МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

Шапорін Володимир Олегович

УДК 004.056.5+004.413.4

МОДЕЛІ ТА МЕТОДИ АНАЛІЗУ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

05.13.06 - Інформаційні технології

Автореферат дисертації на здобуття наукового ступеня

кандидата технічних наук

Одеса - 2016

Дисертацією є рукопис
Робота виконана в Одеському національному політехнічному університеті Міністерства освіти і науки України

Науковий керівник: кандидат фізико-математичних наук, доцент
Тішин Петро Метталінович,
Одеський національний політехнічний університет,
доцент кафедри комп'ютерних інтелектуальних систем та мереж

Офіційні опоненти: доктор технічних наук, професор
Саченко Анатолій Олексійович
Тернопільський національний
економічний університет,
завідувач кафедри інформаційно-обчислювальних систем та управління

кандидат технічних наук, доцент
Шапо Владлен Феліксович
Національний університет
«Одеська морська академія»,
доцент кафедри теорії автоматичного
управління і обчислювальної техніки

Захист відбудеться 4 липня 2016 р. о 13^{30} на засіданні спеціалізованої вченої ради Д 41.052.01 в Одеському національному політехнічному університеті за адресою: 65044, м. Одеса, пр. Шевченка, 1, ауд. 400 – А.

З дисертацією можна ознайомитися в бібліотеці Одеського національного політехнічного університету за адресою: 65044, м. Одеса, пр. Шевченка, 1

Автореферат розісланий 3 червня 2016 р.

Вчений секретар
спеціалізованої вченої ради О.Є. Колесніков

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У зв'язку з конкурентною боротьбою, діяльністю зловмисників та вірусними атаками зростає загроза інформаційній діяльності підприємств. З кожним роком зростає складність атак, з'являються нові види загроз, удосконалюються старі. Згідно звітам за 2015 рік від Kaspersky lab, Dr. Web та SERT UA, Україна входить до ТОП-20 країн світу за рівнем вірусної зараженості комп'ютерів. За цей період 58 % корпоративних комп'ютерів зазнали хоча б однієї атаки з мережі Інтернет, причому здійснювалися ці атаки з використанням браузерів комп'ютерів (62 %), програм для андроїд (14 %), програм JAVA (13 %) та ін. Зокрема, атаки на бізнес-програми зросли у три рази, у порівнянні з минулим періодом 2014 року.

В умовах розвитку кіберзлочинності важливу роль набуває безпека систем та інформаційних ресурсів, яка ґрунтується на правилах та нормах, котрі визначають дії при виявленні інцидентів безпеки та управління факторами загроз (місця вразливості системи). Коректність та адекватність таких норм, в першу чергу, залежить від якості аналізу ризиків на етапі проектування системи заходів безпеки, який є найбільш витратним, як з фінансової точки зору, так і з точки зору витрат часу. В цілях економії коштів, більшість організацій не проводять аналіз ризиків ні на етапі проектування або запуску інформаційної системи, ні періодично, в ході її функціонування, що призводить до створення загроз інформаційній безпеці системи та її складовим, які характеризуються фінансовими, юридичними та моральними втратами.

Існує два підходи до аналізу ризиків: перший – організація експертної оцінки проблеми із залученням відповідних спеціалістів з безпеки та зацікавлених осіб. Другий – використання автоматизованих систем аналізу ризиків для окремих складових системи, або всієї системи в цілому, а також періодичний повтор аналізу під час функціонування системи. У першому випадку забезпечується висока достовірність оцінки ризиків, яка залежить від кількості експертів, однак робота експертів пов'язана з високою оплатою праці та потребує значних часових витрат. У другому випадку використовуються традиційні математичні та статистичні методи, які дозволяють автоматизувати процес аналізу ризиків, однак відомі методи використовують чіткі параметри для описання елементів ризику, що значно знижує достовірність результатів.

Таким чином **актуальною** є розробка методів та моделей для аналізу та оцінки ризиків, які засновані на теорії нечітких множин та нечітких чисел, що дозволить описувати параметри елементів ризику в умовах невизначеності та підвищити достовірність оцінки ризиків за рахунок застосування нечітких функцій агрегації.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалася у рамках держбюджетних науково-дослідницьких робіт: «Технології проектування, контролю і діагностики комп'ютерних систем та мереж» № 571-62, № держреєстрації 0107U001969, 2007-2010 р.р.; «Розробка засобів робочого і тестового контролю та діагностики обчислювальних систем і мереж» № 630-62, № держреєстрації 0108U001197, 2008-2009 р.р.; «Методи проектування та робочого діагностування складних цифрових систем і мереж» №37-62, № держреєстрації

0110U008194, 2011-2014 р.р.; «Методи проектування, аналізу, оптимізації інформаційних систем критичного застосування та їх компонентів» № 97-62, № держреєстрації 0114U005507, почалась у 2014р.

Метою дисертаційної роботи є підвищення достовірності оцінки ризиків в задачах забезпечення захисту інформаційних систем, шляхом розробки моделей якісного та кількісного оцінювання процесів порушення безпеки, а також методів аналізу ризиків.

Для досягнення поставленої мети вирішені наступні **задачі**:

– проведено аналіз існуючих методів і моделей аналізу ризиків, які використовуються в галузі інформаційної безпеки;

– розроблені математичні моделі активів та інцидентів безпеки, з використанням нечіткого інтеграла і нечітких мір;

– розроблено сімейство моделей сценаріїв загроз на основі нечітких часових мереж Петрі та нечіткого логічного висновку;

– розроблено метод оцінки загроз з використанням нечіткого інтеграла і нечітких мір для факторів впливу;

– розроблено метод оцінки ризиків на основі нечіткої кластеризації оцінок ймовірності виникнення інцидентів і збитків від них та правил приналежності до відповідних рівнів ризику;

– проведено практичні випробування результатів дослідження у лабораторних умовах та апробація на реальних об’єктах підприємництва.

Об'єкт дослідження – процес аналізу та оцінки ризиків інформаційної безпеки в умовах невизначеності.

Предмет дослідження – моделі та методи аналізу ризиків інформаційної безпеки в умовах невизначеності.

Методи дослідження. Метод оцінки активів заснований на теорії нечітких множин. Моделювання сценаріїв загроз засновано на теорії мереж Петрі та нечіткого логічного висновку. Метод оцінки ймовірності виникнення загроз заснований на теорії нечіткої міри та нечіткого інтегралу. Метод лінгвістичної оцінки рівня ризиків заснований на теорій нечітких множин та методах нечіткої кластеризації.

Наукова новизна полягає у розвитку методів ідентифікації, аналізу та оцінки ризиків інформаційної безпеки, які використовуються при розробці систем захисту інформаційних ресурсів підприємств та при аудиті ризиків в процесі функціонування інформаційних систем, а саме:

– отримав подальший розвиток метод оцінки активів інформаційної системи, який відрізняється описом активів та їх властивостей у вигляді лінгвістичних змінних, що дозволило давати якісну та кількісну оцінку при описанні та ранжуванні активів для визначення збитків та класифікації ризиків;

– отримали подальший розвиток моделі сценаріїв загроз, які відрізняються використанням нечітких значень параметрів помилок, збоїв, відмов та атак на систему, що дозволило підвищити точність моделей процесів порушення безпеки в умовах невизначеності та обмеженої інформації;

– вперше розроблено метод оцінки ймовірності виникнення загроз, який відрізняється використанням множини нечітких мір для факторів загроз та використан-

ням нечіткого інтегралу по нечіткім мірам для загальної оцінки загроз, що дозволило підвищити достовірність оцінки виникнення загроз;

– отримав подальший розвиток метод лінгвістичної оцінки рівня ризиків, який відрізняється використанням нечіткої класифікації ризиків, на основі кластеризації значень ймовірності виникнення інцидентів та збитків від них, що дозволило підвищити достовірність оцінювання ризиків.

Практичне значення отриманих результатів. В дисертаційній роботі розроблена інформаційна технологія, яка дозволяє підвищити достовірність оцінки рівня ризиків та знизити кількість помилкових оцінок. При використанні запропонованої інформаційної технології достовірність оцінки рівня ризику склала 0.96 з ймовірністю помилки другого роду 0,025. Розроблена інформаційна технологія була застосована при проектуванні інформаційних систем в ТОВ «Телекарт-Прилад», що дозволило підвищити достовірність оцінки рівня ризиків на 7-11% та скоротити час повторного аналізу ризиків у середньому на 23 %, що дорівнює 10 годинам, проти 13 годин до впровадження інформаційної технології.

Основні елементи розроблених методів та моделей впроваджені в навчальний процес Одеського національного політехнічного університету.

Особистий внесок здобувача. У роботах написаних із співавторами автору дисертації особисто належать основні теоретичні і практичні положення, які відображені у характеристиці наукової новизни. В роботах [4, 5, 7] автором запропоновано метод оцінки активів інформаційних систем. У роботах [1, 2, 3, 8, 10] запропоновано моделі сценаріїв з нечіткими значеннями параметрів. У роботах [5, 11, 12, 13, 14] досліджено фактори впливу на виникнення загроз та запропоновано метод оцінки ймовірності виникнення загроз інформаційної безпеки. У роботах [6, 9] запропоновано метод лінгвістичної оцінки рівня ризиків інформаційної безпеки.

Апробації результатів дисертації. Основні теоретичні положення і результати роботи доповідалися й обговорювалися на 8, 12, 14 і 15-й Міжнародних науково-практичних конференціях «Сучасні інформаційні та електронні технології» (Одеса, 2007, 2011, 2013, 2014) та семінару "Моделювання в прикладних наукових дослідженнях" (Одеса, 2015).

Публікації. Результати досліджень були представлені в 14 публікаціях, серед яких 6 статей у наукових журналах та збірниках наукових праць, визначених у МОН України як спеціальні видання з технічних наук і 8 у матеріалах конференції та семінарів. Серед цих публікацій 6 – у виданнях, які включені до міжнародних наукометричних баз Bielefeld Academic Search Engine (BASE), Російський індекс наукового цитування (РІНЦ), Index Copernicus Journals Master List.

Структура дисертаційної роботи. Робота складається з вступу, чотирьох розділів, висновків, переліку використаних джерел та додатків. Робота містить162 сторінок тексту, 50 рисунків і 8 таблиць, список використаних джерел містить 94 найменування.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі наведені загальна характеристика роботи, обґрунтована її актуальність, відповідність державним науковим програмам, наукова новизна та практичне значення, визначено об'єкт і предмет досліджень і сформульовані мета і завдання дослідження.

У першому розділі розглянуті актуальні загрози інформаційній безпеці, сучасні методи аналізу та оцінки рівня ризиків інформаційної безпеки.

На основі аналізу стандартів з інформаційної безпеки було виявлено основні елементи ризиків, які описуються інформаційною структурою та визначають вплив на діяльність інформаційних систем. В даній структурі використовуються наступні об’єкти: *актив* – інформаційні та технічні ресурси організації, порушення властивостей яких оцінюється з позиції грошових, часових або інших витрат; *інцидент* – одна або кілька небажаних подій у системі, які оцінюються з позиції ймовірності їх виникнення, *сценарій та загроза* – комбінація етапів здійснення порушення безпеки та джерела їх виникнення. Оцінюються як ймовірність здійснення сценарію та виникнення загрози. *Вразливість* – набір факторів, які сприяють здійсненню сценарію або виникненню інциденту та оцінюється як ступінь впливу на відповідний елемент ризику. *Ризик* – комбінація оцінки ймовірності виникнення інциденту і ступеня його впливу на актив та оцінюється з позиції рівня ризику для активу. Усі елементи ризику зв’язані між собою певним типом відношень, які описують ступень взаємодії між ними, а саме: відношення *ініціалізації* визначає ступень впливу загрози на початок здійснення сценаріїв; відношення *наслідування* описує ступень впливу здійснення сценарію на виникнення інциденту, а також взаємодію між сценаріями або між інцидентами; відношення *впливу* – описує ступень збитків активу від інциденту; відношення *збитку* – описує ступень впливу на актив збитку іншому активу.

Виявлено, що оцінка рівня ризику інформаційної безпеки складається з трьох етапів: ідентифікація ризиків – процес виявлення елементів ризику, їх структурування та опису; аналіз ризику – аналіз та дослідження інформації про ризик, що дозволяє визначити дані для загальної оцінки рівня ризику; порівняльна оцінка ризику – процес співставлення рівня ризику та критеріїв ризику, що дозволяє виявити значимість ризику для системи. Розглянуті сучасні методи аналізу ризиків мають ряд недоліків, серед яких наступне: по-перше, значна кількість методів передбачає залучення великої кількості експертів у різноманітних галузях; по-друге, значна кількість методів не передбачає структурування об’єктів та процесів порушення безпеки, або цей процес слабо формалізований; по-третє, більшість методів потребує знань про всі процеси, які відбуваються в системі, та точні кількісні характеристики даних процесів. У відповідності до цих проблем, були сформульовані основні вимоги до нових методів аналізу ризиків: а) мінімізація кількості експертів за рахунок автоматизації етапів аналізу ризиків; б) використання моделей, які дозволяють здійснювати етапи оцінки рівня ризиків в умовах невизначеності.

У другому розділі розроблено метод лінгвістичної оцінки властивостей активів та запропоновано підхід до ідентифікації елементів ризику на основі структурування даних елементів з використанням інформаційних структур.

Для аналізу ризиків необхідно провести ідентифікацію елементів, які характеризують ці ризики. Даний процес починається з виявлення активів системи які підлягають захисту, та побудови інформаційних структур елементів ризику для кожного виявленого активу. Наприклад, інформаційна структура для активу «доступність сервісів» може виглядати як показано на рисунку 1.

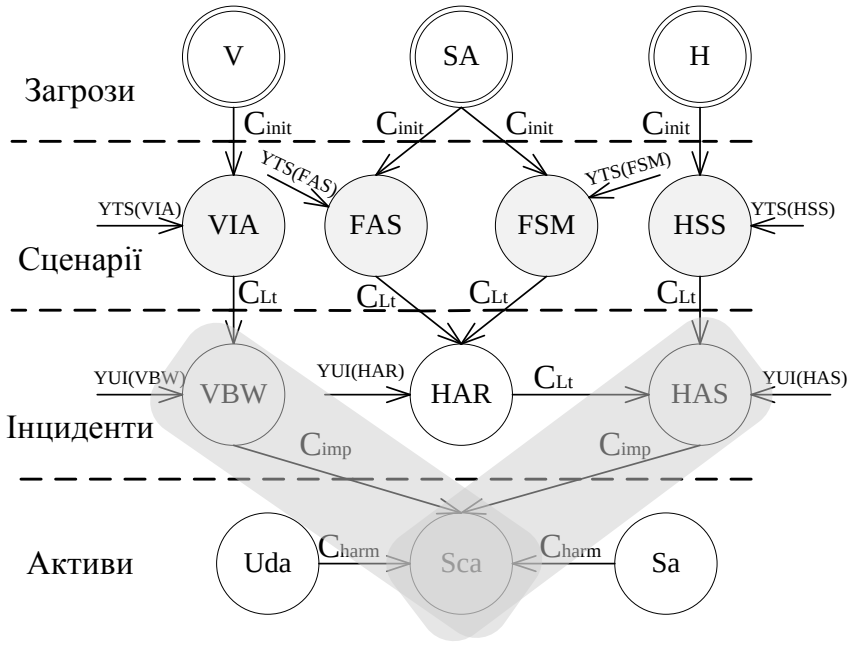


Рисунок 1 – Інформаційна структура для активу «доступність сервісів»

Далі виявляються інциденти, які впливають на актив, сценарії, які до цього призводять та загрози, які є ініціаторами сценаріїв порушення безпеки. В запропонованій структурі кожен її рівень представлений певним набором елементів. Так, рівень «Загрози» представлений елементами V – «вірус», SA – «адміністратор», H – «хакер»; рівень «Сценарії» – елементами VIA – «вірус інфікував застосування», FAS – «адміністратор помилився в налаштуваннях клієнтського застосування», FSM – «адміністратор помилився в керуванні сервісами», HSS – «хакер запустив свої сценарії на сервері»; рівень «Інциденти» – елементами VBW – «блокування роботи системи вірусом», HAR – «хакер отримав доступ до управління сервісами системи», HAS – «хакер отримав доступ до серверів»; рівень «Активи» – елементами Sca – «доступність сервісів» (головний в даній структурі), Uda – «доступність приватних даних», Sa – «доступність серверів». Елементи $YTS(TS_i)$ та $YUI(UI_i)$ визначають оцінки вразливих місць системи, які сприяють здійсненню сценарію та виникненню інциденту. Сірим фоном виділені елементи які безпосередньо формують ризики інформаційної безпеки. Далі визначаються відношення між елементами структури. Це дозволяє визначити характеристики взаємодій між рівнями структури, а також всередині рівня. При цьому, C_{init} є відношенням ініціації, C_{Lt} – відношенням наслідування, C_{imp} – відношенням впливу, C_{harm} – відношенням збитку. Після складання переліку усіх елементів ризику, проводяться заходи щодо вивчення впливу, поведінки та характеристик цих процесів.

Побудовані інформаційні структури дозволяють визначити структури впливу на актив інцидентів та інших активів. Дана структура визначається двома множинами: перша – множина пар оцінок ймовірності інцидентів та відношень впливу від них, друга – множина пар оцінок властивостей активів та відношень збитку від них. Структура допускає три варіанти впливу: інцидент-актив визначає вплив тільки від

інцидентів; актив-актив визначає вплив матеріальних активів на нематеріальні; повна структура визначає вплив від інцидентів та активів разом.

Вплив інцидентів на актив визначає відповідні ризики для активу, а вплив активів та загальна оцінка властивостей активу визначає важливість активу при визначені реакції на виникнення ризику.

Для визначення параметрів ризику, необхідно оцінити ймовірність інцидентів та активів, а також визначити відношення шкоди та впливу.

Моделі інцидентів характеризують ймовірність їх виникнення в результаті виникнення загроз та здійснення сценаріїв. В роботі було виявлено 6 типових моделей взаємодії інцидентів зі сценаріями загроз:

– одинична модель зі сценарієм – описує вплив одного сценарію загрози на інцидент. Даній моделі відповідає композиція блоків 4 та 6 (рисунок 2);

– одинична модель з інцидентом – описує вплив одного інциденту на інший інцидент. Даній моделі відповідає композиція блоків 5 та 6 (рисунок 2);

– паралельна модель – описує вплив на небажаний інцидент незалежних один від одного сценаріїв загрози. Даній моделі відповідає композиція блоків 3, 4 та 6, де блоки 3 та 4 незалежні один від одного (рисунок 2);

– послідовна модель – описує вплив на інцидент сценаріїв, які відбуваються послідовно. Даній моделі відповідає композиція блоків 1, 3 та 6, де блок 3 є результатом виконання блоку 1 (рисунок 2);

– паралельно-послідовна модель – описує одночасний вплив залежних і незалежних сценаріїв загрози. Даній моделі відповідає композиція блоків 1, 2, 3 та 6, де 1, 2 незалежні блоки, які призводять до виконання блоку 3 (рисунок 2);

– змішана модель – описує вплив на небажаний інцидент сценаріїв загроз будь-якої моделі і небажаних інцидентів. Даній моделі відповідає повна структура, зображена на рисунку 2.

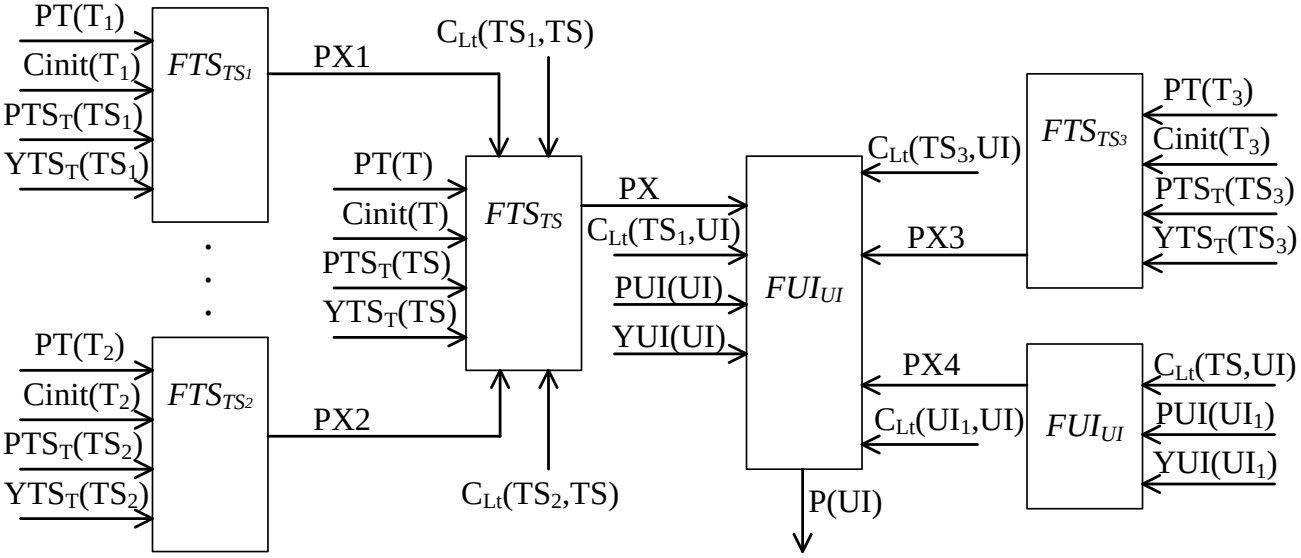


Рисунок 2 – Загальна структура моделі інциденту

В даних моделях на оцінку ймовірності виникнення кожного інциденту $P(UI)$ впливають наступні вхідні параметри:

– $PUI(UI)$ – ймовірність виникнення інциденту безпеки;

– PX_i – загальна оцінка ймовірності здійснення сценарію загрози або виникнення іншого інциденту;

– $C_{Lt}(TS, UI), C_{Lt}(UI, UI)$ – відношення наслідування між сценаріями та інцидентами;

– $YUI(UI)$ – множина оцінок вразливості системи, яка впливає на виникнення інциденту.

При цьому на оцінку ймовірності здійснення сценаріїв впливають наступні параметри:

– $PT(\text{Т})$ – оцінка ймовірності виникнення загрози;

– $C_{init}(\text{Т})$ – відношення ініціації сценарію відповідною загрозою;

– $PTS(TS)$ – ймовірність здійснення сценарію в системі;

– $YTS(TS)$ – множина оцінок вразливості системи, яка впливає на здійснення сценарію;

Множина оцінок вразливості $YUI(UI)$ та $YTS(TS)$ визначається експертом з множини факторів впливу на загрози, які зв’язані з відповідними інцидентами та сценаріями.

Вхідні параметри моделей мають різний ступень впливу на загальну оцінку ймовірності виникнення інциденту або реалізації сценарію, тому вони підлягають ранжуванню в залежності від ступеню впливу та подальшій агрегації. У якості функції агрегації виступає нечіткий інтеграл по нечіткій мірі, який визначає загальну оцінку ймовірності.

Оцінка властивостей активів передбачає наявність детальної інформації про характеристики активу, наприклад поточна ринкова вартість, час відновлення, актуальність і т. п. На практиці, не завжди можливо визначити точні дані про актив і тому в роботі запропоновано метод лінгвістичної оцінки властивостей активів, який визначає *перший пункт* наукової новизни. Даний метод складається з трьох етапів:

На першому етапі визначається ім’я змінної та її область визначення:

– ім’я змінної. Ім’я змінної визначає спосіб оцінювання властивостей активу, наприклад вартість активу, час його відновлення та ін.;

– область визначення. Залежить від типу активу. В загальному випадку область визначення може характеризуватись грошовим еквівалентом вартості активу, його відновленням, заміною або визначатись у бальному еквіваленті, якщо використання інших видів цінності неможливе або ускладнене;

На другому етапі визначається терм-множина, яка дозволяє давати якісну оцінку властивостей активу. На основі емпіричних досліджень рекомендована кількість термів від 3 до 7:

$$T = \{\text{"незначна"}, \text{"середня"}, \text{"висока"}, \text{" критична"}\},$$

На третьому етапі, визначаються функції приналежності визначених термів до області визначення. У роботі запропоновано використовувати функції приналежності *t*-класу, які визначають трапецеїдальну форму функції.

Використання даного методу дозволяє давати нечітку кількісну оцінку властивостей активів відповідно до типу активу, або якісну оцінку у вигляді лінгвістичних змінних. Це дозволяє проводити оцінку не тільки спеціалістам з інформаційної безпеки та мінімізувати кількість експертів аналізу ризиків.

Для оцінювання відношень між елементами ризику також доцільно використовувати лінгвістичні змінні. При цьому ім'я змінних виражають характер відношення – C_{init} = "можливість", C_{Lt} = "наслідок", C_{imp} = "вплив" та C_{harm} = "збиток". В роботі використовувана бальна шкала для області визначення у діапазоні U = [1..10]. Терм-множини для змінних наступні:

$$T(init) = \{\text{"навряд"}, \text{"можливо"}, \text{"скоріше"}\},$$
$$T(Leads\ to) = \{\text{"можливо"}, \text{"скоріше"}, \text{"обовязково"}\},$$
$$T(Impact) = \{\text{"незначний"}, \text{"помірний"}, \text{"серйозний"}, \text{"критичний"}\},$$
$$T(Harm) = \{\text{"малий"}, \text{"помітний"}, \text{"крайній"}\},$$

Модифікація термів як для активів, так і для відношень не передбачається, тому синтаксичні правила $G = \emptyset$ відсутні. Відповідно до цього, семантичні правила M також не використовуються.

У **третьому розділі** розроблені моделі сценаріїв загроз, розроблено метод оцінки ймовірності виникнення загроз.

Сценарії загроз описують етапи здійснення порушення безпеки, які виникають під впливом загроз та призводять до виникнення інцидентів безпеки. При цьому можливі два типи моделювання сценаріїв: перший варіант описує послідовність етапів порушення інформаційної безпеки та нанесення шкоди ресурсам інформаційної системи, другий варіант описує використання коефіцієнтів можливості при оцінці ймовірності у випадках, коли послідовністю етапів процес порушення описати неможливо.

У більшості випадків сценарії – це послідовність певних етапів процесу порушення штатного режиму роботи системи. При цьому, необхідно врахувати невизначеність даних процесів. З цією метою в роботі використано апарат часових мереж Петрі-Маркова для визначення структури сценарію (рисунок 3) та нечітких множин для подальшого описання параметрів сценарію.

Мережі Петрі-Маркова дозволяють шляхом побудови матриць спрацьовувань та диференціальних рівнянь визначити час проходу по мережі та визначити ймовірність атаки, яка моделюється. Кожний стан мережі S_i та відповідний їй перехід t_j визначає відповідні часові параметри τ_{ij}, які характеризують час здійснення відповідного етапу сценарію. Отриманні часові параметри визначають аналітичний вираз, який дозволяє обчислити загальний час проходження по мережі.

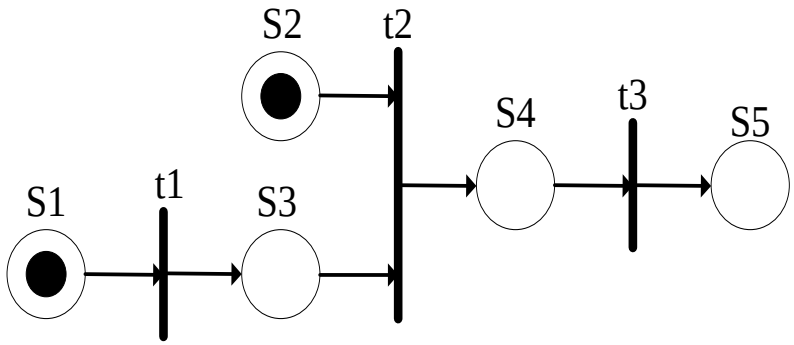


Рисунок 3 – Модель сценарію атаки «відмова в обслуговувані» (HSD)

Для того, щоб врахувати невизначеність процесів сценарію та обмежених знань про його характеристики, вхідні параметри моделі описуються за допомогою нечітких множин, що відповідає *другому пункту* наукової новизни.

Кожний з вхідних параметрів моделі описується діапазоном значень часових витрат на здійснення відповідних етапів сценарію:

$$\tau_{ij}(HSD) = \left[a_{ij}(HSD), b_{ij}(HSD)\right],$$

де a_{ij}, b_{ij} – граничні значення діапазону, i – номер стану мережі, j - номер переходу мережі

Далі використовується система нечіткого логічного висновку типу Сугено, на вхід якої подається визначена нечітка множина параметрів. Використання даної системи дозволяє проводити навчання для відповідної бази знань та мінімізувати розбіжності між моделюванням та результатами імітаційного моделювання відповідного сценарію. В результаті обчислень отримується вихідна множина значень, яка підлягає дефаззифікації. В результаті дефаззифікації отримується значення часу проходу по мережі τ_{HSD}, яке використовується для обчислення ймовірності здійснення сценарію в залежності від часу:

$$PTS(HSD) = 1 - e^{-t/\tau_{HSD}},$$

де τ_{HSD} – отримане дефаззифіковане значення, t – час функціонування системи

Сценарії, які описують помилки персоналу або збій та відмови системи, рідко можливо описати зазначеним вище методом. В таких випадках доцільно оцінити ймовірність сценарію з використанням коефіцієнту можливості помилки або збою за певний період функціонування системи:

$$PTS(TS) = 1 - e^{-\sigma t}.$$

де σ– коефіцієнт можливості помилки, збою або відмови у діапазоні [0..1], t – час функціонування системи або її елементів.

Коефіцієнт можливості характеризує впевненість експерта у тому, що при заданих характеристиках системи, здійснення даного сценарію можливе. Значення коефіцієнту задається на основі емпіричного досвіду експерту, або статистичних дос-

ліджень. В ході експериментальних випробувань було порівняно результати моделювання з експериментальними даними (рисунки 4-5).

Результати моделювання сценаріїв порівняні з відомими методами Coras та Риск-моделями ИТКС. Перший метод визначає статистичний підхід до визначення ймовірності, другий використовує моделі мереж Петрі-Маркова.

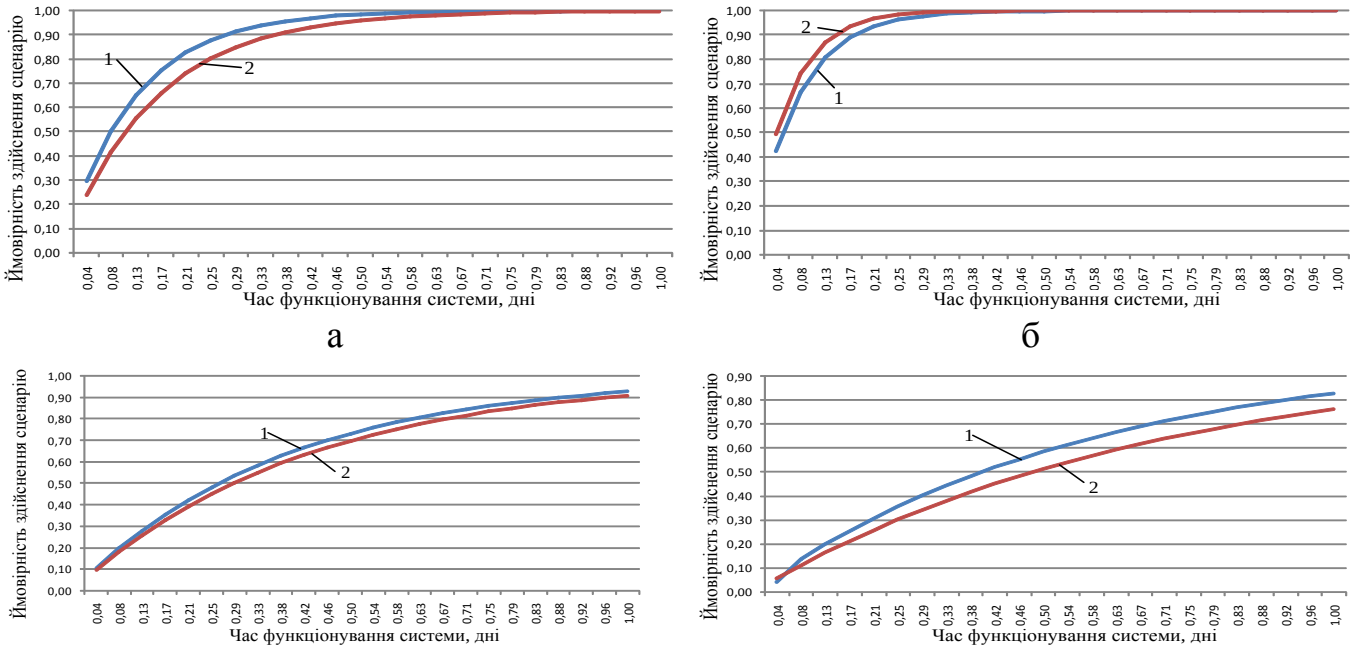


Рисунок 5 – Оцінка результатів моделювання сценаріїв: 1 – модель; 2 – експеримент; а – сценарій *FAS*; б – сценарій; *FSM* в – сценарій *VIA*; г - сценарій *HSS*

Оцінка якості моделювання проводилася з використанням критерію середньоквадратичної помилки (СКП). Генеральна вибірка складала для сценарію VIA – 20 моделювань, для сценаріїв FAS та FSM – 25 моделювань, для сценарію HSS – 35 моделювань Результати представлені в таблиці 1.

Таблиця 1 – Оцінка якості моделювання сценаріїв

Сценарій	Нечіткі моделі	Метод Coras	Риск-моделі ИТКС
HSS	0,002	0,022	0,008
VIA	0,005	0,016	0,0096
FAS	0,005	0,012	0,022
FSM	0,004	0,013	0,024
Сер-нє	0,004	0,016	0,038

Розробка даних моделей дозволяє використовувати нечіткі параметри функціонування системи в ході порушення безпеки та мінімізувати при цьому кількість експертів.

Також в роботі розроблено метод оцінки ймовірності виникнення загроз, який відповідає третьому пункту наукової новизни. Даний метод складається з чотирьох етапів:

На першому етапі будується ієрархічна структура факторів, які сприяють виникненню загрози, наприклад як на рисунку 6. При цьому, для зниження обчислювального навантаження, доцільно об’єднувати фактори за певними ознаками в групи.

На другому етапі проводиться експертна оцінка визначених факторів, яка залежить від ступеню задоволеності фактором, що передбачає не тільки наявність або відсутність даного фактору, але і ступень його впливу на виникнення загрози. Другим параметром є час функціонування системи під впливом загрози з даним фактором:

$$f_i = 1 - e^{-\alpha t}$$

де α – коефіцієнт задоволеності у діапазоні [0..1], t – час функціонування системи в днях.

Коефіцієнт α визначається на основі емпіричного досвіду учасників аналізу.

На третьому етапі проводиться ранжування визначених факторів, засноване на перевагах між факторами. Це дозволяє упорядкувати фактори за ступенем впливу на загрозу, наприклад як для мережного фактору

$$Firewall \succ_C \text{Аутентифікація} \succ_C \text{Шифрування} \succ_C NIDS$$

де $\succ_C$ – відношення переваги між факторами,

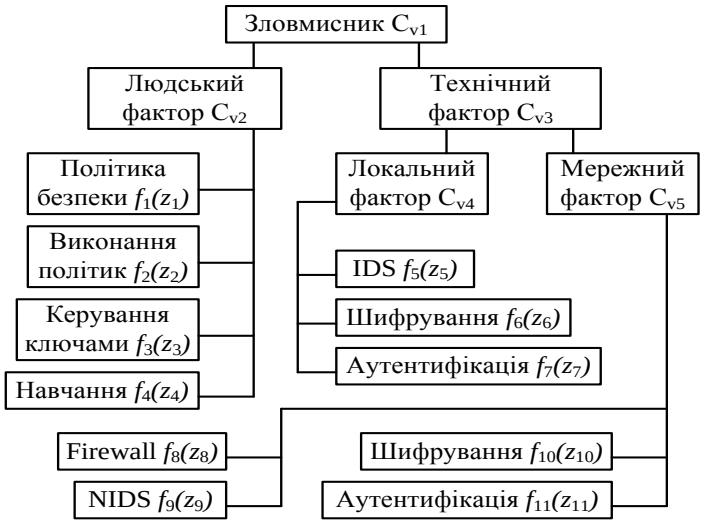


Рисунок 6 – Ієрархічна модель для загрози «зловмисник»

Дане ранжування враховується при агрегації факторів при обчисленні загальної оцінки ймовірності виникнення загрози.

На четвертому етапі визначаються нечіткі міри для кожного узагальнюючого фактору. В роботі використовувалася бібліотека kappalab у прикладному пакеті математичних розрахунків *R*. Кількість значень міри залежить від кількості підпорядкованих факторів і дорівнює 2^n, де n - кількість факторів. Враховуючи, що вхідні параметри інтегралу Шоке є функціями змінних, доцільно використати для нечітких мір обернення Мебіуса, що дозволяє представляти інтеграл лінійною функцією.

На п'ятому етапі виконується згортка визначених факторів. У якості функції згортки запропоновано використовувати нечіткий інтеграл Шоке з використанням коефіцієнтів, які отримані після обернення Мебіуса.

$C_{vi}(T_i) = p_1 f_1 + p_2 f_2 + \cdots + p_j f_j$, для агрегації оцінок окремих факторів

$C_{vk}(T_i) = p_{k1} C_1 + \cdots + p_{ki} C_i$, для агрегації складаних факторів

де f_j – експертна оцінка фактору, p_j, коефіцієнт отриманий після обернення Мебіуса, T_i – відповідна загроза

Оцінка ймовірності виникнення загроз порівняна із статистичним аналізом загроз (Coras) інформаційної безпеки та із експериментальними спостереженнями (рисунок 7). Достовірність визначення загрози складає в середньому 0.9, що на 8 % краще за статистичний метод виявлення загроз. В ході порівняння використовувались різні оцінки факторів впливу на загрозу, а також різні варіанти ранжування факторів при однакових оцінках.

В роботі розроблено метод оцінки ризиків, який характеризується *четвертим пунктом* наукової новизни. Даний метод складається з трьох етапів.

На *першому етапі* здійснюється лінгвістична оцінка рівнів ризику. Визначення ризиків здійснюється з використанням моделі взаємодії активів з розділу 2, де кожному активу ставляться у відповідність інциденти та відношення збитків. Лінгвістична змінна для оцінки рівня ризику визначається наступним чином:

– ім’я змінної – «рівень ризику»;

– область визначення U = [0..100];

– терм-множина T = {"дуже низький", "низький", "середній", високий", "дуже високий"};

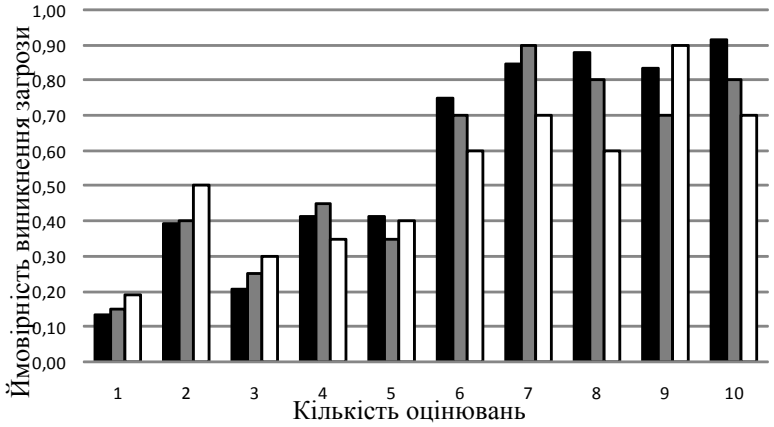


Рисунок 7 – Оцінка ймовірності виникнення загрози інформаційної безпеки: ▒ – експеримент, ■ – оцінка запропонованим методом, □ – оцінка методом Coras

На *другому етапі* здійснюється нечітка кластеризація елементів ризику. Для визначення рівня ризику використовується метод нечіткої кластеризації, який на основі оцінок ймовірності виникнення інцидентів та збитків від них дозволяє об’єднувати параметри ризиків відповідно до значень лінгвістичної змінної. Дослідним шляхом визначено, що початкову кількість кластерів доцільно задавати в діапазоні від 25 до 40, які в подальшому об’єднуються до кількості, яка дорівнює кількості термів змінної для ризику. Це дозволяє експерту втручатись в процес визначення кінцевих кластерів та проводити навчання системи для подальших ітерацій.

На *третьому етапі* здійснюється генерація правил для ризиків. На основі отриманих кластерів визначаються правила для бази знань ризиків, які дозволяють ставити у відповідність кожному рівню ризику множину комбінацій оцінок інцидентів та значень відношень збитків, що дозволяє в подальшому визначати дії, щодо обробки ризику. Для цього необхідно перетворити оцінки ймовірності виникнення

інцидентів та значення збитків у лінгвістичні змінні. Дані правила дозволяють за допомогою логічних висловлювань отримувати відповідність оцінки рівня ризику до вхідних значень інцидентів та збитків. Наприклад, правила, які описують умови низького рівня ризику мають наступний вигляд:

Правило 1: *Якщо* $P(UI)$ є «дуже низький» *та* C_{imp} є «вище середнього» *то* R є «низький»

Правило 2: *Якщо* $P(UI)$ є «низький» *та* C_{imp} є «нижче середнього» *то* R є «низький»

Правило 3: *Якщо* $P(UI)$ є «середній» *та* C_{imp} є «дуже низький» *то* R є «низький»

Також, отримані рівні ризиків доцільно відносити до прийнятних або неприйнятних, з ціллю визначення першочерговості обробки ризику.

Використання методу оцінки ризиків з використанням нечіткої кластеризації та нечітких правил баз знань дозволяє підвищити достовірність рішення про рівень ризику, що підтверджено експериментальними даними, які представлені нижче.

В четвертому розділі розроблена інформаційна технологія аналізу ризиків та проведена її апробація.

З використанням методів та моделей, розроблених в розділах 2 та 3 була розроблена інформаційна технологія аналізу ризиків, яка складається з дев'яти етапів (рисунок 8). Сірим кольором виділені етапи, які виконуються автоматизовано.

На першому етапі за участю групи експертів та уповноважених учасників аналізу ризиків визначається множина активів інформаційної системи, які підлягають захисту. Визначається взаємозв'язок між активами з ціллю виявлення відношень збитку для активів системи.

На другому етапі групою експертів визначаються інциденти, сценарії та загрози, які здатні нанести шкоду виявленим активам. На основі цих даних будується інформаційна структура елементів ризику для кожного активу, яка дозволяє структурувати вплив виявлених елементів на кожний актив.

На третьому етапі групою експертів, за участю уповноважених учасників, визначаються лінгвістичні змінні для усіх типів відношень, активів та ризиків.

На четвертому етапі проводиться оцінка ймовірності виникнення загроз. Із залученням адміністраторів системи, експертом(ми) визначається множина факторів, які сприяють виникненню загрози. Проводиться групування цих факторів, їх ранжування, та обчислюється загальна оцінка кожної виявленої загрози.

На п'ятому етапі проводиться моделювання та оцінка ймовірності здійснення виявлених сценаріїв. За можливої участі адміністраторів, визначаються етапи сценаріїв та їх характеристики здійснення. Визначається множина місць вразливості. За необхідністю проводиться імітаційне моделювання відповідного сценарію.

На шостому етапі проводиться оцінка ймовірності виникнення інцидентів з використанням визначених у роботі моделей інцидентів.

На сьомому етапі проводиться кластеризація оцінок ймовірності виникнення інцидентів та збитків від них, що дозволяє визначити ризиків по відповідним рівням для кожного активу інформаційної системи. Первинна кількість кластерів

об’єднується до кількості, визначеної кількістю термів відповідної лінгвістичної змінної.

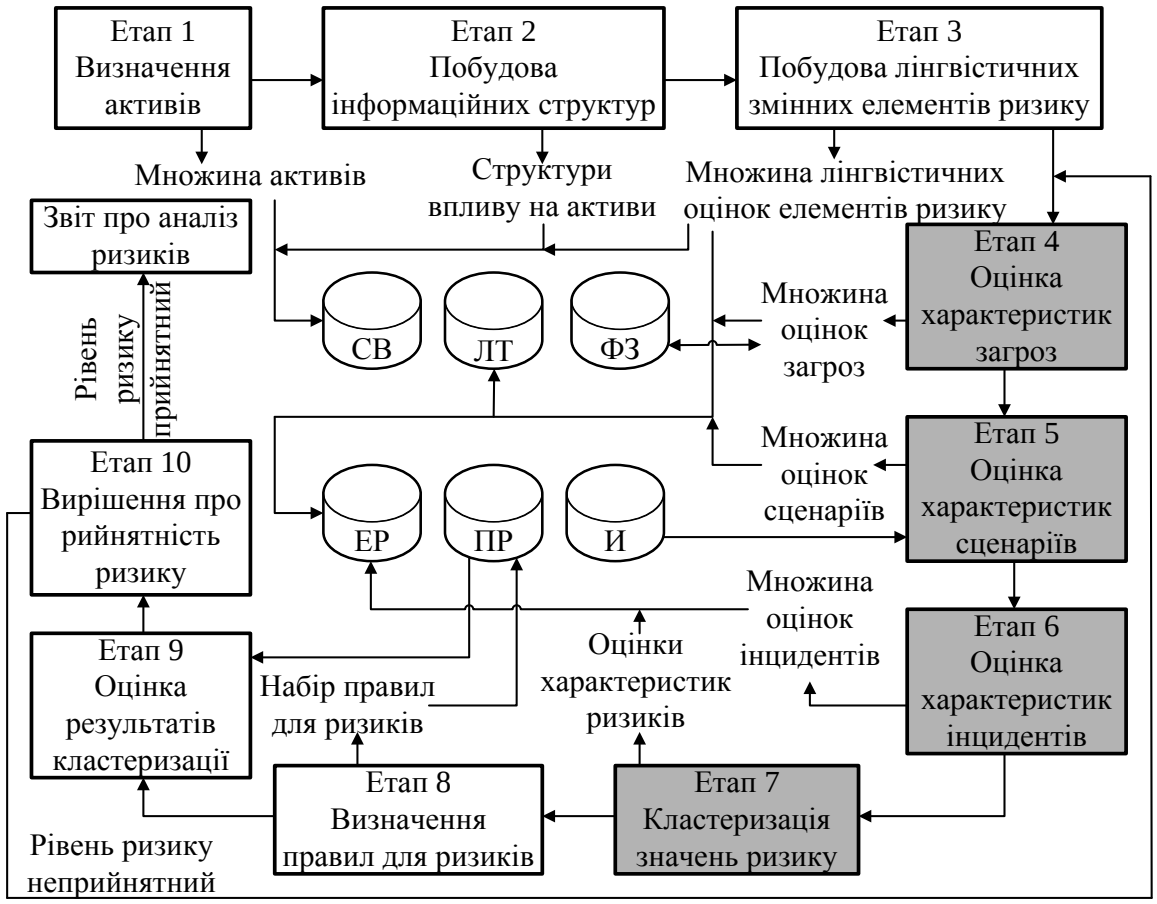


Рисунок 8 – Інформаційна технологія аналізу ризиків: СВ – БД структур впливу на активи, ЛТ – БД лінгвістичних термів, ФЗ – БД факторів впливу на загрози, ЕР – БЗ елементів ризику; ПР – БЗ правил для ризиків; И – БЗ імітаційного моделювання

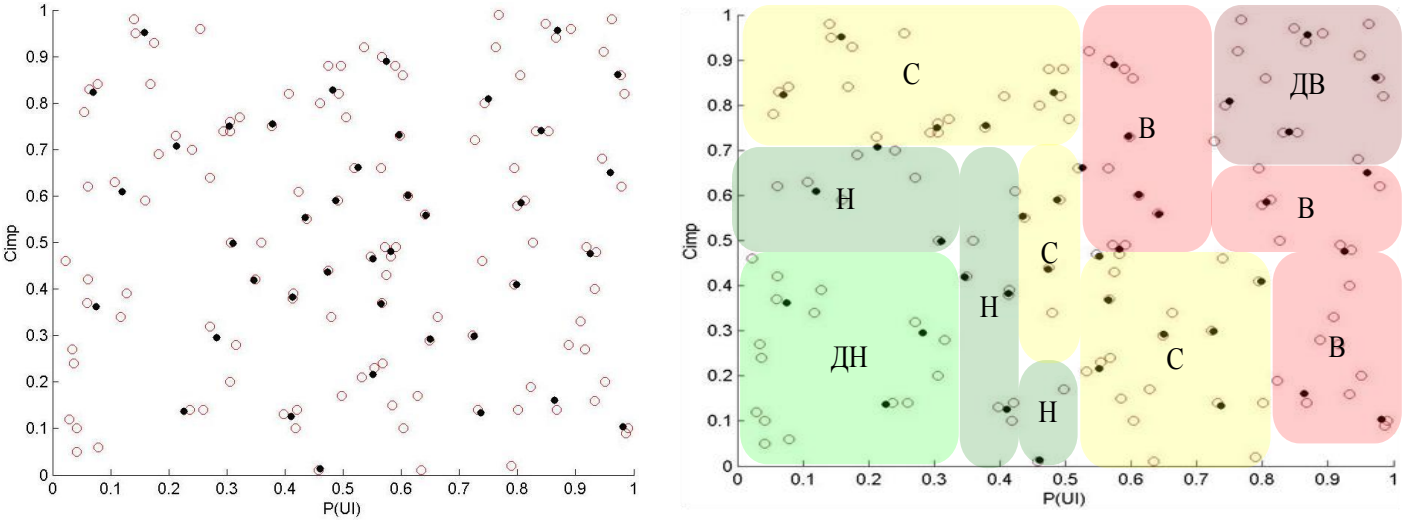
На восьмому етапі на основі отриманої кластеризації будуються відповідні правила для бази знань ризиків, які зв’язують вхідні дані інцидентів та збитків від них з відповідним рівнем ризику.

На дев’ятому етапі здійснюється порівняльна оцінка ризиків. Визначається можливість прийнятного або неприйнятного рівня ризиків для кожного активу у відповідності до цілей менеджменту ризиків.

На десятому етапі приймається рішення про прийнятність рівня ризику. Якщо рівень прийнятний, готується звіт про результати аналізу ризиків, якщо рівень ризику неприйнятний, здійснюється повернення до етапу 4.

Для апробації інформаційної технології було проведено експериментальні дослідження для оцінки ризиків для активу «доступність сервісів». Із залученням п’яти експертів було визначено 3 загрози, 4 сценарії та 3 інциденти. З використанням різних комбінацій оцінки та ранжування факторів загроз, параметрів сценаріїв та вхідних параметрів моделей інцидентів було здійснено 120 оцінок ризиків. На

першої ітерації отримано 40 центрів кластерів (рисунок 10а). Далі кластери об’єднуються до визначеної кількості (рисунок 10б).



а б

Рисунок 10 – Кластеризація ризиків активу: а – вихідні дані та отримані кластери, б – об’єднані кластери; дн – дуже низький, н - низький, с – середній, в – високий, дв – дуже високий

Для визначення відповідності проведеного аналізу ризиків до експериментальних спостережень порушення безпеки, було використано систему нечіткого логічного висновку, де проводилося навчання з використанням отриманих результатів у якості вхідного масиву даних, та результатів експерименту у якості навчальної множини даних (рисунок 11).

Кількість вірних рішень про рівень ризику представлена на рисунку 12.

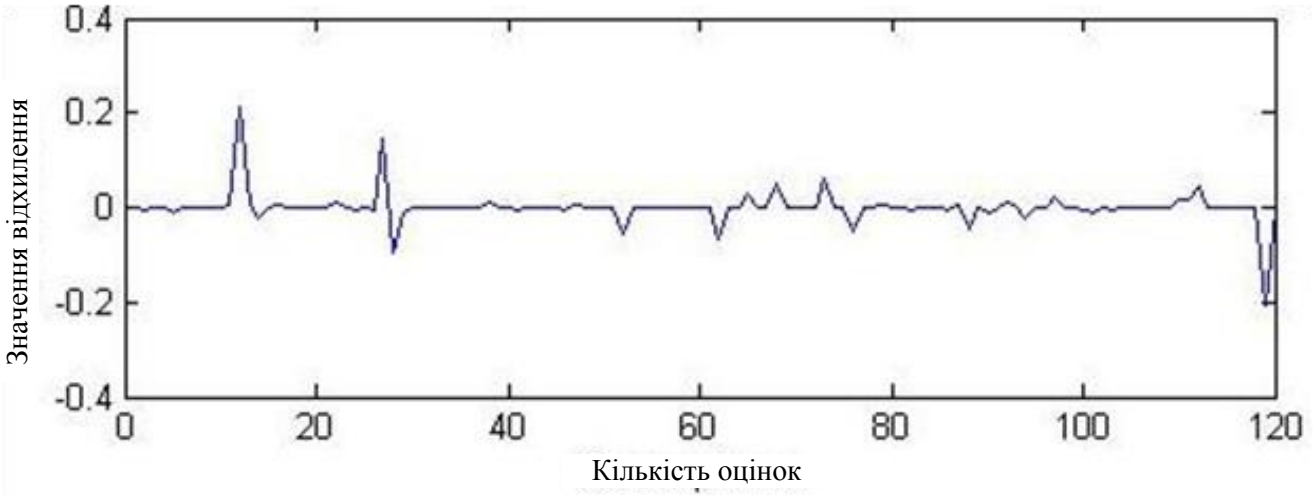


Рисунок 11 – Відхилення значень ймовірності виникнення інцидентів від експериментальних

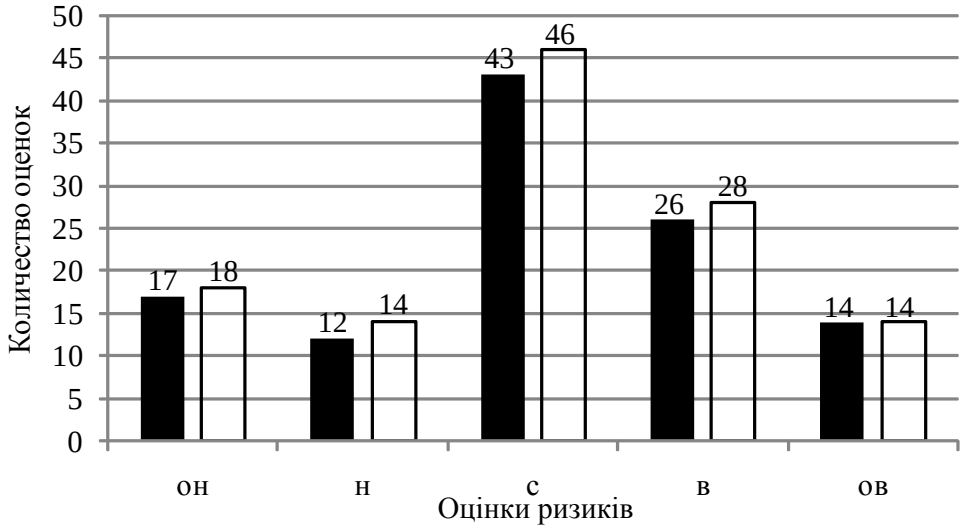


Рисунок 12 – Кількість вірних рішень про рівень ризику: дн – дуже низький, н - низький, с – середній, в – високий, дв – дуже високий; ■ – інформаційна технологія, □ – експериментальні оцінки

Порівняльна характеристика розробленої технології аналізу ризиків з відомими сучасними методами проводилася за наступними показниками:

– оцінка достовірності рішення про рівень ризику;

– оцінка ймовірності помилки першого роду;

– оцінка ймовірності помилки другого роду.

При порівнянні визначалась загальна достовірність рішення, та окремі рішення про кожний рівень ризику (Таблиця 2).

Таблиця 2 – Порівняння методів аналізу ризиків

Рівень ризику	Інформаційна технологія	Coras	Риск-моделі ИТКС
Достовірність			
дн	1	0.94	1
н	0.93	0.87	0.87
с	0.95	0.71	0.90
в	0.94	0.73	0.85
дв	1	0.79	0.93
Середнє	0.96	0.81	0.91
Ймовірність помилки першого роду			
	$\alpha = 0.017$	$\alpha = 0.067$	$\alpha = 0.033$
Ймовірність помилки другого роду			
	$\beta = 0.025$	$\beta = 0.158$	$\beta = 0.067$

Порівняння результатів оцінки ризиків показало, що достовірність оцінки з використанням розробленої інформаційної технології в середньому складає 0.96, що

краще в середньому на 5 % при рішенні про прийнятний рівень ризику та на 8 % при рішенні про неприйнятний рівень ризику ніж у відомих методів. Кількість помилок другого роду склала 2,5 %, що в середньому краще на 4,2 % ніж у математичних методів та до 13 % ніж у статистичних методів.

ВИСНОВКИ

У дисертаційній роботі вирішено науково-технічну задачу, яка полягає у розробці моделей та методів аналізу ризиків безпеки інформаційних систем, на основі застосування та удосконалення моделей з нечіткими параметрами, а також використанні нечіткого інтегралу для агрегації параметрів моделей та нечітких баз знань для оцінки рівня ризиків.

1. Проведено аналіз особливостей загроз інформаційної безпеки та методів аналізу та оцінки ризиків. Це дозволило виділити основні етапи виявлення об'єктів та процесів порушення інформаційної безпеки з подальшою оцінкою ризиків нанесення збитку активів.

2. Розроблено метод лінгвістичної оцінки активів інформаційної системи. Використання даного методу дозволило оцінювати властивості активів як в якісному форматі, так і в кількісному форматі. Це дозволяє проводити оцінку не тільки експертами, але й менш кваліфікованими учасниками аналізу, що дозволяє мінімізувати кількість експертів.

3. Розробка та використання моделей сценаріїв нечіткими параметрами дозволили підвищити точність моделювання сценаріїв порушення безпеки. В ході експериментальних досліджень в роботі було виявлено, що використання даних моделей покращило визначення ймовірності реалізації сценаріїв загроз у системі на 7 – 17 % в залежності від типу сценарію.

4. Розроблений метод оцінки ймовірності виникнення загроз дозволив структурувати фактори впливу на виникнення чинників подій безпеки. Есперементально доказано, що даний метод дозволяє оцінювати можливість виникнення загрози на основі множини факторів впливу з достовірністю 0.9, що на 8 % краще ніж відомі методи.

5. Використання нечіткого інтегралу та коефіцієнтів, заснованих на нечіткій мірі, дозволило підвищити точність оцінювання ймовірностей виникнення загроз і інцидентів, та ймовірність реалізації сценаріїв загроз.

6. Розроблений в роботі метод лінгвістичної оцінки ризиків з використанням нечіткої кластеризації значень інцидентів та збитків від них дозволив виявляти низькі та високі рівні ризиків з достовірністю 0.97 та 0.96 відповідно, за краще за відомі методи на 5 – 8 %.

7. Розроблено інформаційну технологію аналізу ризиків безпеки інформаційних систем, яка дозволяє автоматизувати основні етапи оцінки елементів ризиків та знизити кількість учасників процесу аналізу. Використання даної інформаційної технології дозволило оцінювати рівні ризиків з середньою достовірністю 0.96 з ймовірністю помилкового рішення 0.025.

8. Впровадження розробленої інформаційної технології на ТОВ «Телекарт-Прилад» (м. Одеса) дозволило підвищити достовірність оцінки ризиків на 7-11%. В

ході подальшого періодичного моніторингу ризиків було витрачено на 23 % менше часу, що дорівнює 10 годинам, проти 13 годин до впровадження інформаційної технології.

ПЕРЕЛІК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації

1. Шапорин, В. О. Метод расчета размеров буферов коммутаторов / Шапорин Р. О., Шапорин В. О., Милейко И. Г. // Труды Одесского политехнического университета, № 2(28), 2007 – С. 116-118.

Видання входить до міжнародних наукометричних баз Citefactor, CNKI Scholar, CrossRef, DOAJ, EBSCO, ERIHPLUS, Google Scholar, Index Copernicus, Polish Scholarly Bibliography, Primo Central (ExLibris), Український реферативний журнал «Джерело», Реферативний журнал (ВІНІТІ), РІНЦ, SHERPA/RoMEO, Ulrich's Periodicals Directory, Universal Impact Factor, WorldCat..

2. Шапорин, В. О. Влияние широковещательного и служебного трафика на пропускную способность корпоративной компьютерной сети / Шапорин Р. О., Шапорин В. О. // Електромашинобудування та електрообладнання, № 72, 2009 – С. 113-115.

Видання входить до міжнародних наукометричних баз:Google Scholar, РІНЦ.

3. Оценка вероятности проведения атаки на сетевые ресурсы с использованием аппарата нечеткой логики / В. О. Шапорин, П. М. Тишин, Н. Б. Копытчук, Р. О. Шапорин // Електротехнічні та комп'ютерні системи. – К.: Техника. – 2013.– № 12 (88). – С. 95 – 101.

Видання входить до міжнародних наукометричних баз Google Scholar, РІНЦ.

4. Шапорин, В. О. Лингвистическая оценка активов сложной компьютерной системы для анализа рисков информационной безопасности / В. О. Шапорин, П. М. Тишин, Р. О. Шапорин // Електротехнічні та комп'ютерні системи. – К.: Техника. – 2015.– № 18 (94). – С. 28 – 32.

Видання входить до міжнародних наукометричних баз Google Scholar, РІНЦ.

5. Шапорин, В. О. Разработка моделей угроз информационной безопасности для оценки вреда активам / Шапорин В. О., Плачинда О. Е. // Технологический аудит и резервы производства. – 2015. – Том 4 №2 (24). – С. 10-15.

Видання входить до міжнародних наукометричних баз Google Scholar, Ulrich's Periodicals Director, DRIVER, BASE, Index Copernicus, РІНЦ, ResearchLib, DOAJ, WorldCat, EBSCO, Directory Indexing of International Research Journals, DRJI, OAJI, Sherpa/Romeo, Open Access Articles.

6. Шапорин, В. О. Разработка лингвистической модели оценки рисков активов информационной системы / Шапорин В. О., Тишин П. М., Шапорин Р. О., Копитчук Н. Б. // Восточно-Европейский журнал передовых технологий. – 2015. том 4 №2(76). – С.30-35.

Видання входить до міжнародних наукометричних баз Google Scholar, Ulrich's Periodicals Director, DRIVER, BASE, Index Copernicus, WorldCat, РІНЦ, DOAJ, EBSCO, American Chemical Society,DRJI, CrossRef, OAJI.

Опубліковані праці апробаційного характеру

7. Шапорин, В. О. Метод проектирования коммуникационной системы компьютерной сети масштаба предприятия / Шапорин Р. О., Шапорин В. О., Фомина А. А. // Тез. доп. 8-ї міжнар. конф. СІЕТ, 2007 – с. 135.

8. Шапорин, В. О. Аналіз проблем маршрутизації в mesh-мережах / Шапорін Р. О., Шапорін В. О., Кобилянська О. Л. // Тез.доп. 12-ї міжнародної науково-практичної конференції СІЕТ, 2011 – С.139.

9. Шапорин, В. О. Нечеткие лингвистические модели обеспечения безопасности компьютерных сетей / Шапорин В. О., Тишин П. М., Копытчук Н. Б., Шапорин Р. О. // Тез.доп. 14-ї міжнародної науково-практичної конференції СІЕТ, 2013 – с. 155-156.

10. Шапорин, В. О. Разработка нечетких лингвистических моделей сетевых атак для анализа рисков в распределенных информационных системах / Шапорин В. О., Тишин П. М., Копытчук Н. Б., Шапорин Р. О. //Тез. доп. 15-ї міжнародної науково-практичної конференції СІЕТ, 2014 – с. 131-132.

11. Шапорин, В. О. Определение прав доступа к удаленной лаборатории / Шапорин В. О., Шапорина Е. Л., Перебейнос И. А.// Тез. доп. 15-ї міжнародної науково-практичної конференції СІЕТ, 2014 – с. 100-101.

12. Шапорин, В. О. Автоматизированная система мониторинга экологической ситуации / Шапорин В. О., Шапорина Е. Л., Желиховская Ю. С. //Тез. доп. 15-ї міжнародної науково-практичної конференції СІЕТ, 2014 – с. 60-61.

13. Шапорин, В. О. Способы обеспечения безопасности компьютерных сетей / Шапорин В. О., Шапорина Е. Л., Кощей А. Д. //Тез. доп. 15-ї міжнародної науково-практичної конференції СІЕТ, 2014 – с. 141-142.

14. Шапорин, В. О. Факторы влияния на возникновение угроз безопасности информационной системы / Шапорин В. О. Бабий А. А. // Мат. сем. "Моделювання в прикладних наукових дослідженнях",– 2015. – Вип. XXIII. - с. 77-78.

АНОТАЦІЯ

Шапорін В. О. **Моделі та методи аналізу ризиків безпеки інформаційних систем.** – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. – Одеський національний політехнічний університет, МОН України, Одеса, 2016.

Дисертація присвячена підвищенню достовірності процесу аналізу та оцінки ризиків, а також якості визначення ймовірності виникнення загроз та небажаних інцидентів в інформаційних системах при побудові комплексних заходів щодо забезпечення інформаційної безпеки систем. Досліджено та проаналізовано сучасні методи ідентифікації та аналізу ризиків, методи моделювання атак на інформаційну безпеку, а також методи оцінки ризиків. Розроблено метод оцінки ймовірності виник-

нення загроз інформаційної безпеки. Розроблено моделі сценаріїв загроз з нечіткими параметрами функціонування. Розроблено моделі оцінки інцидентів безпеки у інформаційних системах. Розроблено метод оцінки ризиків на основі нечіткої кластеризації та нечітких правил баз знань. Проведено експериментальні дослідження розробленої технології, а також апробована дана технологія у різних прикладних галузях.

Ключові слова: ідентифікація ризику, аналіз ризику, оцінка ризику, моделювання атак, інформаційна безпека, нечіткі множини, нечіткий логічний висновок

ABSTRACT

Shaporin V. O. **Models and methods of risk analysis of security of information systems. - The manuscript**.

The thesis for the degree of candidate of technical sciences, specialty 05.13.06 - Information technologies. - Odessa National Polytechnic University, Ministry of Education of Ukraine, Odessa, 2016.

The thesis is devoted to increasing the reliability of process analysis and risk assessment, as well as determine the potential threats and unwanted incidents in information systems in the construction of comprehensive measures to ensure the security of information systems. Investigated and analyzed the current methods of identification and risk analysis, modeling attacks on information security and risk assessment methods. The method of assessment of the potential threats to information security. The models scripting threats with fuzzy parameters functioning. The models of evaluation security incidents in information systems. The method of risk assessment based on fuzzy clustering and fuzzy rules knowledge bases. Experimental study of the technology developed and tested this technology in various application fields.

Keywords: risk identification, risk analysis, risk assessment, modem-lation attacks, information security, fuzzy sets, fuzzy logical conclusion

АННОТАЦИЯ

Шапорин В. О. **Модели и методы анализа рисков безопасности информационных систем**. - На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.06 - Информационные технологии. - Одесский национальный политехнический университет, МОН Украины, Одесса, 2016.

Диссертация посвящена повышению достоверности процесса анализа и оценки рисков, а также качества определения вероятности возникновения угроз и нежелательных инцидентов в информационных системах при построении комплексных мероприятий по обеспечению информационной безопасности систем. Исследованы и проанализированы современные методы идентификации и анализа рисков, методы моделирования атак на информационную безопасность, а также методы оценки рисков. Разработан метод оценки вероятности возникновения угроз информационной безопасности. Разработаны модели сценариев угроз с нечеткими параметрами функционирования. Разработаны модели оценки инцидентов безопасности в информационных системах. Разработан метод оценки рисков на основе нечеткой кластеризации и нечетких правил баз знаний. Проведены экспериментальные иссле-

дования разработанной технологии, а также апробирована данная технология в различных прикладных областях.

Научная новизна диссертационной работы заключается в том, что впервые разработаны иерархические модели оценки ущерба активам информационной системы на основе нечеткого интеграла и нечеткой меры, позволяющей повысить достоверность оценки ущерба данным активам. Впервые разработаны модели оценки возникновения угроз информационной безопасности на основе нечеткого интеграла и нечеткой меры, позволяющей повысить достоверность оценки вероятности возникновения угроз. Впервые разработаны модели оценки вероятности инцидентов безопасности на основе нечеткого интеграла и нечеткой меры, позволяющей повысить точность определения и оценки данных событий в информационных системах. Получили дальнейшее развитие методы моделирования сетевых атак за счет применения нечетких параметров и нечеткого логического вывода, позволяет повысить достоверность оценки вероятности осуществления данных атак.

Испытания разработанной информационной технологии показали:

– определение вероятности реализации сценариев угроз в системе улучшилось на 7 - 17%;

– оценка вероятности возникновения угрозы на основе множества факторов влияния осуществляется с достоверностью 0.9, что на 8% лучше чем известные методы;

– лингвистическая оценка рисков с использованием нечеткой кластеризации позволяет выявлять низкие и высокие уровни рисков с достоверностью 0.97 и 0.96 соответственно, что лучше известны методы на 5 - 8%;

– общая достоверность оценки уровней рисков с использованием разработанной информационной технологии составила в среднем 0.96 с вероятностью ошибочного решения 0.025.

Ключевые слова: идентификация риска, анализ риска, оценка риска, моделирование атак, информационная безопасность, нечеткие множества, нечеткий логический вывод