СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ“ – СВИЩОВ

СЪЮЗ НА УЧЕНИТЕ В БЪЛГАРИЯ – КЛОН СВИЩОВ

Международна научна конференция

ПРОБЛЕМИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД ИКОНОМИЧЕСКИТЕ НАУКА И ОБРАЗОВАНИЕ ПРЕЗ XXI ВЕК

Свищов, 22 ноември 2024 г.

Сборник с доклади

Конференцията е посветена на 80 години от създаването на Съюза на учените в България

Академично издателство „Ценов“
Свищов
2024

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ“ – СВИЩОВ

СЪЮЗ НА УЧЕНИТЕ В БЪЛГАРИЯ – КЛОН СВИЩОВ

Международна научна конференция

ПРОБЛЕМИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД ИКОНОМИЧЕСКИТЕ НАУКА И ОБРАЗОВАНИЕ ПРЕЗ XXI ВЕК

Свищов, 22 ноември 2024 г.

Сборник с доклади

Конференцията е посветена на 80 години от създаването на Съюза на учените в България

Академично издателство „Ценов“
Свищов
2024

ПРОГРАМЕН КОМИТЕТ

Доц. д-р Марин Маринов – Ректор на СА „Д. А. Ценов“ – Свищов
Проф. д.б.н. Диана Петкова – Председател на Съюза на учените в България
Проф. д-р Атанас Атанасов – Зам. ректор „Научноизследователска дейност и развитие на кадрите“ на СА „Д. А. Ценов“
Доц. д-р Красимира Славева – Председател СУБ – клон Свищов

ОРГАНИЗАЦИОНЕН КОМИТЕТ

Доц. д-р Христо Сирашки
Доц. д-р Пепа Стойкова
Доц. д-р Любка Илиева
Гл. ас. д-р Зоя Иванова

РЕДАКЦИОНЕН СЪВЕТ

Председател:
Проф. д-р Атанас Атанасов
Членове:
Проф. д-р Анета Денева
Доц. д-р Красимира Славева
Доц. д-р Христо Сирашки
Доц. д-р Пепа Стойкова
Доц. д-р Любка Илиева
Доц. д-р Пламен Петков
Доц. д-р Галина Чиприянова
Full Professor Carlos Coelho, PhD
Full Professor Jan Polowczyk, PhD
Full Professor Тадија Ђукић, PhD
Assoc. Prof. Tatiana Manasterska, PhD

НАУЧНИ СЕКРЕТАРИ

Доц. д-р Любка Илиева
Гл. ас. д-р Зоя Иванова
Гл. ас. д-р Асен Божиков

Публикуваните материали са рецензирани. Авторите носят отговорност за съдържанието на материалите, изразените мнения, използваните данни, цитираните източници и езиковото оформление на текстовете.

ISBN 978-954-23-2522-2 - Печатно
ISBN 978-954-23-2523-9 - Онлайн

СЪДЪРЖАНИЕ

ИКОНОМИКС, ФИНАНСИ, ЗАСТРАХОВАНЕ, СОЦИАЛНО ДЕЛО

ОБЕКТ, ЦЕЛ И РЕЗУЛТАТИ ОТ НАУЧНИТЕ ИЗСЛЕДВАНИЯ НА СЪВРЕМЕННОТО НАЦИОНАЛНО СТОПАНСТВО
Проф. д.ик.н Росица Чобанова 7

КОНЦЕПТУАЛНА РАМКА НА ЕНЕРГИЙНАТА СИГУРНОСТ
Проф. д-р Андрей Захариев, докт. Илиан Илчев 15

PARALLEL ANALYSIS OF THE INVESTMENT ATTRACTIVENESS OF THE LARGE LISTED COMPANIES FROM THE TOURISM SECTOR
Prof. Stefan Simeonov, PhD, PhD student Alexey Gudev 22

МОДЕЛЪТ ЗА АНАЛИЗ „ДЮ ПОНТ“ КАТО ВЪЗМОЖНОСТ ЗА ОЦЕНКА НА ДЕЙНОСТТА НА ЖИВОТОЗАСТРАХОВАТЕЛНИТЕ ДРУЖЕСТВА В БЪЛГАРИЯ
Доц. д-р Венцислав Василев 32

ЗА ЛИПСВАЩАТА ВРЪЗКА МЕЖДУ ДАНЪЧНАТА АВТОНОМНОСТ НА ОБЩИНИТЕ И МЕСТНАТА СТОПАНСКА АКТИВНОСТ
Доц. д-р Людмил Найденов 41

ВЛИЯНИЕ НА НАРАСТВАЩАТА ПРОДЪЛЖИТЕЛНОСТ НА ЖИВОТ НА ЕВРОПЕЙСКИТЕ ГРАЖДАНИ ВЪРХУ ДЪЛГОСРОЧНИТЕ ГРИЖИ
Доц. д-р Николай Нинов 49

ПАЗАРНИ ОСОБЕНОСТИ НА ПРОМЯНАТА НА УЧАСТИЕТО НА ОСИГУРЕНИТЕ ЛИЦА ВЪВ ФОНДОВЕТЕ ЗА ДОПЪЛНИТЕЛНО ДОБРОВОЛНО ПЕНСИОННО ОСИГУРЯВАНЕ В БЪЛГАРИЯ
Доц. д-р Пламен Йорданов, гл. ас. д-р Маргарита Николова 58

ПРОБЛЕМИ В РАЗВИТИЕТО НА ЗАСТРАХОВАНЕТО „КАСКО НА МПС“ НА БЪЛГАРСКИЯ ЗАСТРАХОВАТЕЛЕН ПАЗАР
Доц. д-р Румен Ерусалимов 66

РОЛЯТА НА ВИСШЕТО ИКОНОМИЧЕСКО ОБРАЗОВАНИЕ ЗА ФОРМИРАНЕТО И ПОВИШАВАНЕТО НА ЗАСТРАХОВАТЕЛНАТА ГРАМОТНОСТ
Гл. ас. д-р Анелия Панева 73

АНАЛИТИЧЕН ПРЕГЛЕД НА ТОП 10 НА HEALTHTECH СТАРТЪПИТЕ В БЪЛГАРИЯ (СПОРЕД КЛАСАЦИИТЕ НА TRACXN)
Гл. ас. д-р Валентина Нинова 80

РАЗВИТИЕ И СЪСТОЯНИЕ НА ОСИГУРЯВАНЕТО В УНИВЕРСАЛЕН ПЕНСИОНЕН ФОНД В БЪЛГАРИЯ
Гл. ас. д-р Йордан Йорданов 91

ПАЗАРЪТ НА ТРУДА И ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД УМЕНИЯТА НА РАБОТНАТА СИЛА
Гл. ас. д-р Таня Илиева 100

СТРЕС ТЕСТ НА ПУБЛИЧНИ ПРЕДПРИЯТИЯ ЧРЕЗ ALTMAN'S Z-SCORE МОДЕЛ
Ас. д-р Силвия Заркова 105

АНАЛИЗ НА СТРУКТУРАТА НА СОБСТВЕНИЯ КАПИТАЛ НА БАНКОВИЯ СЕКТОР В КОНТЕКСТА НА РЕГУЛАТОРНИТЕ ИЗИСКВАНИЯ БАЗЕЛ III
Д-р Беатрис Любенова 111

СОЦИАЛНО-ИКОНОМИЧЕСКИ ПАРАМЕТРИ НА ТРАНСПОРТНИЯ СЕКТОР - СРАВНИТЕЛЕН АНАЛИЗ
Докт. Васил Василев 123

ШОКОВИ ВЪЗДЕЙСТВИЯ НА ПАНДЕМИЯТА ВЪРХУ ОТРАСЛИ НА ИКОНОМИКАТА В БЪЛГАРИЯ И ЕС – ЕМПИРИЧНИ СВИДЕТЕЛСТВА
Докт. Горян Милев 131

ИКОНОМИЧЕСКИ ПОКАЗАТЕЛИ И ЕВОЛЮЦИЯ НА ДАНЪЧНАТА ОСНОВА В АГРАРНИЯ СЕКТОР В БЪЛГАРИЯ – ЕМПИРИЧНИ СВИДЕТЕЛСТВА
Докт. Ивайло Здравков 141

СЪСТОЯНИЕ НА ГЛОБАЛНИЯ ПАЗАР НА НЕДВИЖИМИ ИМОТИ - ТЕНДЕНЦИИ И ПРЕДИЗВИКАТЕЛСТВА
Докт. Пламен Илиев 150

ИКОНОМИЧЕСКИ ОСНОВАНИЯ ЗА ДЪРЖАВНАТА НАМЕСА: МОДЕЛИ ЗА ИНТЕРВЕНЦИЯ И COVID-19
Докт. Станислав Младенов 159

РЕГИОНАЛНА КОНВЕРГЕНЦИЯ И ДИВЕРГЕНЦИЯ НА ЦЕНОВИТЕ РАВНИЩА НА НЕДВИЖИМИТЕ ИМОТИ В БЪЛГАРИЯ: ДИНАМИКА И ТЕНДЕНЦИИ
Докт. Цондю Цондев 169

СЧЕТОВОДСТВО, КОНТРОЛ, АНАЛИЗ, СТАТИСТИКА

ВЪЗМОЖНОСТИ ЗА СЧЕТОВОДНО ОТЧИТАНЕ НА СПЕЦИФИЧНИТЕ ПРИХОДИ В ПЕНСИОННООСИГУРИТЕЛНИТЕ ДРУЖЕСТВА
Проф. д-р Атанас Атанасов 183

NEAR-EXACT DISTRIBUTIONS AND FINITE FORM REPRESENTATIONS: PROBLEMS THEY CAN SOLVE
Full Professor, Ph.D. & Hab., Carlos A. Coelho 190

НОРМАТИВНАТА РЕГЛАМЕНТАЦИЯ ОТНОСНО ОПОВЕСТЯВАНЕТО НА НЕФИНАНСОВА ИНФОРМАЦИЯ КАТО ПРЕДПОСТАВКА ЗА НАДЕЖДНА ОЦЕНКА НА УСТОЙЧИВОТО РАЗВИТИЕ НА БАНКИТЕ
Доц. д-р Венцислав Вечев 198

SUSTAINABILITY REPORTING CHALLENGES IN THE CONTEXT OF CHANGES IN ACCOUNTING LEGISLATION
Assoc. Prof. Galina Chipriyanova, PhD,
Assoc. Prof. Mihail Chipriyanov, PhD 204

ПРОБЛЕМИ И ПЕРСПЕКТИВИ ПРИ ОБУЧЕНИЕТО ПО СЧЕТОВОДСТВО В СЪВРЕМЕННИТЕ УСЛОВИЯ
Доц. д-р Галя Иванова-Кузманова 211

ПРОБЛЕМИ ПРИ ОТЧИТАНЕ НА ПРИХОДИТЕ И РАЗХОДИТЕ ПО ДОГОВОРИ ЗА СТРОИТЕЛСТВО
Доц. д-р Диана Крумова 218

COMPARATIVE ANALYSIS OF FINANCIAL INCLUSION IN ROMANIA, BULGARIA, AND THE REPUBLIC OF MOLDOVA THROUGH THE FINANCIAL INCLUSION INDEX OF TRADITIONAL AND FINTECH SERVICES
Assoc. Prof. Eduard Hîrbu, PhD, Hîrbu Ana 226

ИКОНОМИЧЕСКИ РАЗЛИЧИЯ И НЕРАВЕНСТВА МЕЖДУ СЕВЕРНА И ЮЖНА БЪЛГАРИЯ
Доц. д-р Красимира Славева..... 235

СТАТИСТИЧЕСКИ АНАЛИЗ НА СЕЗОННИТЕ КОЛЕБАНИЯ В ПОСЕЩЕНИЯТА НА БЪЛГАРСКИ ГРАЖДАНИ В ЧУЖБИНА
Доц. д-р Пламен Петков, докт. Пламена Колева 247

ДОКЛАДВАНЕ НА УСТОЙЧИВОСТТА НА БИЗНЕСА – СЪДЪРЖАНИЕ И АКТУАЛНИ НАСОКИ НА ЕВРОПЕЙСКИЯ СЪЮЗ
Доц. д-р Радосвета Кръстева-Христова 257

ПОЗИЦИОНИРАНЕ НА ПРИЕМА НА СТУДЕНТИ ПО АДМИНИСТРАЦИЯ И УПРАВЛЕНИЕ И ИКОНОМИКА ЗА УЧЕБНАТА 2023 – 2024 ГОДИНА В Р БЪЛГАРИЯ
доц. д-р Росица Колева 266

УСТОЙЧИВО РАЗВИТИЕ НА ОДИТОРСКИТЕ УСЛУГИ В УСЛОВИЯТА НА ДИГИТАЛНА ТРАНСФОРМАЦИЯ
Доц. д-р Силвия Костова 272

ОБЕЗЦЕНКА НА ВЗЕМАНИЯТА ОТ ПРОДАЖБИ В ПРЕДПРИЯТИЯТА
Доц. д-р Слави Генов 280

ВЛИЯНИЕ НА ДАНЪЧНИТЕ НЕСЪОТВЕТСТВИЯ ВЪРХУ ФИСКАЛНАТА СТАБИЛНОСТ
Гл. ас. д-р Жельо Желев 288

ПРЕДИЗВИКАТЕЛСТВА И ПОСЛЕДИЦИ ОТ ПРИЛАГАНЕТО НА МЕЖДУНАРОДНИЯ СТАНДАРТ ЗА ФИНАНСОВО ОТЧИТАНЕ 9 В МУЛТИНАЦИОНАЛНИТЕ КОРПОРАЦИИ: СРАВНИТЕЛЕН АНАЛИЗ
Гл. ас. д-р Кирил Димитров 296

ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД ОБРАЗОВАНИЕТО ПО СЧЕТОВОДСТВО В КОНТЕКСТА НА ДИГИТАЛИЗАЦИЯТА
Гл. ас. д-р Ралица Данчева 302

НЕЗАВИСИМОСТТА НА ОДИТНИТЕ КОМИТЕТИ И ВЪТРЕШНИЯ ОДИТ В ПУБЛИЧНИЯ СЕКТОР В БЪЛГАРИЯ
Докт. Румен Гъбов 308

АНАЛИЗ НА КЛЮЧОВИ АСПЕКТИ ОТ ОРГАНИЗАЦИОННАТА СТРУКТУРА НА НАЦИОНАЛНИЯ СТАТИСТИЧЕСКИ ИНСТИТУТ
Докт. Цветозария Гатева 316

МЕНИДЖМЪНТ, МАРКЕТИНГ, МЕЖДУНАРОДНИ ОТНОШЕНИЯ, ПЛАНИРАНЕ, ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

DIGITAL THREAT ANALYSIS
Professor Serghei Ohrimenco DSc, Associate Professor Lucia Gujuman, PhD, Valeriu Cernei 329

ДИГИТАЛИЗАЦИЯ НА ПОДБОРА НА ЧОВЕШКИ РЕСУРСИ В БЪЛГАРСКИТЕ ПРЕДПРИЯТИЯ
Проф. д-р Галина Захариева, докт. Маргарита Николова 336

GENERATION Z IN POLAND AND BULGARIA: CORE VALUES AND LIFE PRIORITIES
Prof. UEP. dr hab. Dariusz Nowak, Assist. Prof. Aleksandar Lichev, PhD, Szymon Nowak..... 344

СЪВРЕМЕННОТО УПРАВЛЕНИЕ НА МАРКЕТИНГОВИЯ ПЕРСОНАЛ – СПЕЦИФИКА И ПРОБЛЕМНИ АСПЕКТИ
Доц. д-р Ваня Григорова 352

ИНТЕЛИГЕНТНА СПЕЦИАЛИЗАЦИЯ И РАБОТА В МРЕЖИ
Доц. д-р Евелина Парашкевова, Доц. д-р Маргарита Шопова..... 360

POSITIVE ASPECTS AND CHALLENGES OF GENERATIVE ARTIFICIAL INTELLIGENCE APPLICATIONS
Assoc. Prof. Natalia Marinova, PhD..... 368

УСТОЙЧИВО ВНЕДРЯВАНЕ НА ОБУЧЕНИЕ ПО ПРОЕКТ №: 2022-1-BG01-KA220-VET-000089399 „ПРЕДОСТАВЯНЕ НА ВЪЗМОЖНОСТ НА МСП В СЕКТОРА ХОРЕКА ЗА ЕФЕКТИВНО УСВОЯВАНЕ НА ЗНАНИЯ И ИНСТРУМЕНТИ ЗА ИЗКУСТВЕН ИНТЕЛЕКТ (HORECA 5.0)“
Доц. д-р Христо Сирашки..... 375

ИНТЕРЕСИ И МОТИВАЦИОННИ НАГЛАСИ ПРЕЗ ПОГЛЕДА НА МЕНИДЖЪРА
Гл. ас. д-р Десислава Алексиева..... 382

РОЛЯТА НА СОЦИАЛНИТЕ МЕДИИ В СЪВРЕМЕННАТА ИКОНОМИКА: ПЕРСПЕКТИВИ И ПРЕДИЗВИКАТЕЛСТВА ЗА БИЗНЕСА
Гл. ас. д-р Кремена Маринова-Костова 388

ОСОБЕНОСТИ НА МЕЖДУЛИЧНОСТНИТЕ КОНФЛИКТИ В ОРГАНИЗАЦИИТЕ И ТЯХНОТО РАЗРЕШАВАНЕ
Гл. ас. д-р Милен Динков..... 396

СЪЩНОСТ И ОСНОВНИ ХАРАКТЕРИСТИКИ НА ОТВОРЕНИТЕ ИНОВАЦИИ
Гл. ас. д-р Юлиян Господинов..... 404

ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ В УПРАВЛЕНИЕТО НА ПЪТЯ НА КЛИЕНТА
Ас. д-р Стелиана Василева 412

PROTECTION OF DOCUMENT-CENTRIC SYSTEMS FROM DIGITAL THREATS
Assistant Ghenadie Belinschi 420

ИМПЛЕМЕНТИРАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ В ГЪВКАВА МЕТОДОЛОГИЯ (SCRUM) НА УПРАВЛЕНИЕ НА ПРОЕКТИ ЗА УСТОЙЧИВО РАЗВИТИЕ
Д-р Андрей Йорданов 426

ИКОНОМИКА НА ОТРАСЛИТЕ

УСТРОЙСТВО НА ЗЕМЕДЕЛСКИТЕ ТЕРИТОРИИ – ОСОБЕНОСТИ, РЕГЛАМЕНТИ, ПРОБЛЕМИ
Проф. д-р Гена Велковска 437

КОНЦЕПТУАЛЕН МОДЕЛ ЗА УСТОЙЧИВО РАЗВИТИЕ НА СЕЛСКИТЕ ТЕРИТОРИИ В БЪЛГАРИЯ
Проф. д-р Марина Николова..... 446

AN ANALYSIS OF THE CURRENT STATE AND DEVELOPMENT CHALLENGES OF RETAIL AND WHOLESALE BUSINESSES IN UKRAINE
Prof., Doctor of Economics, Olena Khadzhynova, Assoc. Prof., Candidate of Economic Sciences, Larysa Kapranova, Ph. D., Roman Sharanov 456

НЯКОИ ПРАВНИ И ПРАКТИЧЕСКИ АСПЕКТИ ПРИ МЕНИДЖМЪНТА НА СТОПАНСКИТЕ ДВОРОВЕ
Доц. д-р Валери Велковски..... 462

ПРОБЛЕМИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД ЕВРОПЕЙСКИЯ АГРАРЕН СЕКТОР
Доц. д-р Виолета Блажева **473**

ЕКО-ЕФЕКТИВНИ СТРАТЕГИИ
Доц. д-р Елена Йорданова **478**

INNOVATION AND INDUSTRY 5.0 – SOME CONNECTIONS AND OPPORTUNITIES
Assoc. Prof., Iskra Panteleeva, PhD **483**

OPPORTUNITIES FOR INDUSTRIAL BUSINESS DEVELOPMENT THROUGH TECHNOLOGICAL INNOVATIONS
Assoc. Prof. Iskra Panteleeva, PhD, PhD Student Kalin Borisov **491**

ПРОМОТИРАНЕ НА ТУРИСТИЧЕСКАТА ДЕСТИНАЦИЯ ЧРЕЗ ДИГИТАЛНИ ИНОВАЦИИ
Доц. д-р Любка Илиева **499**

ЛОГИСТИЧНОТО ПОВЕДЕНИЕ НА ФИРМАТА, ОРГАНИЗА-ЦИОННАТА ИДЕНТИФИКАЦИЯ И ПРЕДПРИЕМАЧЕСКАТА АКТИВНОСТ НА БЪЛГАРСКИТЕ ПИВОВАРНИ ПРЕДПРИЯТИЯ
Доц. д-р Сергей Найденов **506**

ПРОУЧВАНЕ НА РЕЛАЦИЯТА МЕЖДУ ДИГИТАЛНИТЕ УМЕНИЯ ЗА ПАЗАРУВАНЕ И РАЗПОЛАГАЕМИТЕ ДОХОДИ НА ПОТРЕБИТЕЛИТЕ В БЪЛГАРИЯ
Доц. д-р Симеонка Петрова **516**

ИКОНОМИЧЕСКАТА СОЦИОЛОГИЯ В КОНТЕКСТА НА ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД ИКОНОМИЧЕСКОТО ОБРАЗОВАНИЕ ПРЕЗ 21 ВЕК
Гл. ас. д-р Ваня Ганева **522**

TRANSFORMATION OF CONSUMER ONLINE PURCHASING BEHAVIOUR IN THE EUROPEAN UNION
Head Assist. Prof. Zoya Ivanova, PhD **529**

METHODS FOR GENERATING INNOVATIONS IN BULGARIAN ENTERPRISES
Head Assist. Prof. Ivaylo Kostov, Ph.D. **537**

РОЛЯ НА ПРЕДПРИЕМАЧЕСТВОТО ЗА УСТОЙЧИВО РАЗВИТИЕ НА СЕЛСКИЯ ТУРИЗЪМ
Гл. ас. д-р Павлин Павлов 545

БАРИЕРИ ПРЕД ОТВОРЕНИТЕ ИНОВАЦИИ В МАЛКИТЕ И СРЕДНИТЕ ПРЕДПРИЯТИЯ
Докт. Виктор Маринов 551

HUMAN RESOURCES IN THE AGE OF DIGITALIZATION
PhD Student Denitsa Gharkova-Zaharieva 557

PROTECTION OF DOCUMENT-CENTRIC SYSTEMS FROM DIGITAL THREATS

Assistant Ghenadie Belinschi[1]
ORCID ID : https :// orcid . org /0009-0009-3361-9890

Resume: *In today's digital world, social engineering attacks pose a significant threat to organizational information security. The advancement of artificial intelligence technologies, such as Deepfake, exacerbates this problem, making it essential to develop systems that can both authenticate users and detect external influences or manipulations. This paper proposes an approach to protecting document-centric systems from such attacks by integrating sensor analysis and artificial intelligence.*

The system's key element is the use of physiological sensors that record users' reactions when interacting with protected documents or performing critical operations. An individual biometric profile is created for each user based on initial data. The sensors measure biometric indicators such as heart rate, breathing, eye movement, and other parameters that reflect the user's emotional state.

The collected data is processed by a microcontroller and transmitted to a trusted server via a secure communication channel, where it is analyzed by machine learning algorithms. Artificial intelligence detects anomalies in user behavior that may indicate manipulation or emotional pressure from attackers. Combining biometric data with intelligent analysis creates a more reliable authentication and monitoring system.

Integrating sensor analysis and artificial intelligence into document-centric systems strengthens the protection of sensitive data.

Key words*: Multi-factor authentication, artificial intelligence, document-centric systems, data protection.*
JEL: C 88, O 33, M 15
DOI: https://doi.org/10.58861/tae.pcesetfc.2024.51

1. Introduction

Digital transformation has significantly increased the volume and value of data, making document-centric systems both critical for organizations and attractive targets for cyberattacks (Stallings, W., Brown, L., 2018). These systems are widely used across industries to store, process, and manage sensitive information. However, the growing importance of data has led to the evolution of traditional threats into more sophisticated attacks, including social engineering, which leverages psychological pressure and artificial intelligence technologies to manipulate users.

Traditional security methods, such as passwords and multi-factor authentication, provide a basic level of security but are not always effective against social engineering threats. These authentication methods verify "what the

[1] ghenadie.belinschi@gmail.com, Academy of Economic Studies of Moldova, Department Information Technology and Information Management, Chishinau, Moldova

user knows" (passwords, PINs) and "what they have" (tokens, smart cards), but rarely take into account behavioral and physiological factors, such as emotional state and stress response. Passwords and other secrets can be disclosed under duress or deception, and physical authentication devices can be stolen or compromised.

Additionally, the development of artificial intelligence technologies—particularly its ability to analyze and correlate large volumes of data—makes the process of deanonymization easier and more effective (Schneier, B., 2016) [3]. Modern attacks, such as Deepfake, use AI to create fake audio and video recordings, deceiving employees and gaining access to critical information (World Economic Forum, 2024). For example, an attacker could generate a video featuring a simulated company executive giving specific instructions, potentially misleading even experienced employees (Schneier, B., 2015). This significantly simplifies identity theft and heightens risks for organizations and individuals.

As traditional security methods become less effective, the need to develop systems that can recognize manipulation and respond to psychological pressure is more urgent than ever. This underscores the importance of more comprehensive security methods that incorporate user behavioral and physiological data to prevent attacks.

2. Document-Centric Systems and Vulnerabilities

A document-centric information system is a software platform designed to manage documents throughout their entire lifecycle. It provides centralized storage, protection, and access to documents and supports creation, editing, and collaboration functions. Additionally, it integrates with other business systems to automate processes.

Full lifecycle document management means that the system covers all stages of document handling, from creation and editing to approval and archiving. Such systems are widely used across various fields, but due to the high concentration of data and active user interaction, they become attractive targets for social engineering attacks.

Social engineering attacks involve various methods of psychologically influencing users to gain unauthorized access to information. In addition to the previously mentioned threat of data deanonymization, attackers actively use phishing and deception through social networks. For example, employees may receive messages from fake social media accounts posing as colleagues or partners. Such messages often contain links to fake pages that collect login credentials or encourage users to perform unauthorized actions, such as downloading malware. This is especially relevant in document-centric systems, where employees exchange documents and use credentials to access internal systems.

Another example of social engineering is vishing (voice phishing), where an attacker calls a company employee, impersonating a member of management,

and uses psychological pressure to coerce the employee into actions such as transferring confidential information or making a financial transaction. In these cases, traditional authentication methods are ineffective because the attacker exploits the human factor rather than attempting a technical hack. These attacks highlight the need for integrating behavioral and biometric analysis methods to protect against such threats.

The topic of data deanonymization in the context of large volumes and availability is widely discussed in the works of various researchers. Authors Viktor Mayer-Schönberger and Kenneth Cukier demonstrate how vast amounts of data can reveal hidden patterns and generate insights that were previously inaccessible (Schönberger et al., 2013)**.** They emphasize that such data, collected from various sources, can be used to deanonymize individuals even when identifying information has been removed. Similar ideas about deanonymization in the context of the "big data landscape" are discussed in the book *Privacy, Big Data, and the Public Good* (Lane, J., et al., 2014). These works highlight that, due to the volume and variety of available data, even anonymized datasets can be reconstructed at the individual level, posing serious risks to data privacy and security.

The development of artificial intelligence technologies, particularly its ability to analyze and correlate large amounts of data, makes the process of deanonymization easier and more effective. Modern attacks, such as Deepfake, use AI to create fake audio and video recordings, deceiving employees and gaining access to critical information. This greatly facilitates identity theft and increases risks for organizations and individuals.

The World Economic Forum’s recent report on the "Top 10 Emerging Technologies for 2024" underscores the importance of technologies that enhance data protection and privacy. These include advancements in AI analytics, synthetic data, and integrated sensor networks, which can be used to safeguard document-centric systems against emerging threats.

Thus, document-centric systems face serious risks in today’s digital landscape. Social engineering attacks, including phishing, social media deception, and vishing, effectively exploit the human factor, bypassing traditional technical protections. Additionally, the capabilities of artificial intelligence and big data simplify deanonymization and identity theft, increasing the vulnerabilities of these systems. The high concentration of confidential information and active user interaction make document-centric systems particularly attractive to attackers.

In this context, the need for new, more comprehensive protection methods that consider both technical and behavioral aspects of security is becoming critical to ensuring data safety and maintaining trust in organizational information systems.

3. Proposed Approach: Sensory Analysis and Artificial Intelligence

To enhance the security of document-centric systems, this approach proposes integrating physiological sensors with artificial intelligence to monitor the user's state when interacting with the system. Physiological sensors record biometric parameters such as heart rate, breathing, eye movement, voice characteristics, and other indicators that reflect emotional state. The collected data is transmitted to a secure server, where machine learning algorithms analyze it and detect anomalies that may indicate possible manipulation attempts or external pressure.

Each user is assigned an individual biometric profile that reflects their normal biometric ranges. Artificial intelligence analyzes current data and compares it with the user's profile. Detecting deviations enables a timely response to suspicious activity, reducing the risk of successful social engineering attacks.

The integration of sensor analysis and artificial intelligence offers several advantages. Considering users' physiological and voice data enables the identification of social engineering attacks that are challenging to detect with traditional methods. The system adapts to each user, reducing the likelihood of false positives. Using a dedicated communication channel for data transmission lowers the risk of data compromise and interception. The use of sensor technologies to enhance data protection is actively discussed in the article *"Access Control in a Document-Centric System"* (Ohrimenco, S., et al., 2024).

4. Technical Description of the System

The proposed system employs physiological sensors to monitor the user's state when interacting with a document-centric system. The sensors record biometric data such as:

Heart rate: Measured using sensors such as the MAX30100, which can detect heart rhythm and stress levels.

Respiration rate: Measured with respiratory sensors that track chest movements.

Eye movement: Tracked using cameras like the ESP32-CAM, which can detect gaze direction and blink rate.

Galvanic skin response: Measures changes in skin conductivity that indicate emotional arousal or stress.

Voice characteristics: Recorded with a microphone such as the MAX9814, which analyzes timbre, intonation, and frequency to detect signs of stress or anxiety.

Data from the sensors is transmitted to a microcontroller, such as the ESP32, which pre-processes it and sends it to a trusted server via a secure communication channel. Using a dedicated SIM card increases the security of data transmission. The server uses artificial intelligence algorithms trained with neural networks and machine learning methods. Pre-trained models like LLAMA and GPT are further fine-tuned with specific user biometric data, enabling them to

detect behavioral anomalies. The algorithms analyze data in real-time, identifying anomalies that suggest deviations from the user's typical state, allowing the system to detect signs of manipulation or emotional pressure.

A combination of real and synthetic data can be used to train AI models. Using synthetic data expands the training set while preserving privacy and minimizing the risk of personal information leaks. This approach also enhances the system's ability to detect anomalies.

5. Application and Advantages

The primary distinction of the proposed approach is the use of both physiological and behavioral data to enhance security. Unlike traditional methods that rely on static data, such as passwords and tokens, our system dynamically adapts to each user by creating an individual biometric profile. This enables the system to distinguish between normal user reactions and those that may occur under pressure from intruders.

Personalization: The system accounts for each user's individual physiological and vocal characteristics, improving the accuracy of anomaly detection.

Counteracting Social Engineering: Monitoring emotional state and voice changes helps identify attempts at external pressure or manipulation.

Enhanced Data Security: Prompt detection of suspicious activity reduces the risk of confidential information leaks.

Regulatory Compliance: Using synthetic data to train AI supports compliance with privacy and personal data protection standards (ISO/IEC 27001:2013) [2].

6. Conclusion

The growth of digital technologies and the rise in cyber threats necessitate new approaches to information security. Integrating sensor analysis and artificial intelligence into document-centric systems offers an effective means of protection against social engineering attacks.

The proposed system combines advanced sensor analysis and artificial intelligence technologies to create a more reliable and adaptive security solution. Integrating physiological sensors, including a microphone for voice analysis, with machine learning algorithms allows the system not only to authenticate the user but also to monitor their physiological state. This provides an additional layer of protection against sophisticated social engineering attacks that are challenging to detect with traditional methods.

The integration of sensor analysis and artificial intelligence represents a promising advancement in information security. The proposed approach can significantly enhance the resilience of document-centric systems to modern digital threats, combining technical and behavioral protection methods to ensure comprehensive data security.

References

Stallings, W., Brown, L. (2018). *Computer Security: Principles and Practice* . Pearson .

ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements* .

Schneier, B. (2016). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* . W. W. Norton & Company.

Sonowal, G. (2023). *Social Engineering Attacks: Rethinking Responsibility and Decisions*. Nova Science Publishers , Inc.

Tully , A. K., Abbott, J., Bochner , A. M., Das, S., Nippert -Eng, K. (2023). *Tips, tricks, and training: supporting phishing awareness among office workers*. CHI 2023 Conference Proceedings.

Winkler, T. H. (2018). *The Dark Side of Globalization and How to Cope with It* . LIT VERLAG GmbH & Co. KG.

Ohrimenco, S., Gujuman, L. Belinschi, G. V., (2024). *Cyber Attacks on Document-Centric Systems*. International Science Forum: Global and National Business Transformations – Proactive Management, Financial-Accounting and Planning Solutions. Tsenov Academic Publishing House.

Mayer - Schönberger , V., & Cukier , K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt .

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (Eds.). (2014). Privacy, Big Data, and the Public Good: Frameworks for Engagement. Cambridge University Press.

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing Group.

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley .

World Economic Forum. (2024). Top 10 Emerging Technologies of 2024. Geneva : World Economic Forum.