

Факултет "Приложна информатика и статистика"
Катедра „Информационни технологии и комуникации“

РЕЗЮМЕТА НА НАУЧНИТЕ ПУБЛИКАЦИИ

на ас. д-р Ивона Пламенова Велкова

Кандидат в конкурс за заемане на академична длъжност „главен асистент“ по професионално направление 3.8. Икономика, научна специалност „Информационни и комуникационни технологии в икономиката (технологии за информационна сигурност в дигиталната икономика и висшето образование)“,
обнародван в ДВ, бр. 65 от 08.08.2025 г.

София, 2025

**"APPLIED INFORMATICS AND STATISTICS" FACULTY
"INFORMATION TECHNOLOGIES AND COMMUNICATIONS"
DEPARTMENT**

**ABSTRACTS OF PUBLICATIONS
of Assist. Ivona Plamenova Velkova, PhD**

A candidate for the academic position "Chief Assistant Professor"
in professional field 3.8. Economics, scientific specialty "Information and communication
technologies in the economy (technologies for information security in the digital economy and
higher education)"
published in State Gazette, Issue 65/08.08.2025 г.

Sofia, 2025

Доклади, публикувани в сборници от научни конференции, индексирани в международни бази данни с научна информация

1. Велкова, И. (2024). Намаляване на рекламните измами в дигиталния маркетинг с помощта на изкуствен интелект. В Иновативни информационни технологии за дигитализация на икономиката: Научна конференция, 2023, УНСС: Сборник с доклади (с. 79-88). София: Издателски комплекс – УНСС.

<https://iited.unwe.bg/iited2023/>

<https://ideas.repec.org/a/nwe/iitfed/y2023i1p79-88.html>

<https://econpapers.repec.org/article/nweiitfed/>

Резюме: Непрекъснатата дигитализация на глобалната икономика поставя началото на свързаност и възможности за бизнеса да се ангажира с потребителите. Въпреки това, тя също така довежда и до различни заплахи в онлайн пространството. Една от тези заплахи е рекламната измама, която застрашава целостта и ефективността на онлайн рекламните кампании в все подигитализираната икономика. Изкуственият интелект (ИИ), оборудван с възможности за анализ на данни в реално време и усъвършенствани алгоритми за идентифициране на модели, предлага възможности за ефективно реагиране срещу този вид атаки. Чрез анализа на множество данни, ИИ може да разграничи истинските потребителски взаимодействия в дигиталното пространство от измамните, да маркира аномалии и да се адаптира бързо към развиващите се измамни тактики. Този документ се представя като подход за решение за смекчаване на рекламните измами, със специфичен акцент върху тяхното въздействие и ролята на ИИ в справянето с това предизвикателство и насърчаването на по-сигурна и устойчива дигитална икономика.

Ключови думи: изкуствен интелект, заплахи, дигитален маркетинг

Abstract: The continuous digitization of the global economy brings about connectivity and opportunities for businesses to engage with consumers. However, it also introduces various threats in the online space. One of these threats is ad fraud, which jeopardizes the integrity and effectiveness of online advertising campaigns in an increasingly digitized economy. Artificial intelligence (AI), equipped with real-time data analysis capabilities and advanced algorithms for pattern recognition, offers effective ways to counteract such attacks. Through the analysis of extensive datasets, AI can distinguish genuine user interactions in the digital realm from fraudulent ones, identify anomalies, and adapt rapidly to evolving fraudulent tactics. This document presents an approach to mitigating ad fraud, with a specific focus on its impact and the role of AI in addressing this challenge, promoting the creation of a more secure and resilient digital economy.

Keywords: artificial intelligence, threats, digital marketing

2. Velkova, I. (2024). Next-Gen Accounting and the Disruptive Power of AI in Financial Forecasting and Efficiency. В Иновативни информационни технологии за дигитализация на икономиката: Сборник доклади от научна конференция, 25 октомври 2024, УНСС (с. 205-213). Университет за национално и световно стопанство.

<https://ideas.repec.org/a/nwe/iitfed/y2024i1p205-213.html>

https://econpapers.repec.org/article/nweiiitfed/y_3a2024_3ai_3a1_3ap_3a205-213.htm

Резюме: Този документ изследва трансформиращото въздействие на изкуствения интелект (AI) в счетоводството, като се фокусира върху финансовото прогнозиране и оперативната ефективност. Основната цел е да се оцени сравнителното представяне на AI моделите спрямо традиционните счетоводни методи. Чрез структурирана методология, проучването оценява ключови показатели, включително точност, скорост и ефективност, в управлявани от AI и конвенционални техники. Констатациите показват, че AI значително намалява времето и усилията, необходими за счетоводните задачи, като по този начин оптимизира процесите на вземане на решения, позволява по-прецизно разпределение на ресурсите и улеснява прогнозирането в реално време. Подобен напредък е от решаващо значение за организациите, които се стремят да поддържат конкурентно предимство на все по-динамични пазари. Проучването заключава, че интегрирането на AI в счетоводните практики е не само полезно, но и от съществено значение за осигуряване на бъдещ растеж и оперативна устойчивост.

Ключови думи: изкуствен интелект, счетоводство, финанси, прогнозиране, TensorFlow

Abstract: This paper explores the transformative impact of artificial intelligence (AI) in accounting, focusing on financial forecasting and operational efficiency. The primary objective is to assess the comparative performance of AI models relative to traditional accounting methods. Through a structured methodology, the study evaluates key metrics, including accuracy, speed, and efficiency, across AI-driven and conventional techniques. The findings demonstrate that AI significantly reduces the time and effort required in accounting tasks, thereby optimizing decision-making processes, enabling more precise resource allocation, and facilitating real-time forecasting. Such advancements are critical for organizations striving to maintain a competitive edge in increasingly dynamic markets. The study concludes that integrating AI into accounting practices is not merely advantageous but essential for ensuring future growth and operational resilience.

Keywords: AI, accounting, finance, forecast, TensorFlow

Статии и студии, индексирани в други международни бази данни с научна информация, публикувани в научни списания

1. Velkova, I. (2024). Cybersecurity Challenges and Solutions in University Enrollment Systems. Knowledge- International Journal , 66(3), 305-311.

<https://ojs.ikm.mk/index.php/kij/article/view/7030/6788>

<https://www.cceol.com/search/article-detail?id=1297590>

Резюме: С оглед на значителния технологичен напредък във всички аспекти на живота ни и нарастващата зависимост от дигитални платформи, университетите се изправят пред нови предизвикателства. Едно от основните предизвикателства е свързано с процеса на записване на студенти. След пандемията от COVID-19 много университетски дейности преминаха в онлайн среда – заплащане на семестриални такси, подаване на документи, провеждане на лекции и др. За мнозина посещенията на университет на място за записване в избрана програма беше затруднено поради разпространената здравна криза. В резултат на това някои университети по света започнаха да въвеждат онлайн системи за записване на новоприети студенти, които предлагат удобство и по-ниски разходи. Въпреки това, нарастването на онлайн системите за записване и обработката на чувствителна информация – като лични данни и финансови детайли – в съчетание с все по-популярните онлайн плащания, увеличават уязвимостта на тези системи към кибератаки. В този контекст разработването на надеждни и адаптивни стратегии за киберсигурност става от съществено значение за защита от потенциални пробиви. През 2023 г. се наблюдава значително увеличение на кибератаките, насочени към висши учебни заведения и техните процеси, включително и тези, засягащи онлайн записването. Това подчертава необходимостта от цялостни и адекватни мерки за киберсигурност, които ефективно да защитават чувствителните студентски данни и да гарантират непрекъснатата цялостност на институционалната дейност. Освен това, динамичният характер на киберзаплахите изисква постоянни актуализации и подобрения на защитните протоколи. Настоящото изследване се фокусира върху казуси, свързани с пробиви и уязвимости, и разглежда процесите на онлайн записване в няколко европейски университета с акцент върху сигурността на данните. Резултатите показват, че основните уязвимости са свързани със слаби практики по удостоверяване, липса на достатъчно многофакторна автентикация и интеграция със стари системи. Провеждането на редовни одити по сигурността и тестове за проникване е от ключово значение за идентифициране и минимизиране на слабостите в системите за студентско записване. Тестовите за проникване, при които етични хакери се опитват да пробият защитата на системата, могат да разкрият слабости, които не се откриват при стандартни одити. Целта на това изследване е да предложи модел за повишаване нивото на сигурност в системите за записване на новоприети студенти. Необходимо е университетите да внедрят цялостни подходи за управление на информационната сигурност, които да гарантират не само защита на данните, но и ефективно управление на рисковете. Чрез идентифициране на съществуващите предизвикателства и препоръка на добри практики, този документ цели да подобри защитата на чувствителната информация и да повиши общото ниво на сигурност в университетските информационни системи. Предложеният метод е тестван в реална среда и е оценен като ефективен за намаляване на риска от изтичане на данни и

повишаване на доверието и сигурността в университетската среда.

Ключови думи: киберсигурност, университет, система за записване, пробиви

Abstract: Given the significant technological advances in all aspects of our lives and the increasing dependence on digital platforms, universities are facing new challenges. One major challenge concerns the student enrollment process. Since the COVID-19 pandemic, many university processes have moved to an online environment - semester payment, online application, conducting lectures, etc. It has been daunting for many to visit universities in person to enroll in their chosen programs due to the widespread health crisis. As a result, some universities around the world have started implementing online enrollment systems for newly admitted students that offer convenience and affordability. However, the rise of online check-in systems and the handling of sensitive information – such as personal data and financial details – combined with the growing popularity of online payments has increased the vulnerability of these systems to cyber-attacks. In light of these challenges, developing robust and adaptive cybersecurity strategies has become essential for safeguarding against potential breaches. In 2023 will see a significant increase in cyber-attacks targeting higher education institutions and their processes, including those affecting online enrollment systems. This highlights the need for comprehensive and appropriate cyber security measures to effectively protect sensitive student data and ensure the ongoing integrity of institutional operations. Additionally, the evolving nature of cyber threats necessitates continuous updates and improvements to security protocols. This study therefore focuses on case studies of breaches and vulnerabilities and reviews the online enrollment processes of several universities in Europe, with an emphasis on data security. The findings reveal that key vulnerabilities relate to weak authentication practices, insufficient multi-factor authentication and integration with legacy systems. Conducting regular security audits and penetration testing is critical to identifying and mitigating vulnerabilities in student enrollment systems. Penetration tests, where ethical hackers attempt to break into the system, can help uncover weaknesses that may not be apparent during routine audits. The purpose of this research is to propose a model to improve the security level of newly admitted student enrollment systems. It is essential that universities implement comprehensive information security management approaches that ensure not only data protection but also effective risk management. By identifying existing challenges and recommending best practices, this document seeks to improve the protection of sensitive data and improve the overall security of university information systems. The proposed method has been tested in a real environment and has been evaluated to reduce the risk of data breaches and increase the trust and safety of the university environment.

Keywords: cybersecurity, university, enrollment system, breaches

2. Велкова, Ивона. (2025). Иновативни системи за управление на идентичности и достъп в академичните институции. *Научни трудове на УНСС*, 2025, бр. 2, с. xx–xx. ISSN 0861-9344.

Резюме: Статията изследва ролята на системите за управление на идентичности в академичните среди и представя модел за включване на утвърдени технологични подходи като еднократно удостоверяване, многофакторна автентикация и управление на достъпа, базирано на роли, както и решения с използване на технологиите за близка комуникация и радиочестотна идентификация. Целта е да се предложат подобрения на образователната среда по време на дигиталната трансформация по отношение на сигурност, мащабируемост и оптимизация на административните процеси. Предложена е архитектура, която демонстрира устойчивост срещу кибератаки и съвместимост със съществуващи платформи, което я прави ключова за устойчиво управление на идентичности в образователните институции

Ключови думи: управление на идентичности, академични институции, SSO, MFA, RBAC

Abstract: The article explores the role of identity management systems in academic environments and presents a model that incorporates established technological approaches such as single sign-on (SSO), multi-factor authentication (MFA), and role-based access control (RBAC), as well as solutions utilizing near-field communication (NFC) and radio-frequency identification (RFID) technologies. The aim is to propose improvements to the educational environment during digital transformation in terms of security, scalability, and optimization of administrative processes. An architecture is proposed that demonstrates resilience against cyberattacks and compatibility with existing platforms, making it a key component for sustainable identity management in educational institutions.

Keywords: identity management, academic institutions, SSO, MFA, RBAC