Юлія КОСТЮК
здобувач Phd, старший викладач кафедри
інженерії програмного забезпечення та кібербезпеки,
Державний торговельно-економічний університет,
м. Київ

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Захищені інформаційні системи є однією з найважливіших складових сучасних інформаційних технологій. Вони є важливими для забезпечення конфіденційності, цілісності та доступності інформації, що зберігається та передається через мережу. Інформаційна безпека стає все більш актуальною, оскільки з розвитком інформаційних технологій з'являються все нові загрози, такі як віруси, хакерські атаки, фішингові сайти, тощо. Захист інформаційних систем (ІС) від посягань з боку зловмисників є однією з найбільш актуальних проблем суспільства. Оскільки інформаційні системи є все більш складними та зв'язаними між собою, їх захист від зловмисників стає складнішим і вимагає використання новітніх методів та технологій.

Зростання кількості кібератак і їх складності ставлять перед спеціалістами завдання постійного покращення методів захисту. Один з інструментів, що допомагає у розв'язанні цієї проблеми − математичне моделювання захищених інформаційних систем. Математичні моделі забезпечують можливість аналізувати захищені інформаційні системи та виявляти потенційні загрози безпеки. Математичні методи дозволяють моделювати процеси захисту інформації, що дозволяє виявляти та усувати проблеми до того, як вони стануть загрозою.

Математичне моделювання є процесом використання математичних інструментів та технік для опису, аналізу та прогнозування поведінки системи. В контексті захищених інформаційних систем, математичне моделювання використовується для аналізу вразливостей системи та розробки ефективних

методів її захисту. Одним із найбільш важливих етапів математичного моделювання захищених інформаційних систем є розробка методів захисту.

Першим кроком в математичному моделюванні захищених інформаційних систем (ЗІС) є побудова моделі системи. Ці моделі можуть бути розроблені на основі статистичного аналізу даних про використання інформаційних систем та їх захисту, а також за допомогою методів теорії імовірностей та математичної статистики. Це також може бути модель в формі математичних рівнянь або графічна модель, яка відображає компоненти системи та зв'язки між ними. Потім модель системи аналізується на наявність потенційних вразливостей. Цей аналіз може бути здійснений як аналітично, так і за допомогою комп'ютерного моделювання. На цьому етапі створюють методи, що дозволяють знизити ризик зламу системи, та розробляють алгоритми для реалізації цих методів. Після того, як алгоритми розроблено, вони перевіряються на ефективність та можливість їх застосування до реальних систем.

Одним з найважливіших методів захисту інформації є шифрування. Шифрування забезпечує захист інформації від несанкціонованого доступу та забезпечує конфіденційність даних. Шифрування може бути виконане з використанням різних алгоритмів, таких як AES, RSA, та DES. Математичне моделювання може допомогти в розробці та покращенні цих алгоритмів шифрування.

Математичне моделювання ЗІС включає в себе використання математичних методів для створення моделей, які можуть допомогти відстежувати, як використовуються інформаційні ресурси, інтерактивних засобів та інших елементів системи. Це дозволяє аналізувати потенційні загрози та забезпечувати безпеку й відповідну реакцію на них. Один з методів математичного моделювання − моделювання стійкості криптографічних протоколів. Криптографічні протоколи використовуються для захисту інформації від несанкціонованого доступу, аналізу та викрадення. Моделювання стійкості криптографічних протоколів дозволяє оцінювати його стійкість до різних видів атак та забезпечувати захист від цих атак.

Окрім криптографічних алгоритмів, в математичному моделюванні ЗІС використовуються такі технології, як системи контролю доступу, ідентифікації користувачів та системи виявлення вторгнень.

Ще одним методом математичного моделювання ЗІС є використання техніки аналізу ризиків. Цей метод передбачає ідентифікацію потенційних загроз безпеці інформації та їх оцінку за допомогою математичних методів. Результати аналізу дозволяють розробити стратегію захисту інформації та визначити необхідні заходи для забезпечення безпеки.

Для створення більш якісних та ефективних засобів захисту необхідне моделювання процесів обробки та захисту інформації в ІС. З метою протидії загрозам створюються системи захисту інформації (СЗІ). Інформаційна система разом із СЗІ утворює захищену інформаційну систему (ЗІС). Кожна ЗІС має свої особливості (значимість оброблюваної та збереженої інформації, умови функціонування тощо), які визначають вимоги до СЗІ. У цих умовах практично важливим є отримання оцінок ефективності різних варіантів реалізації СЗІ, що згодом може бути використано для вибору оптимального з точки зору вимог комплексу захисних методів і засобів, необхідних для її створення.

Теоретичні та експериментальні дослідження базуються на використанні апарату теорії конфлікту, теорії графів, теорії мереж Петрі, теорії вибору та прийняття рішень, теорії ймовірностей та математичної статистики, теорії множин. Теорія графів є математичним інструментом для визначення структури системи та її взаємодії з навколишнім середовищем. Графи можуть бути використані для відображення структури системи та можливих нападів на неї. Цей метод дозволяє знайти слабкі місця в системі, розробити стратегії їх захисту.

Іншим методом є моделювання за допомогою теорії імовірності, який дозволяє оцінювати ризики інформаційних загроз та приймати рішення щодо захисту інформації. Теорія імовірностей дозволяє обчислити ймовірність виникнення певної події, такої як наприклад, успішна атака на систему, та оцінити можливі наслідки цієї події. На основі таких оцінок можуть бути прийняті рішення щодо розробки та впровадження захисних заходів.

Також до методів математичного моделювання захищених інформаційних систем відноситься моделювання через автоматні системи. Автоматні системи є математичними моделями, що описують поведінку системи відповідно до певних правил. Цей метод може бути використаний для виявлення атак та автоматичного реагування на них.

Усі ці методи математичного моделювання захищених інформаційних систем можуть бути використані в комплексі з іншими методами захисту, такими як шифрування, багатофакторна автентифікація та контроль доступу доінформації. Використання математичних моделей дозволяє зменшити ризики тапідвищити рівень безпеки захищених інформаційних систем.

Отже, математичне моделювання є важливим інструментом для забезпечення безпеки захищених інформаційних систем. Воно дозволяє виявляти потенційні загрози та вдосконалювати системи захисту. Застосування математичного моделювання разом з іншими методами захисту дозволяє підвищити рівень безпеки інформації та забезпечити її конфіденційність, цілісність та доступність.

Список використаних джерел

1. Новіков О. М., Родіонов А. М. Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем. *Інформаційні технології та комп'ютерна інженерія*. 2008. № 1(11). С. 170–175.

2. Костюк Ю.В., Самойленко Ю.О., Костюк І.В. Захист інформації в корпоративній інформаційній системі на основі інтелектуальних технологій. *Інноваційні технології XXI століття*: зб. наук. пр. / гол. ред. Л. Г. Білий. Хмельницький : Вид-во МАУП, 2022. Вип. 7. С. 85-93.