The future of print journalism in the digital age is characterized by a complex interplay of challenges and opportunities. While traditional print media grapples with declining circulation, revenue pressures, and digital competition, it also has the potential to thrive by leveraging digital platforms, diversifying revenue streams, and upholding the principles of quality journalism. By embracing digital transformation, fostering innovation, and adapting to evolving reader preferences, traditional print media can continue to be a vital force in shaping the media landscape of the future.

Sushchenko P. R.
Supervisor: Khodakovska A. V.
College of Economics and Law Zaporizhzhia National University

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENHANCING CYBERSECURITY

In today's interconnected digital landscape, the proliferation of cyber threats poses a significant challenge to organizations, governments, and individuals. As cyberattacks grow in complexity and frequency, the role of artificial intelligence (AI) in enhancing cybersecurity has become increasingly pivotal.

The purpose of the study is to explore the multifaceted role of AI in bolstering cybersecurity measures, from threat detection and response to proactive risk mitigation.

Cyber threats encompass a wide array of malicious activities, including malware, phishing, ransomware, and sophisticated hacking attempts. These threats not only jeopardize sensitive data and intellectual property but also undermine the trust and stability of digital infrastructures. Traditional cybersecurity measures, while effective to a certain extent, often struggle to keep pace with the evolving tactics of cybercriminals.

AI-powered cybersecurity systems utilize machine learning algorithms to analyze vast datasets, identify patterns, and detect anomalies indicative of potential security breaches. By continuously learning from new data inputs, AI can uncover previously unseen threats and preemptively thwart attacks.

AI-driven cybersecurity solutions excel in behavioral analysis, enabling them to discern normal user behavior from potentially malicious activities. By establishing baseline behavioral patterns, AI algorithms can swiftly flag deviations that may indicate unauthorized access or insider threats.

AI empowers organizations to automate incident response processes, enabling rapid and targeted actions in the event of a cyber breach. From isolating compromised systems to deploying countermeasures, AI streamlines response protocols, reducing the impact of security incidents.

AI equips cybersecurity professionals with predictive intelligence, enabling them to forecast potential threats and vulnerabilities based on historical data and real-time indicators. By proactively identifying weak points in digital infrastructures, organizations can shore up their defenses before exploitation occurs.

AI-driven vulnerability management systems can systematically scan and assess an organization's network, applications, and devices for potential weaknesses. By automating the identification and prioritization of vulnerabilities, AI enables proactive remediation, reducing the window of exposure to cyber threats.

AI has revolutionized biometric authentication methods, offering robust identity verification through facial recognition, voice authentication, and behavioral biometrics. These advanced authentication techniques bolster access control measures, mitigating the risk of unauthorized access and identity fraud.

AI-powered anomaly detection mechanisms scrutinize access patterns and user behavior to identify suspicious activities. By dynamically adjusting access privileges based on real-time risk assessments, AI contributes to the fortification of identity and access management protocols.

While AI holds immense potential in bolstering cybersecurity, it also presents certain challenges and considerations. Cybercriminals may exploit AI vulnerabilities through adversarial attacks, manipulating AI algorithms to evade detection or extract sensitive information. This necessitates ongoing research and development to fortify AI systems against such threats. The use of AI in cybersecurity raises ethical considerations regarding data privacy, algorithmic bias, and the responsible use of

surveillance technologies. Striking a balance between security imperatives and individual privacy rights remains a critical concern.

The effective deployment of AI in cybersecurity hinges on the availability of skilled professionals capable of developing, implementing, and managing AI-driven security solutions. Bridging the skills gap and fostering AI expertise within the cybersecurity workforce is imperative.

The symbiotic relationship between AI and cybersecurity holds immense potential in fortifying digital defenses, thwarting cyber threats, and safeguarding critical assets. By harnessing the power of AI for threat detection, predictive intelligence, access control, and vulnerability management, organizations can proactively mitigate risks and respond decisively to security incidents. As AI continues to evolve, it is crucial to address the associated challenges and ethical considerations while maximizing the transformative potential of AI in enhancing cybersecurity resilience in an increasingly interconnected world.

Трипольська Н. В.
Науковий керівник: Сущенко Л. О.
Запорізький національний університет

КОМПЕТЕНТНІСНИЙ ПІДХІД ДО ФОРМУВАННЯ КОМУНІКАТИВНОЇ КОМПЕТЕНТНОСТІ ДІТЕЙ ДОШКІЛЬНОГО ВІКУ В ІГРОВІЙ ДІЯЛЬНОСТІ

Інтенсивні зміни, що відбуваються останнє десятиліття у суспільстві, задають нові вимоги до особистості. Головним завданням української політики в умовах реформування є забезпечення якісної освіти на основі змісту його фундаментальності, відповідності актуальним та перспективним потребам особистості, нашого суспільства та держави. Відповідність зазначеним вимогам спонукало до оновлення змісту освітнього процесу в Україні, адаптації його до вимог світового освітнього простору та орієнтації навчальних програм на компетентнісний підхід.

Про актуальність проблеми формування комунікативної компетентності дітей дошкільного віку зазначено у Базовому компоненті дошкільної освіти, де