УДК 534.21, 004.056.5, 681.513.6

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ

К. Д. Алєксєєв[1], Є. В. Морщ[1], В. М. Степаненко[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

В роботі розглянуто можливості використання технологій штучного інтелекту для виявлення закладних пристроїв. Наведено перспективні напрямки для впровадження технолоій штучного інтелекту в процес пошуку закладних пристроїв.

Ключові слова: закладні пристрої, штучний інтелект, комп'ютерний зір

Вступ

У сучасному світі питання забезпечення інформаційної безпеки набуває особливої актуальності. Однією з вагомих загроз у сфері технічного захисту інформації є використання закладних пристроїв — спеціалізованих технічних засобів, призначених для прихованого зняття інформації без згоди власника.

На практиці широко застосовуються перевірені традиційні методи пошуку закладних пристроїв: радіочастотний моніторинг, аналіз електромагнітного випромінювання, тепловізійне обстеження, використання нелінійних локаторів, візуальний контроль і оцінка акустичних характеристик приміщення. Ці методи залишаються ефективними, проте з розвитком технологій закладні пристрої також еволюціонують, зокрема отримують можливості використовувати цифрові способи передачі, працювати за розкладом або активуватись лише за певних умов, що ускладнює їх виявлення.

У зв'язку з цим актуальним є напрям досліджень, пов'язаний з модернізацією традиційних методів пошуку прихованих пристроїв за допомогою новітніх інформаційних технологій, зокрема технологій штучного інтелекту. Методи машинного навчання, комп'ютерного зору, аналізу спектральних та акустичних аномалій дозволяють значно підвищити швидкість, точність і автономність виявлення потенційних загроз. Наприклад, застосування глибоких нейронних мереж дає змогу автоматично аналізувати великі масиви сигналів та зображень, знаходячи характерні ознаки функціонування прихованих пристроїв [1].

Крім того, технології штучного інтелекту поступово впроваджуються у мобільні та портативні рішення, зокрема застосунки для виявлення прихованих камер, що розширює можливості виявлення небезпек навіть поза межами спеціалізованих перевірок [2].

Метою цієї роботи є дослідження можливостей підвищення ефективності виявлення закладних пристроїв шляхом інтеграції технологій штучного інтелекту з класичними методами технічного контролю, а також окреслення перспектив подальшого розвитку таких рішень.

1. Традиційні методи виявлення закладних пристроїв

1.1. Класифікація закладних пристроїв

Закладні пристрої — це технічні засоби, призначені для прихованого збору, фіксації, зберігання або передачі інформації без відома або згоди об'єкта спостереження. Їх можна класифікувати за кількома ознаками [3]:

1. **За каналом передачі:**
   - радіочастотні (передають дані через RF);
   - дротові (забирають інформацію через живлення або мережу);
   - акустичні (передають звук безпосередньо або через середовище);
   - оптичні (включаючи лазерні мікрофони, відеокамери).
2. **За способом активації:**
   - постійної дії;
   - з відкладеним запуском;
   - дистанційно керовані.
3. **За способом маскування:**
   - інтегровані в предмети побуту (ручки, зарядки, датчики руху);
   - вмонтовані в інфраструктуру (розетки, стіни, вентиляція).

1.2. Огляд традиційних методів виявлення

Традиційні засоби пошуку закладних пристроїв сформувалися як результат практичного досвіду технічного захисту інформації. До найбільш поширених належать [4, 3]:

Радіочастотне сканування. Сучасні аналізатори спектру дозволяють виявити активні RF-випромінювачі в широкому діапазоні частот. Недо-

ліком є складність виявлення малопотужних або періодичних сигналів.

Нелінійні локатори. Ці пристрої використовуються для виявлення електронних компонентів за рахунок їхнього нелінійного відгуку на радіосигнали. Вони дають змогу виявити навіть вимкнені пристрої, однак можуть створювати хибні спрацьовування (наприклад, від мобільного телефону).

Тепловізійне сканування. Метод дозволяє виявляти джерела тепла, які свідчать про роботу електронного пристрою. Він є ефективним для активних пристроїв, але менш чутливий до автономних та енергоощадних закладок [5].

Аналіз енергоспоживання. Цей підхід дозволяє виявити сторонні пристрої шляхом фіксації змін навантаження в мережі. Однак він має обмежене застосування в умовах складних об'єктів [6].

Візуальний огляд та інженерна перевірка. Такий метод передбачає виявлення змін у середовищі, перевірку підозрілих предметів, кабельних трас, вентиляційних отворів тощо [7].

1.3. Актуальні виклики виявлення сучасних пристроїв

Попри доведену ефективність традиційних методів технічного контролю, сучасні закладні пристрої все частіше здатні обходити наявні засоби виявлення. Це зумовлено рядом факторів, пов'язаних з розвитком технологій [7, 5].

Використання цифрових або мультичастотних діапазонів. Закладні пристрої дедалі частіше використовують Wi-Fi, Bluetooth, GSM, Zigbee та інші бездротові протоколи. Їхні сигнали можуть маскуватися під звичайну інфраструктуру, що ускладнює їх ідентифікацію.

Застосування алгоритмів маскування або періодичної активації. Деякі пристрої можуть активуватись лише за визначених умов або працювати циклічно, скорочуючи час випромінювання. Це суттєво знижує ймовірність їх фіксації під час стандартних обстежень.

Використання модульних енергонезалежних схем. Деякі закладні пристрої не споживають енергії від об'єкта контролю, що унеможливлює їх виявлення шляхом аналізу енергоспоживання. Вони також не створюють електромагнітного сліду, поки не активуються.

Інтеграція в загальносистемні пристрої. Закладні модулі можуть бути вбудовані у звичайні IoT-пристрої, датчики охоронної сигналізації, IP-камери тощо. Їх важко відрізнити від штатного обладнання без застосування спеціалізованого аналізу [5].

У зв'язку з цим виникає потреба у пошуку нових підходів, здатних підвищити ефективність виявлення закладних пристроїв. Перспективним напрямом є використання інтелектуальних систем аналізу, зокрема алгоритмів машинного навчання, що дозволяють автоматизувати розпізнавання нетипових сигналів, поведінкових аномалій або прихованих фізичних проявів.

2. Застосування технологій штучного інтелекту для виявлення закладних пристроїв

2.1. Потенціал використання штучного інтелекту в системах технічного контролю

Інтенсивний розвиток методів штучного інтелекту відкриває нові можливості в галузі автоматизованого технічного захисту інформації [8]. При застосуванні в контексті виявлення закладних пристроїв, такі технології дозволяють реалізувати інтелектуальні системи аналізу, які здатні виявляти нетипові сигнали або прояви у складному інформаційному середовищі.

Штучний інтелект може бути ефективно інтегрований у класичні методи виявлення шляхом автоматизації таких завдань:

- класифікація або фільтрація сигналів у спектрі радіочастот;
- аналіз структур аудіопотоків для виявлення акустичних аномалій;
- обробка зображень і теплових карт за допомогою комп'ютерного зору;
- виявлення патернів у споживанні енергії або мережевому трафіку.

Інтеграція нейронних мереж (особливо згорткових і рекурентних моделей) дозволяє досягти високої чутливості до слабких або маскованих сигналів. Такий підхід відкриває перспективи створення гібридних рішень, у яких штучний інтелект виступає як інтелектуальний модуль розширення класичних процедур технічної перевірки.

2.2. Основні напрямки застосування штучного інтелекту

Системи на основі штучного інтелекту можуть бути адаптовані до різних видів вхідних даних, що надходять під час пошуку закладних пристроїв [9]. Нижче розглянуто чотири основні напрями застосування таких технологій у межах систем технічного захисту.

Аналіз радіочастотного спектру. Одним із найперспективніших напрямів є застосування глибоких згорткових нейронних мереж (CNN) або моделей класифікації для виявлення нетипових радіочастотних сигналів [10]. Системи можуть навчатися на спектрограмах, розпізнаючи сигнатури передавачів або цифрових протоколів, які відрізняються від фонових умов.

Обробка акустичних сигналів. Методи машинного навчання використовуються для аналізу спектру аудіосигналів, що дозволяє виявляти активність мікрофонів, у тому числі ультразвукових або імпульсних пристроїв. Деякі підходи передбачають розпізнавання «неприродних» шумів або реверберацій, які створюються прихованими пристроями.

Комп'ютерний зір і тепловізійна аналітика. Алгоритми комп'ютерного зору на основі глибокого навчання дозволяють аналізувати зображення з відеокамер або тепловізорів, виявляючи аномалії, які

можуть вказувати на наявність прихованого пристрою [1]. Наприклад, локальні джерела тепла можуть бути ідентифіковані як потенційні об'єкти стеження навіть за відсутності радіовипромінювання.

Виявлення мережевих або енергетичних аномалій. Аналіз нетипових змін у споживанні електроенергії, мережевій активності або передачі даних також може бути автоматизований. Моделі можуть виявляти сигнали, які зазвичай не характерні для стандартної інфраструктури, вказуючи на можливу присутність підключеного закладного пристрою.

2.3. Обмеження, ризики та перспективи розвитку

Незважаючи на потенціал технологій штучного інтелекту, їхнє застосування у сфері виявлення закладних пристроїв має низку обмежень.

По-перше, успішність роботи моделей значною мірою залежить від наявності великих обсягів якісних навчальних даних, які у випадку шпигунських пристроїв можуть бути складними для збирання або імітації. По-друге, високий рівень складності і варіативності закладних пристроїв ускладнює створення універсальних моделей.

Також існує ризик хибних спрацьовувань або, навпаки, ігнорування небезпечного сигналу через обмеження у точності моделі. Високі вимоги до обчислювальних ресурсів та енергоспоживання можуть обмежувати застосування ШІ на мобільних або польових пристроях.

Висновок

У ході дослідження були проаналізовані традиційні та інноваційні методи виявлення закладних пристроїв. Було встановлено, що хоча класичні технічні засоби виявлення — такі як радіочастотне сканування, нелінійні локатори, тепловізійна та візуальна перевірка — залишаються ефективними у багатьох випадках, сучасні закладні пристрої демонструють дедалі вищий рівень складності, маскування та автономності. Це створює виклики для засобів технічного захисту інформації в умовах стрімкого розвитку цифрових технологій.

У відповідь на ці виклики все більш актуальним стає впровадження технологій штучного інтелекту у системи технічного контролю. У статті розглянуто основні напрями застосування штучного інтелекту: аналіз радіочастотного спектру, обробка акустичних сигналів, комп'ютерний зір для аналізу зображень і тепловізійних даних, а також виявлення аномалій у споживанні енергії та мережевій активності. Інтеграція моделей машинного навчання з класичними методами відкриває перспективу створення гібридних систем нового покоління.

Попри значний потенціал, застосування ШІ супроводжується низкою обмежень: складністю доступу до навчальних даних, варіативністю пристроїв, ризиками хибних спрацьовувань та високими обчислювальними витратами. Проте подальший розвиток мультиканального аналізу, edge-AI та розподіленого навчання створює підґрунтя для побудови більш ефективних і надійних систем виявлення загроз.

Таким чином, модернізація традиційних методів технічного контролю шляхом впровадження технологій штучного інтелекту є обґрунтованим і перспективним напрямом підвищення інформаційної безпеки у сучасному середовищі.

Перелік використаних джерел

1. Heat of the Moment: Characterizing Thermal Camera-based Hidden Camera Detection / Z. Yu, Y. Qiao, C. Yu, M. Srivastava // Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22). — New York, NY, USA : Association for Computing Machinery, 2022. — С. 2175—2189. — DOI: 10.1145/3548606.3560595. — URL: https://cybersecurity.seas.wustl.edu/paper/CCS22_HeatDeCam_Yu.pdf.
2. *Agrawal T.* Spy Cam Detection using Deep Learning. — 2023. — Accessed: 2025-05-08. https://github.com/tanishq396/Spy_Cam_Detection.
3. *Jenkins P.* Surveillance Tradecraft: The Professional's Guide to Covert Surveillance Detection. — London : Intel Publishing UK, 2001. — ISBN 095353782X.
4. *Moran W. B.* Covert Surveillance and Electronic Devices. — Port Townsend, WA : Loompanics Unlimited, 1983. — ISBN 0915179202.
5. *Kiriakou J.* Surveillance and Surveillance Detection: A CIA Insider's Guide. — New York, NY : Skyhorse Publishing, 2022. — ISBN 9781510756151.
6. *Coleman R., McCahill M.* Surveillance and Crime. — London : SAGE Publications Ltd, 2011. — ISBN 9781847870647.
7. *Corera G.* Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage. — New York, NY : Pegasus Books, 2015. — ISBN 9781681771540.
8. *Goodfellow I., Bengio Y., Courville A.* Deep Learning. — Cambridge, MA : MIT Press, 2016. — ISBN 9780262035613.
9. *Kritzler M., Rodler D., Eiter T.* Anomaly Detection for Smart Home Systems Using Logic-Based Stream Reasoning // Journal of Web Semantics. — 2019. — Т. 56. — С. 35—55. — DOI: 10.1016/j.websem.2019.02.001.
10. *Goyal H., Abdelhadi A.* Spectrum Anomaly Detection with Deep Learning in Wireless Communication // IEEE Transactions on Cognitive Communications and Networking. — 2020. — Т. 6, № 2. — С. 900—913. — DOI: 10.1109/TCCN.2020.2981527.