

МОДЕЛЮВАННЯ АРХІТЕКТУРИ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ ВРАЗЛИВОСТЕЙ ТА МЕХАНІЗМІВ КІБЕРЗАХИСТУ

Ясільоніс А.В., факультет Інформаційних технологій, група КСЗІ-24007м., науковий керівник: проф. Лахно А.В.

У цифровій реальності зростає значення правильної побудови серверної інфраструктури як фундаменту для забезпечення функціонування критично важливих інформаційних систем. Розширення хмарних сервісів, зростання обсягів оброблюваних даних та впровадження розподілених обчислювальних систем ставлять нові виклики перед фахівцями з комп'ютерної інженерії. Водночас, збільшується кількість потенційних вразливостей у таких середовищах, що підвищує ризики компрометації цілісності, конфіденційності й доступності даних.

Метою цього дослідження є створення моделі серверної інфраструктури, яка враховує сучасні загрози та вразливості, а також впроваджує проактивні методи кіберзахисту. Запропонований підхід орієнтований на поєднання ефективної технічної архітектури з засобами безпеки. На етапі моделювання аналізується структура обчислювальних вузлів, серверів зберігання даних, віртуалізованих середовищ та комунікаційних каналів між ними. Важливою складовою є інтеграція механізмів контролю доступу на основі принципів мінімальних привілеїв. Крім того, проводиться аналіз архітектури з використанням методологій моделювання загроз, зокрема MITRE ATT&CK. Це дозволяє формувати цілісну картину можливих векторів атаки, на основі яких визначаються пріоритети впровадження захисних механізмів.

Практична цінність цієї роботи полягає у створенні універсального підходу до проєктування серверної інфраструктури з урахуванням кібербезпеки на всіх етапах її життєвого циклу — від планування і проєктування до впровадження та подальшої експлуатації. Таким чином, у контексті зростаючого навантаження на цифрові інфраструктури, а також загроз з боку все більш витончених кібератак, питання моделювання безпечної та гнучкої серверної архітектури постає як стратегічно важливе. Впровадження напрацьованих підходів дозволить значно знизити ризики несанкціонованого доступу, порушення роботи сервісів та витоку конфіденційної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. SANS Institute. Event Monitoring and Incident Response. SANS White Papers, 2013. URL: <https://www.sans.org/white-papers/34232/>
2. SANS Institute. Vulnerability Management Resources. SANS Blog, 2021. URL: <https://www.sans.org/blog/vulnerability-management-resources/>
3. Babenko T. Cyber Security Risk Modeling in Distributed Information Systems. Academia.edu, 2023. URL: <https://www.academia.edu/101790174>

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів