УДК 004.056.5:004.9

О. В. Салієва

О. В. Ніколайчук

Перспективи застосування нейронних мереж у сучасних системах кіберзахисту

Вінницький національний технічний університет

Анотація. *У даній роботі розглянуто перспективи застосування нейронних мереж у сучасних системах кіберзахисту. Проаналізовано потенціал нейронних мереж у виявленні, аналізі та протидії кіберзагрозам, а також виокремлено основні виклики і перспективи подальшого розвитку досліджуваної тематики.*

Ключові слова: нейронні мережі, кіберзахист, кіберзагрози, інформаційна безпека.

Abstract. *This paper examines the prospects of using neural networks in modern cybersecurity systems. The potential of neural networks in detecting, analyzing, and countering cyber threats is analyzed, and the main challenges and prospects for further development of the researched topic are identified.*

Keywords: neural networks, cybersecurity, cyber threats, information security.

Вступ

У сучасному цифровому світі, де кіберзагрози стають все більш складними та небезпечними, захист інформаційних систем стає однією з найбільш актуальних та нагальних задач. Зростання кількості та складності кібератак вимагає вдосконалення захисних механізмів і стратегій. Нейронні мережі є потужним інструментом, який може значно посилити кіберзахист. Їхня здатність навчатися на великих обсягах даних та розпізнавати складні патерни робить їх ідеальними для виявлення нових та невідомих загроз. У цьому контексті нейронні мережі виступають як потенційно перспективний інструмент кіберзахисту, здатний ефективно виявляти, аналізувати та блокувати загрози.

Результати дослідження

Нейронні мережі відкривають перед сучасними системами кіберзахисту нові перспективи та можливості, що надзвичайно важливо в умовах постійної еволюції кіберзагроз. Їхня унікальна здатність до самонавчання та адаптації дозволяє аналізувати великі обсяги даних та виявляти складні аномальні патерни поведінки, які можуть свідчити про потенційні загрози безпеці.

Підходи, що базуються на нейронних мережах, надають змогу системам кіберзахисту оперативно реагувати на нові, раніше невідомі загрози, забезпечуючи важливий елемент превентивної стратегії захисту. Крім того, використання нейронних мереж в системах кіберзахисту може покращити процеси ідентифікації та класифікації кіберзагроз, що сприятиме збільшенню швидкості та точності реакції на потенційні загрози. Наприклад, за допомогою нейронних мереж можна ефективно виявляти шкідливі програми, розпізнавати фішингові атаки та ідентифікувати аномальні зміни в мережевому трафіку, що раніше могло залишитися непоміченим.

Розглянемо види задач, які можна розв’язувати методами штучного інтелекту [1]:

- регресія (або прогноз);
- класифікація;
- кластеризація;
- правила пошуку асоціацій – завдання рекомендувати щось на основі попереднього досвіду;
- зменшення розмірності – узагальнення, завдання пошуку найважливіших ознак у ряді зразків;
- генеративні моделі – завдання створення нового на основі попередніх знань про розподіл.

На основі вирішення цих задач можна вдосконалювати технічні системи, стратегії кібербезпеки та впроваджувати новітні технології, такі як штучний інтелект та машинне навчання, для підвищення рівня захисту від кіберзагроз.

Розглянемо основні методи машинного навчання [2]:

- supervised learning (навчання з «учителем»). Умова – розмічені дані із вказівкою, на основі яких приймається рішення про нові дані;
- ensemble learning – розширення простих моделей для одержання більш ефективної складної;
- навчання без «учителя» – підхід, який використовується при відсутності розмічених даних, і при цьому модель повинна розмітити їх самостійно, базуючись на певних властивостях;
- навчання з підкріпленням (reinforced learning) – підхід, орієнтований на зворотний зв’язок від середовища;
- active learning – підклас навчання із підкріпленням, коли «учитель» допомагає виправляти

поведінку додатково до зміни середовища.

Кожен з цих методів має свої переваги і обмеження, та їх комбінація може забезпечити оптимальний результат у боротьбі з кіберзагрозами. Такий різноманітний підхід до машинного навчання дозволяє системам кіберзахисту ефективно адаптуватися до змін у кіберпросторі та надійно захищати інформаційні ресурси від різноманітних атак.

Додатковою перевагою використання нейронних мереж у кіберзахисті є їхня здатність до виявлення атак нульового дня – вразливостей програмного забезпечення, які використовують зловмисники до того, як постачальник дізнається про її існування. Це робить уразливість нульового дня серйозною загрозою кібербезпеці [3].

Нейронні мережі можуть ефективно протистояти атакам нульового дня завдяки їх здатності до навчання на основі нових даних і адаптації до змін у кіберсередовищі. Вони можуть виявляти аномальні патерни, які вказують на потенційні загрози, навіть якщо ці загрози раніше не були відомі. Нейронні мережі забезпечують оперативну реакцію на зміни у кіберпросторі та адаптуються до нових атак, що дозволяє їм надійно захищати системи від атак нульового дня та інших кіберзагроз [4].

Крім того, використання нейронних мереж у кіберзахисті може сприяти розвитку адаптивних захисних стратегій, які змінюються залежно від поточного стану загрози та контексту дії. Такий підхід дозволяє забезпечувати ефективний захист навіть у найбільш динамічних та непередбачуваних середовищах. Також нейронні мережі здатні працювати в режимі реального часу, що дозволяє виявляти та реагувати на загрози миттєво, зменшуючи час реакції та максимізуючи ефективність захисних заходів [5].

Штучний інтелект може автоматично збирати, обробляти та аналізувати дані з різноманітних джерел, пов’язаних, зокрема з інформаційною безпекою: логи подій, результати аудиту, сповіщення систем безпеки, звіти про інциденти тощо. Алгоритми машинного навчання та нейромережі ефективно виявляють у таких даних патерни, кореляції та аномалії, що можуть сигналізувати про вразливості системи, спроби кібератак та інші проблеми. Штучний інтелект здійснює такий аналіз в десятки разів швидше і точніше за людину [6].

Таким чином, використання нейронних мереж у сучасних системах кіберзахисту відкриває нові можливості у забезпеченні безпеки інформаційних систем та захисту конфіденційної інформації від кіберзагроз.

Висновки

Отже, нейронні мережі виявляються потужним інструментом у боротьбі з кіберзагрозами. Вони демонструють здатність до навчання та адаптації до змін у кіберсередовищі, що дозволяє оперативно реагувати на загрози та забезпечує надійний рівень захисту інформаційних систем. Крім того, їхня можливість працювати в режимі реального часу дозволяє оперативно виявляти та реагувати на загрози, максимізуючи ефективність захисту та забезпечуючи безпеку інформаційних систем від кібератак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Богом’я В.І. Особливості використання штучного інтелекту та машинного навчання для виявлення та запобігання кібератак: Водний транспорт, 2023. 336 с.
2. Новіков Олексій Миколайович, Стьопочкіна Ірина Валеріївна, Методи штучного інтелекту в кібербезпеці Київ КПІ ім. Ігоря Сікорського 2022 С. 7
3. ITEDU\\BLOG – Zero day: що таке вразливість нульового дня? URL: https://itedu.center/ua/blog/articles/zero-day/
4. Осіпов Я.В., Світличний В.А. Атака нульового дня (n-day attack). що це і як з цим боротися?, Харків, 2018 307 с.
5. Летичевський О.О. Сучасні наукові проблеми кібербезпеки. Вісник НАН України. 2023. № 2. С. 12—20.
6. WEZOM – Застосування ШІ у кібербезпеці: роль та переваги. URL:https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi

Салієва Ольга Володимирівна − доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Ніколайчук Олександр Вікторович – студент групи УБ-21б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: oleksandernikol@gmail.com

Saliieva Olha V. − Doctor of Philosophy (PhD) in 125 "Cybersecurity", Senior Lecturer, Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@vntu.edu.ua

Nikolaichuk Oleksandr Viktorovich – student of the UB-21b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksandernikol@gmail.com