УДК 519.6

МЕТОДИ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ ЗА ДОПОМОГОЮ АЛГОРИТМІВ ШИФРУВАННЯ

Оксана Онищук, Ірина Явір

METHODS OF PROTECTING CONFIDENTIAL DATA USING ENCRYPTION ALGORITHMS

Oksana Onyshchuk, Iryna Yavir

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *The report discusses the introduction of artificial intelligence and encryption algorithms for reliable data encryption.*

У сучасному цифровому просторі обсяг конфіденційної інформації стрімко зростає, що підвищує ризики її витоку, перехоплення чи викривлення. Надійний захист даних стає пріоритетним завданням для будь-якої організації чи приватного користувача. Основу такого захисту складають криптографічні методи, які забезпечують шифрування інформації з метою запобігання несанкціонованому доступу.

Серед основних підходів до шифрування виокремлюють симетричні та асиметричні алгоритми. До перших належать, зокрема, шифри Віженера та Хілла – вони характеризуються простотою реалізації та швидкістю обробки даних. Асиметричні методи, як-от RSA та протокол Діффі-Гелмана, забезпечують вищий рівень безпеки завдяки використанню відкритого і закритого ключів. Аналіз ефективності цих методів дозволяє зробити висновки про доцільність їх використання в різних умовах: від локального зберігання даних до захисту інформації в мережевих середовищах.

Крім традиційних засобів криптографії, все ширше впроваджуються автоматизовані аналітичні системи на основі штучного інтелекту. Такі системи здатні виявляти витоки інформації, аналізуючи поведінку користувачів, структуру мережевого трафіку та інші дані про активність у цифровому середовищі. Інструменти на базі машинного навчання допомагають у виявленні підозрілих дій, фішингових атак, аномалій у системі — ще до моменту порушення цілісності чи конфіденційності даних.

Таким чином, найбільш ефективним підходом до захисту інформації є комбінування алгоритмів шифрування з сучасними інструментами штучного інтелекту. Це дозволяє створити багаторівневу систему кіберзахисту, яка здатна не лише запобігати загрозам, а й адаптуватися до нових викликів інформаційного середовища.

Бібліографія

1. Difference Between Symmetric and Asymmetric Key Encryption. URL: https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/ (дата звернення: 19.04.2025)
2. The state of AI Cybersecurity in 2025 and beyond. URL: https://www.forbes.com/councils/forbestechcouncil/2025/01/21/the-state-of-ai-cybersecurity-in-2025-and-beyond/ (дата звернення: 19.04.2025)