УДК 004.056:519.6 DOI https://doi.org/10.35546/kntu2078-4481.2025.1.2.2

В. В. БАНДУРА
кандидат технічних наук, доцент,
завідувачка кафедри інженерії програмного забезпечення
Івано-Франківський національний технічний університет нафти і газу
ORCID: 0000-0003-3143-0946

М. В. КРИХІВСЬКИЙ
кандидат технічних наук, доцент,
доцент кафедри інженерії програмного забезпечення
Івано-Франківський національний технічний університет нафти і газу
ORCID: 0009-0000-3285-4308

В. І. ЧУДИК
студентка кафедри інженерії програмного забезпечення
Івано-Франківський національний технічний університет нафти і газу
ORCID: 0009-0007-7041-198X

ПРОГНОЗУВАННЯ КІБЕРАТАК ЗА ДОПОМОГОЮ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ВИЯВЛЕННЯ АНОМАЛІЙ

У науковій статті В. В. Бандури, М. В. Крихіського та В. І. Чудик «Прогнозування кібератак за допомогою алгоритмів штучного інтелекту виявлення аномалій» розглядається нова модель для ефективного прогнозування кібератак, яка використовує інноваційні методи аналізу та виявлення аномалій. Мета дослідження зосереджена на розробці та впровадженні алгоритмів штучного інтелекту для прогнозування кібератак через виявлення аномалій у кіберпросторі. У сучасному цифровому світі, де обсяг даних і складність мережевих структур постійно зростає, стає критично важливою здатність швидко і точно виявляти потенційні загрози. Використання штучного інтелекту в цій сфері дозволяє не лише автоматизувати процес моніторингу та аналізу даних, але й забезпечити більш високу точність прогнозів.

Основна увага приділяється поєднанню кількох передових технологій штучного інтелекту, зокрема рекурентних нейронних мереж (RNN), механізму уваги, згорткових нейронних мереж (CNN), двонаправлених мереж (Bi-RNN) та трансформерів. Запропонована модель поєднує переваги цих технологій для створення комплексного підходу до виявлення аномалій у великих обсягах даних, зібраних з різних джерел. Використання механізму уваги дозволяє моделі зосереджуватись на найбільш значущих частинах даних, тоді як згорткові нейронні мережі підвищують ефективність обробки просторових залежностей у даних. Двонаправлені мережі забезпечують аналіз даних у двох напрямках, що дозволяє виявляти більш складні патерни та кореляції, а трансформери забезпечують високу ефективність обробки великих послідовностей даних. У результаті, запропонована модель демонструє високу точність прогнозування кібератак та значно зменшує кількість хибно позитивних спрацьовувань, що сприяє підвищенню рівня кібербезпеки та захисту інформаційних систем.

Інтеграція згорткових рекурентних нейронних мереж і трансформерів у єдину модель забезпечує високий рівень адаптивності до нових типів загроз і аномалій, що постійно виникають у кіберпросторі. Модель демонструє стабільну продуктивність навіть при аналізі великих обсягів даних у реальному часі, що є критично важливим для сучасних систем кібербезпеки. Висока точність і швидкість обробки даних робить цю модель практичною та надійною для виявлення кібератак.

Ключові слова: *прогнозування кібератак, згорткова нейронна мережа, механізм уваги, виявлення аномалій.*

V. V. BANDURA
Candidate of Technical Sciences, Associate Professor,
Head of the Department of Software Engineering
Ivano-Frankivsk National Technical University of Oil and Gas
ORCID: 0000-0003-3143-0946

M. V. KRYKHISKYI
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Software Engineering
Ivano-Frankivsk National Technical University of Oil and Gas
ORCID: 0009-0000-3285-4308

V. I. CHUDYK
Student at the Department of Software Engineering
Ivano-Frankivsk National Technical University of Oil and Gas
ORCID: 0009-0007-7041-198X

PREDICTION OF CYBERATTACKS USING ANOMALY DETECTION ARTIFICIAL INTELLIGENCE ALGORITHMS

In the scientific paper by V. V. Bandura, M. V. Krykhiskyi and V. I. Chudyk titled "Prediction of Cyberattacks Using Anomaly Detection Artificial Intelligence Algorithms", a new model for effective cyberattack prediction is examined. This model employs innovative methods for analyzing and detecting anomalies. The research focuses on developing and implementing artificial intelligence algorithms to predict cyberattacks by identifying anomalies in cyberspace. In today's digital world, where data volume and network complexity are continuously increasing, the ability to quickly and accurately identify potential threats becomes critically important. The use of artificial intelligence in this field not only automates the process of data monitoring and analysis but also ensures higher prediction accuracy.

The main focus is on combining several advanced artificial intelligence technologies, such as recurrent neural networks (RNN), attention mechanisms, convolutional neural networks (CNN), bidirectional networks (Bi-RNN), and transformers. The proposed model leverages the advantages of these technologies to create a comprehensive approach to anomaly detection in large volumes of data collected from various sources. The attention mechanism allows the model to focus on the most significant parts of the data, while convolutional neural networks enhance the processing of spatial dependencies in the data. Bidirectional networks enable the analysis of data in both directions, allowing the detection of more complex patterns and correlations, and transformers ensure efficient processing of large data sequences. As a result, the proposed model demonstrates high accuracy in predicting cyberattacks and significantly reduces the number of false positives, contributing to increased cybersecurity and protection of information systems.

The integration of convolutional recurrent neural networks and transformers into a single model provides a high level of adaptability to new types of threats and anomalies that continuously emerge in cyberspace. The model shows stable performance even when analyzing large volumes of real-time data, which is critically important for modern cybersecurity systems. The high accuracy and data processing speed make this model practical and reliable for detecting cyberattacks.

Key words: *cyberattack prediction, convolutional neural network, attention mechanism, anomaly detection.*

Постановка проблеми

Прогнозування кібератак за допомогою алгоритмів штучного інтелекту (ШІ) є новаторським підходом, який має величезний потенціал для покращення кібербезпеки. Використання алгоритмів для виявлення аномалій може значно підвищити здатність виявляти і реагувати на загрози, перш ніж вони завдадуть шкоди.

Кількість кібератак зростає з кожним роком, і вони стають все більш складними та небезпечними. Використання ШІ для виявлення аномалій допомагає вчасно виявляти та запобігати загрозам. Кібератаки можуть призвести до значних фінансових втрат, витоку конфіденційних даних та порушення роботи важливих інфраструктур. Прогнозування та запобігання таким атакам може зменшити ці ризики. ШІ дозволяє автоматизувати процес виявлення аномалій та швидко реагувати на загрози, що значно підвищує ефективність систем кібербезпеки. Кіберзлочинці постійно вдосконалюють свої методи атаки. Використання ШІ допомагає відстежувати нові тенденції та адаптувати захисні механізми до нових загроз.

Проблема прогнозування кібератак базується на необхідності підвищення ефективності кібербезпеки в умовах зростаючої складності та частоти кібератак. Сучасні методи захисту часто не в змозі виявляти та реагувати на нові та складні загрози вчасно, що призводить до значних втрат і порушень у роботі організацій та інфраструктур.

Однією з основних проблем є велика кількість даних, які потрібно аналізувати для виявлення потенційних загроз. Класичні методи аналізу даних не завжди здатні ефективно обробляти такі обсяги інформації та виявляти аномалії, що робить їх вразливими для нових та складних атак. Алгоритми машинного та глибокого навчання можуть використовуватися для автоматизованого аналізу великих масивів даних і виявлення підозрілих активностей, які можуть свідчити про кібератаки.

Ще однією важливою проблемою є швидкість реагування на загрози. В умовах швидко змінюваного кіберландшафту важливо не тільки виявити загрозу, але й швидко зреагувати на неї. ШІ дозволяє автоматизувати процес реагування на інциденти, що значно зменшує час від виявлення до нейтралізації загрози.

Крім того, кіберзлочинці постійно вдосконалюють свої методи атаки, що робить традиційні методи захисту неефективними. ШІ дозволяє адаптувати захисні механізми до нових загроз, використовуючи аналіз поведінки та прогнозування можливих сценаріїв атак.

Отже, проблема прогнозування кібератак за допомогою алгоритмів штучного інтелекту виявлення аномалій є надзвичайно важливою для підвищення кібербезпеки та захисту від нових та складних загроз. Використання ШІ для автоматизованого аналізу даних, швидкого реагування на інциденти та адаптації до нових загроз має великий потенціал для забезпечення безпеки організацій та критичних інфраструктур.

Прогнозування кібератак за допомогою алгоритмів штучного інтелекту (ШІ) виявлення аномалій є динамічною галуззю, яка постійно розвивається. Перспективними нам представляються кілька нових підходів та технологій, які покращать прогнозування кібератак:

1. Використання генеративних змагальних мереж (GANs) для створення синтетичних даних, які можуть бути використані для навчання моделей ШІ, що дозволить покращити точність виявлення аномалій, особливо у випадках, коли реальні дані обмежені або важкодоступні.
2. Використання підсилювального навчання (Reinforcement Learning) для адаптивного виявлення загроз. Цей підхід дозволяє системам ШІ навчатися на основі зворотного зв'язку та постійно вдосконалювати свої методи виявлення загроз.
3. Використання графових нейронних мереж для аналізу поведінкових патернів у мережах. Це дозволяє виявляти складні взаємозв'язки між подіями та прогнозувати можливі атаки на основі цих взаємозв'язків.
4. Використання когнітивних обчислень для створення самонавчальних систем, які можуть адаптуватися до нових загроз та прогнозувати їх на основі аналізу великих обсягів даних.

Ці нові підходи та технології можуть значно покращити ефективність прогнозування кібератак та забезпечити вищий рівень кібербезпеки для організацій та інфраструктур.

Аналіз останніх досліджень і публікацій

Останні дослідження та публікації з прогнозування кібератак за допомогою алгоритмів штучного інтелекту демонструють значний прогрес у цій галузі. У статті [1] представлено нову модель Cuttlefish-based Peephole Long Short Term Memory (CbP-LSTM), яка використовується для прогнозування кіберзагрози захисту даних від атак. Модель показала високу точність у виявленні загроз завдяки попередній обробці даних та використанню функції фільтрації шуму.

У дослідженні [2] розглядаються різні методи машинного навчання, такі як графові нейронні мережі, змагальне навчання, федеративне навчання, пояснюваний штучний інтелект та навчання з підкріпленням. Кожен з цих методів відіграє важливу роль у покращенні виявлення та запобігання кіберзагрозам. Зроблено висновок, що ці передові алгоритми разом підвищують ефективність, точність і прозорість заходів кібербезпеки, забезпечуючи надійний захист від нових кіберзагроз.

У роботі [3] аналізуються моделі прогнозування кібератак на основі машинного навчання та їх ефективність у розширенні можливостей виявлення загроз. Дослідження також розглядає основні проблеми технологій штучного інтелекту, такі як фінансові обмеження та необхідність великої кількості даних для навчання.

Стаття [4] розглядає, як штучний інтелект, включаючи машинне навчання та глибоке навчання, разом з метаевристичними алгоритмами, може покращити виявлення кібератак. Дослідження включає аналіз понад шістдесяти останніх досліджень, що показують ефективність цих методів у виявленні та боротьбі з різними кіберзагрозами.

У роботі [5] розглядаються різні методи машинного навчання, такі як графові нейронні мережі, підсилювальне навчання, федеративне навчання, пояснювальний ШІ та підсилювальне навчання. Кожен з цих методів відіграє важливу роль у покращенні виявлення та запобігання кіберзагрозам.

Формулювання мети дослідження

Мета дослідження зосереджена на розробці та впровадженні алгоритмів ШІ для прогнозування кібератак через виявлення аномалій у кіберпросторі. У сучасному цифровому світі, де обсяг даних і складність мережевих структур постійно зростає, стає критично важливою здатність швидко і точно виявляти потенційні загрози. Використання штучного інтелекту в цій сфері дозволяє не лише автоматизувати процес моніторингу та аналізу даних, але й забезпечити більш високу точність прогнозів.

Дослідження передбачає вивчення різноманітних підходів та алгоритмів для виявлення аномалій, таких як машинне навчання, глибоке навчання, нейронні мережі та інші методи. Основна мета полягає в тому, щоб виявити найефективніші з них для аналізу великої кількості даних у реальному часі, а також для адаптації до нових типів загроз. Важливим аспектом дослідження є також розробка методів зменшення кількості хибних спрацювань та підвищення точності виявлення істинних загроз.

Результати дослідження нададуть нові інструменти для кібербезпеки, які зможуть швидко реагувати на нові виклики та загрози, що постійно виникають у глобальній мережі. Це сприятиме забезпеченню захисту критичної інфраструктури, комерційних та урядових установ, а також особистих даних користувачів.

Викладення основного матеріалу дослідження

Для прогнозування та виявлення кібератак пропонується використовувати рекурентні нейронні мережі (РНМ), що дозволить моделювати часові ряди даних і виявляти аномалії в паттернах трафіку, які можуть свідчити про кібератаку.

Щоб використати РНМ для виявлення кібератак, необхідно спершу підготувати дані. Важливо зібрати відповідні часові ряди мережевого трафіку, які включають нормальні патерни і приклади аномальних подій. Це можуть бути різні типи трафіку, наприклад, HTTP-запити, DNS-запити, дані про з'єднання. Дані повинні бути попередньо оброблені, очищені від шуму та розділені на тренувальну, валідаційну та тестову вибірки.

Наступним кроком є створення моделі РНМ з довготривалу короткотермінову пам'ять. Модель буде складатися з шару вхідних даних, одного або декількох шарів довготривалої короткотермінової пам'яті та вихідного шару. Вхідний шар отримує послідовність даних мережевого трафіку, яка потім передається до наступних шарів для оброблення цих послідовностей, зберігаючи інформацію про попередні стани та виявляючи довгострокові залежності в даних. Вихідний шар дає прогноз, чи є дані аномальними чи ні.

Під час тренування мережа навчається розпізнавати патерни нормального трафіку та відрізняти їх від аномальних. Це робиться шляхом мінімізації функції втрат, яка вимірює різницю між прогнозованими та фактичними значеннями. Тут важливою задачею є вибір оптимальних параметрів моделі, такі як кількість LSTM-нейронів, кількість шарів, швидкість навчання і так далі, щоб досягти високої точності прогнозів.

Після тренування моделі необхідно провести її валідацію та тестування на окремих наборах даних, щоб переконатися у її здатності точно виявляти аномалії. Модель повинна мати високу чутливість (для виявлення всіх потенційних атак) і високу специфічність (для мінімізації помилкових спрацювань). Це може вимагати налаштування порогових значень для визначення аномалій.

Після успішного тестування модель можна впровадити у реальне середовище. Вона буде постійно аналізувати вхідні дані мережевого трафіку у реальному часі і виявляти аномалії, які можуть свідчити про кібератаку. Результати аналізу можуть бути використані для автоматичного реагування на загрози або для інформування фахівців з кібербезпеки для подальшого розслідування і вжиття заходів.

Для удосконалення використання рекурентних нейронних мереж для прогнозування пропонується впровадження механізму уваги (МУ). Механізм уваги дозволить моделі зосереджуватися на найбільш важливих частинах послідовності даних, що значно підвищує точність прогнозів і ефективність обробки довгих послідовностей.

МУ надасть можливість визначати, які частини вхідних даних є найбільш важливими для прогнозу в кожний момент часу. Це особливо корисно при аналізі мережевого трафіку, де деякі події можуть мати більший вплив на загальну картину, ніж інші. Впровадження уваги дозволяє моделі більш ефективно обробляти довгі послідовності даних і поліпшувати виявлення аномалій.

Додатково пропонується використовувати двонаправлені РНМ, які враховують як попередні, так і наступні стани в послідовності. Це дозволяє моделі отримати більш повну інформацію про контекст і підвищує точність прогнозів. Також доцільне використання гібридних моделей, що поєднують RNN з іншими методами машинного навчання, такими як згорткові нейронні мережі або трансформери. Згорткові нейронні мережі слід використовувати для виділення просторових особливостей у даних, а РНМ – для обробки тимчасових залежностей. Це дозволить моделі більш точно аналізувати складні патерни в мережевому трафіку і виявляти потенційні загрози.

Висновки

Дослідження, присвячене прогнозуванню кібератак за допомогою алгоритмів штучного інтелекту виявлення аномалій, демонструє значний потенціал використання рекурентних нейронних мереж з механізмом уваги, двонаправленості та згортковості для підвищення точності та надійності виявлення загроз. У ході дослідження була розроблена модель, яка інтегрує механізм уваги в рекурентних нейронних мереж, що дозволяє ефективніше аналізувати послідовності даних і зосереджуватися на найбільш значущих характеристиках трафіку.

Результати експериментів показали, що поєднання РНМ з механізмом уваги дозволяє значно зменшити кількість хибних спрацювань, а також підвищити точність виявлення аномалій у мережевому трафіку. Це досягається завдяки здатності моделі виявляти довгострокові залежності та враховувати контекстні взаємозв'язки між подіями. Відтак, модель забезпечує високий рівень адаптивності до нових типів загроз і аномалій, що постійно виникають у кіберпросторі.

Впровадження механізму уваги дозволяє підвищити ефективність обробки великих обсягів даних у реальному часі, що є критично важливим для сучасних систем кібербезпеки. Модель демонструє стабільну продуктивність навіть при аналізі складних і насичених даних, що підтверджує її практичну цінність для захисту від кібертак.

Дослідження показало, що використання згорткових рекурентних нейронних мереж дозволяє ефективно виділяти просторові особливості даних, що покращує розуміння структури мережевого трафіку. Завдяки цьому модель може точніше ідентифікувати аномалії, які можуть свідчити про потенційну кібератаку. Водночас, трансформери забезпечують здатність моделі обробляти довгі послідовності даних і враховувати контекстні взаємозв'язки між подіями. Це дозволяє моделі зосереджуватися на найбільш значущих частинах даних, що покращує точність прогнозів.

Інтеграція згорткових рекурентних нейронних мереж і трансформерів у єдину модель забезпечує високий рівень адаптивності до нових типів загроз і аномалій, що постійно виникають у кіберпросторі. Модель демонструє стабільну продуктивність навіть при аналізі великих обсягів даних у реальному часі, що є критично важливим для сучасних систем кібербезпеки. Висока точність і швидкість обробки даних робить цю модель практичною та надійною для виявлення кібератак.

Отже, дослідження вказує на значну перспективу використання алгоритмів штучного інтелекту, зокрема рекурентних нейронних мереж з механізмом уваги, для підвищення ефективності систем виявлення і прогнозування

кібератак. Впровадження цих технологій у реальні середовища сприятиме забезпеченню більш надійного захисту критичної інфраструктури, організацій та особистих даних користувачів від загроз, що постійно еволюціонують.

Список використаної літератури

1. Sharma P., Prasad J.S., Shaheen, Ahamed S.K. An efficient cyber threat prediction using a novel artificial intelligence technique. *Multimedia Tools and Applications*. V. 83. 2024. P. 66757–66773. DOI: https://doi.org/10.1007/s11042-024-18169-0

2. Alshathry N., Carare A.-S.,Galiveeti S., Garg R.,Mehta D. Machine learning algorithms for detecting and preventing cyber threats. *OxJournal*. 2024. URL: https://www.oxjournal.org/machine-learning-algorithms-for-detecting-and-preventing-cyber-threats.

3. Kravchuk N., Korobeinikova T. Machine learning-based cyberattack prediction models and their effectiveness in cybersecurity. *Futurity Proceedings*. V. 1. 2024. DOI: https://doi.org/10.5281/zenodo.14588519

4. Salem A.H., Azzam S.M., Emam O.E., Abohany A.A. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*. V. 11. 1 2024. DOI: https://doi.org/10.1186/s40537-024-00957-y

5. Alshathry N, Carare A.-S., Galiveeti S., Garg R., Mehta D. Machine learning algorithms for detecting and preventing cyber threats. *OxJournal*. 2024. URL: https://www.oxjournal.org/machine-learning-algorithms-for-detecting-and-preventing-cyber-threats/?form=MG0AV3

References

1. Sharma P., Prasad J.S., Shaheen, Ahamed S.K. An efficient cyber threat prediction using a novel artificial intelligence technique. *Multimedia Tools and Applications*. V. 83. 2024. P. 66757–66773. DOI: https://doi.org/10.1007/s11042-024-18169-0

2. Alshathry N., Carare A.-S.,Galiveeti S.,Garg R.,Mehta D. Machine learning algorithms for detecting and preventing cyber threats. *OxJournal*. 2024. URL: https://www.oxjournal.org/machine-learning-algorithms-for-detecting-and-preventing-cyber-threats

3. Kravchuk N., Korobeinikova T. Machine learning-based cyberattack prediction models and their effectiveness in cybersecurity. *Futurity Proceedings*. V. 1. 2024. DOI: https://doi.org/10.5281/zenodo.14588519

4. Salem A.H., Azzam S.M., Emam O.E., Abohany A.A. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*. V. 11. 1 2024. DOI: https://doi.org/10.1186/s40537-024-00957-y

5. Alshathry N, Carare A.-S., Galiveeti S., Garg R., Mehta D. Machine learning algorithms for detecting and preventing cyber threats. *OxJournal*. 2024. URL: https://www.oxjournal.org/machine-learning-algorithms-for-detecting-and-preventing-cyber-threats/?form=MG0AV3