Незважаючи на ефективність проаналізованих підходів, існує потреба у подальших дослідженнях. Еволюція тактик атак, специфічність різних архітектур ВММ, обчислювальна складність існуючих рішень та поява нових векторів загроз вимагають розробки більш адаптивних, універсальних та обчислювально ефективних методів захисту ВММ.

1. OWASP Top 10 for LLM Applications 2025. URL: https://tinyurl.com/579xcepd (дата звернення: 22.04.2025).
2. Alexander Robey, Eric Wong, Hamed Hassani, George J. Pappas., SMOOTHLLM: Defending Large Language Models Against Jailbreaking Attacks, 2024. p 8-13.
3. Aounon Kumar, Certifying LLM Safety against Adversarial Prompting, 2025. 18p.

Моделі оцінювання залишкового ризику в інформаційних системах

УДК 004.056.53
Юлія Хохлачова
Державний торговельно-економічний університет,
yuliiahohlachova@gmail.com

Оцінювання залишкового ризику передбачає аналіз взаємодії кіберзагроз із засобами захисту інформації. Основні підходи до моделювання залишкового ризику включають [1, 2]:

- ймовірнісні моделі, які визначають ризик як ймовірність успішної реалізації загроз при існуючих механізмах захисту;
- детерміновані моделі, що базуються на аналізі вразливостей системи та рівня її захисту;
- гібридні моделі, які поєднують ймовірнісні підходи та експертні оцінки.

Доступність інформаційних ресурсів є критичною характеристикою безпеки ІС. Запропонована модель оцінює рівень ризику шляхом аналізу [3, 4]:

- інтенсивності атак типу DoS/DDoS;
- надійності механізмів розподілу навантаження;
- швидкості виявлення та реагування на інциденти.

Ймовірність порушення доступності (P) визначається як сукупність впливу атак (A), ефективності механізмів захисту (Z) та часу відновлення (T):

P=AZ×TP = \frac{A}{Z \times T}.

Чим більша величина P, тим вищий рівень залишкового ризику для доступності ІС.

Практичне застосування розроблених моделей:

1. Оцінювання моделі забезпечення доступності функціонування інформаційних систем на основі залишкового ризику

Модель оцінювання залишкового ризику використовується для аналізу загроз доступності інформаційних ресурсів у системах, зокрема для визначення ймовірності порушення доступності через різні атаки або збої. Основна мета — оцінити залишковий ризик та сформувати стратегії його мінімізації.

2. Оцінювання моделі забезпечення цілісності ресурсів інформаційних систем на основі залишкового ризику. Ця модель оцінювання залишкового ризику використовується для аналізу загроз цілісності інформації в інформаційних системах (ІС). Вона дозволяє визначити ймовірність порушення цілісності даних через несанкціоновану модифікацію, знищення або спотворення інформації.

3. Оцінювання моделі забезпечення конфіденційності ресурсів інформаційних систем на основі залишкового ризику. Ця модель оцінювання залишкового ризику використовується для аналізу загроз конфіденційності інформації в інформаційних системах (ІС). Вона дозволяє оцінити ймовірність порушення конфіденційності через несанкціонований доступ, витік даних або подолання криптографічного захисту.

Для оцінки ефективності запропонованих моделей було проведено тестування на прикладі корпоративної інформаційної системи. Експериментальні результати показали:

- використання моделі оцінювання залишкового ризику дозволило виявити критичні точки у системі безпеки;
- оптимізація механізмів захисту знизила залишковий ризик доступності на 30%, цілісності – на 25%, конфіденційності – на 40%.

Запропоновані моделі можуть бути використані для підвищення ефективності систем кіберзахисту в державних установах, комерційних компаніях та критичних інфраструктурах.

Було представлено нові моделі оцінювання залишкового ризику в інформаційних системах, які дозволяють більш точно визначати рівень загроз та оптимізувати заходи кібербезпеки. Практичне застосування моделей демонструє їхню ефективність для оцінки стану захищеності інформаційних ресурсів та розробки стратегії кіберзахисту. Перспективи подальших досліджень включають удосконалення методик оцінювання ризику та інтеграцію запропонованих моделей у системи моніторингу інформаційної безпеки.

1. ISO/IEC 27005:2018. Information security risk management.
2. NIST Special Publication 800-30. Guide for Conducting Risk Assessments.
3. Ransbotham S., Mitra S., Ramsey J. "Security risk management: frameworks and best practices." Journal of Cybersecurity, 2022.
4. ENISA Threat Landscape Report 2023.

Аналіз безпеки коду веб додатку за допомогою великих мовних моделей

УДК 004.056:004.415.3:004.89

Тарас Цаволик[1], Лукаш Остап[2]
Західноукраїнський національний університет,
[1]calisto2292@ukr.net, [2]oslukash@gmail.com

Веб-додатки є важливими складовими сучасної цифрової інфраструктури, але їхня складність призводить до поширення уразливостей у коді (XSS, SQL-ін’єкції, небезпечне використання eval тощо). Тому автоматизований аналіз