УДК 004.8:004.056

ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМАХ ОБРОБКИ ТА ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Макаренко Д. В.
dimamakar188@gmail.com
Черкаський державний фаховий бізнес-коледж
Бреус Р. В.
м. Черкаси, Україна

Генеративний штучний інтелект стрімко розвивається і дедалі активніше використовується у сфері обробки та захисту інформаційних ресурсів. Сучасні алгоритми здатні не лише аналізувати великі масиви даних, але й генерувати новий контент, моделі поведінки, сценарії кіберзагроз або варіанти рішень для їх запобігання. Завдяки цьому генеративні моделі стають важливим інструментом у системах інформаційної безпеки.

Ідея автоматизованого аналізу інформації виникла задовго до появи сучасного генеративного штучного інтелекту. Традиційні системи кібербезпеки базувалися переважно на сигнатурному аналізі, тобто порівнянні підозрілих дій або файлів із заздалегідь відомими шаблонами загроз. Хоча цей підхід був ефективним для виявлення відомих атак, він мав суттєві обмеження, зокрема, нові або модифіковані загрози часто залишалися непоміченими. Поява машинного навчання дала можливість системам безпеки самостійно виявляти аномалії в мережевому трафіку та поведінці користувачів. Порівняння підходів до забезпечення інформаційної безпеки показано в табл.1.

Генеративний штучний інтелект став наступним етапом розвитку цих технологій. На відміну від класичних моделей машинного навчання, які здебільшого виконують класифікацію або прогнозування, генеративні моделі здатні створювати нові дані на основі вивчених закономірностей. У контексті інформаційної безпеки це дозволяє моделювати можливі сценарії атак, створювати синтетичні набори даних для навчання систем захисту та тестувати стійкість інформаційних систем до нових типів загроз.

Технічною основою генеративного штучного інтелекту є глибокі нейронні мережі, які навчаються на великих масивах даних. Серед найбільш поширених підходів – генеративні змагальні мережі, Variational Autoencoder та трансформерні моделі. Генеративні змагальні мережі працюють за принципом змагання двох нейромереж, у яких одна генерує дані, а інша оцінює їхню достовірність.

Одним із важливих напрямів використання генеративного штучного інтелекту є виявлення аномалій. Наприклад, система може виявити незвичайну активність у мережі, спробу несанкціонованого доступу або аномальні зміни у файлах. Крім того, аналізуючи великі обсяги даних, такі системи можуть виявляти можливі загрози та пропонувати варіанти їх усунення [1].

Дослідники можуть застосовувати генеративний штучний інтелект для створення синтетичних даних, що допомагає безпечно вивчати поведінку шкідливого програмного забезпечення та вдосконалювати біометричні системи захисту [2]. Багато організацій вже використовують штучний інтелект для аналізу загроз і оцінки вразливостей [3].

Зловмисники можуть застосовувати такі технології для створення фішингових повідомлень, підроблених документів, deepfake-контенту або автоматизованих атак. Генеративні моделі здатні формувати переконливі тексти та імітувати стиль реальних людей, що підвищує ефективність соціальної інженерії. Зокрема, попри зростання рівня автоматизації, системи безпеки потребують постійного контролю з боку фахівців, щоб уникнути помилок і зловживань [4].

Однією з ключових проблем є здатність генеративних моделей створювати неточну або оманливу інформацію , що може призвести до неправильного аналізу загроз і прийняття хибних рішень [5].

Системи на основі генеративного штучного інтелекту можуть не лише виявляти загрозу, але й пропонувати або навіть автоматично виконувати заходи з її нейтралізації. Наприклад, система може ізолювати заражений вузол мережі, заблокувати підозрілу активність або змінити політику доступу до ресурсів.

Використання генеративного штучного інтелекту також пов’язане з етичними та правовими питаннями. Необхідно забезпечити прозорість роботи алгоритмів, захист персональних даних та відповідальність за прийняті автоматизованими системами рішення.

Таблиця 1 – Порівняння підходів до забезпечення інформаційної безпеки

№	Характеристика	Традиційні системи безпеки	Системи на основі машинного навчання	Системи на основі генеративного штучного інтелекту
1	Принцип роботи	Використання сигнатур і правил для виявлення відомих загроз	Аналіз поведінки та статистичних закономірностей у даних	Генерація нових сценаріїв атак та моделей поведінки
2	Тип загроз, що виявляються	Переважно відомі загрози	Відомі та деякі нові аномалії	Відомі, нові та потенційні майбутні сценарії атак
3	Необхідність оновлення	Часте оновлення сигнатур	Потрібне перенавчання моделей	Самонавчання та генерація нових даних для навчання
4	Робота з даними	Порівняння з базою шаблонів	Аналіз великих масивів даних	Генерація синтетичних даних та моделювання загроз
5	Автоматизація	Низький рівень	Середній рівень	Високий рівень автоматизації та адаптації
6	Основні переваги	Простота та швидкість виявлення відомих атак	Виявлення аномалій	Прогнозування та моделювання нових атак
7	Основні недоліки	Не виявляє нові загрози	Потребує великих наборів даних	Можливі помилки генерації та ризик зловживань

У результаті проведеного дослідження встановлено, що генеративний штучний інтелект є перспективним інструментом у системах обробки та захисту інформаційних ресурсів. На відміну від традиційних підходів, він дозволяє не лише виявляти відомі загрози, а й моделювати нові сценарії атак, виявляти аномалії. Разом із тим використання генеративного штучного інтелекту пов’язане з певними ризиками, зокрема можливістю генерації неточної інформації та використанням цих технологій зловмисниками. Тому його

впровадження потребує поєднання автоматизованих рішень із контролем з боку фахівців.

Список використаних джерел:

1. Generative AI in Cybersecurity: Balancing Innovation and Risk. URL: https://cert.europa.eu/publications/security-guidance/generative-ai-in-cybersecurity-balancing-innovation-and-risk/ (дата звернення: 13.03.2026).
2. What Is Generative AI in Cybersecurity? URL: https://www.paloaltonetworks.com/cyberpedia/generative-ai-in-cybersecurity (дата звернення: 14.03.2026).
3. What Is Generative AI in Cybersecurity? URL: https://www.sentinelone.com/cybersecurity-101/data-and-ai/generative-ai-cybersecurity/ (дата звернення: 13.03.2026).
4. How Can Generative AI Be Used In Cybersecurity? (Ultimate Guide) URL: https://www.eweek.com/artificial-intelligence/generative-ai-and-cybersecurity/ (дата звернення: 14.03.2026).
5. Generative AI in cybersecurity. URL: https://www.capgemini.com/insights/research-library/generative-ai-in-cybersecurity/ (дата звернення: 13.03.2026).