

УДК 621

Лізунов С.І.¹, Верещака М.П.², Філобок Є.В.²

¹ доц. НУ «Запорізька політехніка»

² асп. гр. А-172-12 НУ «Запорізька політехніка»

МЕТОДИ ПРОТИДІЇ ВІРУСАМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект (ШІ) суттєво трансформує сучасний світ, стимулюючи розвиток технологій у різних сферах, таких як медицина, логістика, автомобільна індустрія та кібербезпека. Однак, поряд з позитивними змінами, ШІ може також використовуватись у злочинних цілях, особливо в кіберпросторі. Одним із загрозливих наслідків його застосування

є поява нових типів комп'ютерних вірусів. Віруси, створені за допомогою ШІ, здатні до самонавчання, адаптації до захисних систем і автоматичної зміни свого коду, що ускладнює їх виявлення та нейтралізацію.

Адаптивні віруси є новітніми загрозами у сфері комп'ютерної безпеки, які використовують штучний інтелект для підвищення своєї ефективності та уникнення виявлення. Головна особливість таких вірусів полягає в здатності адаптуватися до змін у системі та заходів захисту, що ускладнює їхнє виявлення та ліквідацію. ШІ дозволяє їм автоматично аналізувати поведінку системи, виявляти вразливі місця та модифікувати свій код для обходу антивірусних програм. Наприклад, ці віруси можуть змінювати свою кодову структуру під час розповсюдження [1], щоб уникнути сигнатурного виявлення. Їхня здатність до самонавчання та еволюції, використання даних про систему для вдосконалення атак і підвищення захисту від виявлення робить адаптивні віруси особливо небезпечними.

Віруси зі змінним шифруванням (або поліморфні віруси) складні для виявлення завдяки здатності змінювати код під час кожного зараження [2]. Ці віруси використовують різні методи шифрування свого основного коду, роблячи кожен нову версію унікальною. Під час кожного інфікування вони генерують нову версію з іншим ключем шифрування, що дозволяє уникнути виявлення за сигнатурою. При цьому ядро вірусу залишається незмінним, виконуючи свою шкідливу дію після розшифровки. Поліморфні віруси часто використовують ШІ для автоматизації та оптимізації процесу шифрування, що ускладнює їх ідентифікацію антивірусними системами.

Генеративно-змагальні мережі (GAN) — це потужний інструмент ШІ, здатний створювати дані, схожі на вихідні, завдяки взаємодії генератора і дискримінатора. У контексті комп'ютерних вірусів GAN може генерувати нові, унікальні зразки шкідливого програмного забезпечення (ПЗ), які обходять системи виявлення. Генератор створює модифіковані версії вірусів, які виглядають легітимно, а дискримінатор навчається відрізняти справжні віруси, допомагаючи генератору вдосконалювати техніки маскування. GAN можуть також застосовуватися для створення поліморфних або мутаційних вірусів, які постійно змінюють код і таким чином уникати детекції.

Фішингові атаки на основі обробки природної мови (NLP) стають все більш популярними завдяки можливостям ШІ. NLP дозволяє створювати персоналізовані та переконливі повідомлення, які важко відрізнити від справжніх. Основні техніки включають адаптацію мови під стиль спілкування жертви, автоматичне генерування персоналізованих повідомлень для багатьох цілей і імітацію діалогу через чатботи, що переконують користувача надати конфіденційну інформацію. Також NLP дозволяє використовувати соціальну інженерію для маніпуляцій, апелюючи до емоцій або побоювань жертви.

Ботнети, які об'єднують в мережу заражені пристрої, отримали новий рівень автономності завдяки ШІ. Замість постійного контролю кіберзлочинцями, ботнети з ШІ можуть працювати автономно, приймаючи рішення та адаптуючись до обставин. Основні риси таких ботнетів: здатність до адаптивного навчання та аналізу середовища, що дозволяє підлаштовувати атаки; автономне управління, що дає змогу уникати централізованих команд; ефективне маскування, яке ускладнює виявлення; а також використання децентралізованих мереж для зниження залежності від командного центру.

Традиційні антивірусні програми використовували сигнатурний метод для виявлення шкідливого ПЗ порівнюючи файли із заздалегідь відомими зразками вірусів. Проте з появою складніших та динамічних загроз, таких як поліморфні та метаморфічні віруси, цей підхід втрачає свою ефективність. Антивірусні системи на основі ШІ здатні виявляти нові загрози завдяки алгоритмам машинного навчання, що аналізують поведінкові патерни програм [3]. Використовуючи глибокі нейронні мережі, ці системи можуть розпізнавати аномалії та небезпечну поведінку навіть у випадках, коли загроза ще не була класифікована.

Динамічний аналіз у пісочницях (sandboxing) є ключовим методом для виявлення та дослідження комп'ютерних вірусів, створених із використанням ШІ. Цей підхід дозволяє ізолювати підозрілі програми в контрольованому середовищі, де вони можуть виконуватись без загрози для основної операційної системи чи інших додатків.

Сьогодні хмарні технології набувають популярності у сфері кібербезпеки, пропонуючи інноваційні підходи до захисту від комп'ютерних вірусів, зокрема тих, які створюються за допомогою ШІ. Хмарні рішення забезпечують централізований контроль загроз і можливість активної протидії, що дозволяє організаціям оперативно реагувати на нові виклики. Один з ключових аспектів хмарної безпеки полягає у використанні розподілених систем для виявлення та блокування шкідливого ПЗ. Ці системи аналізують великі обсяги даних у реальному часі, що дає змогу ідентифікувати аномалії в поведінці користувачів і пристроїв. Завдяки алгоритмам машинного навчання та ШІ хмарні рішення можуть адаптуватися до нових загроз, навчатись на історичних даних і підвищувати свою ефективність з часом.

Сучасні системи захисту часто виявляються недостатньо ефективними проти адаптивних і самонавчальних загроз. Тому вкрай необхідно розробляти нові стратегії та інструменти для протидії вірусам, створеним за допомогою ШІ. Дослідження передових методів захисту, таких як антивірусні системи з використанням ШІ, поведінковий аналіз, динамічний аналіз у пісочницях та інші інноваційні підходи, є ключовими для забезпечення ефективного кіберзахисту в умовах сучасних загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cybersecurity challenges in the age of AI: Theoretical approaches and practical solutions [Електронний ресурс]. – Режим доступу: <https://fepbl.com/index.php/csitrj/article/view/930/1144>
2. О.С. Саприкін, Models and methods for diagnosing Zero-Day threats in cyberspace, Вісник Сучасних Інформаційних Технологій. 4 (2021) [Електронний ресурс]. – Режим доступу: <https://hait.od.ua/index.php/journal/article/download/107/160/95>
3. Machine learning in cybersecurity: A review of threat detection and defense mechanisms [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/378208150_Machine_learning_in_cybersecurity_A_review_of_threat_detection_and_defense_mechanisms.