УДК 004.896.2:006.3 https://doi.org/10.30837/IYF.PCEIP.2024.137

РОЗВИТОК ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

Павлов О.А.
Науковий керівник – доц. Шаповалова А.С.
Харківський національний університет радіоелектроніки,
каф. інфокомунікаційної інженерії імені В.В. Поповського,
м. Харків, Україна
e-mail: Oleksii.pavlov2@nure.ua.

Artificial Intelligence (AI) is transforming cybersecurity, aiding in threat detection and response. This article explores AI's role in enhancing cybersecurity, utilizing machine learning to analyze vast data sets, identify patterns, and automate threat detection. While offering benefits like improved detection and real-time response, challenges include algorithm complexity and the potential misuse of AI by cybercriminals. Despite these challenges, the efficiency gains and evolving cyber threats highlight the indispensable role of AI in safeguarding digital assets.

Штучний інтелект останні роки отримав величезний розвиток в багатьох галузях, одним з основних направлень, та найважливіший є кібербезпека. В умовах постійного вдосконалення та зростання кількості та якості кібератак та загроз кібербезпеці штучний інтелект став одним з важливих інструментів для вдосконалення кібербезпеки.

Штучний інтелект у кібербезпеці передбачає саме використання алгоритмів машинного навчання та інших технологій для виявлення, реагування та запобігання кіберзагроз. Головним завданням штучного інтелекту є саме аналізування величезних обсягів даних, виявлення закономірностей та навчання на них, для того що б в подальшому виявляти потенційні загрози та аномалії. Кінцевою задачею є автоматизація процесу виявлення та реагування на загрози, що дозволяє команді кібербезпеки швидше реагувати на загрози та запобігати порушенням.

Моделі штучного інтелекту використовують методи машинного навчання як для аналізу поведінки самої мережі, так і для постійного виявлення аномалій. З часом моделі корегуються та проходять адаптацію, для того що б підвищити швидкість та точність виявлення як аномалій так і потенційних загроз безпеці. Саме здатність штучного інтелекту до самостійного корегування та адаптації забезпечує компаніям потужний та надійний захист у кібербезпеці, який здатний швидко та чітко реагувати на нові загрози.

Переваги використання штучного інтелекту для кібербезпеки:

1. Швидке та чітке виявлення загроз - традиційні та більш застарілі методи в кібербезпеці використовують підписи та конкретні правила для виявлення загроз. Одна штучний інтелект інтегрований в методи кібербезпеки

може виявляти нові та невідомі загрози, аналізувати з аномальною швидкістю великі обсяги даних і виявляти певні закономірності, які можуть ідентифікуватися як зловмисна активність.

2. Реагування в режимі реального часу на загрози - інструменти кібербезпеки на основі штучного інтелекту можуть реагувати на загрози набагато швидше, ніж традиційні методи, що дозволяє стороні безпеки вживати негайних заходів та запобігати порушенням.

3. Зменшення проценту хибних показників реагування - більш традиційні методи безпеки часто не вірно реагують на індикатори у системі, що призводить до підвищеної трати ресурсів та зниження ефективності.

4. Підвищення ефективності роботи - інструменти на основі штучного інтелекту можуть автоматизувати більшість процесів, пов’язаних з виявленням та реагуванням на загрози, дозволяючи командам зосередитись на більш важливих цілях.

Недоліки інтеграції штучного інтелекту в кібербезпеці:

1. Проблема прозорості - інструменти на основі штучного інтелекту здебільшого використовують складні алгоритми, що ускладнює розуміння та аналіз того, як саме робляться висновки. Така непрозорість у результатах ускладнює довіру до результатів, що у подальшому може призвести до хибних викликів та тривог.

2. Штучний інтелект як інструмент для злочинців - проблематика штучного інтелекту в тому, що його можуть використовувати злочинці для покращення кіберзлочинів, що призводить до більш складних та потенційно вдалих атак.

3. Конфіденційність даних - штучний інтелект для навчання потребує доступу до велики обсягів даних, які можуть містити конфіденційну інформацію компанії, тому важливо, що б інформація була надійно захищена.

Майбутнє в кібербезпеці напряму пов’язане зі штучного інтелекту, особливо з урахуванням прогресії зростання кількості та якості нових атак та потенційних загроз. Штучний інтелект може використовуватись в боротьбі з різними видами атак пов’язаних з соціальною інженерією, шкідливим програмним забезпеченням та інші.

Сила ШІ полягає в його здатності до безперервного навчання, що перевершує ручні методи виявлення, які використовуються людьми-експертами; його ефективність у запобіганні кібератакам не має собі рівних, оскільки моделі ШІ постійно адаптуються до нових загроз.

Список використаних джерел:

1. Parisi A. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies / Alessandro Parisi., 2019. – 342 с.