УДК 004.056:355.451:005.334

# СЦЕНАРНИЙ ПІДХІД ДО ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ТЕОРІЇ НЕЧІТКОЇ ЛОГІКИ

Діденко Є.С.
Науковий керівник – к.т.н., доц. Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В.Поповського,
м. Харків, Україна
тел. +380(50)-168-14-18

This work is devoted to the study of the scenario approach to the assessment of information security risks based on the theory of fuzzy logic. The quantity and complexity of cyber threats rises at an equivalent rate to the ever-increasing reliance on information technology systems. Creating scenarios based on prospective risks is a key component of a scenario-based approach to risk assessment. Organizations can use fuzzy logic to make better decisions by accounting for the inherent ambiguity in their risk assessments. This study looks at how the scenario method to risk assessment can be combined with fuzzy logic's mathematical foundation.

Кількість і складність кіберзагроз зростає так само швидко, як і залежність суспільства від інформаційних технологій. Щодня компанії будь-якого розміру знаходять нові способи виявлення та пом’якшення загроз доступності, конфіденційності та цілісності своїх найважливіших інформаційних активів. Метод оцінки ризиків інформаційної безпеки на основі сценаріїв на основі нечіткої логіки є одним із методів, які набули популярності в останні роки.

Створення сценаріїв реалізації потенційних ризиків є ключовим компонентом сценарного підходу до оцінки ризиків. Потім ці сценарії оцінюються на основі ймовірності виникнення загрози та її впливу на активи організації. Цей підхід забезпечує більш повну та реалістичну оцінку ризиків інформаційної безпеки, з якими стикається організація.

Нечітка логіка — це математична теорія, яка дозволяє мати справу з невизначеністю та неоднозначністю даних. Це особливо корисно під час оцінювання ризиків інформаційної безпеки, оскільки багато загроз для організацій не є чітко визначеними або важко піддаються кількісній оцінці. Використовуючи нечітку логіку, організації можуть включити невизначеність у свої оцінки ризиків і приймати більш обґрунтовані рішення.

Факторам, які беруть участь в оцінці ризиків, мають бути призначені ступені інтенсивності за умов використання нечіткої логіки в сценарному підході до оцінки ризиків. Наприклад, сценарій, що передбачає фішингову атаку, можна оцінити з точки зору ймовірності отримання зловмисником доступу до конфіденційної інформації, впливу такої інформації на

компрометацію та ефективності існуючих заходів безпеки для запобігання атаці. Справжній ступінь істинності кожного фактора можна визначити на основі наявних даних і експертних знань.

Після визначення ступеня істинності можна використовувати нечітку логіку для визначення загального ризику, пов'язаного зі сценарієм. Це можна зробити за допомогою різноманітних методів, таких як дерева рішень нечіткої логіки, нечіткі когнітивні карти та системи міркування нечіткої логіки. Ці методи дозволяють більш детально і точно оцінювати ризики, з якими стикається організація, таким чином дозволяючи краще приймати рішення.

Однією з головних переваг підходу, який базується на використанні методу сценаріїв з використанням елементів нечіткої логіки, до оцінки ризику є його гнучкість. Його можна адаптувати до конкретних потреб вашої організації та використовувати для оцінки різних сценаріїв і загроз. Це ідеальний підхід для компаній, які прагнуть розробити комплексну та індивідуальну стратегію управління ризиками.

В доповіді приводиться приклад розрахунку ризику інформаційної безпеки для обраних для дослідження кібератак з використанням сценарного підходу. Також показується, що сценарний підхід до оцінки ризиків інформаційної безпеки на основі теорії нечіткої логіки забезпечує точнішу та всебічну оцінку ризиків, з якими стикається організація. Усуваючи невизначеність і неоднозначність даних, організації можуть приймати більш обґрунтовані рішення щодо стану безпеки та розробляти ефективніші стратегії управління ризиками. У міру розвитку та ускладнення кіберзагроз використання нечіткої логіки в оцінці ризиків стає все більш важливим для забезпечення безпеки критично важливих активів.

Список використаних джерел:

1. Діденко Є.С., Снігуров А.В., Слюсар Н.В. Сценарний підхід до оцінки ризику інформаційної безпеки / Є.С. Діденко, А.В. Снігуров, Н.В. Слюсар // Восьма міжнародна науково-технічна конференція «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку» (EMC-2022), ХНУРЕ, 2022.

2. Потій О. В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки рівня зрілості систем забезпечення безпеки інформації / О. В. Потій, А. В. Лєншин. // Радіотехніка. Тематичний випуск «Інформаційна безпека». – 2005. – С. 144–160.