УДК 621.396:004.056]:004.8

# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Крикун Є. О.
e-mail: yelyzaveta.krykun@nure.ua
Науковий керівник – ст. викладач Олейнікова О. І.
Харківський національний університет радіоелектроніки, каф. ІРТЗІ
м. Харків, Україна

The paper examines the application of artificial intelligence technologies in technical information protection systems. The possibilities of using artificial intelligence to detect technical channels of information leakage, analyze electromagnetic, radio and acoustic signals are shown. The advantages of intelligent monitoring systems that can automatically detect anomalies and adapt to environmental changes are identified.

У сучасних умовах стрімкого розвитку інформаційних технологій та активної цифровізації суспільства питання забезпечення інформаційної безпеки набуває особливої актуальності. Зростання обсягів оброблюваних даних, поширення мережевих сервісів і використання складних інформаційних систем створюють нові виклики для захисту інформації. Одним із важливих напрямів забезпечення інформаційної безпеки є технічний захист інформації (ТЗІ), який передбачає комплекс організаційних, програмних та апаратних заходів, спрямованих на запобігання витоку інформації через технічні канали.

Традиційні методи ТЗІ здебільшого ґрунтуються на використанні класичних підходів аналізу сигналів, спектрального моніторингу та ручної обробки результатів вимірювань [1]. Однак із розвитком сучасних технологій зростає складність потенційних загроз, зокрема пов’язаних із побічними електромагнітними випромінюваннями, радіосигналами, акустичними та віброакустичними каналами витоку інформації. Це ускладнює процес своєчасного виявлення загроз і потребує застосування нових підходів до аналізу та обробки даних.

У таких умовах перспективним напрямом розвитку систем ТЗІ є використання технологій штучного інтелекту (ШІ). Алгоритми машинного навчання та глибинного навчання здатні обробляти великі обсяги даних, виявляти приховані закономірності у сигналах та автоматично визначати аномалії у різних середовищах. Застосування ШІ дозволяє підвищити ефективність радіомоніторингу, аналізу побічних електромагнітних випромінювань, а також акустичних і віброакустичних каналів витоку інформації.

Перспективним напрямом використання ШІ є радіомоніторинг та виявлення закладних пристроїв. Застосування алгоритмів машинного навчання дає змогу створювати модель нормального радіочастотного середо-

вища на об’єкті та автоматично фіксувати відхилення від моделі, що дозволяє виявляти нові джерела сигналів.

Іншим напрямом використання ШІ в системах ТЗІ є аналіз акустичних та віброакустичних каналів витоку інформації. Коливання скла або елементів конструкції приміщення можуть передавати інформацію про мовлення. Використання ШІ дозволяє обробляти складні часово-частотні характеристики акустичних сигналів, виділяти характерні, часто неусвідомлені шаблони мовлення, що відображають внутрішній стан, переконання й досвід людини та визначати наявність інформації у фоновому шумі. Алгоритми глибинного навчання здатні автоматично виявляти аномалії в акустичному середовищі, що значно підвищує ефективність технічного захисту [2].

Сучасні системи ТЗІ із застосуванням ШІ дозволяють проводити обробку сигналів безпосередньо на об’єкті, мінімізувати затримки та зберігати конфіденційність даних. Це дозволяє створити автономні системи моніторингу, які самостійно адаптуються до змінного середовища, оптимізують режими сканування спектра і визначають канали, які **можуть бути потенційними джерелами витоку даних**.

Важливою перевагою застосування ШІ є зменшення впливу людського фактору. Традиційні методи ТЗІ потребують висококваліфікованого персоналу та постійного контролю, що збільшує витрати та час на обстеження об’єкта. Автоматизовані системи на основі ШІ здатні безперервно працювати, виявляти потенційні загрози та формувати звіти для адміністраторів без постійного контролю.

Водночас впровадження штучного інтелекту у сферу інформаційної безпеки пов’язане з певними ризиками. До них належать можливість атак на моделі машинного навчання, складність інтерпретації результатів роботи нейронних мереж та потреба у значних обчислювальних ресурсах. Крім того, виникає питання захисту самої системи ШІ від зловмисного впливу, що може призвести до хибних спрацювань.

Таким чином, використання технологій ШІ дозволяє значно підвищити ефективність систем технічного захисту інформації. Інтелектуальні алгоритми здатні виявляти нові типи загроз, швидко обробляти великі обсяги даних та зменшувати кількість хибних спрацьовувань систем безпеки.

Список використаних джерел:

1. Хорошко В.А., Ленков С.В., Перегудов Д.А. Методи та засоби захисту інформації. Київ: Арий, 2008. 344 с.

2. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації. 2020. № 4 (44). С. 6-11.