# SECTION: COMPUTER ENGINEERING

# ARTIFICIAL INTELLIGENCE AS A COMPONENT OF MODERN INFORMATION SYSTEMS

**Cherkashyn Borys**
Bachelor Student
Department of Artificial Intelligence
Kharkiv National University of Radio Electronics, Ukraine

Information systems serve as the backbone of modern organizations by enabling data collection, storage, processing, and communication. As digital environments become more complex and data volumes continue to grow, many tasks can no longer be handled effectively by purely rule-based methods. In this context, artificial intelligence has become a practical tool that complements traditional information system components by extracting patterns from data, predicting outcomes, detecting anomalies, and generating recommendations that support both operational and managerial decisions [1].

Nevertheless, introducing AI into an information system is not simply a matter of adding a model. AI requires stable data flows, adequate infrastructure, and continuous monitoring to remain reliable over time. For this reason, AI should be treated as a system component that interacts with databases, application services, user interfaces, and governance processes [2].

The purpose of this study is to analyze artificial intelligence as a component of modern information systems and to summarize key integration approaches, benefits, and constraints. The objectives include describing the main AI-driven functions in information systems, outlining typical deployment patterns, and discussing challenges associated with data quality, cybersecurity, transparency, and model reliability.

In real-world information systems, AI most often delivers value through recurring functions such as predictive analytics, classification, anomaly detection, recommendations, decision support, and intelligent automation. Predictive models can support forecasting tasks, including demand estimation, workload prediction, and failure anticipation. Classification and detection techniques are widely used for fraud prevention and cybersecurity monitoring, where early identification of suspicious patterns is critical [3].

Recommendation mechanisms improve user experience by suggesting relevant content or actions, while decision support modules provide risk scores or ranked alternatives to assist specialists in making better-informed choices [4].

AI components are integrated into information systems using several established deployment approaches. Service-based deployment is common when a model is provided via an API and can be scaled or updated independently from the core system. Embedded deployment allows a model to run within the application environment,

reducing network dependency. In IoT and mobile contexts, edge AI enables inference directly on devices, which can reduce latency and limit unnecessary data transfer. The choice of deployment pattern depends on system requirements such as performance, maintainability, and security.

A key feature of AI-enabled systems is the need for data pipelines and lifecycle management. Model outputs depend on the quality and representativeness of data, and changes in real-world conditions may lead to performance degradation over time. This problem is often described as technical debt and model drift, which makes monitoring and periodic updates essential. Effective lifecycle management involves controlled data collection, preprocessing, validation, version control, documentation, and continuous monitoring of system behavior in production.

At the same time, the implementation of AI introduces risks related to privacy, security, and trust. Information systems frequently process personal or sensitive data, requiring secure storage, access control, and compliance measures. AI services may be targeted through malicious inputs or attempts to manipulate system outputs. Transparency is also important: when AI influences decisions, users should understand the limitations and meaning of predictions. In addition, biased datasets may lead to unfair outcomes; therefore, ethical considerations and fairness checks should be incorporated into evaluation and deployment [5].

Artificial intelligence has become a crucial component of modern information systems, enhancing data processing, enabling predictive capabilities, supporting informed decision-making, and augmenting automation. However, the impact of AI depends not only on model accuracy but also on system-level engineering, including reliable data pipelines, monitoring, governance, and secure integration. Treating AI as a managed component within the broader information system architecture helps increase stability, transparency, and trust. Future progress in this area will likely focus on stronger lifecycle management, explain ability, and security practices to ensure the long-term effectiveness of AI-enabled information systems.

## References

1. Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
2. ISO/IEC. (2022). ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology. International Organization for Standardization.
3. National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). NIST.
4. Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., Chaudhary, V., Young, M., Crespo, J.-F., & Dennison, D. (2015). Hidden technical debt in machine learning systems. In Advances in Neural Information Processing Systems (NeurIPS 2015) (Vol. 2, pp. 2503–2511).
5. Cherkashyn, B. A. (2024). Artificial intelligence in the field of professional education and development. In Collection of scientific papers “Scientia” (Section 11: Computer and Software Engineering, pp. 93–94). Pisa, Italy.