УДК 004.056

В. О. Пантєлєєв

ПРОГНОЗУВАННЯ ІНСАЙДЕРСЬКИХ ЗАГРОЗ НА ОСНОВІ АЛГОРИТМІВ ОБРОБКИ ПРИРОДНОЇ МОВИ

Харківський національний університет радіоелектроніки

Анотація

Запропоновано підхід до прогнозування інсайдерських загроз за допомогою алгоритмів обробки природної мови. Розглянуто методологію збору, обробки та аналізу текстових даних для виявлення прихованих індикаторів ризику. Основна увага приділена застосуванню глибоких нейронних мереж та їх ефективності у прогнозуванні загроз.

Ключові слова: інсайдерські загрози, обробка природної мови, штучний інтелект, кібербезпека, аналіз текстових даних.

Abstract

The approach to predicting insider threats using natural language processing (NLP) algorithms is proposed. The methodology for collecting, processing, and analyzing textual data to identify hidden risk indicators is considered. The main focus is on the application of deep neural networks and their effectiveness in threat prediction.

Keywords: insider threats, natural language processing, artificial intelligence, cybersecurity, text data analysis.

Вступ

Сучасний цифровий ландшафт характеризується постійно зростаючими викликами інформаційної безпеки, особливо щодо внутрішніх загроз організаційним системам. Інсайдерські загрози становлять надзвичайно серйозну проблему для корпоративної безпеки, оскільки вони походять від осіб, які мають легітимний доступ до внутрішніх інформаційних систем та володіють глибоким розумінням організаційних процесів і технологічної інфраструктури. Застосування передових лінгвістичних технологій дозволяє здійснювати глибокий аналіз комунікативних патернів, поведінкових сигналів та контекстуальних індикаторів, що можуть свідчити про наміри співробітників щодо нанесення шкоди інформаційним активам організації.

Метою роботи є розроблення підходу до прогнозування інсайдерських загроз у корпоративному середовищі, що базується на алгоритмах обробки природної мови (NLP), для виявлення прихованих поведінкових і комунікативних індикаторів, які можуть вказувати на потенційні деструктивні наміри співробітників.

Результати дослідження

Інсайдерська загроза є комплексним поняттям, яке визначається як потенційний або реальний ризик навмисного або ненавмисного заподіяння шкоди організації з боку співробітників, підрядників або партнерів, які мають авторизований доступ до інформаційних систем [1, с. 45]. Науковці виділяють декілька ключових типів інсайдерських загроз: навмисні (злочинні), ненавмисні (випадкові) та такі, що виникають через недбалість. Обробка природної мови (Natural Language Processing, NLP) в контексті прогнозування інсайдерських загроз являє собою міждисциплінарний підхід, який поєднує лінгвістичний аналіз, машинне навчання та кібербезпеку [2, с. 67]. Основною метою такого підходу є виявлення прихованих комунікативних маркерів, які можуть вказувати на потенційні деструктивні наміри співробітників. Методологія прогнозування інсайдерських загроз на основі NLP включає декілька ключових етапів: збір текстових даних, попередню обробку, векторизацію, навчання класифікаційних моделей та валідацію результатів [3, с. 89]. Сучасні алгоритми дозволяють здійснювати аналіз електронного листування, повідомлень у корпоративних месенджерах, службових записок та інших комунікативних каналів. Важливим є застосування глибоких нейронних мереж, зокрема рекурентних (RNN) та трансформерних моделей, які спроможні вловлювати складні контекстуальні залежності в текстових масивах [4, с. 112]. Такі моделі

демонструють високу точність у виявленні емоційних маркерів, що можуть передувати потенційним інсайдерським діям.

Sentiment-аналіз є одним із основних інструментів у прогнозуванні інсайдерських загроз, оскільки дозволяє оцінювати емоційний стан співробітників та ідентифікувати потенційні передумови деструктивної поведінки [5, с. 76]. Машинні алгоритми здатні розпізнавати нюанси негативних емоційних станів, що можуть бути індикаторами внутрішньої напруги або конфліктності. Застосування NLP-технологій у контексті моніторингу персоналу вимагають особливої уваги та дотримання балансу між забезпеченням інформаційної безпеки та приватністю співробітників [6, с. 54]. Необхідною умовою є прозорість алгоритмів та наявність чітких регламентів використання аналітичних інструментів. Кластеризація та профілювання співробітників на основі лінгвістичного аналізу дозволяє створювати диференційовані моделі ризиків для різних категорій персоналу [7, с. 93]. Машинне навчання може ідентифікувати специфічні поведінкові патерни, характерні для потенційних інсайдерів. Інтеграція NLP-технологій з системами управління інформаційною безпекою (SIEM) забезпечує комплексний підхід до превентивного виявлення загроз [8, с. 77]. Такий синергетичний підхід дозволяє корелювати текстові сигнали з іншими поведінковими індикаторами. Перспективними напрямками досліджень є розробка адаптивних самонавчальних систем, здатних у реальному часі оцінювати динаміку внутрішніх комунікативних процесів та миттєво ідентифікувати потенційні ризики [9, с. 61]. Штучний інтелект поступово трансформується з інструменту реагування на інструмент превентивного попередження загроз.Висновки

Прогнозування інсайдерських загроз на основі алгоритмів обробки природної мови є надзвичайно перспективним міждисциплінарним напрямком досліджень, який поєднує здобутки кібербезпеки, лінгвістики та штучного інтелекту. Запропонований підхід демонструє принципову можливість створення випереджаючих систем виявлення потенційно небезпечних внутрішніх сценаріїв на основі глибокого аналізу комунікативних патернів. Основною перевагою NLP-технологій у контексті інсайдерських загроз є здатність виявляти приховані емоційні та поведінкові індикатори, які традиційними методами ідентифікації майже не визначаються. Водночас успішна реалізація таких систем вимагає постійного вдосконалення алгоритмів, дотримання етичних норм та балансу між забезпеченням безпеки та приватністю співробітників. Подальші дослідження мають бути спрямовані на розвиток гібридних інтелектуальних систем, здатних не лише ідентифікувати ризики, але й прогнозувати та превентивно нівелювати потенційні загрози.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Цвєткова Н.М. Теоретичні основи інформаційної безпеки : монографія. Київ : Освіта України, 2020. 215 с.
2. Бондаренко В.О. Сучасні технології кібербезпеки. Харків : Технологічний центр, 2021. 342 с.
3. Kim J., Park H. Advanced Natural Language Processing in Cybersecurity. New York : Springer, 2019. 256 p.
4. Chen X. Machine Learning Approaches to Insider Threat Detection. London : Academic Press, 2020. 412 p.
5. Мельник Р.А. Алгоритми штучного інтелекту в інформаційній безпеці. Львів : Видавництво Львівської політехніки, 2022. 187 с.
6. Johnson M. Ethical Considerations in AI-driven Security Systems. Cambridge : MIT Press, 2021. 189 p.
7. Петренко С.А. Системи управління інформаційною безпекою. Київ : Кондор, 2020. 276 с.
8. Brown L. Natural Language Processing in Enterprise Security. San Francisco : O'Reilly Media, 2019. 203 p.
9. Литвиненко О.В. Інтелектуальні системи кібербезпеки. Дніпро : Науковий світ, 2021. 265 с.

Пантєлєєв Вадим Олегович — Харківський національний університет радіоелектроніки, аспірант кафедри інфокомунікаційної інженерії імені В.В. Поповського, Харків, Україна; e-mail: vadym.pantelieiev@nure.ua

Науковий керівник: ***Радівілова Тамара Анатоліївна*** — доктор технічних наук, професор, Харківський національний університет радіоелектроніки, професор кафедри інфокомунікаційної інженерії імені В.В. Поповського, Харків, Україна; e-mail: tamara.radivilova@nure.ua

Pantielieiev Vadym — Kharkiv National University of Radio Electronics, Postgraduate Student at the V.V. Popovskyy Department of Infocommunication Engineering, Kharkiv, Ukraine.

Supervisor: ***Radivilova Tamara*** — Doctor of Sciences (Engineering), Professor, Kharkiv National University of Radio Electronics, Professor at the V.V. Popovskyy Department of Infocommunication Engineering, Kharkiv, Ukraine.