УДК 658.62.018.012

УПРАВЛІННЯ СКЛАДНИМИ СИСТЕМАМИ З МЕТОЮ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Грінченко Г.С., кандидат технічних наук, доцент
Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету ім. В.Н. Каразіна
Мазорчук К.К., аспірантка
Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету ім. В.Н. Каразіна
Грінченко В.В., аспірант
Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету ім. В.Н. Каразіна
Негодов С.С., аспірант
Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету ім. В.Н. Каразіна

Ключові слова: інформаційна безпека, управління, ризики, складні системи.

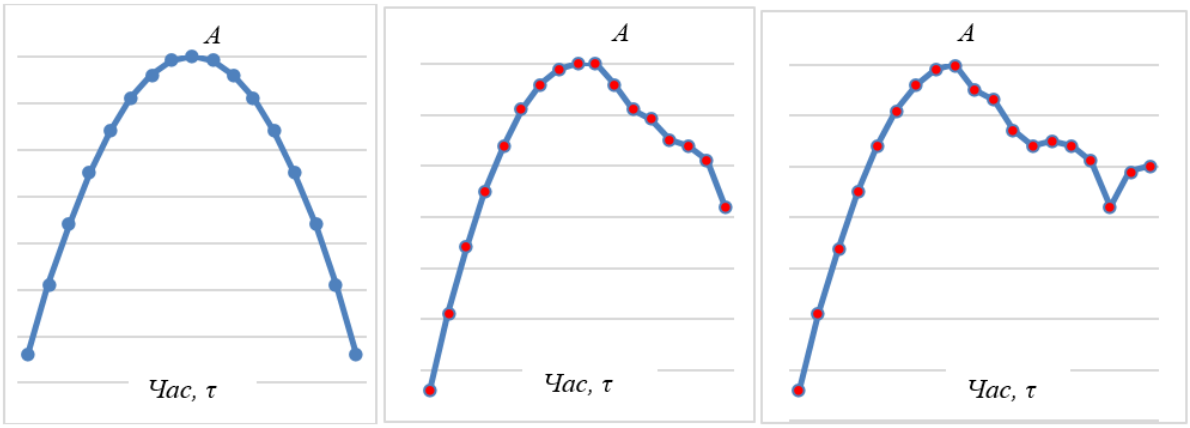
Розвиток управління складними системами з метою забезпечення інформаційної безпеки є важливим аспектом сучасних технологій та організаційної діяльності. У умовах зростаючих загроз, пов'язаних з кібернетичними атаками, витоками даних і порушеннями конфіденційності, управління інформаційною безпекою стає пріоритетом для багатьох організацій різної сфери національної економіки.

Основною метою управління складними системами в контексті інформаційної безпеки є забезпечення цілісності, конфіденційності та доступності інформації. Це передбачає розробку і впровадження ефективних політик безпеки, які охоплюють всі рівні організації — від стратегічного до операційного. Важливими етапами цього процесу є ідентифікація активів, оцінка ризиків та визначення вразливостей, що дозволяє виявити потенційні загрози. Так, для визначення ризиків соціально-економічних систем використовують різні методи, включаючи машинне навчання та застосування нейромережевих алгоритмів.

Сучасні підходи до управління ризиками ґрунтуються на «концепції прийнятного ризику», яка спрямована на досягнення максимальної надійності різних видів діяльності шляхом утримання сукупного ризику в рамках, визначених стратегією розвитку соціально-економічної системи [1-3]. Однак через нелінійний характер розвитку системи неможливо з абсолютною точністю передбачити її поведінку в певний момент часу; ми можемо лише визначити ймовірність настання певної події. Розвиток системи також може проходити через критичну точку або «колапс», за яким настає спад, що важливо враховувати при оцінці ризику (рис.1). При цьому необхідно оцінити здатність системи адаптуватися після колапсу, зокрема її гнучкість і можливості відновлення процесів [4].

Для досягнення ефективного управління інформаційною безпекою необхідно використовувати різноманітні технології та методи, які дають змогу зібрати статистичні дані для подальшого оцінювання. Це можуть

бути системи моніторингу, які в режимі реального часу виявляють аномалії в поведінці системи, або рішення на базі штучного інтелекту, що дозволяють автоматизувати процеси виявлення загроз і реагування на них, тобто ефективно адаптуватися та відновлюватися (Рис.1 в). Використання алгоритмів машинного навчання може значно підвищити ефективність виявлення кіберзагроз шляхом аналізу великих обсягів даних та находити оптимальні рішення для уникнення небажаних подій або находження найращого (найсприятливішого) сценарію відновлення системи.



а *б* *в*

Рисунок 1 – Варіанти функціонування системи: *а* – невідновлювана система; *б* – система частково-відновлювальна; *в* – відновлювальна система

Загалом, розвиток управління складними системами з акцентом на інформаційну безпеку вимагає системного підходу, використання інноваційних технологій і регулярного аналізу ризиків, що дозволяє адаптуватися до швидко змінюваного середовища загроз. Це, в свою чергу, сприяє формуванню стійких і безпечних інформаційних систем, здатних витримувати виклики сучасного світу.

Список використаних джерел

1. Оцінювання ризиків функціонування системи управління якістю (ДСТУ ISO 9001:2015) вищих навчальних закладів / Р. М. Тріщ, Г. С. Кіпоренко, Н. І. Кім, А. М. Денисенко // Системи управління, навігації та зв'язку. – 2016. – Вип. 2 (38). – С. 133–136.

2. Trishch, R., Nechuiviter, O., Hrinchenko, H., Bubela, T., Riabchykov, M., Pandova, I. (2023) Assessment of safety risks using qualimetric methods. MM Science Journal. October 2023, 6668. DOI: 10.17973/MMSJ.2023_10_2023021

3. Грінченко Г.С., Фатєєва Л.Ю., Мазорчук К.К. Удосконалення підходів до оцінювання якості шляхом застосування кваліметричних методів оцінювання ризиків. VII Міжнародна науково-практична конференція "Мехатронні системи: інновації та інжиніринг", Київ: КНУТД, 2023, с. 263. https://doi.org/10.5281/zenodo.10202155

4. Грінченко Г.С., Тріщ Ю.В., Грінченко В.В., Багаєв І.О., Фатєєва Л.Ю. Підходи щодо оцінювання ризиків функціонування систем об'єктів різного призначення. Машинобудування: Збірник наукових праць. 2022. №29. С. 70 -79. DOI: 10.32820/2079-1747-2022-29-70-79