рисковете като условие за отпускане на кредити или инвестиции. [10]

- **Укрепване на репутацията и доверието**

Следването на ESG принципите помага на компаниите да изградят силен обществен имидж и да спечелят доверието на клиентите и партньорите си. Това води до лоялност на клиентите, които предпочитат устойчиви и социално отговорни марки, а също така привлича инвеститори, които виждат в ESG ориентираните компании по-устойчиви и дългосрочни партньори. Прозрачността и отчетността, демонстрирани чрез открити ESG отчети, играят ключова роля за укрепване на доверието сред всички заинтересовани страни.

• Привличане и задържане на таланти

Социалният аспект на ESG е силно свързан с подобряването на условията на труд, което води до по-висока мотивация и продуктивност на служителите. Работниците в компании с ясни социални ценности и ангажменти към устойчивостта се чувстват по-ангажирани и са склонни да останат в организацията за по-дълго време. Това намалява текучеството и свързаните с него разходи, а също така привлича млади и социално отговорни кадри, които са привързани към ESG ориентираните работодатели.

• Регулаторно съответствие и намаляване на правните рискове

Много държави и международни организации наложат все по-строги регулации, свързани с ESG. Компаниите, които се адаптират към тези промени, могат да избегнат санкции и глоби, докато същевременно получават достъп до нови пазари, където устойчивостта е основен фактор за успешна бизнес дейност. Проактивното прилагане на ESG практики също така укрепва корпоративната етика и намалява риска от правни проблеми, свързани с управленски или корупционни скандали.

• Повишаване на конкурентоспособността

ESG инициативите предлагат възможности за иновации, които значително подобряват конкурентоспособността на фирмите. Разработката на устойчиви продукти и услуги отговаря на нарастващото търсене за екологично отговорни решения, а дигитализацията и автоматизацията, свързани с ESG, водят до по-добра ефективност и конкурентни предимства. Оптимизацията на веригата на доставки чрез екологични и социални критерии също така допринася за по-ефективно и сигурно управление на логистичните процеси. Компаниите, които интегрират ESG принципите в своето управление, се намират в по-добра позиция да се адаптират към бъдещите предизвикателства и да привлекат повече клиенти, служители и инвеститори, като същевременно гарантират устойчивото си развитие и дългосрочен успех.

Заклучение

ESG в логистиката не е просто тенденция, а необходимост за бъдещето на индустрията. Компаниите, които внедряват екологични, социални и управленски принципи, постигат не само по-добри бизнес резултати, но и по-силна ангажираност към устойчивото развитие. Чрез иновации, отговорност и стратегическо планиране, логистиката може да се трансформира в по-ефективна, екологична и социално отговорна индустрия. ESG стратегиите са не само отговорност на логистичния сектор, но и възможност за по-ефективно, устойчиво и социално ангажирано развитие. В бъдеще ще наблюдаваме все по-голямо внедряване на иновации и екологични решения, които ще оформят облика на логистиката. ESG стандартите налагат устойчиви и отговорни практики в логистиката, включително за управлението на радиоактивни отпадъци, за да се минимизират рисковете за околната среда.

ЛИТЕРАТУРА

- [1] Allen T., Moore G. Circular Economy in Logistics: Role of ESG in Waste Management and Resource Optimization, 2022, IEEE Transactions on Environmental Engineering, vol. 28, no. 9, DOI: 10.1109/TEE.2022.3149781, pp. 2001-2012.
- [2] Gupta D. Technological Innovations in Logistics: ESG Practices and Their Role in Sustainable Development, 2021, IEEE Transactions on Automation Science and Engineering, vol. 18, no. 3, DOI: 10.1109/TASE.2021.3084914, pp. 1352-1362.
- [3] Kim S., Park B. Integrating ESG Principles in Logistics for Long-Term Sustainability, 2021, IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 8, DOI: 10.1109/TSMC.2021.3097986, pp. 4230-4239.
- [4] Konstantinova E., Tsankov Ts. An overview of sustainable urbanism with the help of Artificial Intelligence. Proceedings of the Ninth student scientific conference "Ecology and environment", 2021, ISSN 2367-5209, pp. 109-121.
- [5] Patel A., Davis D. Social and Governance Aspects in Modern Logistics Operations, 2021, IEEE Transactions on Engineering Management, vol. 67, no. 5, DOI: 10.1109/TEM.2021.3075308, pp. 1245-1255.
- [6] Roberts A., Singh M. The Future of ESG in Supply Chain and Logistics: Trends and Challenges, 2021, IEEE Transactions on Supply Chain Management, vol. 14, no. 4, DOI: 10.1109/TSCM.2021.2950034, pp. 877-887.
- [7] Smith J., Johnson P. Impact of Sustainable Logistics on Carbon Footprint Reduction, 2020, IEEE Transactions on Industrial Informatics, vol. 16, no. 7, DOI: 10.1109/TII.2020.3033456, pp. 2456-2468.
- [8] Tsankov Ts., Konstantinova E. Environmental protection through the use of new technologies for co-generation of electrical and thermal power. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 67, March 2020, ISSN 2367-5721, pp. 91-97.
- [9] Tsankov Ts., Konstantinova E. The neglect of classic electrical insulation materials in modern technology. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 73, September 2020, ISSN 2367-5721, pp. 155-167.
- [10] Yankova-Yordanova Y., Konstantinova E., Tsankov Ts. Forecasting logistics systems through models. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 68, April 2020, ISSN 2367-5721, pp. 105-109.
- [11] Yankova-Yordanova Y., Konstantinova E., Tsankov Ts. Thermal plasma gasification of municipal solid waste and the benefits for the city of Shumen. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 68, April 2020, ISSN 2367-5721, pp. 97-104.

ИЗСЛЕДВАНЕ НА ЕДНОФАЗЕН СТАТИЧЕН ЕЛЕКТРОМЕР

Васил Б. Иванов

RESEARCH OF SINGLE-PHASE STATIC ELECTRICITY METER

Vasil B. Ivanov

ABSTRACT: *Measuring on electrical energy consumed is part of the operation of the network. Measurement accuracy is necessary because errors lead to losses for the supplier. Static electricity meters are displacing induction electricity meters from the market for devices for measuring electricity consumption. In the publication are compares measurement errors with an induction and static (digital) electricity meter.*

KEYWORDS: *measurement accuracy, induction and static (digital) electricity meter, electrical energy*

DOI: <https://doi.org/10.46687/YT24VAS>

Въведение

- Да се изработи лабораторно устройство на монофазен статичен електромер, като се разгледат: архитектурата, схемата на свързване и принципа на действие на два вида електромери – индукционен и статичен.
- Да се направят експериментални измервания с лабораторното устройство и по резултатите да се построят диаграми на грешките, сравнени между двата електромера от индукционен и от статичен вид.
- Лабораторното устройство да се приложи в практическите упражнения, включващи измерване и изследване на електрическа мощност и енергия.

Измерване на електроенергия

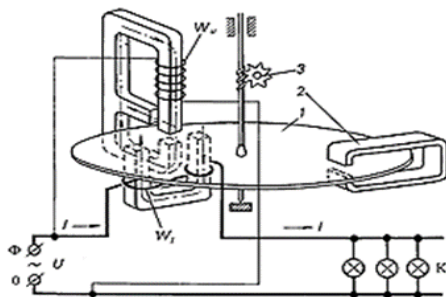
Електромерите са интегриращи измервателни апарати, предназначени за регистриране на количество електрическа енергия за определен интервал от време. Електромерите се използват като средство за търговско измерване между доставчик и потребител (електроразпределително дружество и абонат), така също за баланс и двупосочен обмен („инжектиране“ енергия в мрежата).

• Индукционни измервателни механизми.

Индукционните измервателни механизми използват принципа на въртящия момент на диска, който е пропорционален на честотата на променливия ток. Следователно показанията на апаратите от индукционната система се влияят от измененията на мрежовата честота.

Изводът е, че индукционните измервателни механизми могат да се използват само в променливотокови вериги.

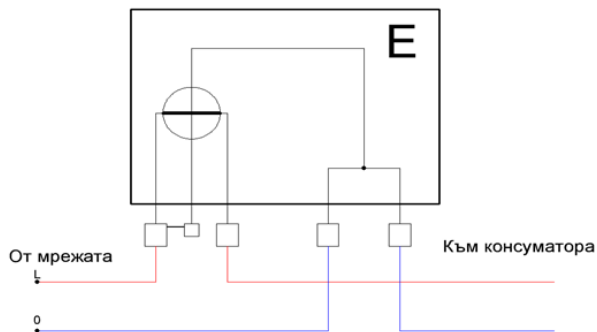
Индукционните електромери се изработват с разнообразна архитектура [6]. Широко разпространение намират електромерите, чието устройство и принцип на действие са разгледани на следната кинематична схема:



Фиг. 1. *Еднофазен индукционен електромер*

В основната конструкция на електромер от фиг.1 са два електромагнита – токов W_1 и напрежителен W_U , чиито магнитопроводи са изработени от листов електротехническа стомана. Бобината на токовия електромагнит W_1 посредством изводите за вход и изход на електромера се включва последователно на консуматора К. Началото на бобината на напрежителния електромагнит W_U е изведено на входящата фазова клемма Φ , която посредством мост се свързва с началото на токовата бобина W_1 . Краят на напрежителната бобина е свързан с нулевата клемма на електромера, като тя се свързва паралелно на консуматорите.

Дискът е означен на позиция 1, а с 2 е означен постоянен магнит, служещ за електромагнитна спирачка. Зъбното колело означено с 3, чрез оста се завърта при задвижване на диска и така задвижва механичния брояч на електромера. При подаване на напрежение двата електромагнита W_1 и W_U се генерират магнитни потоци, които създават бягащо магнитно поле и алуминиевия диск 1 се завърта.



Фиг. 2. *Схема на свързване на еднофазен електромер*

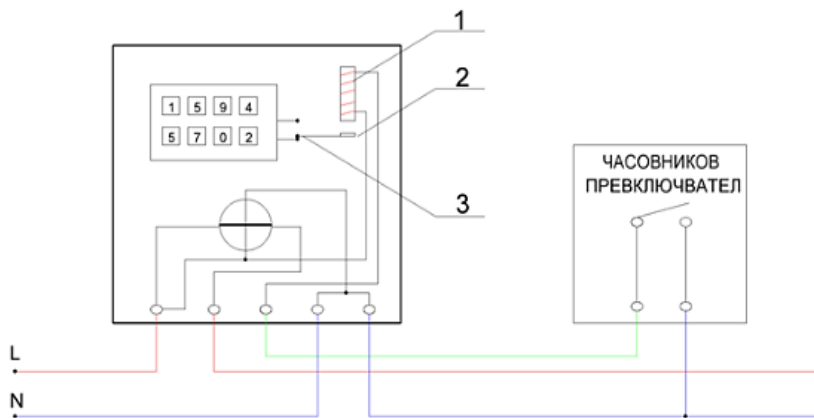
Схемата на свързване на еднофазен електромер е дадена на фиг.2, където фазовия проводник L е свързан последователно на началото на токовата бобина W_1 , а нейният край към изходящата фазова клемма за консуматора. Напрежителната бобина W_U чрез мост на входящата фазова клемма се свързва паралелно на входа и нулевия проводник.

Под действие на въртящия момент дискът на електромера започва да се върти, като пресича магнитния поток на постоянния магнит 2, действащ като магнитна спирачка. Скоростта на движение на диска зависи от големината на консуматора във веригата на електромера.

Извод: Индукционните електромери при номинални условия на работа измерват активна енергия на консуматорите с грешка около 2%. Изменението на напрежението, честотата и температурата влияят сравнително малко на точността им.

• Двойно тарифни индукционни електромери

Електрическата енергия се отчита като нощна и като дневна, посредством специални двойно тарифни електромери. Характерното за двойно тарифните електромери са двата броячни механизма, които се превключват чрез електромагнит и часовник. В определени часове от денонощието механизмите се настройват автоматично чрез превключвател.



Фиг. 3. *Принципна схема на двойнотарифен електромер с часовников превключвател*

На фиг.3 е показана схемата на включване на двойно тарифен електромер с часовников превключвател. Часовникът е електрически и при прекъсване на напрежението трябва да продължи да работи, в противен случай при възстановяване на захранването на консуматорите часовникът няма да показва точно времето и ще превключва броячите в неподходящи часове. Непрекъснатата работа на часовника се осъществява чрез добавяне на акумулаторна батерия включена към електромера.

Грешки от измерването с уредите.

• Абсолютна грешка

Абсолютната грешка се означава с Δ представляваща разликата между показанието на уреда X и действителната стойност X_0 на измерваната величина [3, 7, 8]

$$\Delta = X - X_0 \quad (1)$$

Същата разлика, взета с обратен знак, се нарича корекция (или поправка) на уреда, т.е.:

$$\delta = X_0 - X \quad (2)$$

• Относителна грешка

Относителната грешка ε представлява отношението на абсолютната грешка към действителната стойност X_0 на измерената величина в %:

$$\varepsilon = \Delta / X_0 \cdot 100, \% \quad (3)$$

Относителната грешка ε е най-съществената мярка за точността на измерването. Ако допуснатата от даден измервателен уред абсолютна грешка е еднаква за всички точки от скалата на апарата, големината на относителната грешка ще зависи от стойността на измерваната величина. В началото на скалата допуснатите относителни грешки ще бъдат **по-големи** от тези, които се отчетени при измерването в **края на скалата**.

• Приведена относителна грешка γ

Приведена относителна грешка γ е отношението на абсолютната грешка към номиналното показание X_n , на уреда изразено в проценти.

$$\gamma = \Delta / X_n \cdot 100, \% \quad (4)$$

Тази грешка определя **класа на точност** на измервателните уреди и се записва на скалата или в паспорта на уреда.

Клас на точност на измервателните уреди

Класът на точност е важна обобщаваща характеристика на измервателните уреди. Точността на измерването зависи както от класа на точност, така и от начина на използване на уреда и условията на измерване [5, 8].

• Точността на уредите се нормира чрез техния клас на точност. Оценка за точността на измервателните уреди **по цялата скала дава приведената процентна грешка $\gamma\%$, записана от производителя в паспорта на конкретния модел.**

• **Изчисляване на процентната относителна грешка за аналоговите уреди** използвайки приведената процентна грешка $\gamma\%$:

$$\varepsilon_{\max}\% = \Delta_{\max} / X_n \cdot 100 = (X_n / X_n) \cdot \gamma\% \quad (5)$$

където,

$\Delta_{\max}$ е най-голямата абсолютна грешка в границите на обхвата на стрелковия уред:

$$\Delta_{\max} = (\gamma, \%) / 100 \cdot X_{\text{н}} \quad (6)$$

където,

$\gamma\%$ – процентната приведена грешка (клас на точност), отбелязана на скалата на стрелкови уред;

$X_{\text{н}}$ – номинален обхват на уреда

• **Изчисляване на процентната относителна грешка за цифровите уреди:**

$$\varepsilon_x = \gamma_{\text{(цифр.)}} \% + s / X_{\text{(изм.)}} \cdot 100 \% \quad (7)$$

където,

$\gamma_{\text{(цифр.)}}$ - основната грешка (клас на точност), записана от производителя в паспорта на конкретния модел цифров измервателен уред;

s – разделителната способност (резолюция) записана в паспортните данни, като на практика се определя по най-малката стойност отчетена за дадения обхват;

$X_{\text{(изм.)}}$ – измерената стойност;

Характеристики на измервателните уреди

• Чувствителност

Чувствителността s характеризира способността на измервателния уред да реагира на измененията ΔX на входната величина и определя неговата разделителна способност.

$$s = \Delta Y / (\Delta X) \quad (8)$$

Изменението на изходната величина ΔY се получава при достатъчно малко изменение ΔX на входната величина. От (8) следва, че при **линейна функция** на преобразуването съществува равенството, което означава, че чувствителността s и коефициентът на преобразуване $K = Y/X$ са идентични величини.

$$s = K \quad (9)$$

При **нелинейна функция** на преобразуването (9) не е спазено и тогава

$$s = f(X) \quad (10)$$

• Обхват на измервателният уред ($X_{\text{н}}$)

Обхват на измервателния уред се нарича интервалът между началната $X_{\min}$ и максималната $X_{\max}$ стойност на измерваната величина, която уредът може да измери.

$$X_{\text{н}} = X_{\max} - X_{\min} \quad (11)$$

В случай, че $X_{\min} = 0$, тогава $X_{\text{н}} = X_{\max}$

• Константа (K_x)

Константата K_x се въвежда **при аналогови** (електромеханични) измервателни уреди. Тя представлява число, което се умножава с броя отчетени скални деления θ на уреда, за да бъде получена стойността на измерваната величина.

$$X = K_x \cdot \theta_{\text{отч}} \quad (12)$$

Константата K_x се пресмята чрез формулата

$$K_x = X_n / \theta_n \quad (13)$$

θ_n – общ брой деления на скалата.

• Собствена консумация

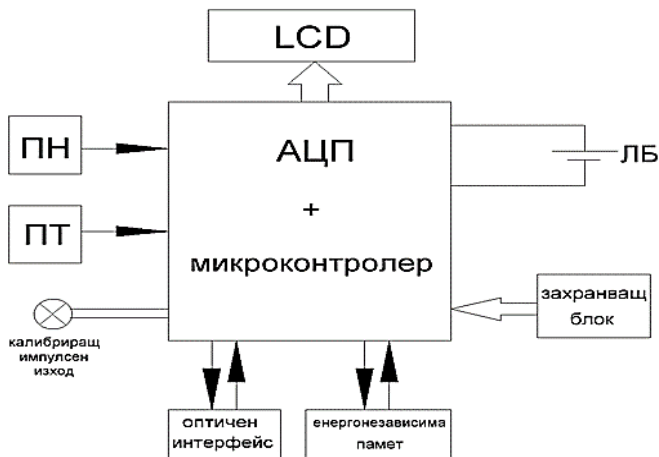
Електрическата енергия консумирана от измервателните уреди през времето на измерванията е собствена консумация.

Анализ: Собствената консумация на уреда за да не влияе върху показанието трябва да бъде сведена до минимум. В противен случай включването на измервателния уред в електрическата верига (ЕВ) на източник с малка мощност би променило режима на работа и грешки при измерването са големи.

Монофазен статичен електромер.

• Устройство и принцип на действие.

Електронните електромери са усъвършенствани измервателни устройства, чиято структура е показана на фиг.4 [1, 2, 4, 8].



Фиг. 4. Блокова схема на съвременен статичен електромер

Статичният електромер от фиг. 4 притежава вградени преобразуватели за **ток** (ПТ-нискоомен високостабилен шунтов резистор - „Датчик на Хол”) и за **напрежение** (ПН-etalонен делител на напрежение). Информацията за големината

на тока се подава от ПТ в аналогов вид към аналогово-цифровия преобразувател (АЦП). Делителят на напрежение ПН подава аналогов пропорционален сигнал към входа на АЦП за преобразуване в цифров вид.

Изчисляването на енергията се извършва от микроконтролер, който е съставен от два модула – изчислителен процесор и процесор с общо предназначение. Енергонезависимата електрически препрограмируема памет (EEPROM) съхранява данните от измерването за години и позволява многократен презапис. Енергонезависимата памет се използва за запис на информацията в регистрите за месечни отчети, системни параметри на електромера и други. Електромерът притежава вграден захранващ блок, осигуряващ напрежения на всички електронни модули. Някои електромери разполагат с вграден часовник-календар, чието предназначение е да превключва тарифите в съответствие с тарифната схема. Непрекъснатата работа на часовника се осигурява от литиева батерия (ЛБ) от фиг.4, гарантираща експлоатация до 10 години. Визуализацията на данните се осъществява на дисплей, който представлява течнокристален индикатор (LCD). Електромерът е снабден с оптичен интерфейс, който предоставя възможност за параметризиране, настройка на дата и час, четене на енергийните регистри, месечни отчети и други.

За проверка на точността на електромера на лицеви панел има изведен **калибриращ импулсен изход (светодиод)**. Когато електромера натрупа активна енергия по-голяма от определено количество ΔE (Wh) той генерира **светлинен импулс**. Най-малката регистрирана енергия ΔE от електромера обуславя преводното число N на електромера:

$$N=1000/\Delta E, \text{ imp/kWh} \quad (14)$$

Светодиодът пулсира с честота на импулсите f_{pulse}

$$f_{pulse}=k.P/3600, \text{ Hz} \quad (15)$$

където:

N – преводното число на електромера

P – активната мощност W

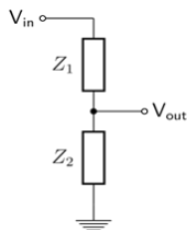
3600 – секунди за един час

В режим „Anti-creep” светодиода започва да свети непрекъснато, когато изходният ток на електромера е по-малък от стартовия. За различните електромери този ток е различен, като варира в диапазона 10 mA до 20mA.

На табелката на електромера са посочени номиналните напрежение и ток, както и максималния ток (в скоби). Максимален е този ток, при който електромерът може да работи продължително без грешката му да надхвърли допустимата. В паспорта на електромера са записани важни характеристики (еднофазен или трифазен, вид измерване, клас на точност, брой тарифи и други).

• Преобразувател на напрежение ПН от архитектурата

ПН е точен високоомен делител показан на фиг.5 изграден от два образцови (точни) резистора $Z1$ и $Z2$, свързани последователно.

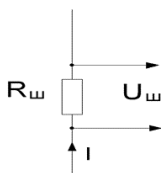


Фиг. 5. *Принципна схема на делител на напрежение ПН*

Делителят се изгражда с образцови резистори свързани последователно и разделящи електрическата верига на два участъка U_{in} и нула и U_{out} и нула.

• **Входен преобразувател на ток ПТ от архитектурата**

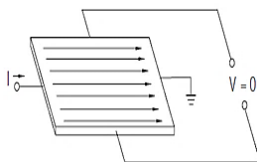
В електронните уреди обикновено токът се преобразува в напрежителен пад $U_{ш}$ чрез електрически шунтове (фиг.6). При променлив и импулсен ток се използват преобразуватели на ток с означение - **сензор на Хол**.



Фиг. 6. *Принципна схема на еталонен шунтов резистор*

• **Сензор на Хол**

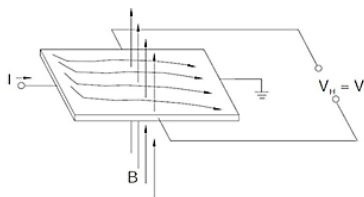
Сензорът на Хол е електронен елемент основаващ се на ефекта на Хол. Проводник във вид на плоска пластинка от фиг.7, по която тече ток е поставена в магнитно поле и се захранва с напрежение V . Когато проводник, по който тече ток е поставен в магнитно поле, възниква електрическо поле (Холова потенциална разлика) в посока перпендикулярна на тока I и на магнитната индукция B .



Фиг.7. *Пластинка на Хол при отсъствие на магнитно поле*

Когато магнитната индукция $B=0$ е перпендикулярна на тока „ I “ (фиг.7), то не се наблюдава потенциална разлика $V = 0$ между горния и долния ръб на пластинката, тъй като „ I “ и токовете носители се разпространяват линейно и не биват отклонявани. При поставяне на пластинката в магнитно поле B на фиг.8,

тогава силата на Лоренц оказва влияние върху протичащия през проводника електрически ток. Нормалното разпространение на тока бива нарушено и в резултат възниква потенциална разлика между точките V_H .



Фиг. 8. *Пластинка на Хол при магнитно поле и възникналата Холова разлика V_H*

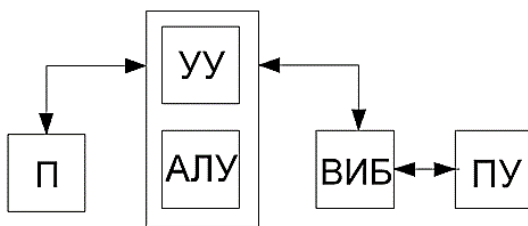
Напрежението на Хол V_H е пропорционално на „I” и „B”, като „U” е между 7 mV -300mV, което налага използването на усилватели, за да може стойността да бъде измерена.

Приложение: Съвременните сензори, работещи чрез ефекта на Хол, се използват при компютърни клавиатури, шевни машини, автомобили, металорежещи автомати, медицински апарати, въздухоплавателни съдове, двигатели, статичните електромери и други.

• Микропроцесори (микроконтролери)

Микропроцесорите в архитектурата на измервателните устройства увеличават тяхната точност, разширяват функционалните им възможности, повишават бързодействието им [1, 2, 4]. Основното предназначение на микропроцесорното устройство е електронно изчислителна обработка на информация, отчитане и съхранение. В изчислителната памет се въвеждат резултатите от измерване и други данни, които се обработват в съответствие с предварително зададен алгоритъм.

Структурната схема на микропроцесорно устройство от фиг.9 съдържа следните блокове:



Фиг. 9. *Структурна схема на микропроцесорно устройство*

- **Аритметичното логическо устройство (АЛУ)** е предназначено за математически операции събиране, изваждане, умножение, деление и др.

Основната математическа операция заложена в микропроцесора като статичен електронен прибор е произведение на ток I , напрежение U и време t , като енергията $W = U \cdot I \cdot t$ се изчислява в $kW \cdot h$.

- **Управляващото устройство (УУ)** координира работата на изчислителните блокове и ги синхронизира с микропроцесора. АЛУ и УУ са обединени в централно процесорно устройство.

- **Паметта (П)** служи за съхранение на програмите в специални регистри.

- **Входно – изходният блок (ВИБ)** осъществява връзката на микропроцесора с различни външни **периферни устройства (ПУ)**.

Всяко устройство с микропроцесорно управление освен микропроцесор (МП) съдържа и други интегрални схеми памет, входно-изходни буфери (В/И) (PIA и ACIA) и др. **Съкупността от микропроцесор, памет и В/И, организирани в цифрова система се нарича микропроцесорна система.** Тя трябва да изпълнява функциите запомняне, обработка, обмен, управление и визуализация. В МП се използват статична ROM и динамична памет RAM, като динамичните памети RAM изискват опресняване на всеки 32 или 16 μs .

Основните операции, чрез които микропроцесорът извършва обмен на данни с останалите блокове от системата, са четене (R) и запис (W). Тези операции се пренасят по трите магистрали.

За да може да се осигури връзка с различни сензори, са необходими средства за въвеждане на аналогова информация в микропроцесорната система. Това се прави с АЦП за преобразуване на аналоговата информация в цифрова.

• Предимства, които се създават в резултат на въвеждането на микропроцесорни системи в измервателните уреди.

- Построяването на многофункционални измервателни уреди, предназначени за измерване на няколко входни величини, като те се определят от изпълняваната програма и могат да бъдат лесно изменени чрез преминаването в друга програма. Това създава гъвкавост при експлоатацията и позволява да се увеличат функциите на уреда по програмен път без съществени промени в апаратната реализация.

- Повишаване на точността на измервателните уреди. Основните възможности за повишаване на точността се състоят в автоматично изключване на систематичните грешки, автоматично изпълнение на калибровъчни операции, намаляване на случайните грешки, чрез провеждане на многократни измервания с последваща обработка на резултатите, откриване и изключване на грубите грешки и други.

- Разширяване на измервателните възможности на уредите. Използването на микропроцесори съществено разширява възможностите за измерване на широка гама от различни физични величини.

- Възможност за математична обработка на измерените стойности. В много случаи с измерената физична величина е необходимо да бъдат извършени различни математични преобразувания. Уредите с вградени микропроцесори позволяват тези преобразувания да бъдат извършени автоматично.

- Използването на микропроцесорните системи в измервателните уреди допринася за намаляване на техните габарити и консумация, за повишаване на

надеждността им и съкращаване на времето за тяхната обработка. Уредите с микропроцесорно управление обикновено имат интерфейсно устройство, с помощта на което те могат да се включват заедно с други уреди в измервателно-изчислителни комплекси.

Приложение: Една от функциите на микропроцесора е изработването на импулси с определена продължителност, която типично е няколко десетки ms. На всеки импулс съответства определено количество енергия, определяна от константата на електромера, зададена на лицеви панел с типични стойности 100, 1000 и 10000 импулса за kWh. Импулсите се подават на измервателен индикатор (обикновено светодиода), чиято честота на мигане е пропорционална на големината на консумираната в момента активна енергия.

Изследване на монофазен статичен електромер

• Общи положения

Експерименталните изследвания на монофазен статичен електромер се базират на измерване на електроенергия в лабораторни условия [8]. При опитите се измерва 100% активна енергия чрез включване на поредица от електрически лампи с нажежаема жичка. Направените измервания с монофазен индукционен електромер се сравняват между работата и

точността на двата електромера – статичен и индукционен. Точността на измерване с електромер е важна характеристика поради търговската дейност за контролно измерване и баланс.

• Проверка на точността на електромера се извършва по методиката:

- Първо се отчитат броя на импулсите на светодиода (обороты на диска при индукционния електромер), като грешката се изчислява по зависимостта:

$$\delta = \frac{C_e \cdot n - P \cdot t}{P \cdot t} \cdot 100\% = \frac{W_{\text{изм.}} - W_{\text{изч.}}}{W_{\text{изч}}} \cdot 100\%, \quad (16)$$

където:

n – брой обороти на диска при индукционния електромер или брой мигания на светлинния индикатор на статичния електромер.

t – времето за което са обработени n импулса от светодиода.

P – мощността измерена с ватметър, W

W_{изм} - Измерената с електромера електроенергия.

$$W_{\text{изм}} = C_e \cdot n, \quad (17)$$

W_{изч} - Изчислената електроенергия

$$W_{\text{изч}} = P \cdot t, \quad (18)$$

Константата при индукционния и статичния електромер:

$$C_e = \frac{1}{N} kWh = \frac{1000 \cdot 3600}{N} Ws/imp, \quad (19)$$

N-преводното число на електромера – например: N=1600imp/kWh.

Преводното число е отбелязано на лицевия панел на електромера, където са дадени основните технически данни.

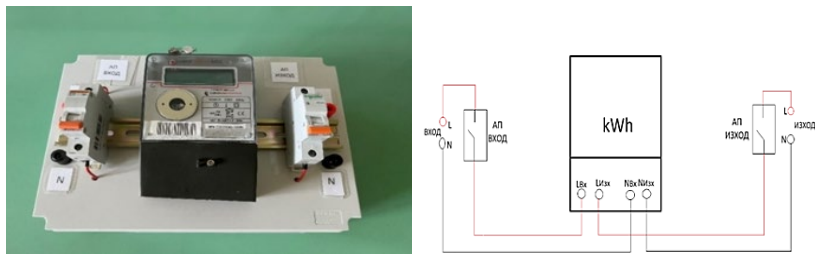
Извод: Статичният (електронен) електромер като съвременен цифров вариант широко се прилага за измерване на електрическа енергия. Микропроцесорното управление създава условие за големи възможности за функционалност и характеристики, осигуряващи редица предимства като дупосочно отчитане, дистанционно мерене по няколко тарифи, таймер за смяна на тарифите и програмиране на нови актуализации.

Сравнителни лабораторни изследвания на двата електромера

• Устройство и технически данни за статичния електромер

Експериментите с лабораторното устройство на статичния електромер е сравняването на неговата точност с електромер от индукционната система [8].

Лабораторното устройство е конструирано от плоска изолационна основа, на която са закрепени: монофазен статичен електромер „Карат МО2“, 4 броя конектори (банан щекери), съответно два броя червени за **фаза L** вход и изход, два броя черни съответно за **нула N** вход и изход. В схемата от фиг.10 задължително се свързват два автоматични прекъсвача (АП) – един 10А на входа и един 6А след електромера.



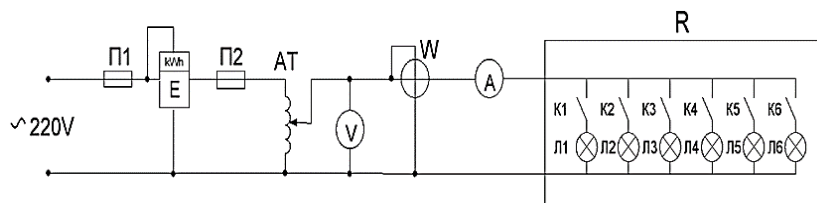
Фиг. 10. Снимка на лабораторното устройство с монтиран статичен електромер и схема на свързване

Техническите данни на производителя Carat Electronics за монофазен статичен електромер „Карат МО2“ са: номинално напрежение – 230V, номинален ток – 10 (60) A, като в скоби е максималния ток при безопасно отчитане, **клас на точност $\pm 2\%$ приведена относителна грешка, константа (преводно число) – 1000 imp/kWh**, отчетни тарифи – нощна и дневна, разрядност – 6/1, измервана енергия – активна.

• Резултати от изследванията на статичен (електронен) и индукционен (електромеханичен) електромер

Направени са изследвания на статичен (електронен) и индукционен (електромеханичен) електромер, като са сравнени крайните резултати между тях.

• Резултати от изследвания на индукционен (електромеханичен) електромер и схема на опитната постановка



Фиг. 11. Схема на опитната постановка

- Елементи изграждащи опитната постановка:
 - Е – Индукционен (електромеханичен) електромер модел: Елиа, тип: А1 – 5Д, номинален ток: 10/40А, номинално напрежение: 220V.
 - П1 и П2 – предпазители със стопяема вложка.
 - АТ-автотрансформатор от 0 – 250V
 - V – Волтметър, 5. А – Амперметър, 6. W – Ватметър
 - R – активно съпротивление изпълнено с лампи с нажежаема жичка - от Л1 до Л6, ключове за всяка лампа - К1 до К6, Л1, Л2 и Л3 всяка по 100 W, а Л4, Л5 и Л6 по 150W.

Опитната постановка се захранва с мрежово напрежение 220V, като при свързването ѝ трябва да се вземат предвид мерки за техническа безопасност. За правилното свързване на електромера е важно да се спази свързване на клемите за фазата и нулата от източника.

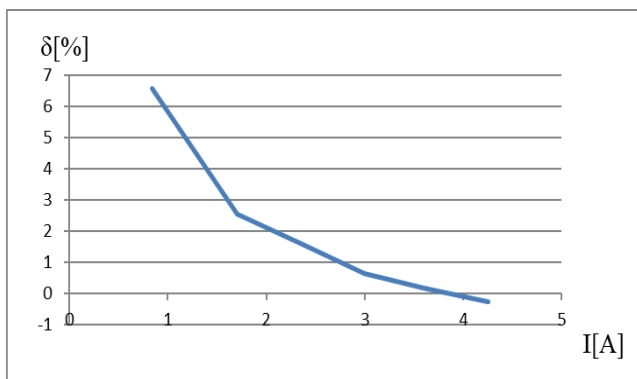
• Резултати от изследванията с включен индукционен електромер

Грешката „ δ ” при измерване с индукционен електромер зависи от **преводното число $N = 600 \text{ об./kWh}$** и времето $t [\text{sec}]$ измерено с хронометър, отчетено при три оборота n на диска. В опитната постановка са използвани аналогови измервателни апарати, като първо се определят техните константи.

Таблица 1. Данни от индукционен електромер

t	P	U	I	n	W _{изм.}	W _{изч.}	δ
[sec]	[W]	[V]	[A]	[об]	[W.S]	[W.S]	%
91,3	185	220	0,84	3	18000	16891	6,57
46,8	375	220	1,7	3	18000	17550	2,56
34,4	515	220	2,35	3	18000	17716	1,6
27,3	655	220	3	3	18000	17881	0,66
22,6	795	220	3,6	3	18000	17967	0,18
19,3	935	220	4,25	3	18000	18045	-0,25

На фиг.13 е построена графика на зависимостта „ $\delta=f(I)$ ” на която се отчита, че при нарастване на консумирания ток, относителната приведена грешка намалява. При много малък ток, т.е. при малка консумация, грешката е относително висока.



Фиг. 12. Графика на грешката на индукционен електромер

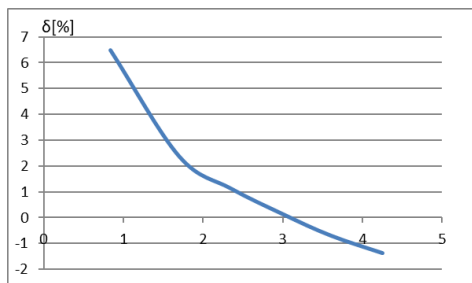
• **Резултати от изследвания със статичен (електронен) електромер** по схемата от опитната постановка на фиг. 11.

Резултатите от измерване със статичния електромер се получават като грешката „ δ ” се определя при отчитане броя на пулсациите от светодиод „n” чрез засичане времето на отброени 10 светлинни импулса с хронометър. Преводното число на електромера „N” е дадено на табелката и за конкретния модел статичен електромер N=1600 имп./kWh.

Таблица 2. Данни от статичен електромер

t	P	U	I	n	W _{изм.}	W _{изч.}	δ
[sec]	[W]	[V]	[A]	[об]	[W.S]	[W.S]	%
114,2	185	220	0,84	10	22500	21127	6,49
58,6	375	220	1,7	10	22500	21975	2,38
43,2	515	220	2,35	10	22500	22248	1,13
34,3	655	220	3	10	22500	22467	0,14
28,5	795	220	3,6	10	22500	22658	-0,69
24,4	935	220	4,25	10	22500	22814	-1,37

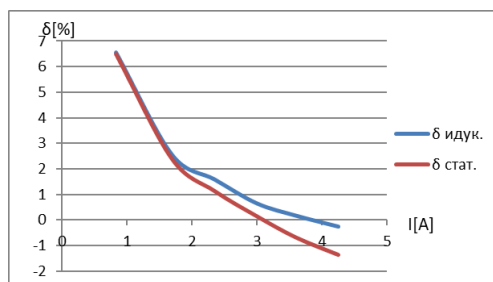
При измерването са използвани същите консуматори при същите условия, както при индукционния електромер. На фиг.13 е построена графиката на зависимостта „ $\delta=f(I)$ ” **при статичния електромер.**



Фиг. 13. *Графика на грешката на статичен електромер*

Изводът от анализа на графиката от фиг.13 при статичния електромер отчита, че колкото повече нараства тока, грешката става все по-малка. При много малък ток, т.е. при малка консумация, грешката е по-малка в сравнение с индукционния електромер.

На фиг.14 са построени две графики за сравняване грешките между индукционния и статичния електромер спрямо тока.



Фиг. 14. *Графика на сравняване на грешките при двата вида електромери*

Анализ и изводи

Получените резултати от лабораторните изследвания са при използване на реални **активни** еднофазни консуматори.

От графиката на фиг.14 следва, че монофазният **статичен електромер измерва и отчита електроенергията по-точно от монофазния индукционен електромер** и при едни и същи консуматори, отчетени след началото на измервателния обхват.

- Електроразпределителните дружества са извели от експлоатация индукционните електромери и са преминали към **статичните електромери поради редица предимства:**

- Статичните електромери притежават много ниско или почти нулево индуктивно съпротивление $X_L = \omega L$ спрямо индукционните, което при тях е много по-високо дължащо се на токовата намотка.

— При статичния електромер липсват въртящи се части и значително се увеличава експлоатационния му срок.

— Статичният електромер притежава вътрешен часовник за превключване на тарифите, програмиран да се настройва при всеки месечен отчет от служител чрез терминално устройство с „оптична глава“, поставена на оптичен приемник към „интерфейса“ на електромера. При статичните електромери с дистанционно отчитане наблюдението на записаните данни се извършва в диспечерски център.

— Недостатък на индукционните електромери е отделния превключвател за тарифите, превключващ се периодично чрез допълнителен външен часовник.

— Статичният електромер измерва и регистрира енергията двупосочно намиращо приложение във възобновяемите енергийни източници (ВЕИ) – вятърни турбини, фотоволтаични системи и др. [6, 7].

— Съвременните модели статични електромери (смайт), не само измерват консумираната енергия, но и отчитат генерираната от ВЕИ източниците активна енергия „инжектирана“ в мрежата, чрез двупосочно измерване.

— Фотоволтаичните системи (ФВС) преобразуващи слънчевата светлина в електроенергия използват двупосочните статични електромери. През деня ФВС присъединена към мрежата произвежда повече енергия от необходимата за консуматорите и излишната се „инжектира“ в електрическата мрежа за търговски цели.

— Статичният електромер притежава по-висок клас на точност, поради дигиталното отчитане.

ЛИТЕРАТУРА

- [1] Атанасов А. Основи на микропроцесорната техника второ издание 2008. ISBN 978-954-9653-06-9.
- [2] Атанасов А. Основи на цифровата информационна техника ISBN 978-954-9653-07-6.
- [3] Панайотова П., Панайотов В. Електрически измервания изд. Матком. ISBN 954-9930-14-9.
- [4] Роджър Токхайм „Цифрова електроника“ изд. Техника София:1999. ISBN 954-03-0523-3.
- [5] Русев Р., Матраков Б., Туренков В. Електрически измервания изд. Техника, ISBN 10:954-03-0597-7
- [6] Ivanov V., “A simulation method for improving the efficiency of power lines from electric networks”, Proceedings of the Union of Scientists - Ruse, Book 1, Technical Sciences, Volume 16, ISSN 1311-106X, стр. 50- 56, 2022.
- [7] Ivanov V., Stoyanov Iv., Kosunalp S., “Applying a Problem-based Learning in the Topic of Modelling of the Power and Improvement the Voltage Stability of Wind Turbines”, DOI: 10.1109/ELMA58392.2023.10202556, ISBN: 979-835031127-3.
- [8] <https://buxtevy.eu/>

ТЕХНОЛОГИЧНИ ТЕНДЕНЦИИ И ЕФЕКТИВНО РАЗВИТИЕ НА СЪВРЕМЕННИ ОТОПЛИТЕЛНИ СИСТЕМИ

Милен С. Давидков, Даниел Р. Денев

TECHNOLOGICAL TRENDS AND EFFICIENT DEVELOPMENT OF MODERN HEATING SYSTEMS

Milen S. Davidkov, Daniel R. Denev

ABSTRACT: *In the context of the growing need for energy efficiency and sustainable development, modern heating systems are undergoing significant technological improvements. This article examines the main trends in the sector, including the implementation of intelligent controls, the integration of renewable energy sources and the increase in the efficiency of traditional heating solutions. Innovative technologies such as heat pumps, hybrid systems and infrared heating are analyzed, which contribute to reducing costs and carbon footprint. Through a comparative analysis, the criteria for selecting an optimal heating system according to the specific needs of users are presented, focusing on future development prospects in this area. In addition to technological progress, regulatory requirements and environmental standards play a key role in the development of modern heating systems, which stimulate the transition to more sustainable solutions. Digitalization and automation further optimize the management of thermal energy, allowing remote control and adaptability to climatic conditions and user habits. In this regard, the development of smart sensors and IoT-based platforms contributes to more precise temperature regulation and reduction of energy losses, which makes heating systems an integral part of the concept of smart homes and energy-efficient buildings.*

KEYWORDS: heating systems, boiler, fuels, automated system

DOI: <https://doi.org/10.46687/YT24DVD>

Въведение

В днешно време има различни начини за отопление на нашите домове. Отоплителните системи могат да бъдат изградени по различни начини относно източника на топлина, като на пример термо помпа, котел на пелети, котел на твърдо гориво (дърва и въглища), газов котел, електрически котел и др. Отоплителната система се състои от елементи предназначени да пренасят и предават топлината на всички отоплителни помещения. В момента най-популярно отоплителна система е изградена с използване на термо помпа вода - въздух. Термо помпата работи на ток и чрез енергия на околния въздух например с температура -10 градуса, чрез компресиране достига температура от

40 градуса на флуида (фреон). Температурата на флуида се предава към отоплителната система чрез топлообменник, като процеса е автоматизиран. Котлите на пелети работят на принципа на котел на твърдо гориво но в този случай горивото което ползват е пелети (гранули). Това отопление е предпочитана за отопление на по- голяма жилище. Тук системата е автоматизирана до толкова, че трябва периодично да чистим котела от пепелта която се получава при горенето на пелети, и съответно да зареждаме пелети. За да се отопляваме с газов котел трябва да има изградена газова инсталация до домът ни. Процеса на работа е изгарянето на природна газ като затопля флуида в отоплителната система. Процеса е абсолютно автоматизиран. [1, 9]

Съвременни технологични тенденции в отоплителните системи

Съвременните отоплителни системи преминават през значителна трансформация, за да отговорят на нарастващите изисквания за енергийна ефективност, устойчивост и икономичност. Развитието на технологиите позволява интегрирането на интелигентни решения, възобновяеми енергийни източници и иновативни методи за отопление, които намаляват разходите и вредните емисии. В този контекст се очертават няколко ключови технологични тенденции, които определят бъдещето на отоплението – от използването на възобновяеми ресурси до автоматизирани системи, базирани на изкуствен интелект и IoT технологии.

- **Внедряване на възобновяеми енергийни източници**

С нарастващата загриженост за околната среда и повишаването на цените на традиционните енергийни източници, все повече отоплителни системи интегрират възобновяеми енергийни източници като слънчева, геотермална и биомасова енергия. Слънчевите колектори, използвани за подгръване на вода и подпомагане на централните отоплителни инсталации, са все по-популярен избор. Геотермалните термопомпи предлагат висока ефективност и устойчивост, като използват топлината от земните недра.

- **Интелигентни и автоматизирани отоплителни системи**

С развитието на технологиите в сферата на изкуствения интелект (AI) и Интернет на нещата (IoT) отоплителните системи стават по-интелигентни и адаптивни. Чрез използването на сензори и свързани устройства, те могат да регулират температурата в зависимост от присъствието на хора, външните атмосферни условия и потребителските навици. Това позволява значително намаляване на енергийните загуби и разходите за отопление. [5]

- **Хибридни отоплителни решения**

Комбинирането на различни отоплителни технологии в хибридни системи става все по-често срещано решение. Например, термопомпите могат да работят в синергия с газови котли или електрически нагреватели, за да осигурят по-гъвкава и ефективна работа в зависимост от климатичните условия.

Таблица 1. Основните технологични тенденции в съвременните отоплителни системи по ключови параметри

Технология	Енергийна ефективност %	Първоначални разходи лв.	Поддръжка лв./год.	Въглероден отпечатък g CO ₂ /kWh	Среден живот години
Слънчеви колектори	60-80	3000-8000	100-300	0	20-25
Геотермални термопомпи	300-500 (COP 3-5)	15000-30000	300-600	0-10	20-30
Интелигентни термостати и IoT системи	10-30% намаление на разходите	200-1000	50-150	Намаляват CO ₂ чрез оптимизация	5-10
Хибридни системи (Термопомпа + Газов котел)	100-150 (COP 1-1.5)	10000-20000	500-1000	100-200	15-20
Инфрачервено отопление	90-98	500-3000	50-200	0 (ако се захранва с ВЕИ)	10-15
Кондензационни газови котли	90-98	4000-10000	300-700	180-250	15-20
Биомаса и пелетни котли	75-90	5000-15000	500-1000	50-100	15-25

Ефективност и предимства на съвременните отоплителни технологии

Енергийната ефективност и устойчивото развитие са основни приоритети в модерните отоплителни технологии. В търсене на оптимални решения, производителите се стремят да намалят разходите за енергия, да увеличат експлоатационния живот на системите и да сведат до минимум вредното въздействие върху околната среда. Новите технологии предлагат не само по-висока ефективност, но и по-голям комфорт за потребителите чрез интелигентно управление и адаптивност към климатичните условия. В тази част на доклада се разглеждат основните предимства на съвременните отоплителни технологии, включително икономическите, екологичните и техническите аспекти на тяхното развитие. [3]

- **Енергийна ефективност и икономически ползи**

Съвременните отоплителни системи са проектирани така, че да постигнат висока енергийна ефективност и да намалят разходите за отопление. Високоэффективните термопомпи, кондензационните газови котли и инфрачервените нагреватели могат да намалят разходите за енергия с до 30-50% в сравнение с традиционните отоплителни методи.

- **Екологични предимства и намаляване на въглеродния отпечатък**

Използването на възобновяеми енергийни източници и енергийно ефективни технологии допринася за намаляване на вредните емисии. Намаляването на зависимостта от изкопаеми горива е ключов фактор за борбата с климатичните промени.

- **Устойчивост и дълготрайност на новите системи**

Модерните отоплителни технологии се характеризират с висока издръжливост и по-дълъг експлоатационен живот. Например, геотермалните термопомпи могат да функционират ефективно над 20-25 години, а соларните колектори – над 30 години, при минимални разходи за поддръжка.

Критерии за избор на отоплителна система

Изборът на подходяща отоплителна система е ключов фактор за осигуряване на енергийна ефективност, икономичност и дълготрайна експлоатация. В зависимост от климатичните условия, характеристиките на сградата и индивидуалните нужди на потребителите, различните технологии предлагат разнообразни предимства и предизвикателства. Освен първоначалните инвестиционни разходи, е важно да се отчетат и дългосрочните експлоатационни разходи, поддръжката и екологичният отпечатък на системата. В тази част се разглеждат основните критерии, които трябва да бъдат взети предвид при избора на оптимално отоплително решение [2, 8, 10]. При избора на подходяща отоплителна система е важно да се вземат предвид няколко основни фактора:

— **Климатичните условия** – някои системи са по-ефективни в определени климатични зони.

— **Големината и изолацията на сградата** – добре изолирани сгради изискват по-малко енергия за отопление.

— **Разходи за първоначална инвестиция и експлоатация** – макар някои технологии да изискват по-висока първоначална инвестиция, те могат да намалят разходите в дългосрочен план.

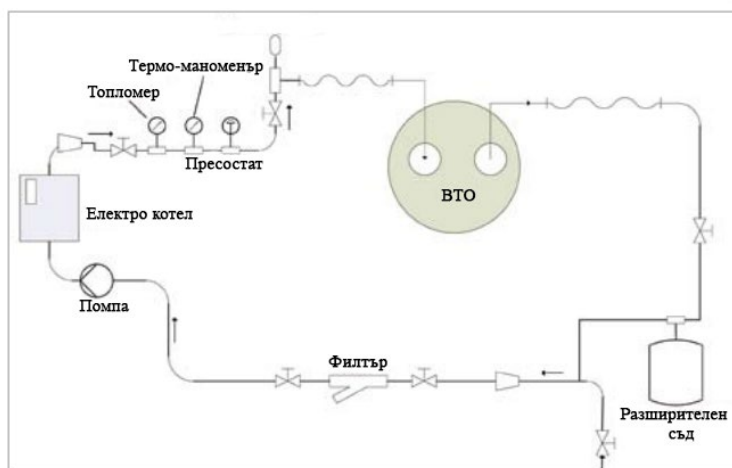
— **Екологичен отпечатък** – използването на екологични решения допринася за устойчивото развитие.

Техническо устройство и принцип на работа на съвременните електрически котли

В тази точка ще разгледаме подробно електрическите котли, техните компоненти и принципа на работа показани на схемата на фиг. 1. Електрическите котли работят, като флуида в отоплителната система преминава през водосъдържател в който има монтиран електрически нагревател. Електрическите нагреватели в електрическите котли са проектирани да са максимално ефективни. След като флуида се загрее до желаната температура преминава през останалите елементи на отоплителната система. Електрическият котел работи на принципа на съпротивително отопление. Това е преобразуване на електрическа енергия в отоплителна. Предимството на електрическия котел е това, че е 100% ефективен при преобразуване на електричеството в топлина. [4]

Нека разгледаме по-подробно електрическите котли, показани на Фиг.2 и 3 техните компоненти и принципа на работа. Електрическите котли работят като флуидът в отоплителната система преминава през водосъдържател, в който е монтиран електрически нагревател. Електрическите нагреватели в електрическите котли са проектирани да бъдат максимално ефективни. След като флуидът се загрее до желаната температура, той преминава през останалите

елементи на отоплителната система. Електрическият котел работи на принципа на съпротивително отопление. Това означава преобразуване на Електрическите котли имат редица предимства, които ги правят популярни за отопление в различни типове сгради. Те са компактни и лесни за инсталация, което ги прави подходящи за малки и средни жилища, а също така и за апартаменти, където мястото е ограничено. В допълнение, тези котли не изискват специална поддръжка, като например почистване на пепелта или зареждане с гориво, както е случаят с котлите на пелети или котлите на твърдо гориво. Те също така не излъчват вредни емисии, което ги прави екологично чисти и подходящи за места с високи изисквания за енергийна ефективност. Един от основните недостатъци на електрическите котли е цената на електричеството. В зависимост от местните тарифи за електрическа енергия, отоплението с електрически котел може да се окаже по-скъпо в сравнение с други източници на топлина, като газ или пелети. Въпреки това, за краткосрочни и средносрочни нужди, електрическите котли могат да бъдат икономически изгодни, особено ако се използват за отопление само на една част от дома или в малки помещения.



Фиг. 1. *Принципна схема на инсталация за провеждане на ОТХ*

Освен високата ефективност при преобразуването на електрическата енергия в топлина, електрическите котли предлагат възможност за интеграция с модерни системи за управление, което допълнително оптимизира потреблението на енергия. Тази автоматизация позволява автоматично регулиране на температурата според реалните нужди на помещението и външните климатични условия, като по този начин се минимизират енергийните загуби и се увеличава общата ефективност на отоплителната система. Компактният дизайн и лесната инсталация ги правят предпочитан избор за малки и средни обекти, където пространствените ограничения и високите изисквания за екологична устойчивост

са от особено значение. В същото време, потребителите трябва да преценят оперативните разходи спрямо местните тарифи за електричество, за да се осигури икономическата изгодност на решението.



Фиг. 2. *Общ вид на системата*



Фиг. 3. *Окабеляване на системата*

Таблица 2. *Приложения на електрическите котли*

Тип сграда	Подходящо за използване	Причина
Малки жилища и апартаменти	Да	Компактен размер, лесна инсталация
Офиси и търговски обекти	Да	Лесна поддръжка, без вредни емисии
Големи промишлени сгради	Не	Висока консумация на електроенергия
Къщи с ограничен достъп до газ	Да	Няма нужда от газова връзка

Допълнително, съвременните технологии в електрическите котли позволяват интеграцията им с различни умни системи за управление на дома, което дава възможност за дистанционно управление на температурата и оптимизиране на енергийната консумация. Това ги прави още по-удобни за използване и предоставят възможност за значително намаляване на разходите за отопление чрез по-добро регулиране на отоплителния процес.

Въпреки тези предимства, изборът на отоплителна система зависи от множество фактори, включително климатични условия, размер на помещението, наличието на достъп до природен газ и финансовите възможности на собствениците. Всеки вид отоплителна система има своите плюсове и минуси, които трябва да бъдат внимателно обмислени преди вземането на решение. [1, 7]

Сравнение на различните видове отоплителни системи

В настоящата част на доклада ще се направи сравнителен анализ на различните видове отоплителни системи, използвани в съвременната практика. Всеки тип система притежава свои особености, които я правят подходяща за конкретни приложения в зависимост от техническите изисквания, наличните ресурси и климатичните условия.

- **Централно отопление (газови, електрически и кондензационни котли)**

Централното отопление е традиционен и широко разпространен метод за затопляне на сгради. Газовите котли са предпочитани заради бързата си реакция и висока мощност, но стандартните модели могат да генерират значителни емисии. Кондензационните котли решават този проблем, като използват технология за възстановяване на топлината от отработените газове, което повишава общата им ефективност. Електрическите котли, работещи на принципа на съпротивително отопление, имат почти 100% ефективност при преобразуването на електрическата енергия в топлина, но разходите за електричество могат да бъдат по-високи в сравнение с газовите решения. [6, 11]

- **Термопомпи (въздушни, водни и геотермални)**

Термопомпите представляват иновативна технология, която извлича топлината от външната среда – въздух, вода или земната повърхност – и я преобразува за отопление. Въздушните термопомпи са лесни за инсталация и подходящи за региони с умерени зимни температури, но ефективността им може да намалее при екстремно ниски температури. Водните и геотермалните термопомпи, от своя страна, осигуряват стабилна и висока ефективност благодарение на постоянната температура на водните източници или земната маса, въпреки по-високите първоначални разходи и по-сложната им инсталация.

- **Инфрачервено отопление и лъчисти панели**

Инфрачервеното отопление работи на принципа на директното излъчване на топлина, като нагрява обектите и хората в помещението, а не въздуха. Този метод предлага бързо затопляне и висока енергийна ефективност, което го прави идеален за допълнително отопление или за локални зони. Лъчистите панели могат да се монтират на таван или стена, осигурявайки равномерно разпределение на топлината, но оптималната им работа изисква прецизно планиране на разположението.

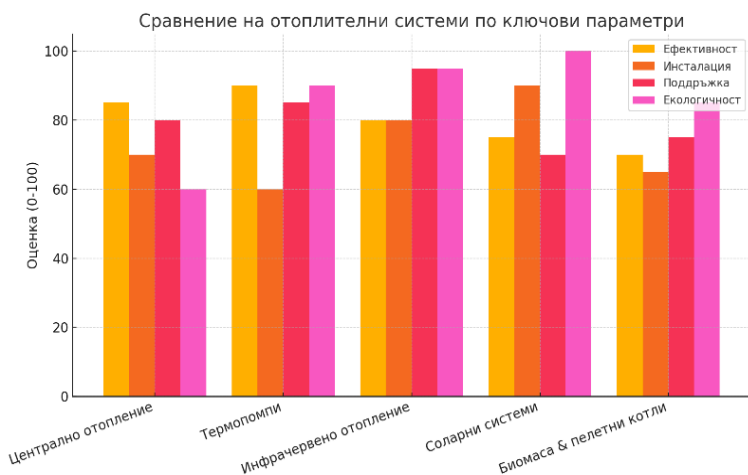
- **Соларни отоплителни системи**

Соларните системи използват енергията на слънцето чрез колектори за предварително загряване на вода или въздух. Този метод е екологично чист и може да значително намали консумацията на конвенционални енергийни

източници. Основният недостатък е зависимостта от атмосферните условия – в по-мрачни и облачни дни ефективността им може да спадне, което обикновено налага интеграция с други отоплителни решения за осигуряване на непрекъсната топлина.

• Биомаса и пелетни котли

Отоплението чрез биомаса използва естествени горива като дървени пелети, стърготини или други органични материали. Тези системи се считат за възобновяеми и устойчиви, особено ако горивото е локално произведено. Те предлагат добро съотношение между разходи и ефективност, като допринасят за намаляване на въглеродния отпечатък. Недостатъците включват необходимостта от съхранение на горивото, редовна поддръжка и управление на емисиите на прахови частици, което може да бъде предизвикателство в урбанизирани райони.



Фиг. 4. Сравнение на отоплителни системи по ключови параметри

Заклучение

В крайна сметка, изборът на подходяща отоплителна система зависи от индивидуалните нужди и условия на всяко домакинство. Термопомпите, котлите на пелети, газовите котли и електрическите котли са само някои от възможностите, които предоставят ефективни решения за отопление. Най-важното е да се избере система, която не само да отговоря на техническите изисквания, но и да бъде икономически и екологично устойчива. Добре проектираната и правилно инсталирана отоплителна система може да осигури комфорт и уют през студените месеци, като същевременно намалява разходите за енергия и вредните въздействия външната електрическа енергия в топлина. Предимството на електрическия котел е, че той е 100% ефективен при преобразуването на електричеството в топлина.

ЛИТЕРАТУРА

- [1] Chen J., Xu Y., "Integration of Renewable Energy Sources in Modern Heating Systems: A Review," 2020, IEEE Access, vol. 8, DOI: 10.1109/ACCESS.2020.2987654, pp. 123456-123470.
- [2] Garcia M., Patel R., "Energy Efficiency Optimization in Modern HVAC Systems Using IoT Technologies," 2022, IEEE Internet of Things Journal, vol. 9, no. 5, DOI: 10.1109/JIOT.2022.3101234, pp. 8765-8776.
- [3] Konstantinova E., Tsankov Ts. Analyzing security threats in smart homes technology. International Scientific Conference "Defense Technologies" DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 373-378.
- [4] Konstantinova E., Tsankov Ts. An overview of sustainable urbanism with the help of Artificial Intelligence. Proceedings of the Ninth student scientific conference "Ecology and environment", 2021, ISSN 2367-5209, pp. 109-121.
- [5] Kumar R., Singh P., "Hybrid Heating Systems Combining Renewable and Conventional Energy Sources," 2021, IEEE Transactions on Sustainable Energy, vol. 12, no. 1, DOI: 10.1109/TSTE.2020.2998765, pp. 123-134.
- [6] Liang X., Zhang T., "IoT-Based Smart Heating Systems: Design and Implementation," 2022, IEEE Internet of Things Journal, vol. 9, no. 5, DOI: 10.1109/JIOT.2021.3079876, pp. 3450-3462.
- [7] Smith J., Liu Y., "Advancements in Smart Heating Systems Integrating Renewable Energy Sources," 2023, IEEE Transactions on Sustainable Energy, vol. 14, no. 3, DOI: 10.1109/TSTE.2023.3056789, pp. 1234-1245.
- [8] Tsankov Ts., Konstantinova E. Environmental protection through the use of new technologies for co-generation of electrical and thermal power. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 67, March 2020, ISSN 2367-5721, pp. 91-97.
- [9] Tsankov Ts., Konstantinova E. The neglect of classic electrical insulation materials in modern technology. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 73, September 2020, ISSN 2367-5721, pp. 155-167.
- [10] Wang L., Li H., Zhang Y., "Intelligent Control Strategies for Energy Efficiency in Smart Heating Systems," 2021, IEEE Transactions on Smart Grid, vol. 12, no. 3, DOI: 10.1109/TSG.2021.3056789, pp. 2345-2356.
- [11] Zhou Q., Wang S., "Advancements in Heat Pump Technologies for Building Heating: A Comprehensive Review," 2019, IEEE Transactions on Industrial Electronics, vol. 66, no. 3, DOI: 10.1109/TIE.2018.2844856, pp. 1812-1825.

КЛАСИФИКАЦИЯ В МАШИННОТО ОБУЧЕНИЕ. КЛАСИФИКАЦИОННИ МОДЕЛИ. МЕТОДИ И МЕТРИКИ ЗА ОЦЕНКА

Мая П. Тодорова

CLASSIFICATION IN MACHINE LEARNING. CLASSIFICATION MODELS. EVALUATION METHODS AND METRICS

Maya P. Todorova

ABSTRACT: *In this article is presented classification as an activity and as a process for creating a classification model in machine learning. The emphasis is also on its application. Five main criteria for comparing models created using different algorithms are formulated. Four methods for cross-validation are described - Hold-Out Validation, Repeated random sampling, K-Fold Validation, Leave-One-Out. Metrics for evaluating a created classification model are presented, such as accuracy, precision, classification error, recall, F-measure and ROC curves.*

KEYWORDS: *Confusion Matrix, Hold-Out Validation, K - Fold Validation, Leave-One-Out, Accuracy, Classification Error, Receiver Operating Characteristic curves*

DOI: <https://doi.org/10.46687/YT24MYA>

Въведение

Класификацията като дейност, разпределя предмети, процеси, обекти, видове, типове според някакви съществени признаци и ги разполага в определен ред, отразяващ степента на сходство помежду им. Класификацията е процес на групиране на данни в съответствие с техни общи признаци [1]. Процесът обхваща изграждане на модели, които описват съществуващи класове от обекти, с цел тяхното използване, за определяне на класа на обект, който е неизвестен. Моделите се изграждат чрез анализ на извадка от обучаващи данни (training data) – обекти с известен клас на принадлежност.

Класификационните модели са подходящи както за описание и интерпретация на данните, така и за предсказване, като и в двата случая се реализира извличане на закономерности чрез обучение. Преди създаването на класификационен модел се прилага анализ на изключения, който позволява те да бъдат премахнати с цел подобряване на качеството на класификатора.

Целта на класификационния модел е да идентифицира повтарящи се взаимовръзки между входни променливи, които описват обектите, принадлежащи на един и същи клас. Откритите взаимовръзки се трансформират в класификационни правила. Класификационните правила се използват за

предсказване на класа на обекта. Класификационните правила могат да бъдат представяни под различна форма в зависимост от типа на използвания модел.

Предсказващото моделиране използва класификационни модели, в които стойността на целевия атрибут може да бъде зададена предварително или изведена от сегментацията. Анализът на изключенията се прилага върху данните преди да бъде създаден класификационният модел с цел неговото подобрене [2].

Критерии за сравнение на методите за класификация

Методите за класификация се оценяват и сравняват на базата на следните основни критерии:

1. Точност на предсказване;

Точността на предсказване на модел е възможността за правилно определяне на класа на нов обект.

2. Време;

Определя се от необходимия изчислителен ресурс използван както при генериране, така и при прилагане на модел.

3. Устойчивост;

Устойчивостта на модела се обуславя от неговото поведение при наличие на шум, липсващи данни, различни типове променливи и др.

4. Скалируемост;

Скалируемостта е възможността на генерирания модел да работи ефективно при наличието на големи обеми данни.

5. Разбираемост;

Разбираемостта се определя от степента на лесно интерпретиране и използване на моделите от потребителите.

Методи за кръстосано валидиране

Оценката на генерираните модели за класификация се реализира чрез прилагане на методи за кръстосано валидиране.

1. Валидация на отложените данни (Hold-Out Validation);

При прилагане на валидация на отложените данни, обектите в обучаващата извадка се избират на случаен принцип, останалите обекти попадат в тестовата извадка. Част от алгоритмите за класификация реализират еднакво пропорционално разпределение на обектите от различните класове в обучаващата и тестовата извадки. Големината на обучаващата извадка може да варира в зависимост от големината на общата съвкупност от данни. Най-често обучаващата извадка включва от 1/2 до 2/3 от общия брой записи в изследваната съвкупност от данни.

Валидацията на отложените данни се прилага при наличие на много голям набор от данни. Методът изисква по-малко изчислителна мощност в сравнение с други методи за кръстосана проверка. Недостатъкът на този метод е, че оценката зависи от разделянето на данните. Точността на оценявания класификационен алгоритъм зависи от избора на тестова извадка, което може да доведе до надценяване или подценяване спрямо действителната точност на предсказване, при промяна на тестовата извадка. За постигане на по-устойчива оценка на

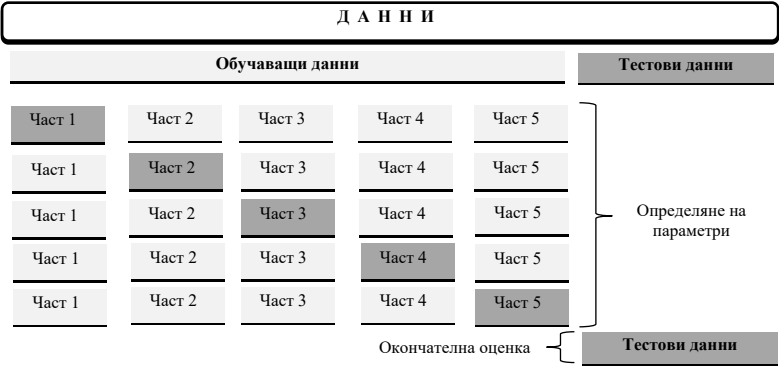
точността на класификационния модел, се използват други методи. Статистически е неефективен, тъй като голяма част от данните не се използват за обучение на модела [3].

2. Многократно случайно избиране на обектите в обучаващата и тестовата извадки (Repeated random sampling);

Методът се характеризира с многократно повторение на процедурата по разделянето на общата съвкупност от данни на две части – обучаваща и тестова. При всяко повторение двете извадки се избират на случаен принцип. Определя се точността на класификация на получения модел, за съответната итерация. Точността на класификатора се изчислява като средноаритметично на получените оценки за отделните итерации. Броят на повторенията може да бъде определен чрез предварително прилагане на различни статистически техники отчитайки големината на изследваната обща съвкупност от данни. Този метод не осъществява контрол над броя на попаденията на даден обект от общата съвкупност от данни в обучаващата и тестовата извадка, което може да окаже неблагоприятен ефект върху генерираните класификационни правила и оценката на точността, в случай при наличието на доминиращ обект, за който една или повече променливи приемат необичайни стойности (изключения).

3. k-кратна кръстосана проверка (K - Fold Validation);

Данните се разделят на k равни подмножества. Методът се повтаря k пъти, така че всеки път, едно от k подмножествата се използва като набор за валидиране, а останалите k-1 подмножества се събират, за да образуват обучаващия набор [11, 12]. Оценката на грешките е усреднена за всички k изпитвания. Всяка точка от данни се среща само веднъж в комплекта от данни за валидиране и k-1 пъти в тренировъчната извадка. Това води до намаляване на пристрастията и на дисперсията. Размяната на учебните и тестовите извадки допринася за ефективността на този метод. Предимството на този метод е, че всички наблюдения се използват както за обучение, така и за валидиране. На Фиг. 1. е представена пет-кратна кръстосана проверка.



Фиг. 1. Процес на пет-кратно кръстосано валидиране

Общата съвкупност от данни се разделя на пет части и алгоритъмът се изпълнява пет пъти, като всеки път четири от пет части се използват като обучаваща извадка, а останалата една част се използва за тестова [3].

4. Кръстосано валидиране на отделни обекти (Leave-One-Out);

Всеки обучителен набор се създава, като се вземат всички наблюдения, с изключение на едно[11]. Тази процедура на кръстосано валидиране не води до загуба на много данни, тъй като само една проба е премахната от тренировъчния комплект. На всяка итерация почти всички данни с изключение на едно наблюдение се използват за обучение и моделът се тества на това единствено наблюдение. Всеки обект участва в тестовата извадка точно веднъж, а дължината на подизвадката за обучение е само с една по-малка от дължината на пълната извадка [4].

Метрики за оценка на класификационни модели

1. Матрица на грешките (Confusion Matrix)

Предсказването на бинарна променлива е най-често срещан случай при решаването на задачи за класификация. При бинарна класификация съществуват два класа - положителен (Positive) и отрицателен (Negative) - и резултатът от класификатора е правилен или неправилен. В този случай матрицата на класификация е с размерност 2×2 . Редовете на матрицата представляват действителните екземпляри от съответния клас, а колоните класовете, получени след прилагането на класификационния модел върху тестовите данни.

Когато предсказваната величина не е бинарна променлива, а може да приема N различни стойности, тогава матрицата на класификация ще бъде квадратна матрица с N реда и N стълба.

На Табл. 1. е представена матрица на грешките при бинарна класификация.

Таблица 1. Матрица на грешки

Реален клас	Предсказан клас	
	Positive / 1	Negative / 0
Positive / 1	True Positive (TP)	False Negative (FN)
Negative / 0	False Positive (FP)	True Negative (TN)

Съществуват четири възможни варианта за класификация на всеки обект:

- **True Positive** – положителните примери от извадката са правилно обозначени от класификатора, като положителни;
- **False Negative** – положителните примери са неправилно обозначени като отрицателни;
- **False Positive** – отрицателните примери са неправилно обозначени като положителни;
- **True Negative (TN)** – отрицателните примери са правилно обозначени като отрицателни [5].

Главният диагонал на матрицата съдържа правилно предсказаните обекти (TP и TN), а останалите елементи на матрицата – грешно предсказаните обекти (FP и FN).

На базата на класификационната матрицата се определят метрики, които се използват за оценка на генерираните модели:

1. Точност (Accuracy);

Работата на класификатора се оценява чрез стойността на допусната грешката или чрез точността на предсказване при решаване на класификационна задача. Точността е относителния брой правилно класифицирани данни от класификатора спрямо общия брой обекти в извадката.

$$Accuracy = \frac{TP+TN}{(TP+TN+FP+FN)} \quad (1)$$

2. Прецизност (Precision)

Прецизността показва частта на правилно разпознатите обекти от клас положителен по отношение на общия брой обекти, приети от класификатора, като обекти от клас положителен.

$$Precision = \frac{TP}{(TP+FP)} \quad (2)$$

3. Пълнота (Recall)

Пълнотата показва каква част са обектите, правилно класифицирани в клас положителен, от общия брой обекти, които действително принадлежат към клас положителен.

$$Recall = \frac{TP}{(TP+FN)} \quad (3)$$

4. Класификационна грешка (Classification Error)

Класификационната грешка е съотношение между броя грешно предсказани обекти от класификатора и общия брой обекти в извадката.

$$Err = \frac{FP+FN}{(TP+TN+FP+FN)} \quad (3)$$

5. F-мярка (F-Measure)

F-мярката е общ критерий, базиран на точност и пълнота.

$$F_{\beta} = (1 + \beta^2) \cdot \frac{Precision \cdot Recall}{(\beta^2 \cdot Precision) + Recall} \quad (4)$$

Където:

β – определя тежестта на точността в показателя;

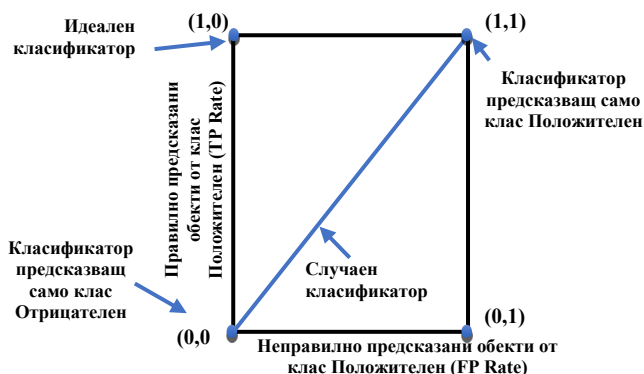
При $\beta=1$ хармоничната средна стойност се определя като:

$$F_{\beta} = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \quad (5)$$

F-мярката достига своя максимум с прецизност и точност, равна на единица и е близо до нула, ако един от аргументите е близък до нула [7].

6. Receiver Operating Characteristic (ROC) крива

ROC кривата е двумерна диаграма, получена чрез изобразяване на правилно класифицираните наблюдения за истинския клас по вертикалната ос спрямо неправилно класифицирани наблюдения по хоризонталната ос от обученния класификатор [8, 9]. На Фиг. 2. е представена ROC крива.



Фиг. 2. *Receiver Operating Characteristic крива*

Маркерът върху графиката показва стойностите на неправилно определените и правилно класифицираните от класификатора наблюдения. Те предоставят визуална оценка за точността на класификаторите.

За количествена оценка на работата на класификационните модели се използва площта под ROC кривата. Тази площ се обозначена с Area under curve (AUC). Максималната стойност е 1, а минималната е 0. Голямата площ под кривата показват добра производителност на класификатора [10].

Заклучение

В статията е формулирана една от основните задачи на машинното обучение – класификационната задача. Акцентирано е върху значимостта и приложението на създадени класификационни модели. Описани са методи за краткосрочно валидиране, които се прилагат при генериране на модел за класификация и са представени шест мерки за оценка – точност, прецизност, пълнота, класификационна грешка, F-мярка и ROC крива.

С предложените методи и метрики могат да се оценяват класификационни модели, които намират приложение в широк клас задачи с практическа насоченост.

ЛИТЕРАТУРА

- [1] Барсегян, А., и колектив. Анализ данных и процессов 3-е издание. БХВ-Петербург, 2009, ISBN 978-5-9775-0368-6.

- [2] Орозова, Д. Извличане на знания от данни в образователно пространство. Годишник на БСУ, том XXXIV, 2016.
- [3] Tantithamthavorn. C., et al. An Empirical Comparison of Model Validation Techniques for Defect Prediction Models. IEEE Transactions on Software Engineering, Volume 43, Issue 1, 2016, ISSN 1939-3520.
- [4] Cawley, G., N. Talbot. Efficient leave-one-out cross-validation of kernel fisher discriminant classifiers. Pattern Recognition, Volume 36, Issue 11, 2003
- [5] Chawla, N., at all. SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research, Volum 16, 2002.
- [6] Davis, J., M. Goadrich. The Relationship Between Precision-Recall and ROC Curves. Proceedings of the 23rd International Conference on Machine Learning, NY, USA, 2006. <https://doi.org/10.1145/1143844.1143874>
- [7] Соколов Евг. Семинары по выбору моделей. стр. 1–стр.10, 2016.
- [8] Davis, J., M. Goadrich. The Relationship Between Precision-Recall and ROC Curves. Proceedings of the 23rd International Conference on Machine Learning, NY, USA, 2006. <https://doi.org/10.1145/1143844.1143874>
- [9] Majnik, M., Z. Bosnić. ROC Analysis of Classifiers in Machine Learning: A Survey. Intelligent Data Analysis, Vol. 17, no. 3, 2013, DOI: 10.3233/IDA-130592
- [10] Hajian-Tilaki, K. Receiver Operating Characteristic (ROC) Curve Analysis for Medical Diagnostic Test Evaluation. Caspian Journal of Internal Medicine, 2013.
- [11] Refaeilzadeh, P., Tang, L., Liu, H. (2009). Cross-Validation. Encyclopedia of Database Systems.
- [12] Lumumba V., et al. Comparative Analysis of Cross-Validation Techniques: LOOCV, K-folds Cross-Validation, and Repeated K-folds Cross-Validation in Machine Learning Models. American Journal of Theoretical and Applied Statistics. Volume 13, 2024, 10.11648/j.ajtas.20241305.13

ДИЗАЙН НА МОБИЛНО ПРИЛОЖЕНИЕ ЗА ANDROID, ПОДПОМАГАЩО САМООБУЧЕНИЕТО ПО ТЕХНИЧЕСКИ НАУКИ

Стела Д. Минчева

DESIGN OF A MOBILE APPLICATION FOR ANDROID, SUPPORTING SELF-STUDY IN TECHNICAL SCIENCES

Stela D. Mincheva

ABSTRACT: *The main objective of the paper is the visual technical presentation of the design and created mobile application to support the self-training of science education, through which knowledge and skills can be acquired in a convenient and easy way for learning.*

KEYWORDS: *education, mobile device, programming*

DOI: <https://doi.org/10.46687/YT24STM>

Увод

Мобилните технологии навлизат с невероятна скорост във все повече сфери от ежедневието на хората, увеличавайки тяхната независимост по отношение на време и пространство.

Според речника на термините по е-обучение [3], значението за електронно обучение е следното: Образование чрез интернет, мрежа или компютър. Това означава, че електронното обучение се отнася не само до свободните (или понякога платени) информационни ресурси, които са на разположение в Интернет, това са и другите аспекти на онлайн обучението, което ако не е проприетарно се предполага, че трябва да е от типа безплатно и достъпно онлайн образование, ако е базирано на свободен и безплатен софтуер за онлайн образование, както в повечето държавни университети.

Основната цел на статията е визуалното представяне на проектирано и създадено мобилно приложение за подпомагане на самоподготовката на обучаемите по технически науки, чрез което да се придобиват знания и умения по удобен и лесен начин за обучаемите.

В [4] е предложена фигура, която чудесно визуализира когнитивно-поведенческа теория, която включва различни етапи при обучението, като спецификата в тази статия е компютърната графика. Предложената фигура в [4] представляваща модел, който обяснява връзката между мислене и емоция. Включването на емоциите при дадено обучение е важно, тъй като се въздейства не само на рационално, а и на емоционално ниво и усвоеното знание е по-трайно.

В [5] е представена възможността да се използват мобилни приложения за предаване на тайни съобщения с помощта на стеганографски софтуер, който е чудесен пример за Android приложение в сферата на киберсигурността.

Електронно обучение и самообучение

Преподавателите, учащите и учебният материал могат да се намират на различни места и да си взаимодействат по различно време. В [1] са представени различните категории електронното обучение според времето и мястото на участниците в учебния процес. Основните аспекти (виж фиг. 1), които трябва да се имат предвид при избора на обучаваща електронна форма и нейното прилагане, са:

- психологически – как влияе дадено електронно средство на мотивацията за учене, на отношението към учебния предмет;
- педагогически – доколко избраната форма отговаря на общата организация на учебния курс;
- методически – помага ли избраното средство и формат за по-добро усвояване на материала;
- организационни – рационално ли е структурирано учебното съдържание.



Фиг. 1. Аспекти, влияещи на избора на обучаваща електронна форма

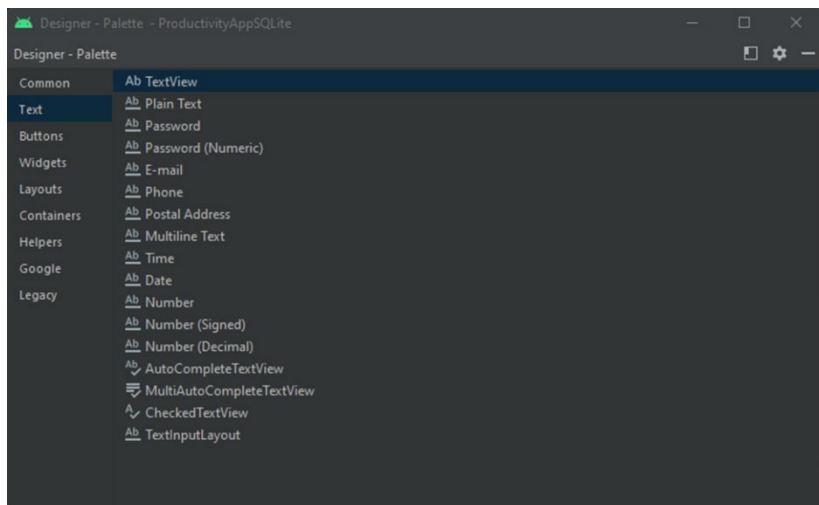
Описание на работата на мобилното приложение

Предложеното приложение има за цел да подпомогне самообучението на обучаемите, но и да улесни учебния процес, като се предлага и преподавателски панел, където могат да се създават курсове, както и да се добавят лекции към тях. Приложението е проектирано с помощта на програмната среда *Android Studio* и е използван на програмен език *Java*. То е напълно динамично, като цялата информация въведена от потребителя се запазва в база от данни (*Firebase firestore*). Приложението съдържа страница за влизане и регистриране, като за създаване и постъпване в акаунт се използва продукт на *Firebase -Firebase Authentication*. Приложението съдържа три секции: начална страница, страница с всички курсове и страница, съдържаща всички курсове, за които даден потребител се е записал (панел за обучаеми) или с всички създадени курсове от даден преподавател (преподавателски панел). Преподавателският панел съдържа бутон за създаване на курс и бутон за създаване на лекции.

Дизайн и функционалност на мобилното приложение

Използвайки насоките на [2] и [6], за създаване на приложения се получи представеният на фиг. 2 обобщен вид на мобилно приложение за Android, подпомагащо самообучението по технически науки.

Дизайнът на приложението има за цел да осъществи ясна и безпроблемна навигация при използване на приложението и да улесни максимално работата с него, като за тази цел се използват редица компоненти от менюто с компоненти на Android Studio, които са видни от фиг. 2.



Фиг. 2. *Designer-Pallet* на *Android Studio*

При първоначален достъп в приложението, се отваря страница за влизане (*LoginActivity*) (виж фиг. 3), където основните компоненти са:

- *TextView*;
- *EditText*;
- *Button*.

Чрез тях потребителя може да въведе необходимите данни и да се впише в профила си. Ако потребителят няма създаден профил, чрез натискане на *TextView* (*Нямате Акаунт*) бутона за създаване на акаунт, който е представен на фиг. 3, ще бъде препратен към страницата за регистриране (*RegisterActivity*), която може да се види на фиг. 4.

В зависимост от това дали профилът на потребителя е преподавателски или на обучаем, изгледът на приложението ще има различен вид. Профил на преподавател ще се създава ръчно, директно в базата от данни.

При избор на бутона „Курсове“, се отваря страница, съдържаща списък с всички съществуващи курсове, която е преставена на фиг. 5.

Фиг. 3.
Layout_login.xml

Фиг. 4.
Activity_register.xml

Фиг. 5.
SecondFragment.class

Фиг. 6. *AlertDialog*
– създаване на курс

Освен списък с всички курсове има и компонент бутон (*FloatingActionButton*). При изборът на този бутон, се отваря компонент *AlertDialog* (виж фиг. 6), който позволява избора на необходимите компоненти за създаването на нов курс. Новосъздаденият курс се добавя към списъка с всички курсове.

За създаване и управление на потребителски акаунти, както и за осъществяване на достъп до мобилното приложение се използва инструментът *Firebase Authentication* [8], [9], [10].

Дизайнът на мобилното приложение е проектиран под формата на XML код, а написаният код ще се съхранява, като XML файл. Важно е да се отбележи, че и сигурността на данните за потребителите е от съществено значение. В [11] и [12] са представени основните методи за повишаване на достоверността на информацията при опознаване в системите за идентификация.

Заклучение

Навлизането на мобилните технологии не подмина и сферата на образованието. Тези технологии обогатяват десктоп-базираната учебна среда с мобилен канал за връзка, а най-същественото е, че са огромна крачка в преодоляване на зависимостта на образованието от времето, пространството и други фактори.

Електронното обучение предлага разнообразни решения за оптимизиране на учебния процес, включително чрез използването на специализирани компютърни дидактични инструменти и платформи за дистанционно обучение. Разработването и прилагането на подобни технологии допринася за усъвършенстването на обучителните методи в инженерните и техническите науки. [13], [14], [15], [16], [17]

Настоящото мобилно приложение предлага още един поглед и възможност за самообучение на всеки, в удобно време, място и настройка. Предвидена е бъдеща разработка в която приложението да бъде подоброено и разширено.

ЛИТЕРАТУРА

- [1] Belanger F., Jordan, D. H. Evaluation and Implementation of Distance Learning: Technologies, Tools and Techniques. Idea Group Publishing, Hershey USA, London UK, 2000, ISBN: 9781930708549, DOI:10.4018/978-1-878289-63-6.
- [2] Наков Св. Въведение в програмирането с Java. 2017. ISBN 978-954-400-055-4. с. 53-80.
- [3] LearnFream, www.learnframe.com, [Online]. Available: [12.12.24]
- [4] Stoyanova V. Use of the opportunities of computer graphics in the education and training of cadets in National Military University "Vasil Levski". International scientific journal "Security & Future, Year 3, Vol.2, 2019, pp: 54-55, web issn 2535-082x; print issn 2535-0668 ".[Online]. Available: [12.12.24]

- [5] Stoyanova V. T. Analysis of the steganography in image whit mobile computing. International scientific journal Industry 4.0, Year2, Vol.2, pp. 80-82, 2017. [Online]. Available: [12.12.24]
- [6] Стоянова В. Визуално програмиране, Фабер, Велико Търново, 2019, ISBN 978-619-00-0991-7, 199 с.
- [7] Стоянова В. Облачни технологии в образованието. Сборник доклади от Научна конференция, факултет „А, ПВО и КИС“, на НВУ „В. Левски“, Шумен, стр. 76-82, ISSN 1313-7433[Online]. Available: [12.12.24]
- [8] Simple, multi-platform sign-in, <https://firebase.google.com/products/auth>
- [9] Using Firebase Authentication, <https://firebase.flutter.dev/docs/auth/usage/>
- [10] Make your app, <https://firebase.google.com/docs/auth>, Available: [01.11.24]
- [11] Dimitrov D, Kirov M. Методи за повишаване на достоверността на информацията при опознаване в системите за идентификация. Научна сесия НВУ “В. Левски”, факултет “А, ПВО и КИС, Шумен, Сборник научни трудове, стр. 153-158, Шумен, 2010г ISSN: 1313-7433.
- [12] Dimitrov D., Kirov M. Using multi-carrier probing signals for detecting non-linear objects. Scientific research and education in the air force-AFASES 2016, Henri Coandă – Air Force Academy, Braşov, Romania, DOI: 10.19062/2247 - 3173.2016.18.1.33.
- [13] Станева Л., Вардева И., Цанков Ц. Моделиране процеса на получаване на код на Хеминг с обобщена мрежа. Годишник на университет „Проф. д-р Асен Златаров“, т. XLIII, Бургас, 2014, ISSN 1312-1359.
- [14] Цанков Ц. С., Диманова Д. В. Компютърна дидактична програма за код на Хеминг. Годишник на ШУ „Епископ К. Преславски“, Шумен, 2016, ISSN 1311-834X.
- [15] Вардева И., Станева Л. Електронно обучение – решения, проблеми и перспективи, Годишник на университет „Проф. д-р Асен Златаров“, т. XXXVI, Бургас, 2007.
- [16] 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.
- [17] 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.

ПРИЧИННО-СЛЕДСТВЕН АНАЛИЗ КАТО МЕТОД ЗА УПРАВЛЕНИЕ НА РИСКА

Нели А. Арабаджиева-Калчева, Цветослав С. Цанков, Мая П. Тодорова

CAUSE-CONSEQUENCE ANALYSIS AS A RISK MANAGEMENT METHOD

Neli A. Arabadzhieva-Kalcheva, Tsvetoslav S. Tsankov, Maya P. Todorova

ABSTRACT: *Cause-Consequence Analysis (CCA) is a risk assessment method that combines elements of fault tree analysis and event tree analysis. It enables the modeling of failure causes and the prediction of their potential consequences, facilitating the identification of critical points in a system. This paper examines a case of a computer network failure, where the method is applied to identify the root causes of the problem and develop effective prevention strategies.*

KEYWORDS: *Cause-Consequence Analysis, risk management, risk assessment, risk analysis, risk assessment methods*

DOI: <https://doi.org/10.46687/YT24NEL>

Увод

Процесът на управление на риска може да се определи като съвкупност от взаимно влияещи се дейности, включващи обмен на информация, консултиране, установяване на контекста, оценяване, въздействие, наблюдение и преглед на риска. Оценяването на риска е неразривно свързано с управлението на сигурността и представлява структурирана последователност от процеси за идентификация, анализ и оценка на риска в даден проект или система [6].

В международния стандарт ISO 31010 [1] са представени различни методи за анализ и управление на риска, всеки от които намира приложение в зависимост от спецификата на оценявания обект. Сред тях е и методът „Причинно-следствен анализ“ (Cause-Consequence Analysis – CCA), който съчетава елементи от анализите на дървото на отказите и дървото на събитията. Този метод се използва за оценка на вероятностите и последствията от откази, като подпомага вземането на информирани решения за подобряване на надеждността и безопасността на системите.

Причинно-следствен анализ като метод за управление на риска

Причинно-следственият анализ (Cause – consequence analysis – CCA) е метод за оценка на риска, който интегрира елементи от анализа на дървото на отказите и анализа на дървото на събитията [1]. Този метод съчетава индуктивните и дедуктивните разсъждения на логическите диаграми за да идентифицира

основните причини и последствия от потенциални аварии [2]. Този подход започва с критично събитие и проследява неговото развитие чрез логически зависимости от типа ДА/НЕ, които определят възможните състояния или откази на защитните механизми в системата. Причините за тези откази се изследват с помощта на дървета на отказите.

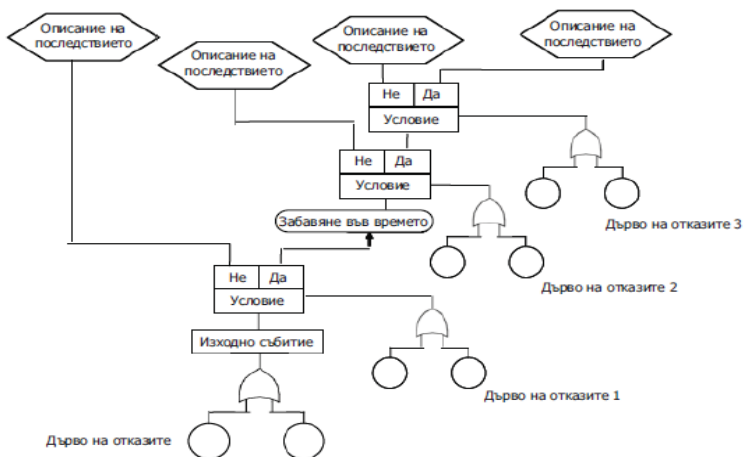
Методът се прилага за изследване на потенциалните сценарии, които могат да възникнат след критично събитие, като отчита реакцията на отделни подсистеми, например системи за управление на кризисни ситуации. Когато бъде подкрепен с количествени данни, анализът позволява да се оцени вероятността за настъпване на различни последствия. Методът на причинно-следствения анализ е ефективен инструмент за определяне на вероятността за възникване на основни събития и за оценка на рисковете, свързани с тях [3].

Получените резултати от причинно-следствения анализ визуализират пътищата, по които може да се развие дадена система, като показват както възможните откази, така и последиците от тях. Освен това те предоставят оценка на вероятността за настъпване на всяко конкретно последствие, като се базират на вероятностния анализ на факторите, следващи критичното събитие.

Методът на причинно-следствения анализ позволява моделиране и анализ на причините и последствията от откази, като подпомага експертите в идентифицирането на всички потенциални хардуерни откази, човешки грешки, възможни смущения и отклонения в процеса, както и влиянието на външни условия върху разглежданото събитие [4].

Причинно-следственият анализ е метод за систематично изследване на причините и последствията от откази, използван в оценката на надеждността и безопасността на сложни технически системи [5].

Концептуална диаграма на типичен причинно-следствен анализ:



Фиг. 1. Пример за причинно-следствен анализ [2]

Процедура за извършване на причинно-следствен анализ:

- Идентифициране на критичното (или изходното) събитие, което представлява крайната точка в дървото на отказите или началната точка в дървото на събитията.

- Създаване и валидиране на дървото на отказите, което изследва причините, довели до изходното събитие. При този процес се прилагат стандартните символи, използвани в класическия анализ на дървото на отказите.

- Определяне на реда на анализ на състоянията, като той следва логическа последователност, например времевата зависимост между тях.

- Генериране на пътищата, водещи до различни последствия, спрямо възникналите състояния. Това наподобява структурата на дървото на събитията, но разклоненията са визуализирани чрез блокове, маркирани с конкретните условия, които ги определят.

- Изчисляване на вероятностите за всяко възможно последствие, ако отказите на условните блокове са независими. Това се реализира чрез присвояване на вероятности към всеки изход на условния блок, като се използват съответните дървета на отказите. Вероятността за конкретна последователност от събития се определя чрез умножение на вероятностите за всяко условие по пътя към съответното последствие. В случай че различни последователности водят до едно и също последствие, съответните вероятности се сумират. Ако има зависимост между отказите в рамките на дадена последователност, тези зависимости трябва да бъдат установени преди провеждането на изчисленията.

Причинно-следственият анализ комбинира силните страни на дървото на отказите и дървото на събитията, осигурявайки детайлно и цялостно изследване на системата. Един от основните му плюсове е възможността да анализира сложни сценарии, при които събитията се развиват във времето, както и взаимовръзките между различните откази и техните последствия.

Методът предоставя ясно графично представяне, което улеснява разбирането на различните последователности от събития и тяхното влияние върху крайните резултати. В сравнение с традиционните методи, причинно-следственият анализ позволява по-добра интеграция на смекчаващи системи и тяхната ефективност при различни условия. Освен това, чрез анализа могат да бъдат идентифицирани ключови зависимости и „ефекти на доминото“, които биха били трудни за моделиране с други техники.

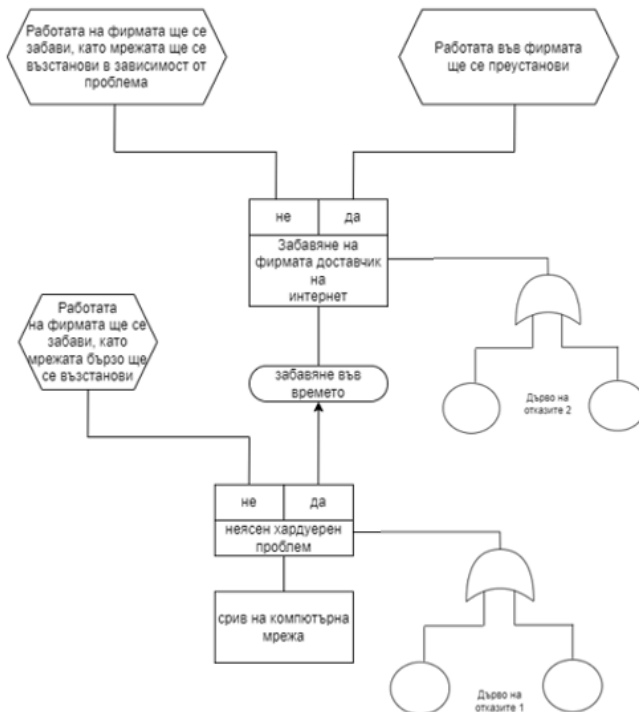
Причинно-следственият анализ е особено полезен за системи с множество взаимозависимости, където не само вероятността за отказ, но и последващите събития са критични за крайния резултат. Това го прави ефективен инструмент за оценка на риска, стратегическо планиране и подобряване на безопасността в сложни инженерни и организационни системи.

Въпреки своите предимства, причинно-следственият анализ има и някои ограничения. Той е по-сложен в сравнение с традиционните анализи на дървото на отказите и дървото на събитията, както при създаването на диаграмите, така и при оценяването на зависимостите между различните състояния. Това води до по-труден процес на количествено определяне и интерпретация на резултатите.

Практическо приложение на метода Причинно-следствен анализ на конкретен казус: „Срив на компютърна мрежа във фирма“

Фигура 2 илюстрира приложението на метода Причинно-следствен анализ за анализ на проблема със срив на компютърна мрежа във фирма. Анализът започва с идентифициране на изходното (критично) събитие – „срив на компютърна мрежа“. След това се разглеждат възможните причини и последствия, като логическите зависимости между тях са представени в графичен вид.

В представената диаграма е показана последователността на събитията, които могат да доведат до прекъсване на работния процес във фирмата. Възможните причини за срива на мрежата включват „неясен хардуерен проблем“ и „забавяне на фирмата доставчик на интернет“. От своя страна, тези фактори водят до забавяне на работните процеси, а в най-крайния случай – до пълно преустановяване на работата.



Фиг. 2. Диаграма на метод: Причинно-следствен анализ за оценяване на риск при „Срив на компютърна мрежа във фирма“

Заклучение

Прилагането на метода причинно-следствен анализ позволява не само оценка на риска, но и формулиране на стратегии за минимизиране на последиците от критични събития. Чрез детайлно моделиране на възможните сценарии и изчисление на вероятностите за настъпването им, анализът подпомага идентифицирането на ключовите слабости в системата. Въпреки сложността на метода, неговата интеграция с други техники за анализ на риска го прави изключително полезен за изследване на сложни системи с множество взаимовръзки.

ЛИТЕРАТУРА

- [1] БДС EN ISO 31010, Управление на риска. Методи на оценяване на риска, <https://www.bds-bg.org/>.
- [2] Saud, Y. E., Israni, C. Applications of cause-consequence diagrams in operational risk assessment. ASSE Professional Development Conference and Exposition, June 3, 2012, ASSE.
- [3] Xin B., Wan L., Yu J., Dang W. Basic event probability determination and risk assessment based on cause-consequence analysis method. Journal of Physics: Conference Series, Vol. 1549, No. 5, 2020, p. 052094, IOP Publishing.
- [4] Virtanen S., Hagmark P., Penttinen J. Modeling and analysis of causes and consequences of failures. Annual Reliability and Maintainability Symposium (RAMS), 23-26 January 2006, pp. 506-511, IEEE.
- [5] Abdelghany M., Tahar S. Cause-consequence diagram reliability analysis using formal techniques with application to electrical power networks. IEEE Access, Vol. 9, 2021, pp. 23929-23943.
- [6] Dimanova D., Kuzmanov Z. Risk management in information security. Scientific Conference with international participation MATTEH 2018, Conference proceeding, Shumen, 2018, ISSN: 1314-3921, vol. 2, part. 1, pp. 139-145.

ЕДИН ПОДХОД ЗА ПОДПОМАГАНЕ РАЗРАБОТВАНЕТО НА WEB ПРИЛОЖЕНИЯ ЧРЕЗ КОГНИТИВНА МАШИНА

Валентин Т. Атанасов

AN APPROACH TO SUPPORTING THE DEVELOPMENT OF WEB APPLICATIONS USING A COGNITIVE MACHINE

Valentin T. Atanasov

ABSTRACT: *With the entry of cognitive machines into broad areas of human activity, it is necessary to understand the construction of a systematic approach in cases of use of a given class of these machines in the processes related to the development of software products. The presence of specific functionality in this class of cognitive machines is based on their essential characteristic - generativity. Such a class of cognitive machines is represented by language models, a subclass of large language models, representatives of which are ChatGPT, Gemini, DeepSeek. Considering the multi-component nature of the WEB-based software architecture, it is assumed that the generativity of a given cognitive machine could be used at different stages of its development. This publication examines an approach to building a systematic order in the main phases of software development of WEB applications.*

KEYWORDS: *cognitive machine, WEB development, cognitive machine support, model*

DOI: <https://doi.org/10.46687/YT24VLA>

Увод

В настоящата публикация се приемат следните основни терминологични постановки:

- Когнитивна машина е научно обоснован израз, използван, за да замени използвания популярен и неинженерен израз „Искусствен интелект“;
- Разглеждането на проблемните аспекти по-долу се опира на разбирането, че когнитивната машина представлява случаи на програмна или апаратна реализация на математически модел, описващ функционирането на човешкия мозък в когнитивни процеси [1];
- Генеративна машина е израз, представящ технологичен дял от когнитивните машини, чиято програмна или апаратна реализация е предназначена да генерира информационни единици;

- Информационна единица е всеки структуриран и организиран набор от данни, предназначени за възприемане от сетивната система на човек и представени от основните типове данни – визуални, звукови и символни(текстови);
- Информационен фрагмент е обособена част от информационната единица;
- Работеща кодова версия е съвместна работа на всички компоненти от програмна логика, напълно или частично удовлетворяващи първоначално зададената цел.

Отчитайки високите темпове, обусловили навлизането на когнитивните машини в широки области на човешката дейност, се налага разбирането за изграждане на системен подход в случаите на употреба на даден клас при тези машини в процесите, свързани с жизнения цикъл при разработването на програмни продукти. Наличието на специфична функционалност при този клас когнитивни машини бива основано на съществена тяхна характеристика - *генеративността*. Такъв клас когнитивни машини представляват езиковите модели, подклас на големите езикови модели, представители на които са ChatGPT, Gemini, DeepSeek, [4][3][5]. Разглеждайки комплексния характер и многокомпонентността на WEB базираната програмна архитектура от една страна, наличието на капацитет за обработка на естествен език от друга страна и натрупването на съществен обем информационни масиви в областта на програмирането се допуска, че би могло да бъде използвана *генеративността* на дадена когнитивна машина при различните етапи на разработване на програмни кодове [6][7][8][10][11], в това число и на WEB приложения и платформи. Настоящата публикация разглежда един подход за построяване на системен ред в основните фази на програмна разработка на WEB приложения посредством когнитивно подпомагане от езиков модел.

Основна теза

Актуалността на този нов аспект на езиковите модели, предполага неговото изследване с оглед приложението на новоустановяващата се функционалност. Разглеждащата функционалност се свързва с генерирането не само на самия текст, но и на способността на езиковия модел да разбира контекста и връзките между извежданите думи от този синтезиран изкуствено логически обоснован текстов набор. Актуалността на тези модели в областта на програмирането се потвърждава както от появата на разработки, базирани на когнитивни машини [7][10][11], така и от актуалните теоретико-практически анализи [6][8].

Инженерното основание за използване на подобни езикови модели почива на обстоятелството, че в процеса на обучение на такъв езиков модел са формирани масиви от данни (точните размери са публично неоповестени), чийто размер надхвърля мерната единица петабайт. Кое то обстоятелство *ergo* предполага допускането за обосновано предположение за наличието на изградени достоверни масиви от нормативи, стандарти, регламенти и правила при широк набор от програмни езици. Според самите езикови модели от 1630 програмни езици [9], в

масивите от данни на два от тези езикови модели [4][5] са обхванати около 85% от тези програмни езици, което обстоятелство определя допускането за използването на този клас модели в случаите на употреба като подпомагащи кодирането. Друга съществена част от тезата е универсалността на математическия език, логически имплементиран и семантично излаган в процеса на диалога *човек-машина* при езикови модели.

Алгоритъм

Разглеждайки характеристиките на езиковите модели и опирайки се на една от техните съществени функционалности – *генеративността*, по-долу ще бъде формиран алгоритъм за използване на абстрактен клас езиков модел като подпомагащ процеса на кодова разработка на WEB базирани приложения или системи.

Като първа стъпка от създаването на системния ред при използването на когнитивно подпомагане в процеса на програмна разработка на WEB приложения или системи се приемат следните принципи:

- *Езиковият модел е способен на анализ и синтез;*
- *Езиковият модел е базиран на разпознаване на естествен език;*
- *Езиковият модел е контекстуално ориентиран;*
- *Езиковият модел обхваща изчерпателен обем от актуални стандарти, норми и правила за основните аспекти на WEB програмирането.*

Като втора стъпка се определят следните ограничения на езиковия модел:

- *Времева и семантична нестабилност на контекстуалността;*
- *Неконтролиран синтез на съществени излишъци от информационни единици или фрагменти;*
- *Обемът на синтезирания кодов фрагмент не следва да надвишава обхвата на когнитивния капацитет на човека (разработчика);*
- *Съществува вероятност за недостоверност на резултата в случаите, задаващи естеството на програмната разработка извън обхвата на познатите модели;*
- *Човекът е валидиращият принципал в процеса на разработката.*

Като трета стъпка се формират следните ключови насоки за подпомагане при кодовата разработка:

- *Предоставяне на примери за код;*
- *Пояснение на програмни концепции и програмен синтаксис;*
- *Помагане чрез кодов разбор на грешките (debugging);*
- *Подпомагане при оптимизация на кодовата и програмна логика;*
- *Предоставяне на статистически анализ.*

Като четвърта стъпка се формират определени правила, които следва да бъдат прилагани:

- *Лексикално минимализиране на текстовото задание;*
- *Недвусмисленост на всяко текстовото задание;*
- *Семантично структуриране на текстовото задание;*

- Винаги да се установява текстов контекст преди текущото предоставяне на информационната единица или фрагмент;
- Възможност за формиране на задание с общ текстов набор, обхващащ едновременно трите основни компонента на WEB програмирането – Html, CSS, JavaScript.
- Преди всяка нова редакция да се предоставя на езиковия модел текущата работеща кодова версия, за да се формира у него повишена степен на семантична и времева устойчивост на контекста;
- Преди всяка нова редакция всички компоненти от текущата работеща кодова версия да се съхраняват в отделна архивна файлова група (времево индексирано име);
- При всяка нова кодова редакция да се подлагат на изпитване всички нейни съставни компоненти (например Html, CSS, JavaScript);
- Използването на коментари повишава разбирането на кодовата логика;
- Изпитването на всяка нова кодова редакция да се извършва чрез поне три клиентски агента;
- Винаги да се подлага на визуален преглед всяка предлагана от езиковия модел кодова редакция, за да се активира визуалният когнитивен процес, част от обща когнитивна обработка в човешкия мозък [2].

Експериментална част

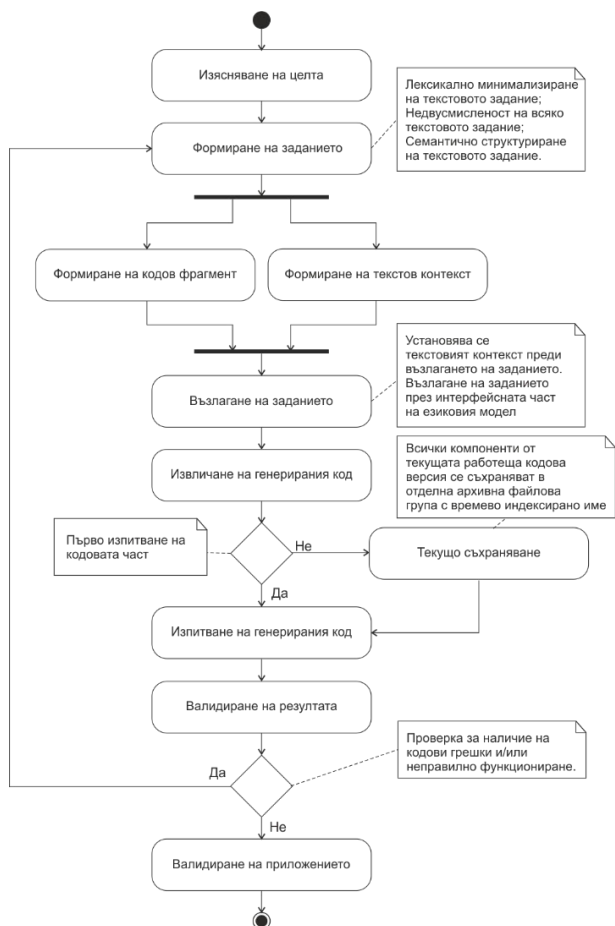
Следвайки добрите практики в процесите на разработка на програмни приложения да се моделира даден процес или етап, се представя процес на приложение в използване на езиков модел като подпомагач кодовата разработка на WEB приложение (фиг.2.). На показания по-долу кодов фрагмент е представен генериран от езиковия модел код, валидиран от програмиста (фиг.1.).

```

218 // Функция за показване на таба
219 ▼ function showTab(tabIndex) {
220     const tabs = document.querySelectorAll(".tab");
221     const tabContents = document.querySelectorAll("#tab-content > div");
222
223     // Премахване на избора от всички табове и скриване на съдържанието
224     tabs.forEach(tab => tab.classList.remove("selected"));
225     tabContents.forEach(content => (content.style.display = "none"));
226
227     // Добавяне на избора към текущия таб и показване на съдържанието му
228     document.getElementById(`tab${tabIndex}`).classList.add("selected");
229     document.getElementById(`tab${tabIndex}-content`).style.display = "block";
230
231     // Затваряне на рорир прозореца при смяна на таб
232     const existingPopup = document.querySelector(".popup");
233 ▼     if (existingPopup) {
234         existingPopup.style.display = "none"; // Скриване на рорир
235         existingPopup.remove(); // Премахване на рорир
236     }
237 }
238

```

Фиг. 1. Генериран от езиковия модел и валидиран кодов фрагмент



Фиг. 2. Алгоритъм за приложение на езиков модел като подпомагач кодова разработка

Показаният по-горе алгоритъм има характеристиката на широка валидност и би могъл да има своето приложение и при използването на езиков модел при други програмни или кодови разработки.

Заклучение

Опирайки се на основните характеристики на езиковите модели, в чиито обхват влиза и една от техните съществени функционалности – *генеративността*, може да се изведе основното заключение за съществуването на вероятност за приложимост на даден езиков модел за подпомагане на кодови

или програмни разработки. Но, отчитайки псевдослучайния резултат в такъв процес, следва да бъде прилаган определен алгоритъм. Предлаганият по-горе алгоритъм формира системен ред в основните фази в процеса на програмна разработка. Ключов момент в този процес следва да бъде човешкият фактор при валидирането на дадената разработка.

ЛИТЕРАТУРА

- [1] Атанасов, В., Иванова, А., Анализ на програмните модели за автоматизиране на когнитивни процеси, *Strategies for Policy in Science and Education*, „Аз-буки“, Volume 32, Number 5s, 2024, pp: 244-254, <https://doi.org/10.53656/str2024-5s-24-ana>.
- [2] Cavanagh, P., Visual cognition, *Vision Research*, Volume 51, Issue 13, 2011, pp: 1538-1551, ISSN: 0042-6989, <https://doi.org/10.1016/j.visres.2011.01.015>.
- [3] <https://gemini.google.com/>
- [4] <https://chatgpt.com>
- [5] <https://deepseek.com>
- [6] Gewirtz, D., How to use ChatGPT to write code - and my favorite trick to debug what it generates, 2025, (<https://www.zdnet.com/article/how-to-use-chatgpt-to-write-code-and-my-favorite-trick-to-debug-what-it-generates/>) (посетен на 18.02.2025)
- [7] Kucia, P., Code Companion, 2024, (<https://gptsapp.io/gpts/code-companion-ai/jbqmgzlzcb>) (Посетен 10.09.2024)
- [8] Lin, P., How to Use ChatGPT for Coding and Programming, *IEEE Computer Society*, 2023, (<https://www.computer.org/publications/tech-news/build-your-career/chatgpt-for-coding>) (Посетен на 11.09.2024)
- [9] Alphabetical List of Programming Languages, (<https://programminglanguages.info/languages/>) (Посетен на 1.10.2024)
- [10] Code with CodeQwen1.5, 2024, (<https://qwenlm.github.io/blog/codeqwen1.5/>) (Посетен 20.12.2024)
- [11] Get started with Llama, (<https://www.llama.com/docs/overview/>) (Посетен 20.01.2025)

ИЗСЛЕДВАНЕ НА ВЗАИМОДЕЙСТВИЕТО НА ПОТРЕБИТЕЛИТЕ СЪС СЕНЗОРЕН ЕКРАН

Стела Д. Минчева

RESEARCH ON USERS INTERACTION WITH A TOUCHSCREEN

Stela D. Mincheva

ABSTRACT: *Smartphones with touchscreen-based interfaces are increasingly used by non-technical groups including the elderly. Purpose of the study is the interaction of users with touch screen using touch gestures. The paper presents an analysis of how different category of people perform gestures on touch-screen smartphones and report their preferences, explaining the procedure and technical implementation that we followed to collect gesture samples. However, application developers have little understanding of how users interact with their products and of how to design friendly interfaces. As an initial study to assess standard mobile touchscreen interfaces for the different category people, the paper conducted performance measurements and observational evaluations of 40 participants.*

KEYWORDS: *touch screen, computer graphic, friendly interfaces*

DOI: <https://doi.org/10.46687/YT24SDM>

Увод

В съвременния дигитален свят взаимодействието със сензорни екрани е неразделна част от ежедневието на хората. Различните жестове с докосване, използвани за управление на устройства с тъчскрийн, са обект на задълбочени изследвания, насочени към подобряване на потребителското преживяване и улесняване на достъпа до технологии.

Настоящото изследване се базира на **Touch Gesture Reference Guide [1]** и цели да проучи как различни възрастови групи усвояват и използват различни жестове за взаимодействие с мобилни устройства. За целите на анализа са проведени интервюта и практически тестове с възрастни хора на възраст между 40 и 50 години и младежи на възраст между 21 и 24 години.

Съществуват множество дефиниции, и преплитане на информация известна за цифровите и сензорните екрани, които биват ежедневно използвани от потребителите. Изглеждат много близки формулировки, но имат една съществена разлика, а именно тяхната функционалност и технология.

Цифровият екран: е всеки дисплей, който показва цифрово съдържание (изображения, видеоклипове, текст и др.), като например light-emitting diodes (LED), liquid-crystal display (LCD), organic light-emitting diode (OLED) и e-ink

екрани в телевизори, монитори и смартфони. Използва се главно за показване на информация.

Сензорен екран: е екран, който има вградени сензори за откриване на докосване, натиск или други входи, като например сензорният екран в смартфони, таблети или банкомати. Използва се както за показване, така и за взаимодействие с устройството.

Ключова разлика между цифровите екрани и сензорните такива е, че първите показват само съдържание, докато вторите могат да откриват взаимодействие с потребителя (докосване, жестове, натиск и т.н.).

Изследване взаимодействието на потребителите със сензорен екран чрез жестове.

В настоящата част се представя изследване на взаимодействието на потребителите със сензорен екран чрез жестове с докосване. Изследването е направено по наръчника за жестове с докосване (Touch Gesture Reference Guide). Този наръчник е лесно достъпен и може да бъде разгледан от [1]. Това справочно ръководство за жестове с докосване е уникален набор от ресурси за софтуерни дизайнери и разработчици, работещи върху базирани на докосване потребителски интерфейси, включително iPhone, Windows, Windows Phone, Android и други. Ръководството съдържа преглед на основните жестове, използвани за повечето сензорни команди. Крейг Виламор и екип, препоръчват и обясняват как да се използва, за да се поддържат основните действия на потребителите, предоставят визуално представяне на всеки жест, който да се използва в дадена проектната документация и ръководство за потребителя, както и допълнително описание за това как популярните софтуерни платформи поддържат основните жестове с докосване. В [2] е изложен един от начините за създаване на дигитални илюстрации с търговска цел. Методът съчетава традиционно рисуване и калиграфия, 3Ds Max, V-Ray и Photoshop. Идеята на статията е да демонстрира как да се изгради цял проект от нулата.

Жестовите в настоящото изследване са разгледани и класифицирани според популярността им, тяхната употреба в ежедневието и сложността им за изпълнение, като са тествани 40 потребителя.

Най-популярни:

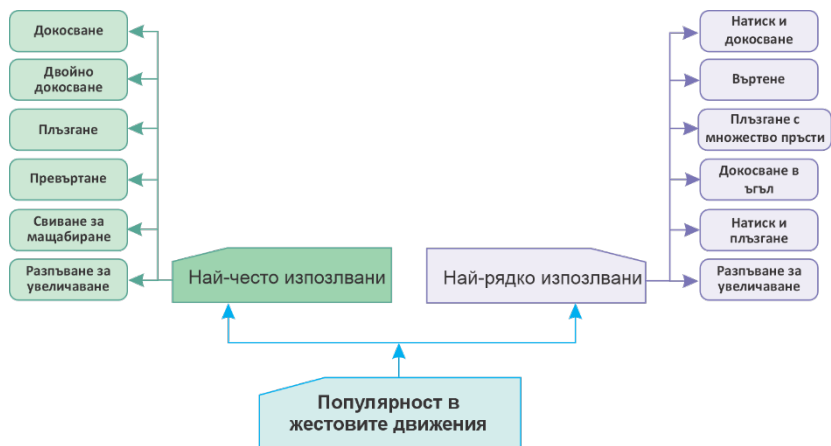
1. Tap (Докосване);
2. Double Tap (Двойно докосване);
3. Drag (Плъзгане);
4. Scroll (Превъртане);
5. Pinch (Свиване за мащабиране);
6. Spread (Разпъване за увеличаване).

По-рядко използвани:

1. Press and Tap (Натиск и докосване);
2. Rotate (Въртене);
3. Multi-finger Drag (Плъзгане с множество пръсти) ;

4. Corner Tap (Докосване в ъгъл) ;
5. Press and Drag (Натиск и плъзгане).

Фигура 1 представя класификация на жестовите движения според честотата на използване и улеснява възприемането ѝ чрез визуализация на възприеманите жестове сред анкетираната група потребители.



Фиг. 1. Класификация на жестовите движения според честотата на използване

Участниците извършиха серията от експериментални процедури, всяка от които се състоеше от изпълнение на измервания жест операции (фиг.2-4) и реалистично използва на интерфейс компоненти. Всеки от участниците след експеримента беше интервюиран, за да сподели усещанията и състоянието си при изпълнение на жестовите.

В [8] и [9], Stöbel и др. предлагат сравнение на по-възрастните с по-младите потребители в начина, по който те си взаимодействат със сензорни екрани. Те се съсредоточават в тестването на 42 различни жестове и директни манипулации за сензорни повърхности и измерване техните скорост и точност. Резултатите им показват, че по-възрастните потребители предпочитат директните манипулации и работят с по-бавна скорост.

В [4] е представена възможността да се използват мобилни приложения за предаване на тайни съобщения с помощта на стеганографски софтуер, който е чудесен пример за Android приложение в сферата на киберсигурността. Описаните приложения са много специфични, но са доказателство за нуждата от анализ на взаимодействието на потребителите със сензорните екрани и познаването и използване на различни жестове и манипулации.

В случай на по-сложни жестове, заоблените форми са много предпочитани пред ъгловите, особено от незрящи хора, които изпитват затруднения при извършването на жестове с прави ъгли. Въз основа на резултатите от изследвания

описани в [3] и на предишни свързани изследвания с тях, в [3] са предложили варианти за подобряване на достъпността на жестове на устройствата със сензорен екран.

Проведените интервюта за установяване на познанията за жестове, както и практически тестове за оценка на изпълнението на задачите са с четиридесет участника. Те споделиха своите впечатления, относно трудността на жестове. При изследването целевата група бе разделена на две групи, които бяха описани. Първоначално се тества основното базово взаимодействие, като на следващ етап изпълниха следните задачи:

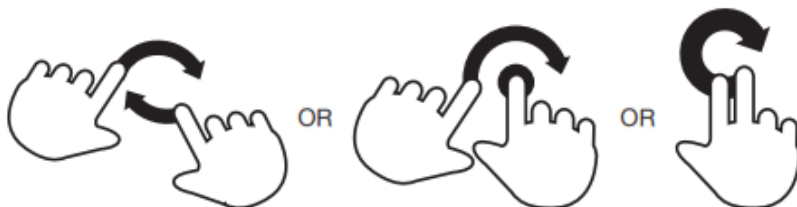
- Увеличаване на изображение чрез Pinch и Spread (виж фиг.2);
- Преместване на обект чрез Drag, (виж фиг.3);
- Въртене на обект чрез Rotate, (виж фиг.4).



Фиг. 2. Увеличаване на изображение чрез Pinch и Spread



Фиг. 3. Преместване на обект чрез Drag



Фиг. 4. Въртене на обект чрез Rotate

Основните жестове като *Tap*, *Scroll* и *Drag* са интуитивни и лесни за усвояване от всички групи потребители. По-сложните жестове като *Rotate* и *Multi-finger Drag* затрудняват по-възрастните участници, които често не са запознати с тях.

При всичките четиридесет потребители са проведени интервюта и практически тестове, както и по-горе описаните задачи на фиг.2, фиг.3 и фиг.4. Групата потребители от 40-50 годишна възраст често познават основните жестове използвани при смартфоните (*Tap*, *Scroll*, *Flick*), но рядко използват сложни жестове като *Bundle* и *Multi-finger Drag*.

По-млади потребители (21-24г.) подобно на възрастните изпълняват същите действия и задачи, но при тях взаимодействието е много по-интуитивно. Тази група демонстрира добро владение на всички жестове, включително по-рядко използваните такива. Това най-вероятно се дължи на по-големия опит и непрекъсната употреба на мобилните устройства.

Като цяло основните жестове са изпълнени успешно от всички групи. Основните жестове са интуитивни и лесно се усвояват. По-рядко използваните жестове изискват допълнителни указания при възрастни потребители.

Препоръките биха били да се разработят образователни материали за по-сложните жестове и да се предложат алтернативни методи за взаимодействие за по-възрастните потребители.

Популярност и усвояемост на жестовете. Специфики на възрастовите групи.

Младешите демонстрират по-голяма интуитивност и умения при използването на всички жестове, включително по-сложните.

Според [5] и [6], мобилните сензорни екрани като цяло са лесни за използване от възрастните хора и едноседмичен опит като цяло подобрява уменията им. Въпреки това, внимателните наблюдения идентифицират няколко типични проблема, които трябва да бъдат разгледани в бъдещите интерфейси. В тези източници се обсъждат резултатите от направените експерименти в тях, като се стремят да предоставят неофициални насоки за разработчиците на приложения за проектиране на по-добри интерфейси за възрастни хора.

Възрастните са склонни да предпочетат операциите с *dragging* и *pinching* пред докосването. Това е откритие, което не се наблюдава в по-ранен експеримент за взаимодействия с много докосвания за по-възрастни потребители се твърди в [7]. Резултат от изследвания представени в [6], за минимален размер на екрана, който потребителят могат оперират с добра бързината и точността е около 8 мм, както за по-млади, така и за възрастни хора.

Заклучение

Това изследване предоставя ценни данни за това как различни възрастови групи взаимодействат с тъчскрийн устройства. Разбирането на тези различия може да допринесе за създаването на по-достъпни и интуитивни интерфейси. Допълнително, резултатите могат да се използват при разработването на нови

обучителни методи, насочени към подобряване на дигиталната грамотност на по-възрастни потребители.

Групата потребители от 40-50 годишна възраст често познават основните жестове използвани при смартфоните (*Tap, Scroll, Flick*), но рядко използват сложни жестове като *Bundle u Multi-finger Drag*. По-млади потребители (21-24г.) подобно на възрастните изпълняват същите действия и задачи, но при тях взаимодействието е много по-интуитивно.

ЛИТЕРАТУРА

- [1] Villamor, C., Willis, D., and Wroblewski, L. Touch Gesture Reference Guide, Last updated April 15, 2010, <https://static.lukew.com/TouchGestureGuide.pdf>, Available: [11.11.24].
- [2] Georgiev, I., V Stoyanova, One way for creating visual effects, Industry 4.0, Vol. 3 (2018), Issue 2, pg(s) 90-93, <https://stumejournals.com/journals/i4/2018/2/90>, Available: [01.11.24].
- [3] Buzzi, M.C., Leporini, B. et al. Analyzing visually impaired people's touch gestures on smartphones. Multimed Tools Appl 76, 5141–5169 (2017). <https://doi.org/10.1007/s11042-016-3594-9>, Available: [11.11.24].
- [4] Stoyanova, V. T. Analysis of the steganography in image whit mobile computing., International scientific journal Industry 4.0, Year2, Vol.2, pp. 80-82, 2017. [Online]. Available: [12.12.24]
- [5] Masatomo Kobayashi, Atsushi Hiyama, Takahiro Miura et al. Elderly User Evaluation of Mobile Touchscreen Interactions,
- [6] Lee, S., Zhai, S.: The Performance of Touch Screen Soft Buttons. In: Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI 2009), pp.309–318 (2009)
- [7] Stoel, C., Blessing, L. Mobile Device Interaction Gestures for Older Users. In: Proceedings Of the 6th Nordic Conference on Human-Computer Interaction (NordiCHI 2010): Extending Boundaries, pp. 793–796 (2010)
- [8] Stöbel, C., Wandke, H., Blessing, L.: Gestural Interfaces for Elderly Users: Help or Hindrance? In:Kopp, S., Wachsmuth,I.(eds.)GW2009.LNCS, vol.5934, pp.269–280. Springer, Heidelberg (2010)
- [9] Stöbel, C., Blessing, L.: Mobile Device Interaction Gestures for Older Users. In: Proceedings of the 6th Nordic Conference on Human-Computer Interaction (NordiCHI 2010): Extending Boundaries, pp. 793–796 (2010)

УВЕЛИЧАВАНЕ НА ОБЕМА ГОТОВА ПРОДУКЦИЯ ЧРЕЗ ВНЕДРЯВАНЕ НА НОВИ ТЕХНОЛОГИИ

Петя К. Велчева-Тодорова

INCREASING THE FINISHED PRODUCT BY IMPLEMENTING NEW TECHNOLOGIES

Petia K. Velcheva-Todorova

ABSTRACT: *In dynamic and competitive business world, increasing the volume of finished goods is critical to the survival and growth of any enterprise. One of the most effective ways to achieve this is through the implementation of new technologies.*

KEYWORDS: *production efficiency, technology, automation, production, investing in the future*

DOI: <https://doi.org/10.46687/YT24PYA>

Въведение

В днешния динамичен и конкурентен бизнес свят, увеличаването на обема готова продукция е критично важно за оцеляването и растежа на всяко предприятие. Един от най-ефективните начини за постигане на това е чрез внедряване на нови технологии. Новите технологични решения не само повишават ефективността на производствените процеси, но и намаляват разходите, подобряват качеството на продукцията и увеличават гъвкавостта на бизнеса.

Във връзка с това основната цел на статията е да разгледа някои от ключовите технологии, които могат да помогнат за увеличаване на обема готова продукция. Чрез тяхното внедряване и използване могат да се постигнат и обезпечат по-големи резултати при еднакви изходни данни.

1. Автоматизация и роботизация

Автоматизацията и роботизацията са сред най – значимите нововъведения в индустриалното производство през последните десетилетия. Роботите и автоматизираните системи могат да изпълняват рутинни и повторяеми задачи с висока точност и скорост, което значително повишава ефективността на производството. Освен това, те намаляват риска от човешки грешки и осигуряват постоянен контрол върху качеството на продукцията. Внедряването на такива системи може да доведе до значително увеличение на обема готова продукция, като същевременно намалява нуждата от ръчен труд.

Автоматизацията включва използването на компютърни системи и технологии за контролиране и управление на производствените процеси без необходимост от човешка намеса. Това може да включва всичко от прости

механични системи до сложни софтуерни платформи, които управляват целия производствен процес.

Роботизацията от своя страна е специализирана форма на автоматизация, която включва използването на роботи за изпълнение на задачи. Роботите могат да бъдат програмирани да изпълняват различни дейности, като например монтаж, опаковане, боядисване и други.

За да сме адекватни с действителните нужди от внедряване на подходящите видове техники и технологии, трябва да сме наясно с конкретните им ползи:

— *Повишена ефективност:* Автоматизираните системи и роботите могат да работят непрекъснато, без да се уморяват или да правят грешки, което води до по-висока производителност и по-добро качество на продукцията.

— *Намалени разходи:* Въпреки че първоначалната инвестиция в автоматизация и роботизация може да бъде висока, дългосрочните спестявания от намалени трудови разходи и по-ниски оперативни разходи компенсират тези разходи.

— *Постоянство в качеството:* Автоматизираните системи и роботите изпълняват задачите си с висока точност и последователност, което гарантира постоянно високо качество на продукцията.

— *Гъвкавост и адаптивност:* Модерните автоматизирани системи и роботи могат лесно да бъдат препрограмирани и адаптирани към нови задачи или промени в производствения процес, което прави предприятията по-гъвкави и способни да реагират бързо на промените в пазарните условия.

— *Безопасност:* Роботите могат да изпълняват опасни или вредни за здравето задачи, като освобождават хората от рисковете, свързани с тези дейности.

Във връзка с изброените ползи можем да систематизираме отделни примери за добри практики и приложения на автоматизацията и роботиката (Таблица 1).

Като извод можем да извлечем твърдението, че автоматизацията и роботизацията са ключови технологии, които могат значително да увеличат обема готова продукция и да подобрят ефективността на производствените процеси. Те предлагат множество ползи, включително повишена ефективност, намалени разходи, постоянство в качеството и гъвкавост. Инвестирането в тези технологии може да помогне на предприятията да останат конкурентоспособни и да се адаптират към бързо променящите се пазарни условия.

Интернет на нещата (IoT)

Интернет на нещата (IoT) представлява мрежа от свързани устройства, които могат да комуникират помежду си и да обменят данни. В контекста на производството, IoT може да предостави ценна информация за състоянието на машините, материалите и процесите в реално време. Това позволява бързо откриване на проблеми и вземане на информирани решения, което води до минимизиране на престойте и увеличаване на производителността. Също така, IoT системите могат да бъдат използвани за мониторинг на енергийната

консумация и оптимизация на ресурсите, което допълнително допринася за увеличаване на обема готова продукция.

Таблица 1

Производствени линии	Автоматизираните производствени линии могат да изпълняват сложни монтажни и производствени задачи с висока скорост и точност. Пример за това са автомобилните заводи, където роботи монтират части и сглобяват автомобили.
Логистика и складове	Автоматизираните системи за управление на складове и логистика могат да оптимизират движението на стоките и да намалят времето за обработка на поръчките. Роботизираните кранове и AGV (автономни мобилни роботи) са примери за такива системи.
Медицински изделия	Роботизираните системи се използват за производство на медицински изделия като протези, ортопедични импланти и хирургически инструменти. Те осигуряват висока точност и качество, което е критично в медицината.
Хранително-вкусова промишленост	Автоматизираните системи и роботите намират широко приложение в хранително-вкусовата промишленост за опаковане, сортиране и проверка на качеството на продуктите.
Електроника	В електронната индустрия роботите се използват за монтаж на електронни компоненти върху печатни платки, както и за тестване и проверка на готовите продукти.

Приемайки че, Интернет на нещата (IoT) е концепция, която описва мрежа от физически устройства, превозни средства, уреди и други елементи, вградени със сензори, софтуер и мрежова свързаност, които позволяват тези обекти да събират и обменят данни, можем да заключим, че целта на IoT е да създаде интелигентна среда, в която различни устройства могат да комуникират помежду си и с централни системи, за да предоставят по-ефективни услуги и решения. За решаването на тази задача устройствата са оборудвани със сензори, които събират данни от околната среда, и актуатори, които трябва да бъдат свързани към интернет или друга мрежа, за да могат да предават и получават данни. Това може да се осъществи чрез Wi-Fi, Bluetooth, Zigbee, LoRaWAN и други технологии. След това софтуерът следва да обработи събраната информация и управлява устройствата.

Платформите за IoT предоставят инструменти за управление, анализ и визуализация на данните, като много IoT приложения използват облачни услуги за съхранение и обработка на големи обеми данни, както и за предоставяне на аналитични услуги.

Примери за приложения на IoT можем да проследим в Таблица 2.

Предизвикателства при внедряването на IoT могат да са сигурността при защита на данните и предотвратяване на неоторизиран достъп до устройствата; осигуряването на оперативна съвместимост между различни устройства и платформи; способност за разширяване на системата без значителни проблеми, както и поверителността при защита на личните данни на потребителите и спазване на регулациите за защита на данните.

Въз основа на казаното до тук, можем да заключим, че IoT има потенциала да трансформира множество индустрии и да подобри качеството на живот чрез създаване на по-интелигентни и ефективни системи.

Таблица 2

Умни домове	Автоматизация на домакинските уреди, контрол на осветлението, отоплението и сигурността.
Индустриална автоматизация	Мониторинг и управление на производствени процеси, предсказуема поддръжка на машини.
Здравеопазване	Следене на здравословното състояние на пациенти, дистанционно наблюдение и телемедицина.
Транспорт и логистика	Проследяване на стоки, оптимизация на маршрути, управление на автопаркове.
Градска инфраструктура	Управление на трафика, мониторинг на качеството на въздуха, интелигентно улично осветление.

Изкуствен интелект и машинно обучение

Изкуственият интелект (ИИ) и машинното обучение (МО) играят важна роля във внедряването на интелигентни производствени системи. Те могат да анализират големи обеми данни и да идентифицират модели и тенденции, които иначе биха останали незабелязани. Това позволява оптимизация на производствените процеси, прогнозиране на търсенето и планиране на ресурсите по-ефективно. Например, ИИ алгоритмите могат да предсказват кога една машина ще се повреди и да планират предварително нейната поддръжка, което предотвратява непланирани престои и увеличава производителността.

Изкуственият интелект (ИИ) и машинното обучение (МО) са две тясно свързани области, които играят ключова роля в развитието на съвременните технологии. Въпреки че често се използват взаимозаменяемо, те представляват различни аспекти на една и съща област.

Изкуственият интелект е широка концепция, която обхваща създаването на компютърни системи, способни да изпълняват задачи, които обикновено изискват човешка интелигентност. ИИ включва различни подходи и техники, като например: основан на правила и логика, използва символи и логически операции за решаване на проблеми; алгоритми, които се учат от данни и подобряват своето представяне с времето; ИИ, което използва сложни невронни мрежи за

моделиране на абстрактни данни и компютърни програми, които имитират процеса на вземане на решения от експерти в определена област.

Машинното обучение е подполе на ИИ, което се фокусира върху разработването на алгоритми и статистически модели, които позволяват на компютрите да се учат от данни и да правят прогнози или решения без да са изрично програмирани за това. Основните типове МО включват Надзорно обучение (алгоритъмът се обучава върху етикетирани данни, където входните данни са свързани с правилните отговори. Примери са линейна регресия, логистична регресия, дървета на решенията и невронни мрежи); Ненадзорно обучение (алгоритъмът се обучава върху неетикетирани данни и открива скрити структури или модели в данните. Примери включват клъстеризация и асоциационни правила); Полунадзорно обучение (комбинация от надзорно и ненадзорно обучение, където алгоритъмът използва малък набор от етикетирани данни и голям набор от неетикетирани данни); Подсилващо обучение (алгоритъмът се учи чрез взаимодействие с околната среда, като получава награди или наказания за своите действия. Този подход е особено полезен за роботика и игри.

В Таблица 3 сме систематизирали някои примери за приложения на ИИ и МО.

Таблица 3

Автономни превозни средства	Разработване на самоуправляващи се автомобили и дроне.
Медицинска диагностика	Анализ на медицински изображения и предсказване на заболявания.
Финансови услуги	Откриване на измами, кредитни оценки и автоматизирана търговия.
Разпознаване на образи и глас	Технологии за лицево разпознаване, гласови асистенти и превод на текст.
Препоръчителни системи	Персонализирани препоръки за продукти, филми и музика.

Знаейки всичко това, трябва да имаме предвид че ИИ и МО продължават да се развиват бързо, предлагайки нови възможности и предизвикателства в различни области на живота и бизнеса.

3D принтиране

3D принтирането, известно още като адитивно производство, е процес на създаване на триизмерни обекти чрез добавяне на материал слой по слой въз основа на цифров модел. Технологията използва различни материали като пластмаса, метал, керамика и дори биоматериали, за да произведе обекти с висока точност и детайлност.

Технологията на 3D принтирането предоставя нови възможности за създаване на сложни и персонализирани продукти с минимални разходи и време. Тя позволява бързо прототипиране и производство на малки серии продукти, което е особено полезно за компании, които искат да тестват нови идеи или да отговорят на специфични клиентски нужди. 3D принтирането също така намалява нуждата от складови наличности и транспортни разходи, което допринася за увеличаване на обема готова продукция.

Съществува няколко техники за 3D принтиране. Моделирането чрез топено отлагане е най-разпространеният метод, който използва топене и екструзия на термопластични нишки през дюза върху платформа за изграждане. Стереолитографията използва лазер за втвърдяване на течна смола слой по слой. Селективното лазерно синтероване от своя страна използва лазер за спичане на прахообразен материал, обикновено пластмаса или метал. Цифровата светлинна обработка е подобна на Стереолитографията, но използва проектор за втвърдяване на цял слой смола наведнъж.

Струйното нанасяне на материали е друг вид техника за 3D принтеринг, при която материалите се изхвърлят от печатащата глава под формата на капки, които се втвърдяват веднага след контакт с платформата. Всички методи са приложими на практика и мога да се използват в различни сфери на производството (Таблица 4).

Таблица 4

Медицина	Производство на протези, импланти, хирургически инструменти и модели за обучение.
Инженерство и промишленост	Прототипиране, производство на резервни части, функционални компоненти и инструменти.
Архитектура	Създаване на мащабни модели и архитектурни елементи.
Мода и дизайн	Дизайнерски аксесоари, обувки и дрехи.
Образование	Образователни модели и учебни пособия.

Предимства на 3D принтирането са възможността за създаване на уникални и персонализирани продукти, намаляването на времето за разработка и производство на нови продукти, ефективното използване на материалите, тъй като се добавят само необходимите количества, както и възможността за създаване на сложни и детайлни форми, които са трудни или невъзможни за производство с традиционните методи.

Въпреки изброените плюсове, трябва да се споменят и недостатъците на тази нова технология, за да се вземе решение дали да се внедри и да направи правилен избор на метод. 3D принтирането има ограничения в размера на получавания продукт поради ограниченията на принтерите, може да бъде по-бавно в сравнение с масовото производство, както и факта че някои материали могат да бъдат скъпи, особено специализираните метали и полимери.

Изреждайки всичко, не трябва да забравяме, че 3D принтирането продължава да се развива и намира нови приложения в различни индустрии, което го прави една от най-иновативните и бързо развиващи се технологии на нашето време.

Големи данни и анализ

Големите данни (Big Data) и анализът на тези данни са ключови концепции в съвременния свят, където информацията играе централна роля във вземането на решения, оптимизацията на процеси и откриването на нови възможности. Те представляват мощни инструменти за управление на производствените процеси. Чрез събиране и анализ на данни от различни източници, предприятията могат да идентифицират слаби места в своите операции и да предприемат коригиращи действия. Това води до подобряване на ефективността и намаляване на разходите. Анализът на големи данни може също така да помогне за оптимизация на веригата на доставки, което допринася за по-бързо и ефективно производство.

Големите данни се отнасят до огромни обеми структурирани и неструктурирани данни, които се генерират със скорост, която надхвърля способността на традиционните системи за обработка на данни да ги управляват ефективно. Тези данни включват текстове, изображения, видеоклипове, сензорни данни и други формати. Характеризират се с обем, скорост, разнообразие, истинност и стойност.

Анализът на големи данни от своя страна включва техники и технологии за извличане на смисъл и полезни знания от тези огромни обеми данни. Те могат да са:

— *Предсказуем анализ*: Използва статистически алгоритми и машинно обучение за прогнозиране на бъдещи тенденции и поведение. Например, предсказване на потребителско поведение, продажби и пазарни тенденции.

— *Дескриптивен анализ*: Фокусира се върху разбирането на минали и текущи събития и тенденции. Това включва визуализация на данни, отчетност и бизнес интелигентност.

— *Диагностичен анализ*: Търси причините зад определени резултати или проблеми. Често използва корелационен анализ и регресионни модели за идентифициране на фактори, влияещи на даден резултат.

— *Прескриптивен анализ*: Комбинира предсказуемия и диагностичния анализ, за да предложи действия или препоръки за подобряване на резултатите. Използва се в области като оптимизация на веригата за доставки, маркетинг и финанси.

Обработката на големи данни и анализирането им предоставя мощни инструменти за вземане на информирани решения, подобряване на ефективността и откриване на нови възможности в различни индустрии (Таблица 5).

Киберфизични системи

Киберфизичните системи комбинират физически компоненти с цифрови технологии, като сензори, софтуер и мрежи, за да създадат интелигентни и адаптивни производствени линии. Те позволяват интеграция на различни аспекти

на производството и улесняват координацията между различните етапи на производствения процес. Киберфизичните системи също така предоставят възможност за дистанционно управление и мониторинг на производствените процеси, което увеличава гъвкавостта и ефективността на производството.

Основните компоненти на киберфизичните системи са сензори, актуатори и механични устройства, които взаимодействат с физическата среда; компютри, микроконтролери и други хардуерни устройства, които обработват данни и изпълняват алгоритми; Комуникационни мрежи, които свързват различните компоненти и позволяват обмен на данни в реално време, както и алгоритми, програми и операционни системи, които контролират и управляват системата. Примерни приложения на киберфизичните системи са обобщени в Таблица 6.

Таблица 5

Здравеопазване:	Персонализирана медицина, епидемиологични изследвания, управление на болници.
Финанси	Управление на риска, откриване на измами, клиентски анализи.
Маркетинг	Сегментация на клиенти, таргетиран кампани, анализ на социални медии.
Производство	Оптимизация на производствени процеси, предсказуема поддръжка, контрол на качеството.
Транспорт	Управление на трафика, логистика, автономни превозни средства.

Таблица 6

Умни градове	Системи за управление на трафика, енергийни мрежи, мониторинг на замърсяването на въздуха и управление на водните ресурси.
Индустриална автоматизация	Роботизирани производствени линии, предсказуема поддръжка и оптимизация на производствените процеси.
Здравеопазване	Медицински устройства, телемедицина, дистанционно наблюдение на пациенти и персонализирано лечение.
Енергетика	Умни електропреносни мрежи, управление на възобновяеми енергийни източници и оптимизация на потреблението на енергия.
Транспорт	Автономни превозни средства, управление на трафика и логистика.

Предимствата, които ни дава внедряването и използването на киберфизичните системи са много – повишена ефективност – чрез автоматизация

и оптимизация на процесите; гъвкавост и адаптивност – имат способността да се адаптират към променящите се условия и изисквания в реално време; безопасност и надеждност - могат да осигурят по-високо ниво на безопасност чрез непрекъснат мониторинг и контрол и интегрирани решения обединяват различни технологии и системи в едно цялостно решение, което може да работи синергично

Предизвикателства при разработването и внедряването на киберфизични системи са защита на данните и комуникациите от кибератаки и неоторизиран достъп, интеграцията на различни технологии и системи, които може да работят на различни стандарти и протоколи, гарантиране на надеждността и устойчивостта на системата при различни условия и ситуации и спазване на регулаторните изисквания и стандарти, които могат да варират в различните региони и индустрии.

Киберфизичните системи представляват бъдещето на много индустрии, като предлагат нови възможности за иновации и подобрения в различни области. Те също така поставят предизвикателства, които трябва да бъдат преодоляни чрез сътрудничество между инженери, учени и политици.

Заклучение

Внедряването на нови технологии в производствения процес е ключът към увеличаване на обема готова продукция и постигане на конкурентно предимство. Автоматизацията, IoT, AI, 3D принтирането, големите данни и киберфизичните системи са само част от инструментите, които могат да трансформират традиционните методи на работа и да доведат до значителни подобрения в ефективността и качеството на продукцията. Инвестирането в тези технологии не само ще увеличи обема на произведената продукция, но и ще подготви предприятията за бъдещите предизвикателства на пазара.

ЛИТЕРАТУРА

- [1] Василев, Г. (2017). Управление на производствените процеси в условията на Индустрия 4.0. Издателство "Труд и право", София.
- [2] Димитров, Д. (2020). "Технологични иновации и тяхното въздействие върху конкурентоспособността на българските производители. "Международни икономически отношения, 2(3), 78-95.
- [3] Иванов, И. (2022). "Влияние на автоматизацията върху производителността в българската промишленост." Икономика и управление, 3(2), 45-67.
- [4] Костов, Н. (2018). Автоматизация и роботика в производството: Теория и практика. Техника, София.
- [5] Петрова, М., & Георгиева, А. (2021). "Ролята на Индустрия 4.0 в модернизацията на българските предприятия." Производствени технологии и машиностроене, 45(1), 12-25.
- [6] Стоянов, П. (2019). Дигитална трансформация в българската индустрия: Възможности и предизвикателства. Университетско издателство "Св. Климент Охридски".

ИНТЕЛИГЕНТНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА РЕСУРСИТЕ В КОМПЮТЪРНИТЕ МРЕЖИ

Силвия Х. Николова, Цветослав С. Цанков

INTELLIGENT RESOURCE MANAGEMENT SYSTEMS IN COMPUTER NETWORKS

Silvia H. Nikolova, Tsvetoslav S. Tsankov

ABSTRACT: *With the growth of data volume and the complexity of computer networks, effective resource management has become a top priority for optimizing performance and reducing costs. Intelligent management systems based on technologies such as artificial intelligence (AI), machine learning (ML), and optimization algorithms offer new approaches to automation and adaptability. This paper reviews architectures, methodologies, and applications of intelligent resource management systems in modern computer networks.*

KEYWORDS: *intelligent systems, resource management, computer networks, artificial intelligence, machine learning*

DOI: <https://doi.org/10.46687/YT24SIS>

1. Въведение

Съвременните компютърни мрежи са гръбнакът на дигиталната ера, обслужвайки нарастващи обеми от данни и свързвайки разнообразни устройства и платформи. Управлението на ресурсите в тези мрежи – като пропускателна способност, изчислителна мощност и енергийна ефективност – е ключов фактор за поддържане на надеждността и производителността им. Въпреки това, традиционните методи за управление често се сблъскват с ограничения при справянето с динамичните изисквания на модерните мрежови среди. Интелигентните системи за управление, които използват технологии като изкуствен интелект и машинно обучение, предоставят нови възможности за автоматизация, адаптивност и оптимизация на ресурсите.

С развитието на технологиите компютърните мрежи се използват в широк спектър от приложения – от персонални устройства до големи изчислителни центрове. Управлението на ресурси като пропускателна способност, изчислителна мощност и енергия е критично за поддържане на качеството на услугите (QoS).

Традиционните методи обаче често са недостатъчни, когато се изправят пред динамичните изисквания на съвременните мрежи. Настоящата статия изследва концепцията за интелигентни системи за управление на ресурсите, техните приложения и потенциалните им ползи за бъдещите мрежови архитектури.

2. Преглед на интелигентните системи за управление

Интелигентните системи за управление на ресурсите в компютърните мрежи са резултат от интеграцията на напреднали технологии като изкуствен интелект (AI), машинно обучение (ML) и алгоритми за оптимизация. Те позволяват динамично адаптиране на мрежовите ресурси, вземане на решения в реално време и автоматизация на рутинни задачи. Тези системи представляват съвременен отговор на предизвикателствата, породени от непрекъснато нарастващия обем на данни и сложността на мрежовите инфраструктури. В центъра на интелигентното управление стоят възможностите за анализ на големи данни и извличане на информация, която да подпомогне оптималното разпределение на ресурси, намаляване на закъсненията и подобряване на сигурността. С внедряването на тези системи се преминава от традиционни, реактивни подходи към проактивни стратегии за управление. Това включва автоматично разпознаване на модели в мрежовия трафик, предвиждане на възможни претоварвания и динамично адаптиране към тях. Освен за повишаване на производителността, интелигентните системи са критични за поддържане на енергийната ефективност и устойчивостта на мрежите, което е от съществено значение за центрове за данни, IoT инфраструктури и облачни услуги. [8]

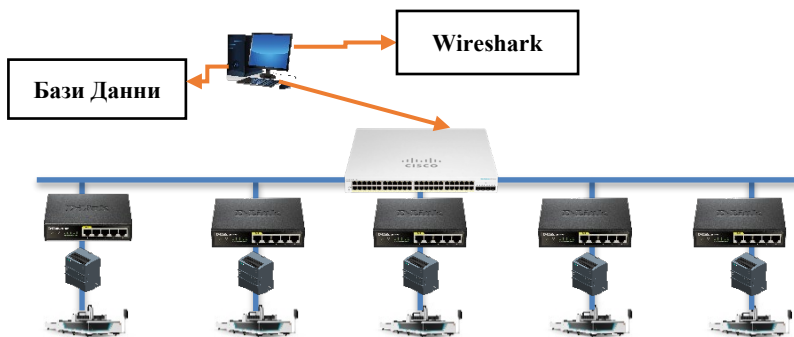
• Концепция и принципи

Интелигентните системи се базират на използването на алгоритми, които адаптират своето поведение според текущите условия в мрежата. Основните технологии включват:

- Машинно обучение – за прогнозиране на трафика и идентифициране на модели.
- Алгоритми за оптимизация – за динамично разпределение на ресурси.
- Системи за автоматизация – за вземане на решения в реално време.

• Архитектури и компоненти

Типичната архитектура на интелигентна система за управление включва модули за мониторинг, анализ и контрол. Тези модули работят съвместно чрез централизирани или разпределени подходи за обработка на данни.



Фиг. 1. Интелигентна система за управление

3. Методи за управление на ресурсите

Ефективното управление на ресурсите в компютърните мрежи е от съществено значение за поддържане на качеството на услугите (QoS) и оптимално използване на наличните ресурси. В този раздел се разглеждат ключови методи и технологии, използвани за управление на мрежовия трафик, енергийната ефективност, сигурността, както и ролята на интелигентните комутатори.

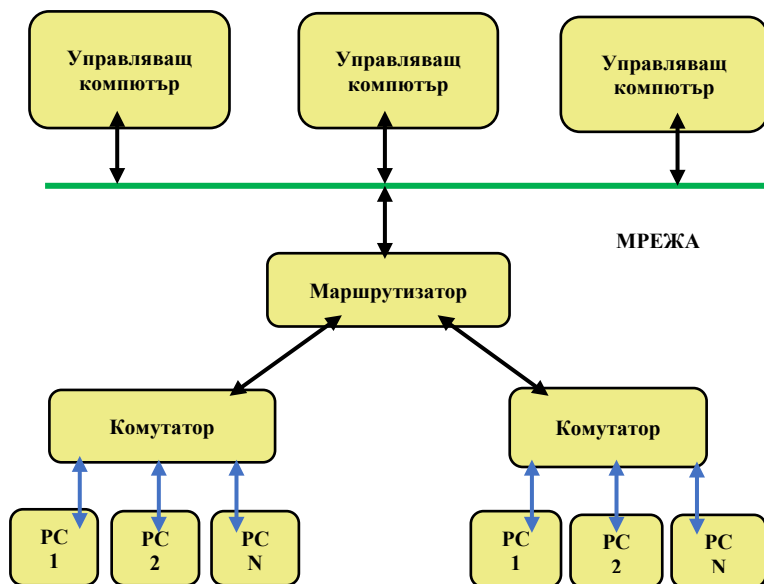
• Управление на трафика

Интелигентното управление на трафика е основополагащ компонент за гарантиране на стабилност и висока производителност в мрежите. Традиционните статични методи за маршрутизиране често са недостатъчни в контекста на съвременните мрежи, които се характеризират с непредсказуеми натоварвания.

— Прогнозиране на трафика: Машинното обучение и алгоритмите за анализ на големи данни позволяват на системите да предвиждат пикове в трафика въз основа на исторически данни.

— Динамично маршрутизиране: Алгоритми за оптимизация автоматично насочват данните по най-малко натоварените пътища, като по този начин се избягват "тесни места" и загуба на пакети.

— Технологии за мултиплексиране: Подобрения в мултиплексирането (напр. TDM и WDM) позволяват по-ефективно използване на мрежовата инфраструктура.



Фиг. 2. Управление на информационен трафик

- **Енергийно ефективно управление**

С нарастването на енергопотреблението в центрове за данни и големи мрежови инфраструктури, енергийната ефективност става критичен аспект от управлението на ресурсите.

— Динамично регулиране на мощността: Мрежовите устройства могат да регулират своята консумация на енергия според натоварването, като използват интелигентни алгоритми за включване и изключване на ресурси.

— Оптимизация на охлаждането: Внедряването на IoT сензори и машинно обучение позволява по-ефективно управление на охлаждащите системи.

— Зелени мрежи: Използването на възобновяема енергия и дизайн, насочен към минимизиране на загубите, спомага за намаляване на екологичния отпечатък.

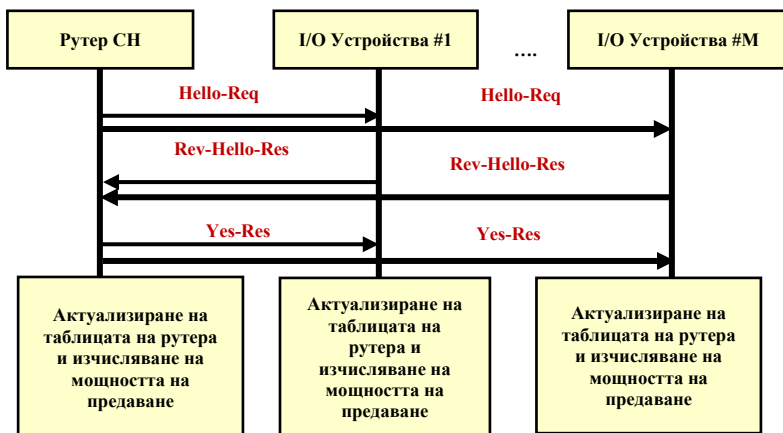
- **Сигурност и устойчивост**

Сигурността и устойчивостта на мрежите са от решаващо значение, особено в условията на нарастващи заплахи от кибератаки.

— Идентифициране на аномалии: Системите за разпознаване на шаблони в реално време могат да откриват подозрителен трафик, като се базират на исторически данни и модели.

— Автоматизирани реакции: Интелигентните системи за управление могат автоматично да блокират неоторизиран достъп или зловреден трафик, без намесата на администратор.

— Устойчивост на атаки: Алгоритмите за оптимизация могат да минимизират въздействието на DDoS атаки чрез разпределение на натоварването в различни точки на мрежата.



Фиг. 3. Клъстер за енергийно управление

- **Интелигентни комутатори за управление на мрежовия трафик**

Интелигентните комутатори (smart switches) са ключов компонент в съвременните компютърни мрежи, които използват технологии като изкуствен

интелект и машинно обучение за оптимизация на управлението на мрежовия трафик. Те предлагат динамична конфигурация, автоматизация и възможности за вземане на решения в реално време, като осигуряват:

- Динамично маршрутизиране: Интелигентните комутатори анализират в реално време трафика в мрежата, разпознават претоварвания и автоматично пренасочват данните по алтернативни пътища, за да минимизират латентността.

- Качество на услугата (QoS): Възможност за приоритизиране на критичен трафик, като видео-конференции или IoT данни, което гарантира надеждност и ефективност.

- Адаптивно управление на пропускателната способност: Използване на прогнозни алгоритми за предвиждане на натоварването и динамично разпределение на ресурсите.

- Сигурност: Вградените системи за разпознаване на аномалии могат да идентифицират и блокират злонамерени действия, като DDoS атаки, преди те да засегнат производителността на мрежата.

Тези комутатори са особено полезни в големи корпоративни мрежи, центрове за данни и IoT инфраструктури, където изискванията за мащабируемост и надеждност са критични. Внедряването на интелигентни комутатори води до значително намаляване на разходите за поддръжка и повишаване на ефективността на мрежовите операции. [3]

Таблица 1. Данни от мониторинг на мрежовия трафик [4]

Източник	Дестинация	Протокол	Размер (байтове)	Време на предаване	Статус
192.168.0.1	192.168.0.2	TCP	1500	1ms	Успешно
192.168.0.1	192.168.0.3	UDP	1024	2ms	Забавяне
192.168.0.2	192.168.0.3	Zigbee	64	0.5ms	Успешно
192.168.0.3	192.168.0.4	Z-wave	2000	1.2ms	Загуба

4. Приложения в индустрията

Интелигентните системи за управление на ресурсите намират приложение в широк спектър от индустриални сектори, където оптимизацията на мрежовата инфраструктура и ресурсите е критично важна. Тези приложения демонстрират как интеграцията на изкуствен интелект, машинно обучение и автоматизация може да преобрази съвременните технологии, подобрявайки ефективността, мащабируемостта и сигурността на мрежите.

• Центрове за данни (Data Centers)

Центровете за данни са ядрото на съвременните облачни услуги и обработка на големи обеми информация. Управлението на ресурсите в такива среди е предизвикателство поради високата динамика на натоварването и разнообразието от приложения, които се изпълняват паралелно.

- Динамично разпределение на натоварването: Интелигентните системи позволяват автоматично насочване на работни натоварвания към сървъри с по-ниско текущо натоварване, което минимизира закъсненията и повишава ефективността.

— Енергийна оптимизация: Използване на алгоритми за управление на охлаждането и намаляване на излишната енергийна консумация чрез изключване на неизползвани ресурси. [5]

— Сигурност: Разпознаване на аномалии и автоматично реагиране на потенциални заплахи, като кибератаки или нарушения в мрежовата инфраструктура.

• **Интернет на нещата (IoT)**

IoT екосистемите, които включват милиарди свързани устройства, изискват надеждни и ефективни мрежови решения за управление на ресурси и сигурност.

— Оптимизация на мрежовия трафик: Интелигентните системи регулират трафика между устройствата, като приоритизират критичните данни и осигуряват ниска латентност за време-чувствителни приложения. [6]

— Управление на енергията: Алгоритмите за оптимизация удължават живота на батериите в IoT устройства чрез минимизиране на ненужните комуникации и разходи.

— Мащабируемост: Интелигентните технологии позволяват лесно добавяне на нови устройства и адаптация към нарастващите изисквания за обработка на данни.

• **Облачни услуги и виртуализация**

С нарастващата популярност на облачните технологии, интелигентните системи играят важна роля в оптимизацията на виртуалните ресурси.

— Автоматично мащабиране: В реално време системите анализират натоварването и автоматично увеличават или намаляват наличните ресурси според нуждите на приложенията.

— Оптимизация на разходите: Чрез намаляване на излишните ресурси, интелигентните системи спомагат за значително намаляване на разходите за облачни услуги.

— Устойчивост: Системите автоматично разпределят натоварването между различни центрове за данни, за да се осигури непрекъсната работа дори при повреда в даден регион.

• **Телекомуникационна индустрия**

Телекомуникационните мрежи, които се развиват с настъпването на 5G и други авангардни технологии, се възползват от интелигентни системи за управление на ресурсите.

— Оптимизация на спектъра: Интелигентните системи могат динамично да разпределят честотния спектър между потребители, за да осигурят висока скорост на комуникация.

— Управление на мрежова топология: Автоматизирано адаптиране към променящи се условия, като например претоварване в дадена клетка, чрез пренасочване на ресурси.

— Намаляване на закъсненията: Време-чувствителните приложения като автономни автомобили и дистанционна хирургия се възползват от минимална латентност, осигурена от интелигентните технологии.

- **Производствена индустрия и автоматизация**

Производствените предприятия все повече разчитат на интелигентни мрежови решения за управление на автоматизирани системи и роботизирани процеси.

- Управление на индустриалните IoT (IIoT): Интелигентните системи подпомагат координацията между машини, като осигуряват надеждна комуникация и минимизират времето за престой.

- Прогнозна поддръжка: Чрез анализ на данни от сензори, системите предвиждат повреди и минимизират прекъсванията в производството.

- Ефективно използване на ресурси: Интелигентните технологии намаляват загубите и увеличават производителността чрез оптимизация на производствените линии.

- Образователни и здравни институции

Интелигентните мрежови решения трансформират начина, по който се предоставят образователни и здравни услуги.

- Дистанционно обучение: Системите оптимизират трафика за видеоконферентни платформи, гарантирайки гладко и надеждно взаимодействие между участниците.

- Здравеопазване: Интелигентните мрежи осигуряват надеждност при трансфер на критични медицински данни и поддържат свързани устройства за телемедицина.

Интеграцията на интелигентни системи за управление в тези индустрии води до повишаване на ефективността, намаляване на разходите и подобряване на цялостното качество на услугите. Тези приложения демонстрират трансформационния потенциал на интелигентните технологии в различни сектори.

5. Предизвикателства и ограничения

Въпреки значителните предимства, които предлагат интелигентните системи за управление на ресурсите в компютърните мрежи, тяхното внедряване и поддръжка са свързани с редица предизвикателства. Тези ограничения произтичат както от технически, така и от организационни и икономически фактори. Разглеждането на тези аспекти е от ключово значение за успешното приложение на интелигентни технологии в мрежовите инфраструктури.

- **Високи първоначални разходи**

Интеграцията на интелигентни системи изисква значителни инвестиции в хардуер, софтуер и обучение на персонал.

- Инфраструктурни изисквания: Много мрежови устройства, които са част от съществуващите системи, не са съвместими с модерните интелигентни технологии, което налага тяхната подмяна или надграждане.

- Разходи за внедряване: Процесът на интеграция включва проектиране, конфигуриране и тестване на системите, което може да бъде скъп и времеемък процес.

— Обучение на кадри: За да се възползват ефективно от възможностите на интелигентните системи, организациите трябва да инвестират в обучение на ИТ персонал и мрежови инженери.

• ***Сложност на управлението***

Внедряването на интелигентни системи значително увеличава сложността на мрежовата инфраструктура.

— Трудности при интеграция: Комбинирането на съществуващи мрежови технологии с нови интелигентни решения може да доведе до проблеми със съвместимостта.

— Необходимост от постоянна поддръжка: Интелигентните системи изискват редовни актуализации на софтуера, мониторинг и настройки, за да работят ефективно.

— Сложност при мащабиране: Разширяването на интелигентните мрежи в глобален мащаб изисква координирани усилия и добре структурирано управление.

• ***Данни и поверителност***

Използването на интелигентни системи изисква обработка на големи обеми от данни, което повдига въпроси за сигурността и поверителността.

— Рискове за сигурността: Уязвимости в интелигентните системи могат да бъдат използвани за кибератаки, компрометиращи чувствителни данни и мрежови операции.

— Поверителност на данните: Някои приложения изискват обработка на лична информация, което поражда опасения относно спазването на законодателства като GDPR. [7]

— Управление на данните: Наличието на голямо количество данни изисква надеждни методи за съхранение, анализ и унищожаване на излишните данни.

• ***Етични и социални въпроси***

С навлизането на интелигентните системи възникват и въпроси, свързани с тяхното въздействие върху работните места и обществото като цяло. Автоматизация и загуба на работни места: Внедряването на интелигентни технологии може да замени ръчната работа, което води до съкращения в някои индустрии.

— **Етични въпроси при вземането на решения:** Алгоритмите могат да вземат автоматизирани решения, които да не отразяват напълно етичните и правните стандарти.

— Приемане от обществото: Някои потребители и организации може да се противопоставят на внедряването на нови технологии, поради страх от неизвестното или недоверие към технологиите.

• ***Ограничения на технологиите***

Въпреки напредъка на изкуствения интелект и машинното обучение, съществуват ограничения, които възпрепятстват пълното реализиране на потенциала на интелигентните системи.

— Точност на алгоритмите: Алгоритмите, които обработват данни и вземат решения, невинаги са напълно точни или адекватни в непредвидени ситуации.

— Зависимост от качеството на данните: Интелигентните системи изискват надеждни и обширни данни за обучение и функциониране. Недостатъци в данните могат да доведат до неправилни решения.

— Изчислителни изисквания: Високите изисквания за изчислителна мощност могат да бъдат пречка за внедряване в по-малки организации или в среди с ограничени ресурси.

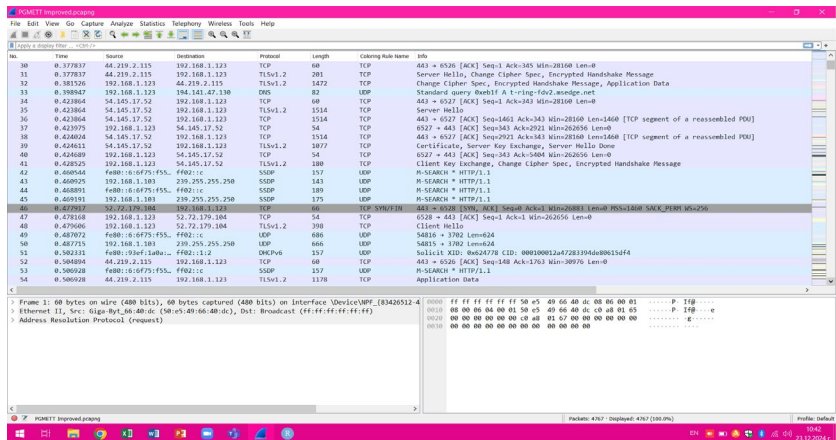
С оглед тези предизвикателства, непрекъснатото развитие на технологиите и иновациите предлага решения за преодоляване на голяма част от ограниченията. За организациите, които успеят да се справят с тези трудности, ползите от интелигентните системи за управление значително надхвърлят предизвикателствата.

6. Свързване на интелигентните системи с Wireshark и Cisco

Wireshark и Cisco са две ключови технологии, които играят важна роля в мониторинга, анализа и управлението на мрежите. Интеграцията на тези инструменти с интелигентни системи за управление на ресурсите може да значително подобри ефективността и сигурността на компютърните мрежи. [1]

• Wireshark за анализ на трафика

Wireshark е мощен инструмент за мониторинг на мрежовия трафик в реално време, който позволява на интелигентните системи да откриват аномалии и натоварвания в мрежата. Данните от Wireshark могат да се използват за анализ на мрежовото състояние, диагностика на проблеми и оптимизация на ресурсите чрез интелигентни алгоритми. [9]

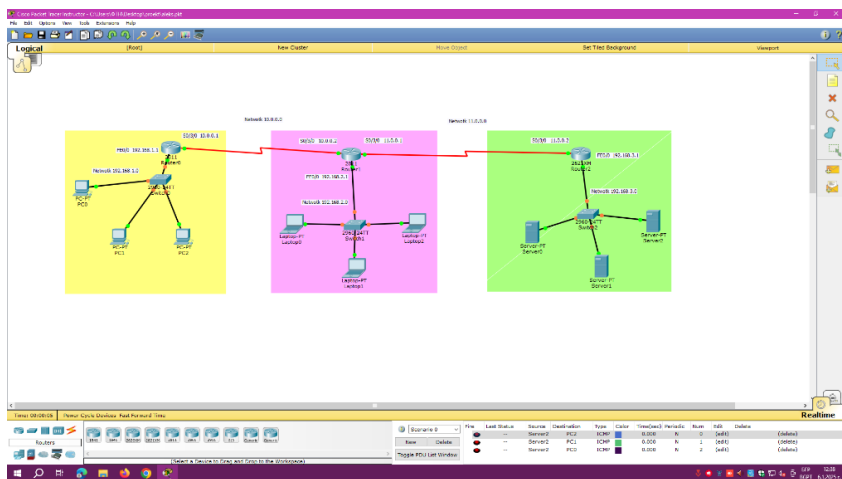


Фиг. 4. Мониторинг на трафик с Wireshark

• Cisco и интелигентните мрежи

Cisco предоставя интелигентни рутери, суичове и платформи като Cisco DNA Center, които автоматизират управлението на мрежата и осигуряват

оптимизация на трафика. Когато се свържат с интелигентни системи за управление, тези устройства позволяват динамично пренасочване на трафика и подобрена сигурност, като автоматично откриват и реагират на мрежови проблеми. [10]



Фиг. 5. Управлението на мрежи чрез Cisco packet tracer

• Синергия между софтуерни продукти Wireshark и Cisco с интелигентните системи

Комбинирането на Wireshark, Cisco решения и интелигентни алгоритми създава интегрирана и адаптивна мрежова инфраструктура. Това води до проактивно управление на мрежовите ресурси, подобрена сигурност и оптимизация на мрежовите услуги чрез анализ на трафика, автоматизация на конфигурациите и бързо реагиране на аномалии. Тази интеграция осигурява повисока ефективност, надеждност и сигурност в съвременните мрежи. [2]

7. Заключение

Интелигентните системи за управление на ресурсите в компютърните мрежи са в основата на модернизацията и оптимизацията на глобалните мрежови инфраструктури. С напредъка на изкуствения интелект, машинното обучение и анализа на големи данни, тези технологии предоставят мощни инструменти за динамично управление, прогнозиране и адаптиране на мрежовите ресурси. Те не само че подобряват ефективността и производителността на съществуващите мрежи, но и отварят нови възможности за създаване на интелигентни и самоуправляващи се мрежови екосистеми, които могат да отговорят на нарастващите изисквания на потребителите и индустриите.

Приложенията на интелигентните системи обхващат различни индустрии, включително центрове за данни, интернет на нещата (IoT), облачни услуги и телекомуникации, като всяка от тях извлича ползи от оптимизирането на

ресурсите и намаляването на разходите. Въпреки това, тяхното внедряване среща значителни предизвикателства, свързани с високите първоначални разходи, сложността на интеграцията, сигурността на данните и етични въпроси, които трябва да бъдат внимателно разгледани и преодолені.

ЛИТЕРАТУРА

- [1] National Dimensions, 2019, Cadet-Students Scientific Conference, Collection of Papers, National Military University „Vasil Levski“, Veliko Tarnovo, ISSN 2367-7481, pp. 300-310.
- [2] Denev D., Konstantinova E., Main Issues in the Protection of Information in the system of National and Corporate Security, 2020, Conference with international participation MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 110-115.
- [3] Denev D., Z-WAVE Communication for Home Automation, 2020, Conference with international participation MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 96-103.
- [4] Denev D., Terziev H., Zigbee Communication Protocols and Their use to Manage Smart Devices, 2020, Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of technical sciences, ISSN 1311-834X, pp. 83-89.
- [5] Denev D., Low Energy Real-Time Routing, 2022, Annual University Scientific Conference, Proceedings of National Military University „Vasil Levski“, Veliko Tarnovo, 2022, ISSN 2367-7481, pp. 1267-1276.
- [6] Denev D., Tsankov Ts., Communication-Based Dynamic Packet Optimization for Visual PLC Monitoring, 2022, Annual University Scientific Conference, Proceedings of National Military University „Vasil Levski“, Veliko Tarnovo, ISSN 2367-7481, pp. 1259-1266.
- [7] Denev D., Tsankov Ts., A Survey of Data Quality and Processing of Information in Innovative Smart Devices, 2022, International Conference Automatics and Informatics (ICAI) 2022, <https://ieeexplore.ieee.org/>, Varna Bulgaria, 06-08 October, ISBN 978-1-6654-7625-6 and 10.1109/ICA155857.2022.9960040
- [8] Denev D., Modeled Security in Communication Network Coding, 2022, Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, ISSN 1311-834X, pp. 153-161.
- [9] Denev D., Surveillance with Wireshark and its Use in Communication Networks, 2023, Annual of Konstantin Preslavski University of Shumen, Volume XIII E, ISSN 1314-8818, pp. 104-109.
- [10] Denev D., Tsankov Ts., Use of Cisco Packet Tracer in Evaluation of Communication Networks, 2023, XVI International Scientific Conference, Belovo, ISBN 978-5-00137-315-5 (item 1), ISBN 978-5- 00137-314-8, pp. 163-171.

АСПЕКТИ НА БЕЗПИЛОТНИ ЛЕТАТЕЛНИ АПАРАТИ

Владислава С. Георгиева, Никола П. Петров

ASPECTS OF UNMANNED AERIAL VEHICLES

Vladislava S. Georgieva, Nikola P. Petrov

ABSTRACT: *Nowadays, unmanned aerial vehicles have found wide application in many aspects of modern times and have proved their usefulness. In this article, several types of unmanned aerial vehicles for the needs of the Bulgarian army will be considered. One of the possible control systems will also be analyzed.*

KEYWORDS: *drones technologies, radio control, LoRa communication*

DOI: <https://doi.org/10.46687/YT24VLD>

1. Въведение

Безпилотните летателни апарати (БЛА) са намерили широко разпространение в съвременния технологичен свят. Те заместват скъпоструваща техника и дори жива сила. Именно благодарение на това, БЛА се използват и за военни цели.

Първият БЛА е създаден още през 1916 г. САЩ започват да разработват технология на БЛА по време на Първата световна война през 1916 г. и създават първия безпилотен самолет. От тогава САЩ, както и други държави, не спират да разработват тази технология.

Използването на безпилотни летателни апарати играе неразделна и незаменима роля във военните операции на САЩ по време на войните, както в Афганистан, така и в Ирак [9]. Оттогава дроновете приемат нови форми, намират място в ръцете на любителите, а наскоро играят и роля в постмодерния транспорт. Въпреки своите първоначални военни цели, безпилотните летателни апарати са намерили и своето гражданско предназначение. За него те са получили и по-краткото наименование – дрон, което стана дори по-разпространено. Целите, за които може да бъде използван летящия дрон са много. Освен вече посоченото по-горе военно предназначение, те се занимават и с аерозаснемане, мониторинг на безопасността, научни изследвания.

Индустриите, имащи в арсенала си тези апарати са много: селското стопанство, риболова, лесоохраната, картографирането, енергетиката, геологията, строителството, медиите и т.н.

БЛА са намерили място в свертата на сигурността и отбраната и на Република България и в настоящата статия ще бъдат разгледани **някои от тези БЛА и съща така една от системите за управлението им.**

2. Безпилотни летателни апарати разработени за Българската армия

2.1. БЛА TERES-02

Разработен от българската компания Telesys Ltd., TERES-02 е безпилотен летателен апарат, проектиран за военни приложения, включително интеграция с радарни и сензорни системи, които отговарят на стандарти като MIL-STD-810F (издръжливост и устойчивост на екстремни условия). Изработен е изцяло от композитни материали, което подобрява издръжливостта и намалява теглото. TERES-02 се използва както за военни тренировки (например като въздушна мишена), така и за граждански задачи като наблюдение и сбор на данни. Той е интегриран в системи на българските въоръжени сили и има международни продажби. TERES-02 отговаря на строги стандарти за качество (ISO 9001) и военна издръжливост (MIL-STD-810F), като е проектиран за работа в синхрон с радарни системи в X-диапазон.

Ето основните характеристики и възможности:

- Максимална скорост-180 km/h (97kts IAS);
- Круизна скорост-110 km/h (60kts IAS);
- Разпереност на крилете – 3.90 m;
- Максимална продължителност на полета – 5 часа;
- Максимална височина – 4500 m;
- Система за управление – Наземна контролна станция, автономен автопилот с възможност за програмиране по време на полет, шумоустойчива криптирана комуникационна система;
- Навигационна система – Шумоустойчива GPS, MEMS базирана инерциална навигационна система, магнитен компас, въздушна сигнална система, отопляем пост за наблюдение на въздуха, система за избягване на сблъсък с други въздухоплавателни средства (Mode-S ADS-B);
- Максимално излетно тегло – 45 kg.

Липсата на изрични данни за неговата собствена комуникационна честота предполага, че тя може да варира в зависимост от конфигурацията и приложението. [2] [6] [7]

2.2. Textron Aerosonde Mk 4.7

Textron Aerosonde Mk 4.7 е семейство безпилотни летателни системи (БЛС), проектирани за експедиционни операции на суша и море. Те се отличават с висока надеждност, гъвкавост и възможност за изпълнение на множество мисии в едно летене. Ето основните характеристики и възможности:

- Тип Фиксирано крило (съществуват и VTOL модификации, като Mk 4.
- Размах на крилете - 4.4 m
- Максимална излетителна маса (MGTOU) - 42.2 кг.
- Товароподемност – до 14.5 кг, с възможност за монтиране на до 6 полезни товара в едно летене.
- Двигател: Тежък горивен двигател – Lycoming EL-005, съвместим с JP-5, JP-8, Jet-A и други видове горива.

— Автономност: До 19.8 часа полет (при пълна товароподемност – до 12 часа).

— Скорост: 45–65 възела (83–120 км/ч).

— Радиус на действие: 140 км (75 морски мили).

— Работна височина: До 14,700 фута (4,481 m)

Оперативни възможности

Мултимисионност: Поддържа едновременно използване на:

— EO/IR камери (дневни и нощни).

— Синтетичен апертурен радар (SAR) за наблюдение при всякакви метеорологични условия.

— Сигнален разузнавател (SIGINT) и електронна война (EW).

— Комуникационни релета (включително MANET мрежи).

Aerosonde Mk 4.7 е намерил приложение във военни мисии, разузнаване, наблюдение и целеуказване (ISR), морски операции (напр. автоматично идентифициране на кораби чрез AIS), поддръжка на комуникации в отдалечени зони, граждански приложения и др. [3] [4] [5]

2.3. БЛА МБД-01

Разработен от учени от Българската армия, безпилотен летателен апарат, проектиран за военни приложения, включително интеграция с радарни и сензорни системи, които позволяват: подпомагане на артилерийските системи, разузнаване и бонбандировки. Изработен е изцяло от композитни материали, което подобрява издръжливостта и намалява теглото.

Ето основните характеристики и възможности на дрона и съпътстващата наземна станция:

— Навигационна система – Шумоустойчива с външен GPS притежаващ в себе си отделен барометър, жирокоп, акселерометър и компас които се добавят към основните на бордовия компютър. Поддръжка на RTK с точност до 2 см, MEMS базирана инерциална навигационна система, магнитен компас, въздушна сигнална система, отопляем пост за наблюдение на въздуха, система за избягване на сблъсък с други въздухоплавателни средства (Mode-S ADS-B);

— 360 Lidar за избягване на препятствия и Mapping;

— OpFlow сензор за подобряването на позиционирането с или без GPS(до 8 метра височина);

— Комуникацията с оператора е с две честотни ленти 2,4GHz и 915MHz едновременно;

— Видео връзката отново е в две честотни ленти 1,2GHz аналогова и 5,8GHz дигитална с опция за Head Tracking;

— Тегло без полезен товар- 5757гр. с 32 Ah батерия;

— Полезен товар по изчисления до 5 кг;

— Полет в зависнало положение без външни фактори и с максималния полезен товар 18,5 мин;

— Максимална подемна сила с перки със заредена батерия- 19200 гр.

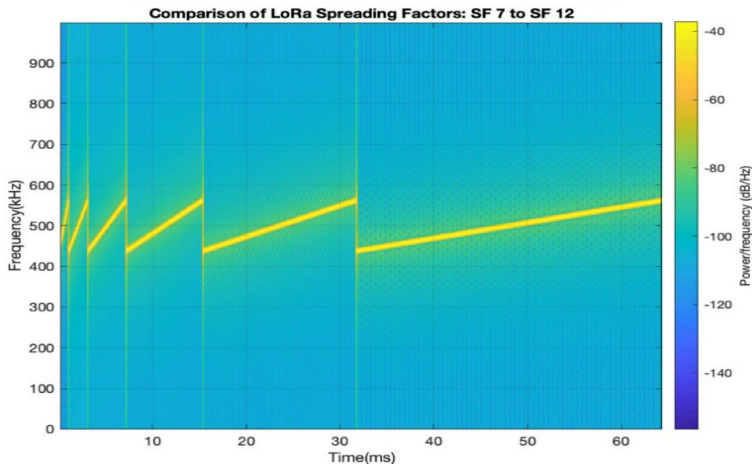
— Куфар MIL standart IP67;

— 4x12V 9Ah акумулатори за захранване на станцията;

- Индустриален компютър Panasonic Toughpad за управление и телеметрия с мин. 6ч. живот на батерията;
- Аналогов монитор с аналогови приемници на 1,2 и 5,8 GHz + аналогови към дигитални конвертори за четене на сигнала и от таблета;
- RTK модул с външна GPS антена поставяща се на тринога;
- LoRa 915 MHz телеметрично радио с мощност от 1W за двупосочна връзка;
- Радио управление Radiomaster TX16S работещ 2,4 GHz ELRS и Bandit модул на 869-915 MHz.
- Максимална продължителност на полета – 40 минути;
- Максимална височина – 1200 m;
- Максимално тегло – 11 kg.

3. LoRa комуникации за дронове: Далекобойност и ефективност

LoRa (Long Range) комуникациите са безжична технология, която намира все по-широко приложение при дроновете благодарение на ниското си енергопотребление и способността да предава данни на големи разстояния. Тази технология използва модулация с разширен спектър, която позволява връзка на разстояние от няколко километра дори при наличие на препятствия. В сравнение с традиционните Wi-Fi или 4G/5G решения [8], LoRa е значително по-ефективна при изпращането на малки пакети данни, като телеметрия, GPS координати и сензорна информация.



Фиг. 1. Фактор на разпространение на LoRa сигналът

В сферата на дроновете LoRa се използва основно за мисии, изискващи надеждна комуникация в отдалечени или труднодостъпни райони, като селскостопански мониторинг, наблюдение на горски пожари и инспекция на

инфраструктура. Макар и да не поддържа високоскоростен пренос на видео, технологията е идеална за дронове с автономни функции, където е важно предаването на команди и данни за състоянието. Комбинацията ѝ с IoT мрежи и сателитни комуникации също разширява възможностите ѝ, правейки LoRa ключов инструмент за бъдещето на безпилотните летателни апарати. [1]

4. Заключение

LoRa комуникацията играе важна роля в развитието на дроните технологии, като предлага надежден и енергийно ефективен начин за предаване на данни на големи разстояния. Макар че не е подходяща за високоскоростен трансфер на видео, нейните предимства в телеметрията, IoT интеграцията и автономните операции я правят ценен инструмент за безпилотните летателни апарати.

Дроните Textron Aerosonde Mk 4.7 и TERES-02 са примери за съвременни безпилотни системи, които използват усъвършенствани комуникационни технологии за изпълнение на сложни мисии. Textron Aerosonde Mk 4.7 е проектиран за военни и разузнавателни цели, осигурявайки дълга продължителност на полета и стабилна комуникационна връзка, докато TERES-02 представлява гъвкава платформа с възможност за различни приложения, включително граждански и военни операции.

В бъдеще комбинирането на LoRa с други безжични технологии и сателитни комуникации ще подобри ефективността на дроните, разширявайки обхвата им на действие и повишавайки автономността им. Тези иновации ще продължат да играят ключова роля в развитието на дроните технологии за военни, индустриални и граждански приложения.

ЛИТЕРАТУРА

- [1] <https://medium.com/@prajzler/what-is-lora-the-fundamentals-79a5bb3e6dec>
- [2] <https://aero-bg.com/2021/11/22/devet-kandidata-za-dostavka-na-bla-za-suhopatni-vojski/>
- [3] <https://www.naval-technology.com/projects/aerosonde-mark-47-small-unmanned-aircraft-system-suas/>
- [4] <https://www.textronsystems.com/products/aerosonde-uas>
- [5] <https://www.canadianuavs.ca/post/aerosondetm-mk-4-7-operational-at-cfb-edmonton>
- [6] https://pan.bg/?page=view_article§ion_id=4&article_id=23250
- [7] <https://defense-guide.com/item/telesys-ltd/>
- [8] Nikolov L. Error rate analysis in Ricean channel and complex radio environment, Defence Technology Forum, Shumen, 2016, ISSN: 2367-7902.
- [9] Borisova A. R., Nikolov L. Systems with artificial intelligence for defense and security. Scientific research and education in the air force – AFASES 2023, pp. 53-58, <https://doi.org/10.19062/2247-3173.2023.24.7>

ВРЪЗКА МЕЖДУ ПРИРОДНИТЕ БЕДСТВИЯ И ЕКОКАТАСТРОФИТЕ СЪС ЗАОБИКАЛЯЩАТА НИ СРЕДА

Весела Р. Петрова

CONNECTION NATURAL DISASTERS AND ECODISASTERS WITH SURROUNDING AREA

Vesela R. Petrova

***ABSTRACT:** Connection natural disasters and ecodisasters whit surrounding area, early warning systems and GNSS supervision.*

***KEYWORDS:** natural disasters, ecodisaster, GNSS*

***DOI:** <https://doi.org/10.46687/YT24VES>*

Въведение

Използването в научната литература и публичното пространство на термина „инженерно-технически съоръжения“ не е еднопосочно, а отразява различна отраслова, социална или териториална насоченост.

Всички инженерно-технически съоръжения се поставят под общото наименование-инфраструктурни обекти и съоръжения.

Американският учен Розенщейн-Родан (1955) дава едно по-общо определение за инженерно-технически съоръжения, в което е подчертано тяхното съществено значение за регионалното развитие на отделните териториални формирования и социално-икономическите отрасли – „Комплекс от общи дадености, осигуряващи благоприятни условия за развитието на основните отрасли на икономиката, строителството и удовлетворяване потребностите на населението“.

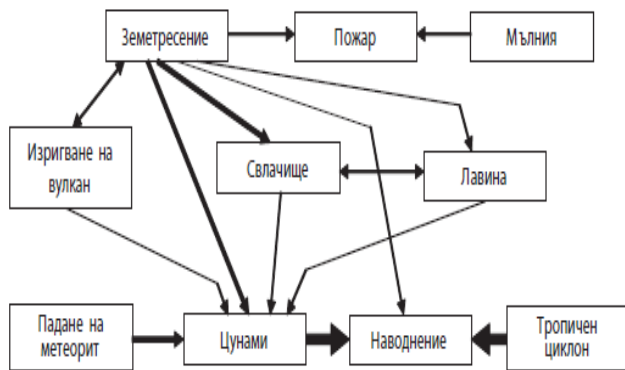
Връзката между различните бедствия и екокатастрофи със заобикалящата ни среда

Въпреки прогресиращото технологично и обществено развитие, хилядолетния човешки житейски опит натрупан в борбата за оцеляване и формиралата се през последните десетилетия тенденция за преосмисляне на взаимовръзката със заобикалящата среда, рисковете породени от природните бедствия и тяхното влияние върху инженерно-техническите съоръжения стават все по-значими.

Световната статистка показва тенденция към увеличаване броя на екстремни прояви на природни явления и процеси, чието негативно въздействие води до все по-мощни физически загуби, което обуславя и противопоставянето на природните рискове като особено актуален проблем [1].

В литературата съществуват и се дискутират различни определения свързани с природните бедствия. Използват се понятия като „криза“, „бедствие“, „извънредна ситуация“, „катастрофа“. Общото обаче между тях е, че тези събития имат разрушителен характер и нанасят значителни щети за населението, техническата инфраструктура и икономиката на всяка страна.

Типични примери за природни бедствия са вулканичните изригвания, земетресенията, наводненията, лавините и тропическите циклони. Възможно е от своя страна едно природно бедствие да породии след себе си и друго, например вулканичните изригвания често са съпътствани от земетресения.



Фиг. 1. *Модел на връзката между различните екокатастрофи*

Размерът на загубите обикновено зависи от подготвеността на хората и от способността им да реагират навременно и адекватно на бедствието, най-вече по спасителните работи.

Това разбиране се изразява с популярната фраза, че „бедствията възникват, когато опасността се съчетае с уязвимост“.

В предстоящите десетилетия се очаква промените в климата да доведат до нарастване на честотата и мащаба на бедствията и аварията на инженерно-технически съоръжения.

В България често възникват бедствия, предизвикани от природни явления или човешка дейност, чиито социални и икономически последици могат да оказват значителен неблагоприятен ефект на нейното развитие и икономически растеж, поради което намаляването на риска от бедствия е от изключително значение за устойчивото развитие на страната.

Поради сложността и обхвата на бедствията, е необходимо обединяване на усилията и активното включване в дейностите за намаляване на риска от бедствия и аварии, което се очаква да доведе до значително намаляване на човешки, социални, икономически и природни щети и загуби.

За понятието „*риск*“ са предлагани и се използват различни дефиниции. В речници, тълковни речници и енциклопедии рискът се определя най-общо като

несигурност, вероятност за негативни последици, очаквани или потенциални загуби. [2]

В зависимост от характера на природните бедствия (сила, физически особености, начин на въздействие – ударно или постепенно) и характерните особености на различните инфраструктурни съоръжения, последиците за тях могат да имат различен характер, което на практика означава-различна уязвимост.

Таблица 1. Уязвимост на някои съоръжения от различни природни бедствия

Природно бедствие/ Съоръжение	ЗЕМ.	СВЛ.	ВУЛК.	П и С	Н	Ц	Б	МП	СВ	Г(П)П
Хидросъоръж.	1*-3	1*-3	1*-3	3	4	4	3	11	3	1
Мостове	1*-3	1*-3	3	5	1	4	4	11	2	2
Пътни и жп линии	4	4	5	2	5	5	3	44	4	1*
Ел.проводи	4	4	3	1	3	4	5	5	5	5
Тръбопроводи	5	5	5	2	5	4	3	55	4	1*-5
Открити мини	4	5	4	3	4	4	3	11	3	2
Под.мини	3	5	1	4	4	4	1	11	1	1
Хранилища за отпадъци	2	5	4	4	5	5	5	11	4	4
Морски платформи	4	1	4	0	0	5	5	44	5	0
Солзави	4	4	4	3	5	5	5	55	5	4
Бензиностанции	4	3	5	1*	5	5	5	33	5	5
Тунели	2	4	1	1*	4	4	1	00	0	0
Заводи/Фабрики	4	4	4	1*	4	4	5	22	5	1*

Различните елементи на техническата инфраструктура са различно уязвими от въздействието на различните природни бедствия и тяхната мощ. В Таблица 1 са дадени възможните уязвимости на различните обекти и съоръжения от въздействията на различни природни бедствия: Зем.-Земетресения; Свл.-Свлачища; Вулк.-Вулкански изригвания; П и С – Пропадания и срутища; Н-Наводнения; Ц- Цунами; Б-Бури; М/П-Мразове и поледици; СВ-Силни ветрове; Г(П)П-Горски (полски) пожари.

Стойностите от 0 до 5 означават различните нива на уязвимост: 0-няма или не се отнася за съответния обект, 1-слаба, 2-слаба-средна, 3-средна, 4-средна-силна, 5-силна, *-означава, че обикновено съоръженията от този тип се осигуряват при проектирането им с регламентирани противобедствени мероприятия.[3]

Системи за ранно оповестяване

Освен ефективна борба с последиците от природни бедствия, не по-малко важно е осъществяването на мониторинг и превенция, както и изграждането на надеждни системи за ранно предупреждение. Тези системи са важен компонент от стратегиите за адаптация към климатичните промени и управлението на риска от бедствия.

Основната цел на системите за ранно предупреждение е да известяват населението, когато предстои бедствие или то вече се случва.

Съществуващите системи за ранно оповестяване или предупреждение на населението при настъпване на бедствия и аварии са запазили структурата и функциите си от 70-80 години на миналия век. По същество те използват централизирани технически подходи, решения и инструменти, които не могат да бъдат ефективни при съвременни условия.

Изискванията към системите са регламентирани в *„Наредба за условията и реда за функциониране на националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия и за оповестяване при въздушна опасност“*¹:

— Системата следва да бъде лесно надграждана и интегрирана с други информационни системи, имащи отношение към превенцията от бедствия и аварии на местно, регионално и национално ниво;

— Да осигурява набиране на информацията от мониторинговите точки на определен период от време, метеорологичните станции и разположените камери за наблюдение на мониторинговите станции в реално време;

— Комуникационният софтуер следва да осигурява предаване и валидиране на данни в реално време, събрани от мониторинговите точки към Оперативния център;

Наземните и сателитните наблюдения в съвременните системи за ранно предупреждение играят важна роля в превенцията на бедствията. Те могат да намалят както загубите на живот и имущество така и разрушителни последици върху техническите съоръжения от съществуващи опасности.

Обединението и използването на технологии и комуникационни канали от сателитни и наземни наблюдения, улеснява бързото и масово разпространение на важна информация в реално време в случай на бедствия.

Способността на ГНСС структурите да предоставят широк обхват и висока резолюция на наблюдаваната територия позволява бързо и точно откриване на наводнения, свлачища, компрометирани инженерно-технически съоръжения като язовирни стени, мостове, виадукти и други и оценка на възможните последиствия.

Основната цел на системите за ранно предупреждение и оповестяване е разпространяване на навременна и значима информация, която позволява на хората и организациите да се подготвят и да действат по подходящ начин, с цел намаляване на възможните вреди или загуби. Тук можем да заключим, че тези технологии за ранно оповестяване през последните години обхващат широка гама от иновативни решения от системи за ранно оповестяване и иновационни

¹ „Наредба за условията и реда за функциониране на националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия и за оповестяване при въздушна опасност“

Обн. ДВ. бр.20 от 9 Март 2012г., изм. ДВ. бр.60 от 22 Юли 2014г., изм. и доп. ДВ. бр.61 от 2 Август 2019г., изм. и доп. ДВ. бр.65 от 6 Август 2021г., изм. ДВ. бр.47 от 24 Юни 2022г.

инженерни решения до управлявани от AI² анализи, роботика и обучение за виртуална реалност.

ГНСС за наблюдение и ранно предупреждение от природни бедствия

Технологичният напредък изиграва ключова роля в трансформирането на стратегиите за смекчаване на последиците от бедствия.

Новостите в технологията не само увеличават способността ни да предвиждаме и да се подготвяме за потенциални бедствия, но и осезаемо повишават ефикасността и ефективността на усилията ни за реакция и последващо възстановяване. Благодарение на силата на технологиите, днес можем да създадем по-устойчиви и адаптивни общности, които могат да издържат на предизвикателствата, породени от гнева на природата, и опасностите, причинени от човека.

Съвременните технологии предлагат широк спектър от методи за измерване, но най-интересни и ефективни са задачите, свързани със събирането и използването на геоданни от спътниковите GNSS технологии и създадените на тази база GNSS приемници.

Съществуват три основни вида космически технологии като сателитни телекомуникации, наблюдение на Земята и сателитна навигация или сателитна навигационна система за автономно геопозициониране, които играят важна роля в ранното предупреждение различни за начало и проследяване. Те могат да наблюдават както обширни по площ територии от земната повърхност, така и милиметрови отклонения от движението на земните маси, изместване на открити фундаменти и други технически особености.

1. **Сателитни телекомуникации** – използват се за предаване на данни от сензори, разположени на отдалечени райони, до обсерватории за анализиране на данни и да предават предупреждения от един географски регион в друг;
2. **Наблюдение на Земята** – използвани за наблюдения за следене на развитие на природни бедствия в широк обхват; проследяване на урагани и тайфуни, преди достигането им до суша, проследяване на активни движения на инфраструктурни обекти (пътища, мостове, виадукти, язовирни стени и др.) както и на свлачища.
3. **Сателитна навигация или сателитна навигационна система за автономно геопозициониране** – тази система носи названието GNSS или Глобална навигационна спътникова система и представлява комбинация от всички съществуващи до момента навигационни системи – **GPS, GLONASS, WAAS, EGNOS, MSAS**. Последните три представляват само допълнение към система, тъй като са сателити, разположени в

² **AI модел**- мощен, ефективен и достъпен начин за обработка на данни в който изкуственият интелект изследва огромни количества данни, за да открие тенденции и модели.

геостационарна орбита и осигуряват корекции със значително по-ниска точност.³



Фиг. 2. *Сателитно наблюдение*

В България Центърът за аерокосмическо наблюдение (ЦАН) като част от Министерството на вътрешните работи е предназначен за подпомагане борбата с природни бедствия и аварии в национален мащаб. Той е първата структура у нас разполагаща с наземни станции и пълен набор от хардуерно и софтуерно оборудване за прием и обработка на аерокосмически данни в реално време.

Заклучение

У нас се подценява значението на превантивната дейност, чрез която бедствията и аварията могат да бъдат не само очаквани, а и управляеми. Усилията са насочени преди всичко към изграждане на способности за реакция при възникнало бедствие, а не и за превенцията му.

От особено значение е създаване на оперативна съвместимост на системите с тези на съседни страни.

Адаптирането на ГИС, ГНСС и дистанционните методи, системите за автоматична регистрация, предаване и обработка на данни в институциите за съвременно моделиране на оптимални решения е от изключително значение.

Изключително важно е създаване на модели, включващи разработване на методики за:

- работа със системите за придобиване, регистрация и предаване на данни при настъпили аварии и бедствия
- оценка на критична инфраструктура,
- компетентни институции и организации за превенция,
- подготовка, реакция и възстановяване от бедствия и аварии.

³ A.Krastanov.(2023, September 14). Systems that save life <https://www.climateka.bg/sistemi-ranno-preduprejdienie-spasyavat-jivot/>

ЛИТЕРАТУРА

- [1] Теодор Матеев Масов, Влияние на природните рискове върху националната сигурност“, Автореферат
- [2] Mardirossian G., Natural disasters and ecological catastrophes, Prof. Marin Drinov, Academic Publishing House
- [3] Rangelov B. The angry Earth, the natural hazards, Prof. Marin Drinov, Academic Publishing House Sofia 2012

ПРОБЛЕМИ В РАЗВИТИЕТО НА АВТОМОБИЛНИЯ ТРАНСПОРТ В ЕВРОПЕЙСКИЯ СЪЮЗ

Силвия Х. Николова, Ива Б. Такова

PROBLEMS IN THE DEVELOPMENT OF ROAD TRANSPORT IN THE EUROPEAN UNION

Silvia H. Nikolova, Iva B. Takova

ABSTRACT: *The report examines the main challenges in the European Union related to pollution from land transport and the goals for reducing harmful emissions, as well as its development in the coming years.*

KEYWORDS: *transport, European Union, Trans-European Transport Network, multimodal transport*

DOI: <https://doi.org/10.46687/YT24SYS>

Въведение

Транспортът е стратегически важен сектор за икономиката на Европейския съюз (ЕС), който пряко въздейства върху ежедневието на всички граждани на съюза, а в сферата на транспортните услуги осигуряват приблизително 11 милиона работни места. BRIEF STATEMENT [cited 2018], Транспортът е един от най-важните дялове в Европейския съюз тъй като е взаимосвързан с транспортните мрежи, които са така важни за правилното функциониране на европейския пазар. Чрез него улесняваме движението на многобройни стоки и обслужването на потребителите.

Обемите на пътнически и товарен транспорт в ЕС са нараснали през последните десетилетия и се очаква тази тенденция да продължи, макар и с по-бавни темпове.

Транспортът е област със споделена компетентност на ЕС, което означава, че държавите-членки могат да упражняват собствената си компетентност, освен ако ЕС не е формулирал общ транспорт, политики и стратегии. Договорът за функционирането на ЕС (ДФЕС) установява, основа за Трансевропейската транспортна мрежа (TEN-T), интегрирана мултимодална мрежа, позволяваща на хората и стоките да се движат бързо и лесно в целия ЕС.

Отговорността за развитието, финансирането и изграждането на транспортна инфраструктура е главно на държавите-членки. Има разнообразие от финансиране от ЕС с 5 инструмента, на обща стойност около 193 милиарда евро за периода 2007÷2020 г., които осигуряват подкрепа на транспорта в ЕС.

Развитието на транспортната инфраструктура на ЕС изисква значителни финансови средства. Комисията на ЕС оценява, че общите нужди от инвестиции в тази област са около 130 милиарда евро годишно, като са необходими допълнителни значителни инвестиции за поддръжка. Само основната мрежа на

трансевропейската транспортна мрежа ще струва около 500 милиарда евро за периода от 2021 до 2030 г.

Въпреки това, след икономическата криза през 2008 г., инвестициите в транспортната инфраструктура са драстично намалени, със средни нива на инвестиции доста под необходимото, за модернизиране на пътната мрежа, но има нужда от значителни финансови средства за постигане на целите на трансевропейската транспортна мрежа по график.

Темпът на развитие на инфраструктурата се простира в рамките на ЕС, в зависимост от качеството и наличието на инфраструктура, но все още това развитие и работа по инфраструктурата изостава, най-вече в източните региони на ЕС. Official website of the European Union [https://european-union.europa.eu/priorities-and-actions/actions-topic/transport_en]. Докато основните мрежи на трансевропейската транспортна мрежа са вече завършени или близо до края на работата по тях, в някои държави-членки, в други има още много да работят по развитието на пътищата.

Освен това автоматизацията, дигитализацията и споделяната мобилност са бързо разрастващи се тенденции, които имат потенциала да направят транспортните системи по-ефективни. Но технологиите и моделите на мобилност също създават проблеми и предизвикателства пред ЕС, свързани със законодателната рамка, защитата на поверителността, безопасността, отговорността и сигурността на данните.

Транспортът представлява приблизително една четвърт от вредните емисии. Секторът се превръща в едно от основните предизвикателства пред екологията на ЕС. [2, 4, 5]

1. Автомобилен транспорт в ЕС

Транспортът е стратегически сектор на икономиката на ЕС, с транспортни услуги, които представляват около 5 % от брутната добавена стойност на ЕС или около 11 милиона души от всички работни места през 2016 г. Това пряко засяга ежедневието на всички европейски граждани.

Необходими са ефективни транспортни услуги и инфраструктура, за да се използват икономически силните страни на всички части на ЕС, за укрепване на вътрешния пазар и растеж и за развитие на икономическото, и социалното сближаване и най-вече развитие на автомобилния транспорт.

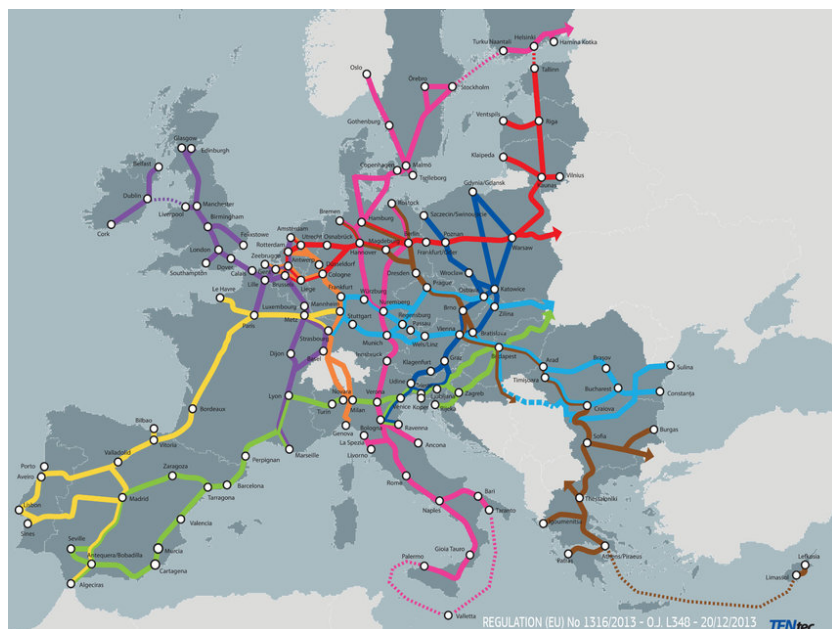
Транспортната политика на ЕС е заложена в Договора за функционирането на ЕС (ДФЕС), това е основна договор, който формира конституционната основа на ЕС. Това е една от първите области, в които ЕС заявява, че желае да създаде общ пазар и транспортни мрежи, като цяло създаване на свобода между държавите-членки за транспортиране на стоки свободно.

За да се развие и интегрира мултимодалната мрежа, позволяваща хора и стоки да се експортират бързо и лесно в рамките на ЕС. Договорът за функционирането на ЕС също полага основата за трансевропейската транспортна мрежа (TEN-T). Комисията публикува Трансевропейски транспортни мрежови насоки през 1996 г. като основа за разработване на политика за тях. Регламентът определя срокове за завършване за „основния“ (2030 г.) и „всеобхватния“ (2050 г.)

слой на мрежата и, преминава от подход, основан на индивидуални проекти, към този на мултимодална коридорна мрежа за целия ЕС. Проектите вече се планират в планове за коридори, обхващащи всички видове транспорт в 12-те европейски координатори.

Таблица 1. Обхват на трансевропейската транспортна мрежа

Трансевропейска транспортна мрежа(Теп-Т)	Ядро (най-важна част в km)	Обхват в km
ЖП-линии	50 762	138 072
Пътища	34 401	136 706
Вътрешни водни пътища	12 880	23 506



Фиг. 1. Коридори на основната трансевропейската транспортна мрежа

Atlantic (атлантическа), Baltic-Adriatic (Балтийско-адриатическа), Mediterranean (Средиземноморска), North Sea-Baltic (Северно море-балтийско), North Sea-Mediterranean (Северно море-средиземноморска), Orient-East Mediterranean (Ориентоизточно средиземноморска), Rhine-Alpine (Рейн-Алпи), Rhine-Danube(Рейн-Дунав), Scandinavian Mediterranean (Скандинавска-Средиземноморска).

Цялостната мрежа е проектирана да гарантира достъпност и свързаност за всички региони на ЕС. Основната мрежа се състои от стратегически най-важните връзки и възли в цялостната мрежа, организирана в девет коридора.

1.1. Основни заинтересовани структури в транспортния сектор на ЕС

Транспортът е област, в която ЕС и държавите членки споделят компетентност. Тоест, ЕС и държавите-членки могат да приемат законодателство и приемат правно обвързващи актове. Държавите членки могат да приемат закони и правила, освен ако ЕС формулира общи транспортни политики и стратегии. Основните заинтересовани структури в държавите членки са национални, регионални и местни органи, отговарящи за транспортната и инвестиционната политика, както и за товарните превози и пътнически превозвачи.

1.2. Финансиране

Милиони граждани и предприятия се възползват от транспортните мрежи и услуги.

Отговорността за развитието, финансирането и изграждането на транспортна инфраструктура е главно на държавите членки. Финансирането от ЕС, може да действа само като катализатор и покрива част от общите нужди. Развитието на транспортната инфраструктура на ЕС изисква значителни финансови средства. Комисията оценява общите нужди от инвестиции в тази област (и двете Трансевропейската транспортна мрежа и градска инфраструктура) да е около 130 милиарда евро годишно. Допълнително, важни и необходими са инвестиции за поддръжка. Смята се, че инвестицията, която трябва да развие основната мрежа възлиза на 500 милиарда евро за периода от 2021 г. до 2030 г.

След икономическата криза от 2008 г. обаче инвестициите в транспорта намаляват и инфраструктурата възпрепятства модернизацията на транспортната мрежа. [1, 4, 6]

2. Състояние и значение на транспорта в ЕС

Обемът на транспорта непрекъснато нараства и се очаква да продължи да нараства. Обемът на пътнически и товарен транспорт в ЕС непрекъснато нараства последните години, от 5 335 милиарда пътник-километра през 1995 г. до 6 802 милиарда в 2016 г. за пътнически транспорт. И от 2 846 милиарда тон-километра през 1995 г. до 3 661 милиарда през 2016 г. за товари. Обзорен доклад [<https://op.europa.eu/webpub/eca/landscape-review-transport/bg/>] 2018. ЕС смята, че ще продължат да растат, макар и с по-бавни темпове, той предвижда увеличение от 42 % за пътнически превоз и 60 % за вътрешния товарен между 2010 и 2050 г. А прогнозното увеличение за морския транспорт е с цели 71% за този период. Увеличаването на обемите на транспорта може да доведе до предизвикателства за капацитета в ЕС за някои видове транспорт. Задръстванията вече са основен екологичен и икономически фактор, притеснение, което сега струва на ЕС около 140 милиарда евро всяка година. Разходите за задръствания се очаква да се увеличат с повече от 40 % до 2050 г. спрямо 2010 г. Автомобилният транспорт представлява основната част от пътуванията на пътници и товари [2]. Пътуването

с кола е доминиращият вид с около 71 % от всички транспортни дейности в пътни километри, следвана от въздушен, автобусен и железопътен транспорт с около 10 %, 8 % и 7 % съответно. Пътищата също заемат 49% от дейността на товарния транспорт в ЕС, следван от морския с 32% и железопътния с около 11%. Въпреки целта на ЕС за прехвърляне на 30 % от автомобилния товар към други видове транспорт, като железопътен или воден транспорт до 2030 г. и повече от 50 % до 2050 г. и въпреки акцента на ЕС върху екологично съобразните видове транспорт, делът на използването на пътищата за вътрешния товарен транспорт всъщност нараства от 75,1 % през 2011 г. на 76,4 % през 2016 г. Автомобилният транспорт е предпочитаният начин за изпращане на стоки в рамките на ЕС, тъй като има предимства на гъвкавост, надеждност, цена, време и доставка от врата до врата.

В доклад за железопътния транспорт в ЕС, са сравнени предизвикателствата пред, които са изправени товарните превозвачи, използващи железопътен транспорт, и тези, пред които са изправени, когато използват шосе. Понастоящем пазарът не стимулира достатъчно потребителят да премине от автомобилен към друг вид транспорт, като става икономически по-малко конкурентоспособен. Транспортът генерира отрицателни външни ефекти като аварии, емисии на парникови газове, замърсяване на въздуха и шум, които водят до социални и икономически разходи. Тези отрицателни външни ефекти от транспорта се оценяват на около 4 % от brutния вътрешен продукт (БВП) на ЕС през 2011 г. В момента Комисията извършва проучване на външните разходи („Таксуване за устойчива транспортна инфраструктура и интернализация на външните ефекти от транспорта“), с оглед на оценката на степента, за които вече се прилагат принципите потребителят да заплаща, както и замърсителят да заплаща. Увеличаване на използването на мултимодален транспорт, който е един от основните в ЕС са целите на транспортната политика в продължение на много години, това може да изиграе роля в промяната на вида на транспорта и транспортните операции по трасето. Мултимодалността се отнася до използването на различни средства за транспорт по време на едно пътуване. Въпреки известен напредък през последните години, мултимодалният транспорт все още не е широко разпространен в Европа. [8, 9]

Интелигентните системи за управление на транспорта ще бъдат неразделна част от бъдещето на транспорта. Интелигентните системи за управление на транспорта се отнасят до набор от цифров трафик, системи за управление и информация, обхващащи няколко вида транспорт. Комисията признава, че успешното координирано разполагане на такива системи са жизненоважни за постигането на общоевропейски, съвместни и истински интегрирана транспортна система и ще представлява неразделна част от бъдещето на транспорта. Автоматизацията, дигитализацията и споделената мобилност са бързо разширяващи се тенденции, които имат потенциала да направят транспортните системи по-ефективни за подобряване на пътната безопасност, намаляване на въздействието върху околната среда и облекчаване на задръстванията. Разширяването на ЕС от 15 на 28 държави членки доведе до промени в логистиката. Темпът на развитие на инфраструктурата варира в рамките на ЕС, в зависимост от качеството и наличието на инфраструктура, но все още изостава, особено в източните региони. Освен все още съществуват тесни

места по транспортната мрежа на ЕС, които са сериозни препятствия пред транспортните потоци. Граничните пунктове са особено засегнати в това отношение.

Докато някои държави членки вече са завършили или са близо до завършване на техните участъци от основната TEN-T мрежа, други имат още много за работа. Постигнат е напредък, но като цяло може да се предположи, че в повечето случаи все още са необходими значителни подобрения и значителни инвестиции необходими за постигане на целите на TEN-T. Около 70 милиарда евро са планирани за съфинансиране от ЕС – 34 милиарда евро за TEN-T инфраструктура и 36 милиарда евро за транспортни инвестиционни проекти, които свързват или допълват проекти по TEN-T. Тази инвестиция ще обхване 977 km вътрешни водни пътища, изграждане на 3 414 km и повторно полагане на 9 742 km пътища, изграждането на 1 136 km и обновяването на 9 680 km жп линии, и 748 km нови или подобрени трамвайни и метро линии. Въпреки финансирането и значителния прогрес, все още има върху какво да се работи за постигането на целите на TEN-T. Отговорността за развитието, финансирането и изграждането на транспортна инфраструктура е главно на държавите членки. Годишният държавен дефицит не трябва да надвишава 3% и съотношението на държавния дълг към БВП не трябва да надвишава 60 %.

През октомври 2014 г. лидерите на ЕС имат цел за намаляване с най-малко 40% на парниковите газове . През 2015 г. ЕС и всичките 28 държави-членки подписаха Парижкото споразумение. Съгласно това споразумение те са задължени да представят дългосрочни планове до 2020 г., показващи усилията на всяка страна за намаляване на вредните емисии и да се адаптират към въздействията на изменението на климата.

През март 2018 г. европейският съвет прикани Комисията да представи предложение до първото тримесечие на 2019 г. за дългосрочна стратегия на ЕС за намаляване на емисиите на парникови газове в съответствие с Парижкото Споразумение, като се вземат предвид националните планове.

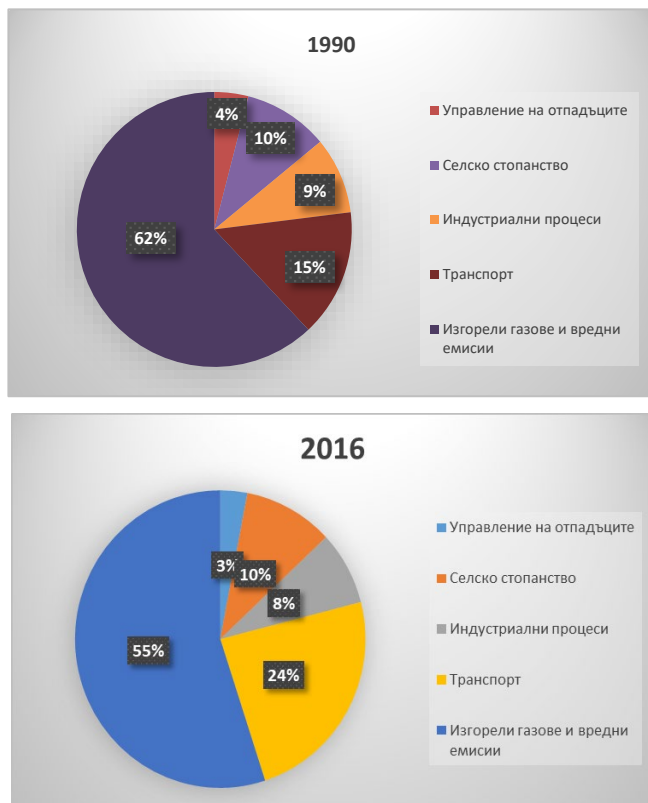
Диаграмата показва, че през 2016 г. транспортът представлява приблизително една четвърт от всички емисии на парникови газове в ЕС (в сравнение с 15 % през 1990 г.), което го прави вторият най-големият производител на емисии след енергийния сектор. ЕС има за цел за намаляване на вредните емисии на парникови газове от транспорта (с изключение на международните морски транспорт) с най-малко 60 % в сравнение с нивата от 1990 г. до 2050 г.

Според Европейската агенция по околна среда, емисиите от транспорта са се увеличили през и между 1990 и 2007 г. и след това са паднали до 2014 г. През 2015 и 2016 г. те отново са се покачили. Това означава, че секторът се превръща в едно от основните предизвикателства пред ЕС.

Съгласно текущите политики, като се вземе предвид очаквания ръст на товарния и пътническия транспорт, до 2050 г. емисиите на парниковите газове (ПГ) от транспорта се очаква да намалее с 15 % в сравнение с 2005 г. Въпреки това емисиите все още ще бъдат 10 % отколкото през 1990 г.

Постигането на целите за намаляване на емисиите ще изисква фундаментална промяна към използване на по-малко енергия и по-чиста енергия, както и по-ефективно използване на транспортна инфраструктура. ЕС приема

законодателни мерки за ускоряване на декарбонизацията на транспорта. Стратегията за енергийния съюз от 2015 г. определя прехода към енергийно ефективен, декарбонизиран транспортен сектор като зона от критична важност.



Фиг. 2. *Графика на разпределение на вредните емисии*

Много усилия за намаляване на емисиите както на ниво ЕС, така и на ниво държави членки са фокусирани върху пътищата, секторът, отговорен за най-големия дял (72%) от транспортните емисии през 2016 г. Тъй като емисиите от автомобилния транспорт са концентрирани в гъсто населени места и са сред основните причини за замърсяване на въздуха в градовете, декарбонизацията на автомобилния транспорт също е от решаващо значение за подобряване на качеството на въздуха и здравето на хората.

През 2017 и 2018 г. трите „пакета за мобилност“ на Комисията съдържа предложения, които включват преглед на чистите превозни средства на ЕС, евровинетка и директиви за комбиниран транспорт, план за действие за увеличаване на инвестициите в алтернативни горива инфраструктура, първите

стандарти за емисии на CO₂ за тежкотоварни превозни средства, нов CO₂ стандарти за емисии за леки и лекотоварни автомобили след 2020 г., подобро етикетирани за горивна ефективност на гуми и план за действие за акумулаторите.

3. Проблеми и предизвикателства пред развитието на автомобилен транспорт в ЕС

ЕС си е поставил редица много амбициозни цели за всички видове транспорт: по-специално завършването на основната Трансевропейската транспортна мрежа до 2030 г. Предвид значителните финансовите разходи и времето, необходимо за завършване на голяма транспортна инфраструктура, за постигане на тези цели е необходимо задълбочено планиране, подкрепено от стабилен и надежден анализ на прогнозните разходи, за които трябва да има достатъчно финансови средства. Поставяне на амбициозни политически цели и приоритети, без да се гарантира наличието на ресурси намалява вероятността да бъдат постигнати навреме и по този начин се отразява на достоверността на цялата политика. Въпреки, че е постигнат напредък е необходима допълнителна работа.

Дългосрочният план за изграждане на останалата инфраструктура, в частност за основната мрежа на Трансевропейската транспортна мрежа трябва да бъде подсилена с точни етапи, които са редовно наблюдавани, надеждни и оценки на разходите, съпоставени с наличните финансови средства ресурси и особен акцент върху трансграничните участъци. Това би увеличило вероятността за постигане на целите на транспортната политика навреме и в рамките бюджета.

Въпреки че регламентът за Трансевропейската транспортна мрежа установява коридорите, по които предстои изграждане на инфраструктура и европейските координатори се стремят да координират работата по планове, държавите членки осигуряват по-голямата част от необходимото финансиране и остават отговорни основно за планирането и доставката на транспортните мрежи. Те сами могат да решат дали и кога да изградят инфраструктура. По този начин съществува риск Трансевропейската транспортна мрежа да се развива като съвкупност от отделни мрежи, а не като интегрирана система, която най-добре ще отговори на нуждите на ЕС като цяло.

Трябва да се обърне внимание на съществуващата инфраструктура. Висококачествената инфраструктура е от съществено значение за ефективната и устойчива функционирането на вътрешния пазар на ЕС. Въпреки това, в редица случаи са докладвали за неадекватна поддръжка на съществуващи пътни, железопътни и железопътни речна инфраструктура в различни страни от ЕС, с отражение върху качеството, безопасност, ефективност и устойчивост.

Поддръжката на инфраструктурата е отговорност на националните и местните власти. Комисията повдига въпроса, че пътната и железопътната инфраструктура в целия ЕС се влошава поради твърде малко поддръжка. Той отбелязва, че поддръжката бюджетите често са недостатъчни и не са в крак с нарастващия мащаб на инфраструктурата и остаряването на важни връзки, което води до значително изоставане на поддръжката. Както Европейският парламент,

така и ЕС също подчертават важноста да се обърне дължимото внимание на поддръжката на транспортната инфраструктура.

Адекватната поддръжка на инфраструктурата е ключова предпоставка за развитието на устойчива транспортна мрежа на ЕС.

Заинтересованите страни трябва да обърнат внимание не само на инвестициите в нова инфраструктура, но също и за осигуряване на поддръжка и обновяване на съществуващата инфраструктура, която в момента е незадоволителна.

Друго предизвикателство, посочено в параграф 58, са транспортните емисии. Те са едни от основните предизвикателства пред общите цели на ЕС за декарбонизация.

Прехвърляне на стоки от пътища към други по-екологични видове транспорт може да спомогне за намаляване на емисиите от транспорта, които са концентрирани главно в пътя.

Заинтересованите страни трябва да се стремят към прехвърлянето на товари от пътища към друг транспорт начини чрез засилване на интермодалната конкуренция и чрез определяне на принципи изисквайки външните разходи за всички видове транспорт да бъдат взети предвид по подходящ начин, и застъпване на тяхното прилагане. [2, 3, 7]

Заклучение

Транспортът е стратегически сектор на икономиката на ЕС, с транспортни услуги, които представляват около 5 % от брутната добавена стойност на ЕС или около 11 милиона души които работят в тази сфера, през 2016 г. Това пряко засяга ежедневието на всички европейски граждани.

Необходими са ефективни транспортни услуги и инфраструктура, за да се използват икономическите силните страни на всички части на ЕС, за укрепване на вътрешния пазар и растеж и за развитие на икономическото, и социалното сближаване и най-вече развитие на автомобилния транспорт.

Обемът на автомобилният товарен транспорт в ЕС непрекъснато нараства през последните години. Увеличаването на обемите на транспорта може да доведе до предизвикателства за капацитета в ЕС за някои видове транспорт. Задръстванията вече са основен екологичен и икономически фактор, проблем който струва много на ЕС.

Разходите за задръствания се очаква да се увеличат все повече. Безпроблемната мобилност от врата до врата за стоки в ЕС зависи от добре развитата и добре функционираща транспортна инфраструктура.

Като най-гъвкавия вид транспорт, автомобилният (сухопътният) се адаптира най-лесно към нова инфраструктура, докато железопътният транспорт, например, изисква повече усилия за модернизиране и развитие мрежи и връзки. Както става ясно най-важната идея е подобряването на инфраструктурата в ЕС и нейното добро обслужване.

За да се избегнат бъдещи проблеми, трябва всяка държава членка да осигури поддръжка на инфраструктурата на нейните пътища, защото това осигурява безопасността на нейните жители.

ЛИТЕРАТУРА

- [1] Цанков Ц., Янкова-Йорданова Й. Намаляване на последствията от транзитно преминаващите товарни автомобили по пътищата на Република България. Седма международна научна конференция „Техника. Технологии. Образование. Сигурност“, Велико Търново, 2019, ISSN 2535-0315, с. 83-85.
- [2] Янкова-Йорданова Й., Цанков Ц. Необходимостта от намаляване на неблагоприятните последствия за околната среда при транзитен превоз на товари. Седма международна научна конференция „Техника. Технологии. Образование. Сигурност“, Велико Търново, 2019, ISSN 2535-0315, с. 110-112.
- [3] Yankova-Yordanova Y., Konstantinova E., Tsankov Ts. Forecasting logistics systems through models. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 68, April 2020, ISSN 2367-5721, pp. 105-109.
- [4] Yankova-Yordanova Y., Konstantinova E., Tsankov Ts. Thermal plasma gasification of municipal solid waste and the benefits for the city of Shumen. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 68, April 2020, ISSN 2367-5721, pp. 97-104.
- [5] Yankova-Yordanova Y., Tsankov Ts. New approaches in the management of reverse logistics. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 62, October 2019, ISSN 2367-5721, pp. 64-69.
- [6] Yankova-Yordanova Y., Tsankov Ts. Reverse logistics and innovations for managing non-reusable tire waste. Scientific Conference with international participation MATTEH 2024, Conference proceeding, vol. 2, Shumen, 2024, ISSN 1314-3921, pp. 332-337.
- [7] Official website of the European Union – Section: Safe, sustainable and connected transport., https://european-union.europa.eu/priorities-and-actions/actions-topic/transport_en (11:45 26.09.2024 г.) .
- [8] https://transport.ec.europa.eu/news-events/news/new-eu-transport-report-current-trends-and-issues-2024-06-27_en - Country overview
- [9] <https://op.europa.eu/webpub/eca/landscape-review-transport/bg/> – Обзорен доклад 2018 г.

ИЗПОЛЗВАНЕ НА МОБИЛНИ УСТРОЙСТВА ЗА РАЗПОЗНАВАНЕ И НАБЛЮДЕНИЕ В РЕАЛНО ВРЕМЕ

Даниел Р. Денев, Екатерина М. Христова

USING MOBILE DEVICES FOR REAL-TIME RECOGNITION AND SURVEILLANCE

Daniel R. Denev, Ekaterina M. Hristova

ABSTRACT: *Traditional machine learning methods rely on convolutional neural networks (CNNs). They are now a staple in a variety of object recognition applications. However, resource-constrained, low-power devices are not suited to run algorithms originally designed for high-performance computing systems. This need has led to the development of a new smartphone-based architecture that is optimized for mobile and wearable devices.*

KEYWORDS: *Snapdragon, Microsoft, Google, APPLE A9*

DOI: <https://doi.org/10.46687/YT24KAT>

Въведение

С развитието на изкуствения интелект се отключва неговият огромен потенциал за приложение в различни сфери. Това го превръща във водеща технология за стартиращи машинни системи, сред които са и смартфоните. Те са удобни за разработване на AI-базирани технологии поради ниската си цена и възможността за бързо внедряване. Вградените сверточни невронни мрежи (CNN) в смартфоните позволяват прилагането на нови технологии за разпознаване на обекти. Въпреки това съществуват предизвикателства, свързани със свободата на движение на потребителите, инфраструктурните ограничения и покритието на мрежите.

През последните години изчислителната мощ на смартфоните значително нарасна, което ги доближи до настолните компютри. Обработката на CNN на мобилни устройства е сериозно предизвикателство за инженерите, поради ограниченията в изчислителните възможности и високата консумация на енергия. За изпълнение на сложни математически задачи на смартфони са разработени различни платформи като TensorFlow Lite (TFL), TensorFlow Mobile (TFM), Qualcomm Snapdragon и OpenCV. Всяка от тези рамки има предимства и недостатъци, които трябва да бъдат анализирани, за да се избере най-подходящата архитектура за разпознаване на обекти. [2, 4]

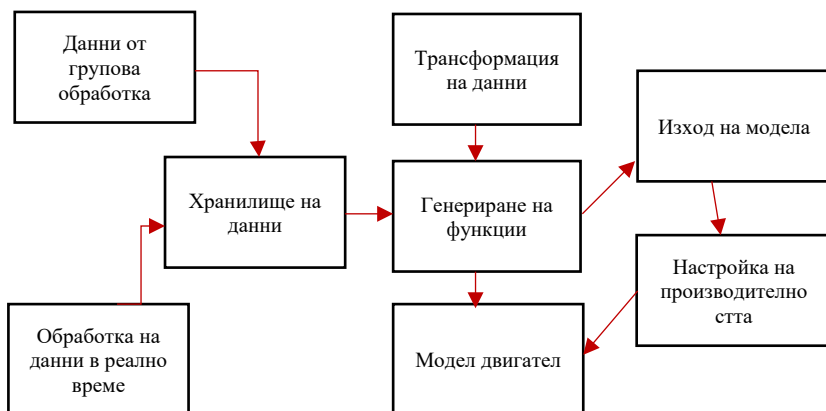
Системата за разпознаване на обекти включва три основни етапа: разпознаване на изображение, предварителна обработка и проследяване на изображението.

Мобилни платформи за дълбоко обучение

Този параграф представя анализ на няколко популярни рамки, внедрени в преносими платформи, като основният акцент е върху смартфоните. В изследването са разгледани четири библиотеки с отворен код: OpenCV, Software Development Kit, TensorFlow Lite и Qualcomm Neural Processing. Платформи като Keras не са включени, тъй като те добавят значителен абстракционен слой върху TensorFlow, което води до повишено натоварване и усложнен контрол върху следващото поколение архитектури. Фигура 2 в тази работа ще илюстрира цялостната архитектура на библиотека за машинно обучение, която ще бъде подложена на анализ и сравнение. За тестване на предложената архитектура е използван съвременният модел CNN YOLOv3. На базата на тази архитектура и модела YOLOv3 файловете и техният формат ще бъдат адаптирани в нов файл, който впоследствие ще бъде анализиран, интегриран и трансформиран във формат, съответстващ на избраната рамка.



Фиг. 1. Система в реално време базирана на смартфон



Фиг. 2. Циклична архитектура на библиотеките за машинно обучение

Изследването разглежда четири популярни платформи с отворен код:

- **OpenCV** – Универсална рамка за обработка на изображения и видео, която предлага основни функции за машинно обучение. Ограничението ѝ е свързано с ниската съвместимост с мобилни процесори.
- **TensorFlow Mobile (TFM)** – Версия на TensorFlow, оптимизирана за мобилни устройства и вградени системи, която обаче изисква значителни оптимизации за работа в ограничена среда.
- **TensorFlow Lite (TFL)** – Олекотена версия на TFM, предназначена за смартфони. Поддържа конвертиране на невронни мрежи, но има нужда от допълнителна обработка на конфигурационните файлове.
- **Qualcomm Snapdragon Neural Processing SDK (SNPE)** – Платформа на Qualcomm за оптимизиране на невронните мрежи върху процесори Snapdragon.

Предложен модел на система

Този раздел описва предложената и внедрена система за разпознаване на обекти на смартфони. Извършена е индиректна оценка, за да се определят най-ефективните кадри и резултати, които могат да подобрят работата на системата. Освен това, системата се адаптира въз основа на получените данни, които формират поредица от действия за разпознаване на обекти.

- **Критерии за емпирична оценка на платформата при проектирането на системата**

Тази част съдържа детайлен анализ на платформата за проектиране на системата, с цел избор на оптималната рамка и най-подходящите проектни решения. Процесът на разпознаване на обекти включва три ключови етапа: проследяване на изображения, предварителна обработка на данните и основния процес на разпознаване. За постигане на висока ефективност е необходимо да се подбере най-добрата платформа за всяка от тези фази. Оценката се основава на фактори, които влияят върху производителността на системата.

- **Предварителна обработка**

Този етап обхваща мащабиране на изображенията, тяхното нормализиране и преобразуване в различни цветови пространства. Мащабирането намалява входния размер от 1280×720 на 416×416 , което осигурява баланс между скоростта и точността, улеснявайки работата в реално време при критични приложения. Подобно на методологията, използвана от авторите на YOLO, и в настоящото изследване е избран входен размер от 416×416 , за да се осигури лесно сравнение на резултатите с други платформи.

- **Размер на модела**

Методите, използващи Snapdragon и TensorFlow Lite, разчитат на сериализация за преобразуване на конфигурационния файл и теглата на невронната мрежа във формат, подходящ за обработка. В настоящото изследване flat buffer моделът е избран за TensorFlow Lite. В същото време, двойното преобразуване от Proto Buff към DLC в SNPE води до

намаляване на размера на модела. В таблица 2 са представени размерите на YOLOv3 моделите в различни формати, съобразени със съответните платформи за машинно обучение.

- **Време за зареждане**

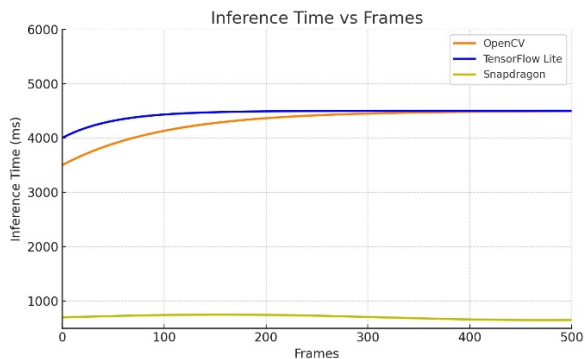
По-малкият размер на модела не винаги гарантира по-бързо зареждане в паметта. Най-бързо стартиращият модел е DLC версията на Qualcomm Snapdragon. Вторият по скорост е OpenCV, който зарежда два или повече файла отделно за 456 ms – стойност, която се счита за приемлива. Най-бавен е flat buffer интерпретаторът. В таблица 2 е представена зависимостта между платформата, формата и средното време за зареждане на всеки модел. Въпреки това, средното време за зареждане не се разглежда като основен или критичен фактор.

Таблица 1. Сравнение на емпирични фактори за всяка платформа за машинно обучение

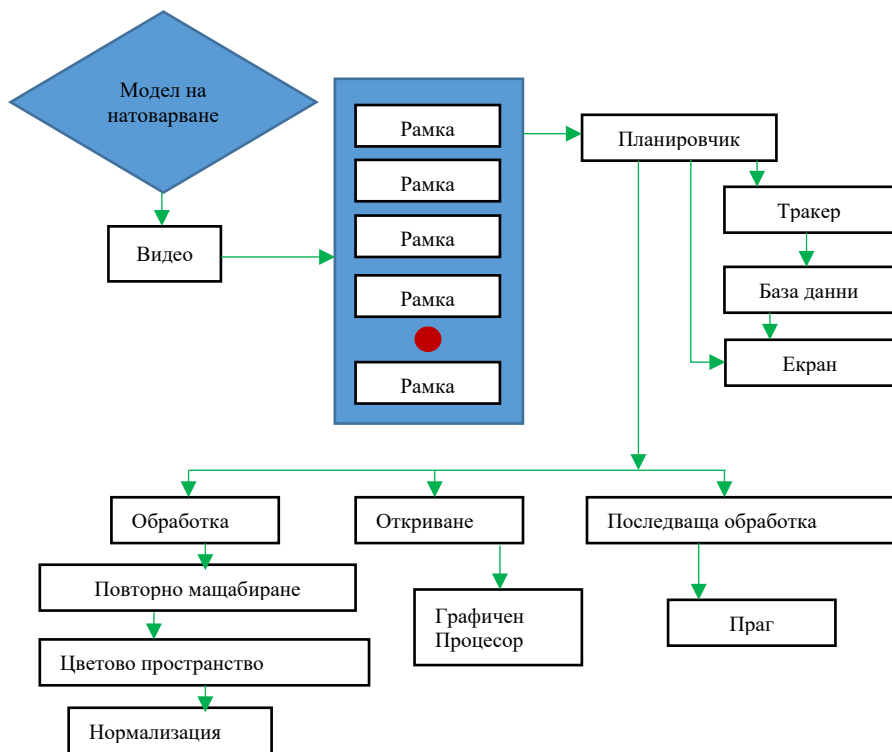
Factor	OpenCV	TF Lite	SNPE
Предварителна обработка	9.3 ms	56.3 ms	56.3 ms
Размер на модела	237.08 MB	236.66 MB	212.41 MB
Време за зареждане	456 ms	271 ms	2618 ms
Точност	Зависи от алгоритъма	Независи от платформа	Независи от платформа
Скорост (инф. време)	5203ms	4379 ms	595 ms
Средна RAM	633 MB	263 MB	707 MB
Максимална RAM	1.5 GB	1 GB	1.1 GB
Батерия	3280 mAh	3280 mAh	3280 mAh
Температура	46 °C	46 °C	46 °C
Тракер	Последователен	Едновременен	Не е предоставен

- **Скорост**

В различни среди скоростта е от решаващо значение и играе съществена роля. Времето за извеждане на резултатите (inference time) се измерва от момента, в който устройството започва обработката на даден кадър, до получаването на резултата за разпознаване на обекта или субекта. В таблица 2 са представени стойностите на времето за разпознаване на обекти на кадър в зависимост от използваната платформа. Най-бавно изпълнение е отчетено при OpenCV, като подобни резултати са наблюдавани и при TFL. Най-висока производителност е постигната при контекстните библиотеки на Snapdragon, които са обработвали близо два кадъра в секунда повече. Освен това, фиг. 3 илюстрира работеща система със средна стойност, изчислена върху 500 кадъра.



Фиг. 3. Натрупана средна стойност на времето за извод от изпълнението на YOLOv3 за всяка платформа за машинно обучение



Фиг. 4. Дизайн на предложената система

В тази подсекция се предлага нова система, интегрирана с най-добрите емпирично обосновани компонентни рамки. Предложената система следва класическите три основни процеса: анализ на изображение или обект, разпознаване на обект и проследяване на обект. Фигура 4 показва основния работен процес и информацията, когато видеото се кодира и декодира, като кадрите се показват за разпознаване на екрана. [1, 5]

Експериментални резултати

Тестовата среда в настоящото изследване е изпълнена на смартфон "Xiaomi Black-shark" с процесор Qualcomm "Snapdragon 845", който има 8 ядра с тактова честота от 2,8 GHz и 8 GB RAM памет за обработка на информацията. За да се намали нагряването на процесора, е интегрирана многослойна течностна охладителна система поради повишените температури. Поради популярността на процесора Snapdragon 845, той е избран за основа на проучването на предложената архитектура. Кратко казано, Таблица 2 има за цел да обобщи техническите спецификации на смартфона и версията на реализираната платформа. Алгоритъмът за машинно обучение и обработка, използван в настоящото изследване, е YOLOv3. Чрез нишката, свързана с процеса на разпознаване на обекти, резултатите от настоящото изследване ще бъдат с висока точност.

Таблица 2. Спецификации на смартфон и версия на платформи за машинно обучение

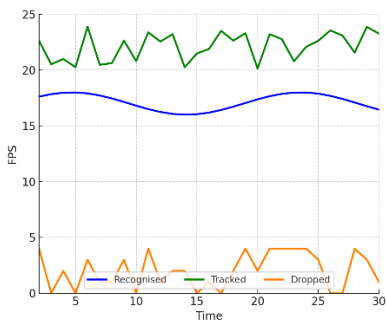
Смартфон спецификации	
Модел на централен процесор	Snapdragon 845
Архитектура на централен процесор	ARMv8-A
Ядра на централен процесор	4× 2.8 GHz Kryo 385, 4 × 1.8 GHz Kryo
Честота на централен процесор	2800 MHz
Графичен процесор	Qualcomm Adreno 630, 710 MHz
Честота на графичен процесор	710 MHz
L1 Кеш	32 kB + 32 kB
L2 Кеш	1536 kB
L3 Кеш	2048 kB
РАМ памет	8 GB, 1866 MHz
Капацитет	256 GB
Операционна система	Android Version 9
Версия на платформи за машинно обучение	Version 2
OpenCV	4.0.0
TensorFlow	2.0.0

Оценка на подхода и изградената система в реална среда

Както беше споменато по-рано, стандартният YOLOv3 беше реализиран и тестван в скрипта с цел максимално натоварване на системата. Тази част се фокусира върху реализирането на нашата идея за алгоритъм, проектиран за класически ограничени среди, като например Tiny-YOLOv3 и подобни. Текстът е разработен с помощта на популярния COCO набор от данни. Изчислително скъпите набори от данни и алгоритми постигат точност над 45%. В допълнение, бяха проведени тестове с различни оптимизации на архитектурата, като намаляване на размерите на мрежата и променливи стратегии за компресия на данни, които позволиха постигането на по-добри резултати при ограничени ресурси. Така, с използването на техники за ускорение на обработката, като например преработка на слоевете и използването на ефективни алгоритми за компресия, беше постигнато значително намаление на изискванията към процесора и паметта, което позволи реализацията на алгоритъма на мобилни устройства с ограничени ресурси.



Фиг. 5. Екранна снимка от смартфона по време на изпълнение на предложения подход



Фиг. 6. Кадри обработени от Tiny-YOLOv3

Резултатите от експериментите показаха, че предложената архитектура е много по-ефективна в сравнение с традиционните методи. Въпреки че съществуват някои ограничения в точността при по-сложни задачи за разпознаване на обекти, благодарение на оптимизациите, постигнахме значителни подобрения във времето за отговор и възможността за работа в реално време. Това прави подхода особено подходящ за мобилни приложения, където бързината на обработка и ефективността са от първостепенно значение.

Заклучение

Предложена е архитектура от ново поколение за разпознаване на обекти, използваща платформи с машинно инженерство, подходящи за смартфони, които обикновено имат ограничени ресурси. Предложената система използва най-доброто от своите видове в трите основни компонента от група популярни рамки за машинно обучение, въз основа на емпирична оценка. В резултат на това системата значително надмина алтернативните подходи. Основните резултати от експериментите показаха производителност в реално време, близка до 17.7 кадъра в секунда, с точност от 33.1 mAP и размер на файла от 33.8 MB. [3, 6]

ЛИТЕРАТУРА

- [1] Golcarenarenji G., Martinez-Alpiste I., Wang Q. Alcaraz-Calero, J.M.: Efficient real-time human detection using unmanned aerial vehicles optical imagery. *Int. J. Remote Sens.* 42(7), 2440–2462 (2021).
- [2] Idris M.I., Zabidi A., Yassin I.M., Ali M.S.A.M. Human posture recognition using android smartphone and artificial neural network. In: 2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC), pp. 120–124.
- [3] Ignatov A., Timofte R., Chou W., Wang K., Wu M., Hartley T., Van Gool L. AI benchmark: running deep neural networks on android smartphones. vol. 11133 LNCS, pp. 288–314. Springer (2019).
- [4] Kawano Y., Yanai K. FoodCam: a real-time food recognition system on a smartphone. *Multim. Tools Appl.* 74(14), 5263–5287 (2015).
- [5] Sotirov S, Kukenska V., Hristova M., Vardeva I., Staneva L., Barzov J., Dimitrov S., Stognova S. Modeling the nonlinear autoregressive network with exogenous inputs with Generalized net, Development in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and related topics. Applications. Vol. II, System Research Institute, Polish Academy of Science. Warsaw, 2010, 223-230.
- [6] Tsankov Ts., Staneva L., Vardeva I., Iliev D. Application of a Generalized Net Model in the Communication of Two Independent Traffic in Faculty of Technical Sciences at Konstantin Preslavski University of Shumen. Proceedings of the 15th International Scientific and Practical Conference “Environment. Technology. Resources.”, Vol. II, Rezekne, Latvia, 2024, ISSN 1691-5402, pp. 293-296.

EXPERIMENTAL DETERMINATION OF THE MAXIMUM SIGHT LENGTH TO THE MOST DISTANT BRIDGE PIERS FROM THE SHORES. CALCULATION OF THE ANGULAR SETTING OUT ACCURACY

Ani A. Stefanova

ABSTRACT: *The article describes a determination method of the maximum sight length from the points of a horizontal geodetic network to the most distant bridge piers which can be set out directly using linear-angular measurements. An experimental determination of the sight length in average atmospheric conditions was also conducted using a total station and two signals with different diameters. The angular setting out accuracy of the centers of bridge piers for the defined maximum sight length was determined, when measuring/setting out in one set of rounds.*

KEYWORDS: *sight length, horizontal network, bridge piers, linear-angular measurements, angular accuracy*

DOI: <https://doi.org/10.46687/YT24ANI>

1. Introduction

A key factor for providing reliable geodetic assurance in the bridge construction is creating a network with a sufficient number of points that are appropriately located considering using all modern geodetic methods for horizontal setting out.

Horizontal setting out works cover setting out and monitoring the bridge piers position and the supporting superstructure elements during all construction stages.

Direct setting out methods were mainly used in the past few years - straight-angular intersection, polar method and longitudinal method.

With the development of geodetic technologies and the appearance of modern total stations in the past 20 years, the opportunities to apply "reduction" setting out methods via resection intersection, combined intersection, the so-called "free station" and GNSS have significantly expanded.

It is widely known that the accuracy of setting out points, using linear-angular measurements depends on the accuracy of the measured elements, the accuracy of the initial points and the mutual location of the newly defined and initial points (network geometry). In the specific case, this means that in order to achieve the accuracy of coordinate definitions required in bridge construction, besides using precise tools, it is also necessary to create horizontal networks with geometry suitable for using the direct or indirect setting out methods listed above.

In another article, the author has developed a method for designing the locations of the initial points of geodetic networks [5] which ensures a suitable geometric shape allowing direct setting out of the centers of bridge piers with the required accuracy using linear-angular measurements.

A key moment in the design of the initial points of the horizontal network [5] is the determination of the maximum sight length ($S_{\max}$) to the most distant bridge piers

which can be set out directly using linear-angular measurements (straight-angle intersection, linear intersection and bipolar intersection). The author suggests a determination method of $S_{\max}$ described below.

2. Determination of the maximum sight length (SMAX)

The maximum sight length ($S_{\max}$) can be approximately determined based on the following factors:

- Error from sighting Δ_S , as a function of the mean error in human eye sighting α and the magnification v^X of the sighting telescope of the angular tool [1], [3]:

$$\Delta_S = \frac{\alpha^{cc}}{v^X} \quad (1)$$

Given a mean error value $\alpha = 120^{cc}$ and magnification $v^X = 30^X$, we receive $\Delta_S = 4^{cc}$ for the sighting error.

- Allowable value of the transverse error q^{allow} resulting from the sighting error Δ_S and sight length ($S_{\max}$) regardless of the atmospheric conditions:

$$q^{allow} = S_{\max} \frac{\Delta_B}{\rho^{cc}} \quad (2)$$

The allowable transverse error q^{allow} can be calculated by the allowable error in setting out the center of the bridge pier $M_p^{allow} = 9.5mm$. M_p^{allow} value is defined in the justification of the accuracy of the horizontal bridge geodetic networks and the setting out works in another article by the same author [4]. Assuming that $q^{allow} \leq \frac{1}{3} M_p^{allow}$, it follows that $q^{allow} \approx 3mm$.

From formula (2) where $\Delta_S = 4^{cc}$ and $q^{allow} = 3mm$, for the maximum sight length regardless of the atmospheric conditions, it comes: $S_{\max} = \frac{q^{allow} \cdot \rho^{cc}}{\Delta_S} \approx 480m$.

Based on the methodology described in [5] for the design of horizontal bridge geodetic networks (when bridging wide water obstacles) and the maximum $S_{\max}$ sight length to the most distant bridge piers calculated above, an exemplary scheme of a horizontal network was developed for setting out bridge piers where the project location and geometry of "Danube Bridge 2" (fig. 1) were used as reference data. From the initial points of the designed horizontal network (fig. 1), part of the bridge piers can be set out using direct setting out methods realized by linear-angular measurements.

For the remaining bridge piers (fig. 2) when the required accuracy cannot be reached by direct setting out methods (straight-angle intersection, linear intersection, bipolar intersection), it is recommended [5] to use reduction setting out methods. For this purpose, it is proposed designing a pair of additional initial points on each bank (M, N, M' and N' - fig. 2) located symmetrically to the midpoint while using a detection angle defined for the middle bridge pier [5].

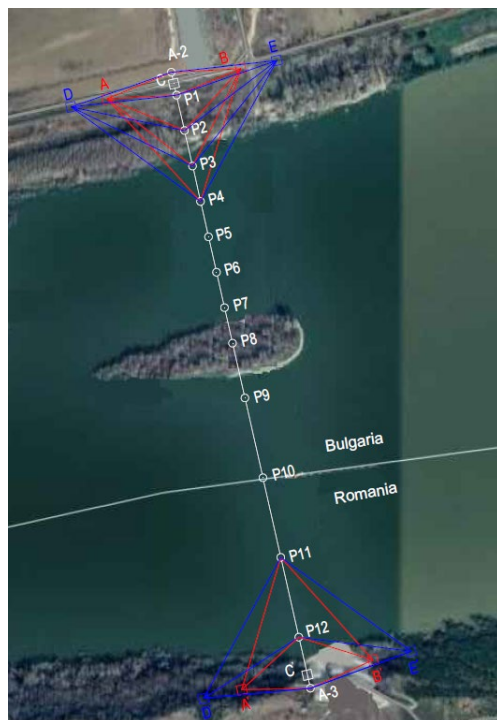


Fig. 1. Exemplary scheme of a horizontal network of “Danube bridge 2”

Network on figure 2 does not show all of the connections in order to avoid drawing clutter.

Experimental determination of the sight length

It is logical to assume that, in real conditions, the sight length where a transverse error $q \leq q_{\text{allow}}$ can be ensured, is less than 480 m. To determine it in a real situation, an experiment was conducted under the following conditions:

- Atmospheric state - average atmospheric conditions (slight cloudiness, light wind, air temperature 15° C, light haze when sighting targets at a distance more than 150m).
- Used tool – Hi Target HTS-420R total station (sighting telescope magnification 30x, angular accuracy 2", distance meter accuracy 2 mm + 2ppm).
- Target signals – mini prism pole with a diameter of 12 mm and standard prism pole with a diameter of 30 mm.

The experiment aims to:

- Determining the sight length when it is possible to reliably see in the tip, respectively in the axis of the specified two types of target signals.
- Determining the sight length when the operator is able to settle the transverse displacement of the signal with values of 5 mm and 10 mm, i.e. to set out a point with a transverse error of up to 5 and 10 mm, respectively.

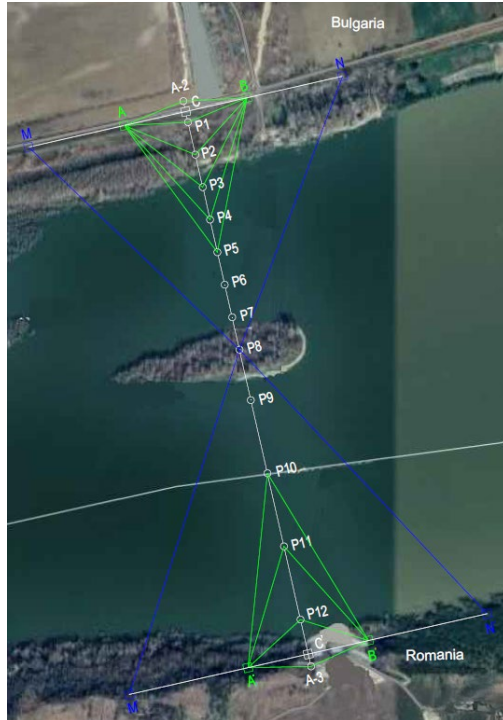


Fig. 2. Horizontal network scheme of “Danube bridge 2” with additional initial points

The experiment was conducted as follows: using the total station, a straight line with 10 intermediate points was set out at an interval of 50 m. A signal was successively placed on each of the set out points - a mini prism pole with a diameter of 12 mm and a standard prism pole with a diameter of 30 mm. The tip of the prism pole and its axis were targeted. The reliability of sighting in each of the cases is defined by "yes", "no" and "uncertain".

Transverse setting out error testing was performed by successively shifting the signals at 5 and 10 mm from the sight where again by “yes”, “no” and “uncertain” the

reliability of signal displacement is assessed by the operator. The results of the experiment are given in the following table.

Table 1

Sight length S [m]	12 mm prism pole				30 mm prism pole			
	Tip target- ing	Axis target- ing	Displacement		Tip targeting	Axis target- ing	Displacement	
			5mm	10mm			5mm	10mm
100	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
150	Yes	Yes	Uncert.	Yes	Yes	Yes	Yes/Uncert.	Yes
200	Uncert.	Yes	Uncert.	Yes	Yes	Yes	Yes/Uncert.	Yes
250	No	Yes	Uncert.	Yes	Yes (light haze)	Yes	No (light haze)	Yes/Uncert. (light haze)
300	No	Uncert.	No	Uncert. (light haze)	Yes (light haze)	Yes	No (light haze)	Yes/Uncert.
350	No	Uncert. (light haze)	No (light haze)	Uncert. (light haze)	Uncert. (light haze)	Yes	Uncert. (light haze)	Uncert. (light haze)
400	No	Uncert. (light haze) covers the strand	No	Uncert. (light haze)	Uncert. (light haze)	Yes	Uncert. (light haze)	Yes/Uncert.
450	No	Uncert. (light haze) covers the strand	No	No	Uncert. (light haze)	Yes	Uncert. (light haze)	Yes (light haze)
500	No	Uncert. (light haze)	No (light haze)	No	No	Yes/Uncert. (light haze)	No (light haze)	Uncert. (light haze)
550	No	Uncert. (light haze)	No	No	No	Yes/Uncert. (light haze)	No	Uncert. (light haze)

3. Determination of the angular setting out accuracy

Setting out accuracy m_{β}^{allow} is determined for the maximum sight length S_{max} (for setting out the most distant pier) when measuring/setting out in one set of rounds as a function of the remaining device errors, the sighting error in different atmospheric conditions, the effect of lateral refraction, the device and signal eccentricities.

Measuring/setting out angle accuracy is expressed by mean square error of the measured/set out direction m_R which can be represented as follows [2]:

$$m_R^2 = m_S^2 + m_{read}^2 + m_i^2 + m_h^2 + m_{ref}^2 + m_{ei}^2 + m_{es}^2 \quad (3)$$

The meaning of the arguments in formula (3) is as follows:

- m_S – impact of the sighting error

$$m_S = \frac{\omega}{V\sqrt{2nn_1N}} \quad (4)$$

where:

V – magnification of the sighting telescope;

ω – coefficient whose mean value depends on the sighting conditions (clear and calm atmosphere, distance and type of signal, quality of the sighting telescope, etc.);

n – number of set of rounds in which the directions are measured;

n_1 – targeting number and readings towards signal in one point;

N – number of series in which the directions are measured.

For the arguments in formula (4) the following values are assumed: $\omega=120^{\text{cc}}$ (average sighting conditions); $V=30^{\text{x}}$; $n=1$, $n_1=1$; $N=1$.

Thus, assumed values indicate that for the impact of the error sighting, we obtain: $m_s=2.8^{\text{cc}}$.

- m_{read} – impact of the sum error from coincidence and reading.

Provided that a precision digital device is used, it is assumed that $m_{\text{read}}=0.3^{\text{cc}}$ (0.1").

- m_i – impact of the device (instrument) errors whose total impact is in the range of 2^{cc} . When measuring the directions in N series with n set of rounds, this impact is:

$$m_i = \frac{2^{\text{cc}}}{\sqrt{nN}} \quad (5)$$

Given $n=1$ и $N=1$, for the impact of device errors, we obtain: $m_i=2^{\text{cc}}$.

- m_h – impact of the inclination of the horizontal axis of the device caused by inaccurate leveling.

$$m_h = \frac{v_{\text{mean}} t g \gamma}{\sqrt{2nN}} \quad (6)$$

where:

v_{mean} – mean square value of the inclination of the horizontal axis measured by the device alidade level. It is in the range of $12-15^{\text{cc}}$.

γ - sight vertical angle.

n and N have the same importance and value as in the formula (4).

With the assumed values: $v_{\text{mean}}=12^{\text{cc}}$; $\gamma=20^{\text{g}}$; $n=1$ и $N=1$, for the impact of the inclination of the device horizontal axis, we obtain: $m_h=2.8^{\text{cc}}$. When working over wide water spaces, the sights are almost horizontal and $m_h \approx 0^{\text{cc}}$.

- m_{ref} – impact of the lateral refraction on the measured direction.

$$m_{\text{ref}} = \frac{24.5 P_{\text{aver}} S \Delta t}{(273.2+t)^2 \sqrt{N}} \quad (7)$$

where:

P_{aver} – the average atmospheric pressure in the area of the object in hP.

S – sight length in meters.

t – measuring temperature in $^{\circ}\text{C}$.

Δt – mean square value of the horizontal temperature gradient in $^{\circ}\text{C}/\text{m}$.

With the following assumed values of the arguments participating in formula (7): $P_{\text{aver}}=950\text{hPa}$; $S_{\text{max}}=480\text{m}$; $t=20^\circ$; $\Delta t=0.09$; $N=1$, for impact of the lateral refraction on the measured direction, we obtain: $m_{\text{ref}}=11.7^{\text{cc}}$.

- m_{ei} and m_{es} – the impact of the device (instrument) and signal eccentricity.

Provided that observation monuments with a forced centering mechanism are used to conduct the measurement/setting out, the impact of device eccentricity can be neglected, i.e. $m_{\text{ei}}=0$.

The impact of the signal eccentricity can also be neglected in case a direct view to the set point is settled. Thus, we assume that $m_{\text{es}}=0$.

With the so calculated values of the arguments in formula (3) for a mean square error of the measured/set out direction m_R , we obtain that $m_R=12.5^{\text{cc}}$.

For the allowable accuracy of an angle setting out, it follows that:

$$m_{\beta}^{\text{allow}} = m_R \sqrt{2} = 18^{\text{cc}} \quad (8)$$

Table 2 represents the m_{β} [$^{\text{cc}}$] values determined experimentally with sight length S in the range 50 to 500 m in very good, good and average sighting conditions, air temperature 20°C , mean atmospheric pressure 950 hPa and mean value of the horizontal temperature gradient 0.09°C/m .

Table 2

S	m_s (v.g.c.)	m_s (g.c.)	m_s (a.c.)	m_{rad}	m_i	m_h	m_{ei}	m_{es}	m_{ref}	m_R (v.g.c.)	m_R (g.c.)	m_R (a.c.)	m_{β} (v.g.c.)	m_{β} (g.c.)	m_{β} (a.c.)
50	1.4	2.1	2.8	0.3	2	2.8	0	0	1.2	3.9	4.2	4.6	5.5	6	6.5
100	1.4	2.1	2.8	0.3	2	2.8	0	0	2.4	4.5	4.7	5.1	6.3	6.7	7.2
150	1.4	2.1	2.8	0.3	2	2.8	0	0	3.7	5.2	5.4	5.8	7.4	7.7	8.1
200	1.4	2.1	2.8	0.3	2	2.8	0	0	4.9	6.1	6.3	6.6	8.7	8.9	9.3
250	1.4	2.1	2.8	0.3	2	2.8	0	0	6.1	7.1	7.3	7.5	10.1	10.3	10.7
300	1.4	2.1	2.8	0.3	2	2.8	0	0	7.3	8.2	8.4	8.6	11.6	11.8	12.1
350	1.4	2.1	2.8	0.3	2	2.8	0	0	8.5	9.3	9.4	9.6	13.2	13.3	13.6
400	1.4	2.1	2.8	0.3	2	2.8	0	0	9.7	10.4	10.6	10.7	14.8	14.9	15.2
450	1.4	2.1	2.8	0.3	2	2.8	0	0	11	11.6	11.7	11.8	16.4	16.5	16.7
500	1.4	2.1	2.8	0.3	2	2.8	0	0	12	12.7	12.8	13	18	18.2	18.3

It can be seen from the table that when determining m_{β} , the lateral refraction m_{ref} has the predominant impact whose values in the same conditions will vary from 1.2^{cc} to 12.2^{cc} depending on the sight length. The calculations were done on the basis of an empirical mathematical model of the lateral refraction set by formula (7) [2].

In order to study the impact of air temperature changes on the value of m_{ref} , error caused by lateral refraction, similar calculations were made at temperatures of 0, 5, 10, 15, 25 and 30°C and the same values of the remaining parameters in formula (3)

as those in the calculations from table 2. The results of the calculations (including $t = 20\text{ }^{\circ}\text{C}$) are given in the following table.

Table 3

S	m_{ref} ($t=0^{\circ}\text{C}$)	m_{ref} ($t=5^{\circ}\text{C}$)	m_{ref} ($t=10^{\circ}\text{C}$)	m_{ref} ($t=15^{\circ}\text{C}$)	m_{ref} ($t=20^{\circ}\text{C}$)	m_{ref} ($t=25^{\circ}\text{C}$)	m_{ref} ($t=30^{\circ}\text{C}$)
0	1.4	1.4	1.3	1.3	1.2	1.2	1.1
100	2.8	2.7	2.6	2.5	2.4	2.4	2.3
150	4.2	4.1	3.9	3.8	3.7	3.5	3.4
200	5.6	5.4	5.2	5.0	4.9	4.7	4.6
250	7.0	6.8	6.5	6.3	6.1	5.9	5.7
300	8.4	8.1	7.8	7.6	7.3	7.1	6.8
350	9.8	9.5	9.1	8.8	8.5	8.2	8.0
400	11.2	10.8	10.4	10.1	9.7	9.4	9.1
450	12.6	12.2	11.8	11.3	11.0	10.6	10.3
500	14.0	13.5	13.1	12.6	12.2	11.8	11.4

Based on the results in this table, the following conclusion can be drawn: the impact of the lateral refraction at the same sight length S but in different air temperature decreases with the temperature increase. For example, at 50 m distance when temperature rises from 0 to $30\text{ }^{\circ}\text{C}$, the impact of the lateral refraction decreases with 0.3° . At 500 m distance, it decreases with 2.6° .

4. Conclusion

Based on the results of the conducted experiment to determine the sight length under average atmospheric conditions, the following conclusions can be elicited:

- When using 12 mm prism pole, points can be set out at a distance of about 150 m from the station – when targeting the tip of the signal and at a distance of about 250 m - when targeting its axis.
- When using 30 mm prism pole, points can be set out at a distance of about 300 m from the station - when targeting the tip of the signal and at a distance of about 450-500 m – when targeting its axis.
- When using 12 mm prism pole, setting out accuracy (transverse error) of 5 mm at a distance of about 100 m and a corresponding setting out accuracy of 10 mm at a distance of 250 m can be ensured.
- When using 30 mm prism pole, setting out accuracy of 5 mm at a distance of about 200 m and setting out accuracy of 10 mm at a distance of 450 m can be ensured.

It was established that the impact of the lateral refraction (the refraction angle) at a sight length 450 m for the temperature range from 0 to $30\text{ }^{\circ}\text{C}$, it changes from 10.3 to 12.6° which corresponds to a transverse error in the range of 7-9 mm. From the comparison of this value with the required setting out accuracy of the centers of the bridge piers $M_p^{\text{allow}} = 9.5\text{ mm}$ [4], it follows that the angular setting out accuracy is

determined practically only by the lateral refraction error where the sights length is limited to 450 – 500 m. This conclusion is also confirmed by the aforementioned results from the conducted experiment to determine the maximum sight length.

REFERENCES

- [1] Atanasov, S., L. Todorov. Geodesy 1. Sofia. Technique. 1990
- [2] Dimitrov, A. Engineering geodesy. Sofia. Technique. 1989
- [3] Peevski, V., M. Venedikov. Geodesy. Sofia Technique. 1996
- [4] Stefanova, A., Kostadinov, T., Accuracy of geodetic activities in bridge construction, Journal of Geodesy, Cartography, Land Management, issue 1-2` 2019
- [5] Stefanova, A., Design of 2D geodetic control network for overcoming wide water obstacles, Journal of Geodesy, Cartography, Land Management, issue 5-6` 2019

ГОДИШНИК
НА ШУМЕНСКИЯ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“
Т. XIV Е 2024

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

Университетско издателство
„Епископ Константин Преславски“

ISSN: 1314-8818 (print)

ISSN: 2815-4703 (online)

DOI: <https://doi.org/10.46687/AN24FTN>

