

УДК 004.8

Hlib Kharybin¹, Nataliia Zhukova²

¹student of group SEC-813 NU “Zaporizhia Polytechnic”

²PhD (Philology), associate professor NU “Zaporizhzhia Polytechnic”

THE ABSOLUTE BENEFITS OF AI IN CYBERSECURITY

AI is at the heart of modern cyberdefense strategies, and its impact spans crucial areas such as network security, threat management, protection of confidential data, automation of security processes, and predicting future threats.

Network Security. AI-driven algorithms continuously monitor network traffic, spotting anomalies and potential threats in real-time. Machine learning models analyze network behavior, foreseeing possible breaches, while AI-powered intrusion detection and prevention systems react swiftly to neutralize cyberattacks.

Analysis, Threat Management, and Incident Response. Leveraging AI analytics, vast volumes of security data are sifted through to pinpoint emerging threats and vulnerabilities. AI-powered threat intelligence platforms bolster detection capabilities, and automated incident response, powered by AI algorithms, ensures quick containment and mitigation of security breaches.

Protection of Confidential Information. AI-based data loss prevention systems vigilantly watch over confidential data across networks and endpoints, while AI-driven encryption techniques fortify the security of sensitive information, thwarting unauthorized access attempts.

Automation of Security Processes. AI automates various security processes, from patch management to vulnerability scanning and policy enforcement.

Integration of AI-powered orchestration platforms streamlines incident response workflows, enhancing overall security operations efficiency.

Forecasting Threats and Trends. AI predictive analytics forecast emerging cyber threats and trends by analyzing historical data and contextual information. Machine learning algorithms delve into cybersecurity trends, enabling organizations to proactively adapt their defense strategies, staying ahead of potential threats.

By weaving AI technologies into cyberdefense strategies across these fields, organizations fortify their security posture, sharpen threat detection capabilities, and mount more effective responses against evolving cyber threats. As a result, safeguarding critical assets and sensitive information becomes more robust and resilient.