УДК 004.056.5:378.1

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ КІБЕРЗАХИЩЕНОСТІ МОДЕЛІ НАВЧАЛЬНО-МЕТОДИЧНОГО КОМПЛЕКСУ ОСВІТНЬОГО ПРОЦЕСУ

Уляна ПАНОВИК[1,2], Богдана ФЕДИНА[1,2], Роман ПАНОВИК[2]
[1]Львівський державний університет безпеки життєдіяльності,
[2]Національний університет «Львівська політехніка»

Анотація. *Подано методику імітаційного моделювання кіберзахищеності навчально-методичного комплексу (НМК) у середовищі Python + SimPy. Модель відтворює сценарії атак і відмов, оцінює стійкість системи та ефективність заходів безпеки. Результати моделювання і розрахунку ключових метрик підтвердили ефективність моніторингу, двофакторної автентифікації та резервування бази даних, що дає змогу оптимізувати архітектуру освітніх інформаційних систем.*

Ключові слова: *імітаційне моделювання, кіберзахищеність, навчально-методичний комплекс.*

Abstract. *A methodology for simulation modeling of the cybersecurity of the educational-methodical complex (EMC) in the Python + SimPy environment is presented. The model reproduces attack and failure scenarios, assesses system resilience and the effectiveness of security measures. The obtained results and calculated key metrics confirmed the efficiency of monitoring, two-factor authentication, and database backup, allowing optimization of the architecture of educational information systems.*

Keywords: *simulation modeling, cybersecurity, educational-methodical complex.*

Освіта активно переходить у цифровий формат, де більшість процесів здійснюється через автоматизовані платформи. Зростання кіберзагроз робить захищеність даних ключовим аспектом цифрової трансформації вищої освіти. Навчально-методичні комплекси (НМК) містять значні обсяги чутливої інформації, тому рівень їхньої безпеки варто оцінювати ще на етапі проєктування. Метою дослідження є створення імітаційної моделі подій безпеки та аналіз стійкості НМК до типових кіберзагроз. Практика показує, що безпеку освітніх систем часто враховують уже після запуску, тому необхідні інструменти для попередньої оцінки їхньої кіберстійкості. Попередні дослідження авторів стали основою запропонованого підходу. У [2] розглянуто імітаційне моделювання процесів управління освітнім середовищем, що підтвердило ефективність симуляційного аналізу потоків даних у ВНЗ, а міжнародні роботи [3] демонструють доцільність використання моделювання для оцінки ризиків кібербезпеки освітніх платформ. Водночас не проводилась оцінка захищеності архітектури НМК і не розглядалися сценарії атак чи відмов. Тому імітаційне моделювання є доціль-

ним інструментом для оцінювання кіберстійкості освітніх систем, оскільки дає змогу виявляти вразливості ще на етапі проєктування.

Навчально-методичний комплекс (НМК) є основою управління освітнім процесом, поєднуючи навчальні програми, методичні матеріали та цифрові інструменти моніторингу. Він складається з трьох підсистем — нормативно-методологічної, методологічної та інфраструктурно-організаційної, які взаємодіють у межах єдиної архітектури. Ключові точки контролю безпеки охоплюють модуль автентифікації, API-з'єднання, базу даних і канали обміну, що є потенційно вразливими до атак типу brute-force, SQL-ін'єкцій, несанкціонованого доступу та перехоплення даних. Для аналізу взаємодії компонентів НМК створено Data Flow Diagram, що відображає рух даних між підсистемами та визначає потенційно вразливі точки. На її основі побудовано карту ризиків (рис. 1), яка охоплює спроби несанкціонованого доступу, перевантаження серверів, втрату чи підміну даних і відмови сервісів.

Для оцінювання кіберзахищеності навчально-методичного комплексу (НМК) створено імітаційну модель, що відтворює взаємодію користувачів, серверів і бази даних за умов навантаження та кіберзагроз. Моделювання виконано у Python з використанням бібліотеки SimPy, яка забезпечує подійне середовище для опису паралельних процесів, управління ресурсами та вимірювання часових параметрів. Такий підхід дозволяє дослідити не лише роботу системи в нормальному режимі, а і її поведінку під час атак або відмов компонентів. Модель охоплює п'ять сценаріїв: нормальну роботу, несанкціонований доступ (brute force, SQL-injection), перевантаження серверів (DoS), відмову бази даних та відновлення після інциденту із залученням резервних механізмів і поверненням системи до стабільного стану.

Імітаційний алгоритм моделі (рис. 2) реалізує подійний цикл, у якому після ініціалізації середовища SimPy створюються основні ресурси — пул серверів (server_pool) та база даних (db). Запускаються два генератори: користувачів і атак, що формують потоки подій різної інтенсивності. Усі події надходять до блоку Dispatcher, який визначає їх тип — звичайний запит чи атака. Якщо сервер вільний, запит обробляється; за перевантаження — потрапляє в чергу або тайм-аут. Для атак визначається тип загрози (brute, SQLi, DoS, DB-fail); при виявленні інциденту виконується блокування і відновлення, а якщо він не виявлений — подія фіксується як компрометація. Усі події реєструються в журналі логів, що є основою для подальшого аналізу. Моделювання триває до досягнення встановленого часу T, після чого система переходить до етапу оцінки результатів.

Рисунок 1 – Концептуальна модель НМК та критичні точки безпеки

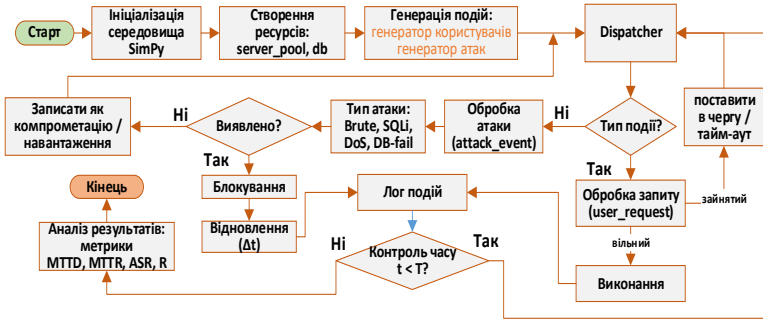

Рисунок 2 – Алгоритм імітаційного моделювання кіберзахищеності інформаційної системи

На завершальному етапі проведено аналіз журналів подій і розраховано ключові метрики кіберстійкості, що дало можливість оцінити ефективність політик безпеки та оптимізувати архітектуру НМК. Імітаційне моделювання підтвердило здатність системи ефективно реагувати на кіберінциденти в п'яти сценаріях, зокрема, під час пікових навантажень, коли різко зростає частота brute force та SQL-injection атак (рис. 3). Аналіз результатів (табл. 1) засвідчив, що впровадження моніторингу, 2FA та резервування бази даних суттєво підвищило кіберстійкість системи, скоротивши час виявлення та відновлення після інцидентів.

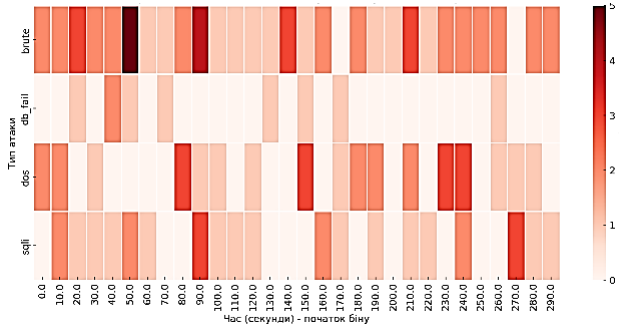

Рисунок 3 – Heatmap частоти атак

Таблиця 1. Порівняльні показники ефективності кіберзахищеності для різних сценаріїв

Сценарій	**MTTD (с)**	**MTTR (с)**	**ASR**
Базовий	9,6	7,2	0,64
Моніторинг	3,4	7,2	0,64
2FA	3,4	7,2	0,87
Резервування БД	3,4	3,4	0,87

MTTD (с) – час виявлення, MTTR (с) – час відновлення, ASR – частка заблокованих атак

У результаті дослідження розроблено методику імітаційного моделювання кіберзахищеності навчально-методичного комплексу (НМК) у середовищі Python + SimPy, що дозволяє відтворювати сценарії атак і відмов без ризику для реальної інфраструктури. Отримані метрики підтвердили ефективність моніторингу, двофакторної автентифікації та резервування бази даних. Імітаційний підхід довів свою придатність для виявлення вразливостей, порівняння конфігурацій безпеки та підвищення кіберстійкості освітніх систем.

Література

1. Пановик Р., Пановик У., Федина Б. Імітаційне моделювання для цифрової трансформації підсистеми управління освітнім процесом ВНЗ. *Вимірювальна та обчислювальна техніка в технологічних процесах,* 2025. 82(2), с. 159–166

2. Palko D. et al. Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences*. 2023. Vol. 13, no. 4. P. 2393. URL: https://doi.org/10.3390/app13042393