The savings rate for highly developed countries is significantly higher than that of underdeveloped countries due to higher income levels, more stable economic conditions, and a developed financial infrastructure. Highly developed countries have greater opportunities for capital accumulation due to high levels of economic stability, access to financial instruments and savings programs, and cultural and social norms that encourage savings. In contrast, in underdeveloped countries, limited incomes, economic instability, and insufficient access to financial services prevent significant savings from being generated. These resource constraints and high levels of consumer spending in such countries reduce their ability to accumulate capital, which affects their economic development and investment activities.

In order to improve the economic model based on the analysis, two key factors should be taken into account: cyclical parameters and parameters with constant dynamics. First, in order to more accurately reflect real economic conditions, it is necessary to take into account cyclical fluctuations of parameters such as the level of depreciation of private sector capital, which behaves according to the phase of the economic cycle. Secondly, for parameters with constant dynamics, such as decreasing depreciation of public capital or decreasing population growth, it is important to integrate long-term trends into the mathematical model, i.e., to dampen certain factors. This will allow the model to better predict the future behavior of the systems under study.

References:

1. Kolyada Y., Poznyak S., Ramskyi A., Shevchenko S. (2024). Adaptation Applying of Economic Growth Theoretical Models, Digit. Econ. Concepts Technol. Workshop 2024, 22–35, https://ceur-ws.org/Vol-3665/paper3.pdf

2. Kolyada Y., Poznyak S. (2024). Adaptive Model of Economic Growth for an Open Economy. National interests of Ukraine, 2(2). https://doi.org/10.52058/3041-1793-2024-2(2)-267-286

3. Kolyada Y., Poznyak S. (2024). Adaptive Model of Open Economy Growth. The theory of modernization in the context of modern world science. https://doi.org/10.62731/mcnd-02.08.2024.001

4. World Bank (2024). World Bank. Retrieved September 15 2023, from https://data.worldbank.org/

ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНИХ ДАНИХ ЗА ДОПОМОГОЮ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

Полуектова Наталія Робертівна, д.е.н., доц.
Запорізький інститут економіки і інформаційних технологій
ORCID ID 0000-0001-5664-2131
e-mail: *n.poluektova@econom.zp.ua*

Сучасні вимоги цифрової ери сприяють перебудові інформаційних систем і змушують компанії приймати нові стратегії для вирішення проблем інформаційної безпеки. Окрім переваг (наприклад, скорочення часу на підготовку та представлення корпоративної інформації, автоматизації виконання поточних операцій, підвищення точності для кращої зовнішньої звітності), використання IT несе нові виклики (наприклад, підвищені ризики витоку даних, порушення конфіденційності корпоративних даних, фішинг, електронне шахрайство, видавання себе за іншого та інші проблеми інформаційної безпеки) [1].

Інформаційні системи компаній і підтримуючі бізнес-процеси можуть бути інтегровані лише через набір основних характеристик інформаційної безпеки. Тобто, будь-яка система безпеки повинна забезпечувати конфіденційність, цілісність, доступність та зберігання оброблених даних. Це відповідає концепції CIA [2], яка була запропонована ще в 70-ті роки минулого сторіччя, але згідно з сучасними дослідженнями залишатиметься унікально актуальною для фахівців з безпеки і продовжуватиме служити точкою відліку в управлінні безпекою [3].

Елементи моделі CIA (конфіденційність, цілісність та доступність) тісно пов'язані з різними типами загроз, які можуть виникати в сфері інформаційної безпеки. Кожен з компонентів тріади відповідає за захист від конкретних типів загроз, що впливають на безпеку інформації в системах. На рис. 1 показано, як елементи моделі CIA співвідносяться з різними типами загроз та які методи захисту від них найбільш розповсюджені.

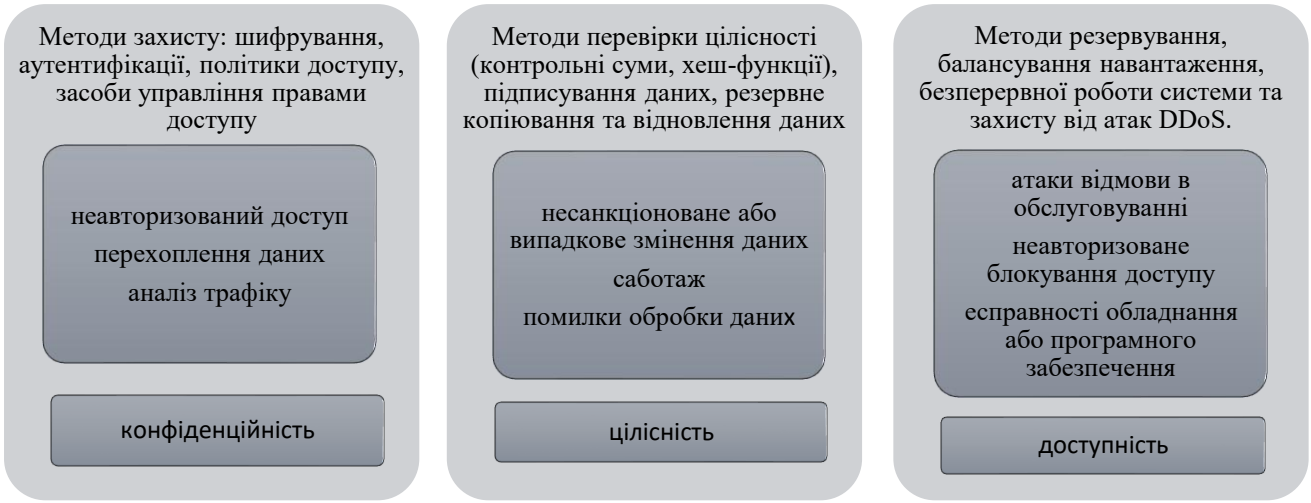

Рисунок 1. – Вплив типів атак безпеки корпоративних даних на елементи моделі CIA та методи захисту

Джерело: узагальнено та формалізовано авторкою.

Для аналізу стану системи безпеки на підприємстві, особливо в умовах обмеження ресурсів, можуть використовуватись методи імітаційного моделювання, які дозволяють виконувати віртуальні експерименти для оцінки впливу різних загроз на рівень захищеності корпоративної інформації.

Модель була реалізована на мові Python з використанням наступних підходів.

Для кожного типу атаки задана початкова ймовірність, яка відображає базовий рівень ризику без врахування часу або ефективності захисту.

Час впливає на ступінь ушкоджень системи внаслідок атаки, що триває довше. Протягом кожного періоду часу атака може збільшувати вплив на систему. Наприклад, з часом атака може викликати більші порушення в конфіденційності, цілісності чи доступності.

$$D(t) = D_{base} \times (1 + time_{factor} \times t) \quad (1)$$

де:D(t) — ушкодження в часі (масштаб ушкоджень);D_{base} — початкові ушкодження (якщо атака була б миттєвою);time_factor — коефіцієнт, який визначає, як швидко зростають ушкодження з часом;t — кількість періодів часу, що пройшли.

У моделі також враховується ефективність захисту, що зменшує ймовірність успішної атаки.

Щоб врахувати взаємодію різних загроз одна з одною, ми можемо додати взаємозалежність між атаками, де одна атака може збільшувати ймовірність або масштаб ушкоджень іншої. Наприклад, якщо відбулася атака типу Brute Force, це може підвищити ймовірність SQL-ін'єкції через зниження безпеки облікових даних або вразливостей у системі. Результати застосування моделі представлені на рис. 2.

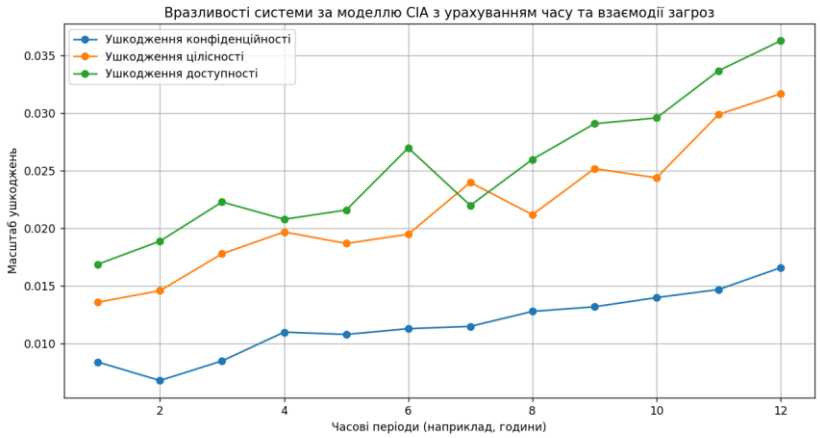

Рисунок 2. – Результати імітаційного моделювання

Представлений підхід дозволяє визначати потенційні ущерби для конфіденційності, цілісності та доступності даних у системах безпеки з урахуванням часу та взаємодії між різними загрозами. Вдосконалення підходу може полягати у додаванні нових типів атак, введення більш складних залежностей між загрозами, де одна атака не тільки підвищує ймовірність іншої, але й змінює ефективність захисту або додатково знижує рівень безпеки, моделювання соціальних факторів, додавання динамічних змін захисту, та ін.

Література:

1. Demertzis, K., Kikiras, P.,. Tziritas, N., Sanchez, S. L., & Iliadis, L. (2018). The next generation cognitive security operations center: network flow forensics using cybersecurity intelligence.Big Data and Cognitive Computing vol. 2, no. 4.
2. Anderson, B., McGrew, D. (2017) Machine learning for encrypted malware traffic classification: accounting for noisy labels and non-stationarity. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1723-1732
3. Samonas, S. Coss, D. (2015).The CIA strikes back: redefining confidentiality, integrity and availability in security. Journal of Information System Security, Volume 10, Issue 3, ISSN: 1551-0123

МЕТОДИ І МОДЕЛІ МАШИННОГО НАВЧАННЯ В СИСТЕМАХ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ

Полянський Владислав, PhD, викладач
Харківський національний економічний університет імені Семена Кузнеця
Харків, Україна
ORCID ID 0000-0001-7178-2132
e-mail: vladislav.polya94@gmail.com

Методологія оцінки рівня фінансової безпеки країн в умовах впливу «шоків» ґрунтується на інтеграції сучасних методів машинного навчання та економетричного моделювання, що дозволяє створити гнучкий інструмент для комплексного аналізу. Цей підхід поєднує як кількісні, так і якісні методи, що дозволяють не лише оцінити поточний рівень стійкості макроекономічних систем, але й передбачити можливі зміни в умовах різних екзогенних впливів.

Структура цієї методології складається з двох основних модулів, кожен з яких виконує специфічну роль у процесі оцінки та прогнозування. Перший модуль зосереджений на оцінці стійкості та вразливості макроекономічних систем до різних екзогенних «шоків», включаючи фінансові, економічні та соціальні кризові ситуації. Другий модуль орієнтований на прогно-