

УДК 004.056

Савченко Ю. В.<sup>1</sup>, Воскобойник В.О.<sup>2</sup>, Сумовський О.М.<sup>3</sup>

<sup>1</sup> канд. техн. наук, доц. Університету митної справи та фінансів

<sup>2</sup> канд. техн. наук, доц. НУ «Запорізька політехніка»

<sup>3</sup> студ. гр. Б-21-1 Університету митної справи та фінансів

## **МЕТОДИ ОЦІНЮВАННЯ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ КРИТИЧНИХ ІНФРАСТРУКТУР**

Кібербезпека залишається головною проблемою в сучасному ІТ-світі оскільки кількість хакерських інцидентів зростає. Багато аспектів нашого життя перемістилися в Інтернет, що комерційний і приватний світи можуть багато втратити через порушення безпеки.

Ціллю даної роботи є аналіз архітектурно—орієнтованого підходу побудови структурних схем безпеки кібернетичних активів критичних інфраструктур (КІ).

Хмарні системи можна розглядати як перспективні засоби по забезпеченню функційної та кібернетичної безпечності КІ. Можливість застосування хмарних активів для підвищення рівня готовності системи SCADA як однієї з найважливіших компонентів контуру управління КІ.

Для новоутвореної структури виникає актуальне завдання, яке полягає в розробці основних положень методології оцінювання функційної безпечності критичних інфраструктур, які базуються на архітектурно—орієнтованому моделюванні внутрішніх та зовнішніх факторів негативного впливу на активи КІ і визначенні відповідних ризиків.

Розглянемо етапи реалізації методу побудови структурних схем безпеки активів критичних інфраструктур.

Для розв'язування завдання визначення рівня функційної безпечності КІ було запропоновано застосовувати архітектурно—орієнтований метод побудови структурних схем безпеки [1], схему алгоритму реалізації якого зображено на рис. 1.

Для моделювання відмов фізичних активів критичних інфраструктур можуть застосовуватися різноманітні методи. Перевага надається аналітико-стохастичним методам.

Серед аналітико-стохастичних методів, які враховують ІТС досліджуваних систем особливу увагу слід приділити апарату моделювання на основі напівмарковських процесів [2]. Для упорядкування та визначення послідовності виникнення тих, чи інших негативних подій стосовно до фізичних активів КІ можуть застосовуватися детерміністські підходи

Моделювання виконується згідно з функціональною схемою реалізації сценарію ЗВШВ. В залежності від умов, припущень та обмежень, що спостерігаються та вводяться, пропонується застосовувати як апарат марковського моделювання, так і апарат напівмарковського моделювання [3] зловмисних шкідливих впливів (ЗВШВ) на кібернетичні активи КІ. Слід зауважити, що застосування апарату марковського моделювання ЗВШВ на кібернетичні активи критичних інфраструктур вимагає попереднього обґрунтування з урахуванням динаміки розвитку процесів за умов, коли спостерігається марковська властивість. Такі умови, наприклад, можуть виникати, коли кібератака реалізується в певний поточний момент часу і їй не передуює попередній збір інформації про об'єкт атаки, тобто відсутній етап цільового фішингу. Завжди існує деякий період, так званої, предісторії, на якому проводиться цільовий фішинг. У цьому випадку марковська властивість не спостерігається і тому необхідно застосовувати інші немарковські моделі ЗВШВ. Найкраще для цього підходить апарат

моделювання напівмарковських процесів, який в подальшому застосовується при оцінці функційної безпечності КІ з урахуванням ризиків негативного впливу на їхні активи.

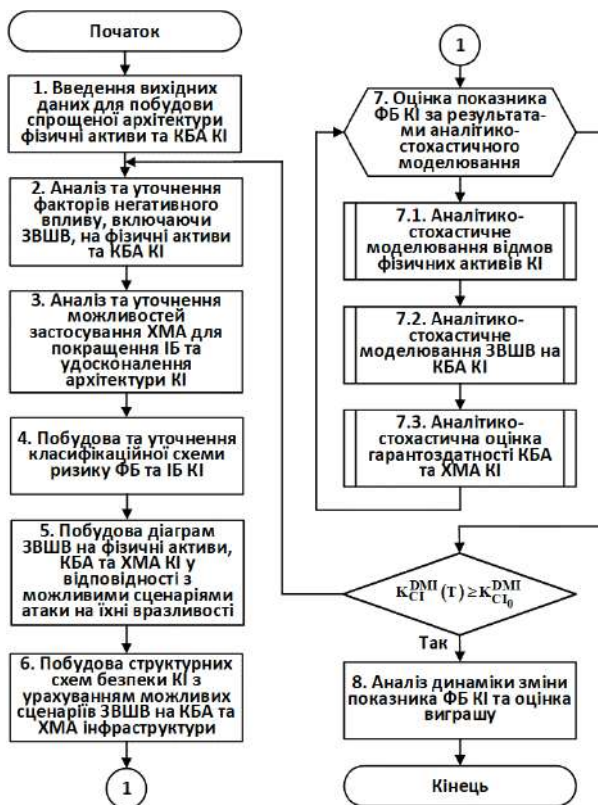


Рисунок 1 – Схема алгоритму реалізації етапів аналітико—стохастичного методу побудови структурних схем безпеки кібернетичних активів КІ

Для побудови адекватних моделей ЗВШВ визначається тривалість інтервалу загального циклу оцінювання рівня безпеки кібернетичних активів КІ та формулюється складна подія, що відбувається на певному інтервалі часу. Після чого виконується декомпозиція зазначеної події та з застосуванням теорем складання і множення імовірностей визначається комплексний показник безпеки.

Аналітико—стохастичне моделювання може виконуватися для декількох сценаріїв ЗВШВ. Результати моделювання в подальшому

використовуються для вибору найкращого варіанту захисту від кібератак, включаючи побудову електронного периметру кібербезпеки.

Слід приділити особливу увагу розробці методичного апарату оцінювання функційної безпечності критичних інфраструктур з урахуванням ризику зловмисних шкідливих впливів на їхні активи.

Метод складається з таких етапів:

- розробка функціональної схеми реалізації зловмисних шкідливих впливів на активи критичної інфраструктури;
- побудова діаграм системних відмов критичної інфраструктури з урахуванням зловмисних шкідливих впливів на інфраструктурні активи;
- оцінка комплексного показника безпеки активів критичної інфраструктури за результатами аналітико—стохастичного моделювання;
- кількісна оцінка ризику негативного впливу на активи критичної інфраструктури;
- оцінка показника безпеки КІ з урахуванням ризику негативного впливу на активи інфраструктури.

На основі відомого досвіду розробляється сценарій розвитку ЗВШВ. Сценарій кібератаки, функціональна схема реалізації якого представлена на рис. 2. Вважатимемо, що зловмисники створюють і застосовують шкідливий трафік, який впливає на фізичні, кібернетичні та хмарні активи критичної інфраструктури.

На наступному етапі з урахуванням можливих сценаріїв реалізації ЗВШВ (рис. 2) будуються діаграми системних відмов критичної інфраструктури.

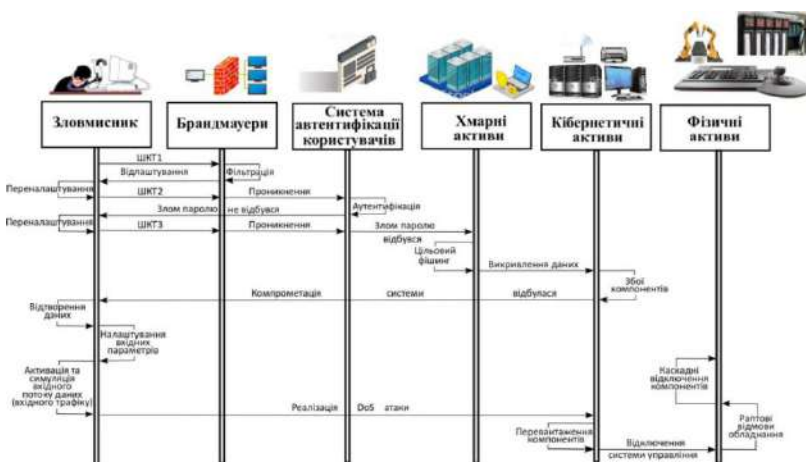


Рисунок 2 – Функціональна схема сценарію реалізації ЗВШВ на активи КІ.

Таким чином зосереджуючись на архітектурно—орієнтованого підходу побудови структурних схем безпеки кібернетичних активів критичних інфраструктур необхідно виконати моделювання і дослідити, яким чином застосування додаткових сервісів подій впливає на загальний рівень функційної безпечності кібернетичних та хмарних активів системи SCADA KI.

### **СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ**

1. Іванченко О. В. Аналітико—стохастична модель гарантоздатності кібернетичних та хмарних активів системи SCADA критичної інфраструктури // Системи та технології. 2020. № 1 (59). С. 14–59.
2. Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment / M. Ceriotti, L. Mottola, G. Picco et al. // 2009 International Conference on Information Processing in Sensor Networks, San Francisco, April 13–16, 2009, San Francisco, CA, USA. P. 277–288.
3. Іванченко О. В. Оцінювання рівня безпеки системи SCADA критичної інфраструктури з урахуванням доступності кібернетичних та хмарних активів // Системи та технології. 2019. № 2 (58). С. 5–32.