ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ КРИПТОАНАЛІЗУ

Леонова А.О., В'юхін Д.О., Лук`яненко М.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Криптоаналіз - це процес виявлення вразливостей у криптографічних алгоритмах з метою дешифрування інформації без доступу до ключа. З появою штучного інтелекту (ШІ), криптоаналіз отримав інструменти для автоматизації, зокрема методи машинного та глибокого навчання, - тим самим зменшуючи час, підвищуючи точність і дозволяючи аналізувати навіть складні шифри.

Метою роботи є розглядання переваг використання інструментів ШІ у сучасному криптоаналізі.

Основну увагу варто приділити практичним перевагам автоматизованого криптоаналізу з використанням ШІ. Це значне скорочення часу, необхідного на аналіз складних криптографічних структур, зменшення людського фактору та можливість обробки великих обсягів даних у реальному часі. Наприклад, системи, що використовують нейронні мережі, можуть автоматично розпізнавати зашифровані повідомлення, аналізувати їх на предмет шаблонів, а також оцінювати ефективність захисту. У режимі «чорного ящика» ШІ здатен розпізнавати приховані закономірності в зашифрованих даних, здійснювати статистичний аналіз і вивчати поведінку криптографічних протоколів [1]. Це дозволяє автоматизувати атаки, які раніше виконувалися вручну, наприклад, атаки з відкритим текстом або диференціальний криптоаналіз.

ШІ може імітувати поведінку шифру та поступово навчатися обходити його, що дає можливість здійснювати автоматизований криптоаналіз без явного декодування алгоритму [2].

ШІ також застосовується в контексті квантової криптографії, де традиційні засоби криптоаналізу часто безсилі. Алгоритми машинного навчання можуть допомагати в аналізі квантових каналів, виявленні вразливостей протоколів квантового обміну ключами та симуляції квантових атак [3]. Поєднання ШІ та квантових обчислень створює новий клас інструментів криптоаналізу, здатних адаптуватися до систем, які досі вважалися незламними. Але масове впровадження ШІ в криптоаналіз створює нові ризики. Технології, які використовуються для захисту, можуть бути адаптовані і для атак.

Загалом, використання штучного інтелекту для автоматизації криптоаналізу є потужним інструментом, що дозволяє значно підвищити ефективність інформаційної безпеки.

Список літератури

1. AI in Cryptography. (електронний ресурс): URL: https://insights2techinfo.com/ai-in-cryptography.

2. Neural Cryptography: (електронний ресурс): URL: https://en.wikipedia.org/wiki/Neural_cryptography.

3. Artificial Intelligence and Quantum Cryptography.: (електронний ресурс): URL: https://jast-journal.springeropen.com/articles/10.1186/s40543-024-00416-6.