ШТУЧНИЙ ІНТЕЛЕКТ У ЗАХИСТІ МЕРЕЖ ВІД АТАК ТИПУ ZERO-DAY: ПОТЕНЦІАЛ ТА ВИКЛИКИ

Мирончук Я.[1], Світличний В.[1]

Харківський національний університет внутрішніх справ

Вступ

У сучасному світі кібербезпека стає одним з найважливіших аспектів захисту інформаційних систем від все більш складних та витончених загроз. Однією з найнебезпечніших форм кібератак є атаки типу zero-day (уразливість нульового дня), що використовують невідомі вразливості програмного забезпечення або апаратних систем. Ці атаки характеризуються тим, що до моменту їх використання зловмисниками розробники не мають змоги вчасно випустити патч або оновлення для виправлення уразливості, що робить системи беззахисними [1]. Традиційні засоби захисту, такі як антивірусні програми та фаєрволи, часто не можуть виявити такі загрози, оскільки вони орієнтовані на відомі сигнатури або патерни атак.

Основна частина

Етичні та юридичні аспекти застосування нейромереж у кібербезпеці стоять на передньому плані серед найбільш вагомих і комплексних проблем. Прозорість роботи алгоритмів, забезпечення захисту інформації, контроль над ризиками автоматизації та моральна відповідальність — ключові фактори, що вимагають пильної уваги з боку фахівців з розробки, кінцевих споживачів та органів регулювання. У майбутньому значення етичних принципів та правових рамок у сфері кіберзахисту тільки зростатиме, а розвиток штучного інтелекту диктуватиме необхідність у впровадженні нових стратегій управління технологіями та охорони прав людини.

Одним з ключових векторів прогресу стає застосування глибинних нейронних мереж (DNN, Deep Neural Networks) для побудови досконаліших та більш точних моделей виявлення загроз. Завдяки властивості опрацьовувати значні масиви інформації та самостійно здобувати знання, DNN мають потенціал ідентифікувати нові типи атак, зокрема атаки нульового дня (zero-day attacks), що є недосяжним для традиційних сигнатурних систем. Скажімо, DNN здатні здійснювати аналіз великих обсягів інформації в режимі реального часу, що є критично необхідним для сучасного кіберзахисту [2].

До того ж, 2024 рік відзначився збільшенням кількості вразливостей нульового дня (zero-day) у таких браузерах, як Chrome та Edge. Зловмисники активно використовували їх, вдаючись до дедалі складніших тактик. Chrome, зокрема, зазнав впливу кількох вкрай серйозних вразливостей, зокрема CVE-2024-7971. Ця вразливість була пов'язана з механізмом JavaScript V8. Це дозволяло хакерам дистанційно виконувати шкідливий код, отримуючи доступ до корпоративних систем та конфіденційних даних, ще до того, як були випущені виправлення. Наслідки були значними: компанії, що активно використовують веб-платформи, зазнали збоїв, витоків даних та дорогого відновлення. Це наголошує на критичності наявності надійних превентивних заходів захисту до того, як такі вразливості стануть об’єктом атак [3].

Платформи GenAI, такі як ChatGPT та Midjourney, перевернули робочий процес, але 2024 рік продемонстрував їх потенційну небезпеку при роботі з конфіденційною інформацією. Згідно з доповіддю CybSafe, майже 40 відсотків респондентів зізналися у розповсюдженні конфіденційних бізнес-даних через інструменти штучного інтелекту, часто не усвідомлюючи супутніх ризиків.

Під час масового витоку даних, пов’язаного з ChatGPT у жовтні 2024 року, понад 225 000 облікових записів були скомпрометовані внаслідок атаки шкідливого програмного забезпечення. Ці події служать тривожним сигналом щодо нагальної потреби в належних заходах безпеки при

інтеграції ШІ в бізнес-процеси. Для захисту від атак нульового дня застосовують:

1. Windows Defender Exploit Guard. Вбудований захисний механізм Windows 2010. Здатний виконувати роль першої лінії оборони, що протистоїть атакам нульового дня.

2. Антивірус наступного покоління (NGAV). Здійснює аналіз загроз та спостереження за поведінкою, використовуючи машинне навчання і специфічні прийоми для захисту від експлойтів. Традиційні антивірусні програми не надто ефективні проти загроз нульового дня, оскільки останні використовують відомі слабкі місця в програмному забезпеченні.

3. Своєчасне оновлення. Автоматизовані засоби не тільки допомагають організаціям виявляти системи, які потребують оновлення, але й сприяють оперативному отриманню патчів та їхньому швидкому впровадженню, перш ніж зловмисники зможуть здійснити атаку [4].

Висновок

Атаки типу zero-day є одними з найсерйозніших загроз у кібербезпеці, оскільки використовують невідомі вразливості, які не можуть бути виправлені вчасно. Традиційні методи захисту часто не ефективні, тому важливим є застосування штучного інтелекту та нейронних мереж для виявлення таких атак. Разом із технологічними інноваціями виникають етичні та юридичні питання, зокрема щодо прозорості алгоритмів та захисту конфіденційності. Так як зловмисники використовують дедалі складніші тактики, важливо впроваджувати надійні системи захисту, своєчасно оновлюючи програмне забезпечення. Вдосконалення технічних та етичних аспектів є необхідним для ефективного захисту від атак нульового дня.

Список використаних джерел

1. Атака нульового дня. ESET Online Help. URL: https://help.eset.com/glossary/uk-UA/zero_day.html.

2. Suman, Kashyap. The Influence of Artificial Intelligence on Cybersecurity. International Journal of Innovative Research in Computer and Communication Engineering, 2024. doi: 10.15680/ijircce.2024.1203503.

3. Небезпеки для браузерів через штучний інтелект і вразливості нульового дня. *B2B Cyber Security*. URL: https://b2b-cyber-security.de/uk/gefahren-fuer-browser-durch-ki-und-zero-day-schwachstellen/.

4. Що таке вразливість нульового дня: zero day - IT Education Blog. IT Education Center Blog. URL: https://itedu.center/ua/blog/articles/zero-day/?srsltid=AfmBOoo64t5c-MrPVirgVivM_zr_O02w9-hpYSDulMZezMLwI98z10MW.