УДК 004.048:004.056

ЗАСТОСУВАННЯ AI/ML ДЛЯ ПРОТИДІЇ КІБЕРАТАКАМ НА ЕНЕРГЕТИЧНІ СИСТЕМИ

Ковилін А.В., аспірант, anton.v.kovylin@gmail.com, ІПМЕ НАН України
Гільгурт С.Я., д.т.н., с.н.с., hilgurt@ukr.net, ІПМЕ ім. Г.Є. Пухова НАН України

Енергетичні системи в сучасному світі відіграють критичну роль у забезпеченні ефективного функціонування суспільства. Вони здійснюють постачання електроенергії необхідної для медичних послуг, життєдіяльності суспільства, ведення господарства, виробництва, забезпечення комунікації. А також відіграють ключову роль у підтримці та розвитку інфраструктури. В свою чергу, зростання рівня залежності даних систем від цифровізації підвищує рівень загрози кібератак.

Кібератаки на енергетичні системи є серйозним викликом сучасного світу. Зловмисники активно використовують новітні технології і методи для проникнення в системи, що мають пряме чи опосередковане відношення до керування виробництвом та розподілом енергії. Це може призвести до: надзвичайних ситуацій, відключень електроенергії, матеріальних та репутаційних збитків.

Саме через це застосування штучного інтелекту (AI) та машинного навчання (ML) є надзвичайно важливим в наш час. AI/ML технології дозволяють створювати системи (або окремі рішення), які можуть допомагати з виявленням (або прогнозом) потенційних кібератак. Це дозволяє ефективно реагувати та створювати запобіжні заходи щодо їх усунення.

Використання AI/ML для розробки систем виявлення вторгнень ML значно підвищило ефективність розпізнавання та ідентифікації потенційних загроз. Покращення моделей ML в сенсі підвищення точності розпізнавання та мінімізації хибних тривог (false positives) є важливими викликами, які потрібно подолати під час розробки та використання систем виявлення кібератак [1].

Виявлення кібератак та вчасне реагування на них - це, на даний момент, один з важливих функцій кібербезпеки, метою яких є не стільки виявлення вже здійснених атак, але насамперед своєчасна ідентифікація потенційних загроз, що надає можливість реагувати на них до завдання шкоди інформаційним системам [3]. Традиційно системи прийняття рішень в сфері кібербезпеки застосовували методи, здебільшого засновані на певних правилах і сигнатурах. Враховуючи рівень відповідальності даних систем, вони мають ефективно виявляти нові загрози чи адаптуватися до змін в підходах до кібератак [4]. Саме

тому для підвищення точності та ефективності систем прийняття рішень дослідники звернулися до методів штучного інтелекту та машинного навчання.

Виявлення аномалій є поширеним підходом ідентифікації потенційних кібератак, шо базуються на використанні AI/ML. Він розглядає відхилення поведінки системи від стандартної як потенційну загрозу безпеці [2]. Аналізуючі логи системних журналів операційних систем, мережевий трафік або дії користувачів, підхід на основі аномалій знаходить певні закономірності, що можуть сигналізувати про кібератаку [3].

До інших засобів виявлення кібератак, які також базуються на використанні AI/ML відносяться методи контрольованого та неконтрольованого навчання. Вони передбачають навчання ML моделей з використанням даних, попередньо підготовлених дата аналітиком з використанням відповідного програмного забезпечення. Такі підходи також можуть бути використані для виявлення закономірностей в поведінці інформаційних систем, логах мережевого трафіку та системних журналах [2].

Таблиця 1 – Переваги та виклики технік виявлення вторгнень на базі AI/ML

Техніки виявлення підозрілої активності	Переваги	Виклики
Виявлення аномалій	Ефективно для ідентифікації невідомих загроз	Важко розрізнити позитивні та зловмисні аномалії
Контрольоване навчання	Висока точність у виявленні відомих загроз	Вимагає попередньо опрацьованих тренувальних даних
Неконтрольоване навчання	Ідентифікація невідомих загроз	Обмежена інтерпретація та пояснювальність

Для кожного підходу існують різні ML моделі виявлення підозрілої активності.

Виявлення аномалій:

– ***Isolation Forest***. Ефективний для ідентифікації аномалій, особливо в великих наборах даних;

– ***Autoencoders***. Використовуються у глибокому навчанні для виявлення аномалій шляхом реконструкції вхідних даних;

– ***DBSCAN***. Застосовується для кластеризації даних і виявлення точок даних, що вибиваються із загальних патернів.

Контрольоване навчання:

– ***Random Forest.*** Добре підходить для класифікації та виявлення відомих патернів вторгнення;

– ***Support Vector Machines (SVM).*** Ефективний для класифікації на наборах даних з чітко визначеними границями між класами;

– ***Logistic regression.*** Корисний для проблем бінарної класифікації.

Неконтрольоване навчання:

– ***K-means Clustering.*** Використовується для групування даних і виявлення аномальних кластерів;

– ***Principal Component Analysis (PCA).*** Дозволяє зменшити вимірність даних і виявлення нестандартних патернів;

– ***Gaussian Mixture Models (GMM).*** Базуються на щільності та використовуються для виявлення аномалій та незвичайних відхилень у розподілі даних.

Дана робота присвячена дослідженню моделі Isolation Forest. Ця модель передбачає аналіз статистичних даних з використанням низки технологій: Sigma, NodeJS, Javascript.

В якості джерела даних було використано Windows Event Log. За допомогою системи Sigma форматувалася та відфільтровувалася найбільш значуща інформація. Отриманий набір даних подавався в якості вихідних даних для аналізу моделлю. На виході було отримано наступні результати:

Anomalous Login Attempts


```
[
  {
    "timestamp": "2023-10-07 11:10",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:11",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:12",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:13",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:14",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:15",
    "EventID": "4625",
    "targetUserName": "User2'",
    "status": " OR '1'='1",
    "__parsed_extra": [
      "0xc000006d"
    ]
  },
```


Detected SQL Injections


```
[
  {
    "timestamp": "2023-10-07 11:35",
    "EventID": "4625",
    "targetUserName": "Admin'",
    "status": " DROP TABLE users;--",
    "__parsed_extra": [
      "0xc000006d"
    ]
  }
]
```


Detected Phishing Attempts


```
[
  {
    "timestamp": "2023-10-07 11:50",
    "EventID": "4624",
    "targetUserName": "http://phishing.com",
    "status": "0x00000000"
  }
]
```


Рисунок 1 – Результати виявлення аномальної активності в системі

Як ми бачимо, дана модель відфільтрувала дані таким чином, що було виявлено наступну підозрілу активність: спроба користувачів отримати доступ до системи використовуючи логін, потенційну Phishing, а також SQL injection активність. Дуже важливо, що модель швидко адаптувалась та навчилась виявляти аномалії після отримання відносно невеликого набору даних порівняно з моделями контрольованого та неконтрольованого навчання [5].

Висновок. Використання систем виявлення потенційних кібератак має важливе значення та допомагає в забезпеченні безперебійної роботи об’єктів критичної інфраструктури. Результати проведенного дослідження свідчать, що моделі машинного навчання розширюють можливості дата аналітиків та спеціалістів з безпеки комп'ютерних систем щодо виявлення підозрілої активності і вживання заходів з підвищення рівня захисту, що є особливо важливим для об’єктів критичної інфраструктури в наш час. В свою чергу, з ціллю підвищення рівня ефективності, швидкості та точності рекомендовано своєчасно проводити збір даних щодо активності інформаційних систем (в т.ч. поведінки користувачів) і проводити навчання ML моделей. Використання AI/ML підходів для протидії кібератакам є перспективним і в найближчому майбутньому популярним напрямом розвитку безпеки інформаційних систем. Розвиток даного напряму надасть можливість постійно піднімати рівень захисту та резильєнтності цих систем (в тому числі на об’єктах критичної інфраструктури).

Список використаних джерел

1. Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. Heliyon, 4(11), e00938. https://doi.org/10.1016/j.heliyon.2018.e00938

2. Afrifa, S., Varadarajan, V., Appiahene, P., Zhang, T., & Domfeh, E. A. (2023). Ensemble machine learning techniques for accurate and efficient detection of botnet attacks in connected computers. Eng, 4(1), 650-664; https://doi.org/10.3390/eng4010039

3. Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: Feature selection, model, perfor-mance measures, application perspective, chal-lenges, and future research directions. Artificial Intelligence Review, 55(1), 453–563. https://doi.org/10.1007/s10462-021-10037-9

4. Sufi, F. (2023). Algorithms in low-code-no-code for research applications: A practical review. Algorithms, 16(2), 108. https://doi.org/10.3390/a16020108

5. А.В. Ковилін, Використання моделей машинного навчання при аналізі логів Sigma для забезпечення резильєнтності об’єктів критичної інфраструктури., Безпека енергетики в епоху цифрової трансформації, V науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 22 листопада 2023 р.). Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2023. 152 с., https://doi.org/10.5281/zenodo.10531706