DOI: 10.34185/1991-7848.itmm.2025.01.092

СУЧАСНІ ТЕНДЕНЦІЇ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Вдовиченко І.Н.

Криворізький національний університет, к.т.н., доцент, Україна

Анотація. *Представлене дослідження є одним з кроків у розумінні та оптимізації систем безпеки, які використовують ШІ для протидії непередбаченим кіберзагрозам та забезпечення безпеки від витоку інформації на підприємстві.*

Проаналізовано сучасні методи забезпечення безпеки в контексті запобігання витоку даних, а також розглянуто актуальність використання штучного інтелекту у цьому процесі. Досліджено переваги використання ШІ для захисту інформації. У дослідженні підкреслюється, що ефективність системи запобігання витокам даних значною мірою залежить від якості та обсягу зібраної інформації з таких основних джерел даних, як лог-файли системи, мережевий трафік, історії дій користувачів.

Для проведення дослідження використано три основних підходи: SVM, CNN, LSTM та їх комбінації, проведена перевірка їх ефективності.

Ключові слова: *штучний інтелект, кіберзагрози, виток інформації, захист, аномальні процеси, аналіз.*

Вступ. У сучасному світі, де цифровізація охоплює всі сфери діяльності, питання забезпечення інформаційної безпеки стають критично важливими. Кількість кібератак та витоків даних постійно зростає, що створює серйозні виклики для компаній та організацій. Традиційні методи захисту інформації, такі як системи запобігання витокам даних (DLP) та засоби захисту кінцевих точок (EDR), демонструють обмежену ефективність у виявленні складних загроз, зокрема, аномальної поведінки користувачів та внутрішніх загроз. У зв'язку з цим виникає потреба у впровадженні інтелектуальних систем аналізу поведінки користувачів (UEBA), що базуються на алгоритмах штучного інтелекту.

Організації всіх рівнів, від малих підприємств до великих корпорацій, залежать від своєї здатності безпечно зберігати та використовувати дані. Проте з розвитком технологій зростає і кількість загроз, спрямованих на отримання несанкціонованого доступу до цих даних. Згідно зі звітом IBM 2023 року, середня вартість витоку даних для компанії становить понад 4,35 мільйона

доларів, що підтверджує актуальність цієї проблеми. Сьогодні кіберзлочинність є одним із найактуальніших викликів для бізнесу та суспільства загалом.

Основний матеріал

Штучний інтелект є саме тим інструментом, який дозволяє організаціям вирішувати складні завдання кібербезпеки.

Серед переваг використання ШІ для захисту інформації можна виділити наступні:

1. Автоматизація інформаційних процесів. ШІ можна використовувати для автоматизованого виявлення загроз та відповіді на них, це скорочує час реагування та розвантажує працівників системи захисту.

2. Швидке виявлення аномальних процесів. Завдяки ШІ скануються великі інформаційні масиви на нестандартні дані чи ситуації, які можуть вказувати на спроби несанкціонованого доступу.

3. Підвищення результативності шифрування. ШІ сприяє створенню більш криптостійких шифрів.

Але, проблема інформаційної безпеки з використанням штучного інтелекту враховує як його переваги, так і потенційні обмеження. Використання ШІ дозволяє забезпечити проактивний захист даних, підвищуючи адаптивність і точність систем кібербезпеки.

У дослідженні пропонується виконати розробку, моделювання та впровадження інтелектуальної системи аналізу поведінки користувачів для запобігання витокам інформації з використанням технологій штучного інтелекту.

Глибинне навчання (Deep Learning) є однією з найбільш перспективних технологій для аналізу складних даних і виявлення прихованих закономірностей у сфері інформаційної безпеки. Його здатність адаптуватися до змін у кіберсередовищі та обробляти великі обсяги даних у реальному часі робить цю технологію надзвичайно ефективною у запобіганні витокам інформації та протидії кіберзагрозам.

У сучасних умовах кібербезпеки, аналіз поведінки користувачів (UBA, User Behavior Analytics) є важливим підходом для виявлення загроз і запобігання витокам даних. UBA використовує алгоритми машинного навчання для моніторингу дій користувачів, виявлення аномалій і створення профілів поведінки. Виявлення аномалій у поведінці користувачів представлено на рис.1. Це дозволяє системам реагувати на внутрішні ризики, які традиційні методи захисту часто ігнорують.

Рисунок 1 – Використання глибинного навчання для виявлення аномалій у поведінці користувачів

Ефективність системи запобігання витокам даних значною мірою залежить від якості та обсягу зібраної інформації. Збір та обробка даних є важливими етапами, що забезпечують основу для подальшого аналізу і виявлення аномалій. Для системи на основі ШІ, спрямованої на виявлення аномалій, необхідні різноманітні дані, які охоплюють інформацію про діяльність користувачів, поведінкові патерни, мережевий трафік та логи системи. Основні джерела даних включають: Лог-файли системи; Мережевий трафік; Історії дій користувачів.

Велике значення має попередня обробка даних в інтелектуальних системах захисту від витоків даних на основі аналізу поведінки користувачів (UEBA). Ці системи використовують машинне навчання та глибинне навчання для забезпечення точного виявлення аномалій, що дозволяє зменшити

кількість хибнопозитивних спрацьовувань та підвищити ефективність реакції на загрози.

Перспективи розвитку систем ШІ у сфері інформаційної безпеки є надзвичайно широкими. Інтеграція з технологіями розширеної аналітики відкриває можливості не лише для виявлення аномалій, але й для прогнозування потенційних загроз. Наприклад, використання прогнозної аналітики дозволяє системам передбачати сценарії атак на основі аналізу попередніх інцидентів. Це дає змогу підприємствам запобігати кіберзагрозам на ранніх етапах.

Суттєвим напрямом розвитку є впровадження алгоритмів самонавчання, здатних адаптуватися до змін у середовищі. Завдяки цьому системи можуть ефективно протидіяти атакам типу "zero-day", які є невідомими для традиційних рішень. Інтеграція таких технологій дозволяє створювати проактивний захист, що є критичним у динамічному цифровому середовищі.

В роботі була виконана оцінка ефективності різних алгоритмів ML у реальному середовищі з урахуванням таких параметрів, як точність виявлення загроз, швидкість

реагування та ресурсомісткість.

Для проведення дослідження використовувалися реальні корпоративні дані, які були поділені на навчальну та тестову вибірки. Використано три основних підходи:

1. Класифікаційні алгоритми (SVM, Decision Trees) для створення профілів поведінки користувачів.

2. Глибинні нейронні мережі (CNN, LSTM) для аналізу великих обсягів даних і виявлення прихованих закономірностей.

3. Комбіновані підходи, що використовують переваги як простих класифікаторів, так і нейронних мереж.

Результати дослідження показали, що ефективність алгоритмів варіюється залежно від типу завдань. Наприклад, для швидкого виявлення нетипової активності на робочих станціях найбільш ефективними виявилися дерева рішень, які забезпечили:

Точність: 82%. Час реакції: 3 секунди

Однак для складніших загроз, пов'язаних із послідовними аномаліями у великому масиві даних, LSTM продемонстрували значно вищу точність (91%) при середньому часі обробки запиту 7 секунд.

На базі проведеного аналізу було виконано реалізацію та впровадження системи захисту інформації. Архітектура системи захисту інформації побудована за модульним принципом, який забезпечує її гнучкість, масштабованість і простоту інтеграції у корпоративну інфраструктуру. Такий підхід дозволяє адаптувати систему до змін у кіберсередовищі, додаючи нові функціональні компоненти без порушення роботи існуючих. Архітектура системи містить: модуль збору даних, модуль аналізу, модуль виявлення аномалій, модуль автоматичного реагування. Елемент модуля виявлення аномалій представлений на рис. 2.

```python
from sklearn.ensemble import IsolationForest

def detect_anomalies(data):
    """
    Виявляє аномалії у наборі даних за допомогою Isolation Forest.
    """
    model = IsolationForest(n_estimators=100, contamination=0.1, random_state=42)
    model.fit(data)
    predictions = model.predict(data)
    anomaly_indices = [i for i, x in enumerate(predictions) if x == -1]
    print(f"Виявлено {len(anomaly_indices)} аномалій.")
    return anomaly_indices
```

Рисунок 2 – Виявлення аномалій

Висновки. Таким чином, використання штучного інтелекту у сфері інформаційної безпеки демонструє значні переваги, забезпечуючи більш високий рівень захисту та адаптивність у динамічному кіберсередовищі. Водночас виклики, пов’язані з його впровадженням, вимагають подальших досліджень і вдосконалень, щоб максимально розкрити потенціал цієї технології.

Підсумовуючи, успішне впровадження системи ШІ для інформаційної безпеки вимагає системного підходу. Розв’язання викликів, пов’язаних із сумісністю, ресурсами, якістю даних, підготовкою персоналу та

конфіденційністю, дозволяє організаціям отримати максимальну користь від інноваційних рішень і створити безпечне інформаційне середовище.

ЛІТЕРАТУРА

1.Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту. Київ: Ліра-К, 2021. 554с.
2.CISCO Annual Cybersecurity Report. (2023). "Analytics in Modern Data Security". Retrieved from https://cisco.com.
3.Microsoft Azure Security Blog. (2023). "UEBA Solutions: Enhancing Data Security". Retrieved from https://azure.microsoft.com.
4.IBM Security Report. (2023). "Cost of a Data Breach". Retrieved from https://ibm.com.

CURRENT TRENDS IN THE USE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Vdovychenko I.N.

Abstract. *The presented study is one of the steps in understanding and optimizing security systems that use AI to counter unforeseen cyber threats and ensure security against information leakage in the enterprise.*

Modern security methods in the context of data leakage prevention are analyzed, and the relevance of using artificial intelligence in this process is also considered. The advantages of using AI for information protection are investigated. The study emphasizes that the effectiveness of a data leakage prevention system largely depends on the quality and volume of information collected from such basic data sources as system log files, network traffic, and user action histories.

Three main approaches were used to conduct the study: SVM, CNN, LSTM and their combinations, and their effectiveness was tested.

Keywords: *artificial intelligence, cyber threats, information leakage, protection, anomalous processes, analysis.*

REFERENCE

1.Bohush V.M., Bohush V.V., Brovko V.D., Nastradin V.P. Osnovy kiberprostoru, kiberbezpeky ta kiberzakhystu. Kyiv: Lira-K, 2021. 554s.
2.CISCO Annual Cybersecurity Report. (2023). "Analytics in Modern Data Security". Retrieved from https://cisco.com.
3.Microsoft Azure Security Blog. (2023). "UEBA Solutions: Enhancing Data Security". Retrieved from https://azure.microsoft.com.
4.IBM Security Report. (2023). "Cost of a Data Breach". Retrieved from https://ibm.com.