ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ОЦІНКА ЕФЕКТИВНОСТІ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КРИТИЧНИХ ІНФРАСТРУКТУРАХ: АНАЛІЗ РИЗИКІВ ТА РЕКОМЕНДАЦІЇ»

на здобуття освітнього ступеня бакалавра
зі спеціальності __125 _____
Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____Серафім ТОДОРІКА

Виконав: здобувач вищої освіти групи УБД 42
__ТОДОРІКА Серафім_____

Керівник:___МУЖАНОВА Тетяна_____
к.н.д.у, доцент (ПРІЗВИЩЕ, Ім’я)

Рецензент:_____
к.т.н., доцент (ПРІЗВИЩЕ, Ім’я)

Київ 2024

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____Світлана Легомінова

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУРОБОТУ

_____Тодіріці Серафіму Юрійовичу_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Оцінка ефективності тестування на проникнення в критичних інфраструктурах: аналіз ризиків та рекомендації»
керівник кваліфікаційної роботи Тетяна Мужанова к.н.д.у, доцент
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « » 2024 р. №

2. Строк подання кваліфікаційної роботи 15.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
__Цільові комп'ютерні атаки на критичні інформаційні інфраструктури.
__Найбільш безпечні уразливості для інформаційних систем критичної інфраструктури.
__Стійкість в забезпеченні цілісності та доступності інформації, що обробляється в інформаційних системах критичних інфраструктур.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.__Аналіз ризиків, які породжують уразливості інформаційних систем критичної інфраструктури
2.__Аналіз цільових комп'ютерних атак на критичні інформаційні структури
3.__Аналіз методів забезпечення стійкості обчислень в умовах впливу шкідливого програмного забезпечення на інформаційні системи критичних інфраструктур

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах_____
_____

6. Дата видачі завдання _____15.10.2023_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Серафім ТОДОРІКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Тодоріка С.Ю. «Оцінка ефективності тестування на проникнення в критичних інфраструктурах: аналіз ризиків та рекомендації».

Кваліфікаційна робота зі спеціальності 125 «Кібербезпека та захист інформації», рівень освіти другий «Бакалавр», галузь знань 12 «Інформаційні технології», – Державний університет інформаційно-комунікаційних технологій: Київ, 2024.

В кваліфікаційній роботі здійснено ретельний аналіз стандарту *NIST SP* 800 – 115, зокрема розглянуто: форми заходів оцінювання інформаційної безпеки (ІБ); етапи оцінювання ІБ; способи аналізу та тестування, які використовуються під час оцінювання ІБ; форми та послідовність проведення тестування на проникнення; вразливості, що перевіряються; рекомендований інструментарій проведення аналізу та тестування, що подано в *NIST SP* 800 – 115 . Зроблено висновки про сильні та слабкі сторони стандарту *NIST SP* 800 – 115. Надано рекомендації щодо використання стандарту *NIST SP* 800 – 115 під час розроблення галузевого проекту стандарту тестування на проникнення.

Робота складається із вступу, трьох розділів, висновків, списку використаних джерел : 60 с., 6 рисунків, 14 таблиць, 35 джерел. У вступі обґрунтовується актуальність теми та формуються завдання дослідження.

Об'єкт дослідження – процеси забезпечення інформаційної безпеки в інформаційних системах критичних інфраструктур.

Предмет дослідження – методи та алгоритми щодо оцінок ризиків успішно реалізованих цільових комп'ютерних атак на інформаційні системи критичних інфраструктур.

Мета роботи – розробка методу керування ризиками інформаційної безпеки інформаційних систем критичної інфраструктури в умовах цільових комп'ютерних атак.

Методи дослідження – методи теорії нечітких множин, теорії ймовірності.

Галузь використання – захист інформації на об’єкті інформаційної діяльності.

Ключові слова: *інформаційні системи, ризики інформаційної безпеки, цільові комп'ютерні атаки, функція ризику інформаційної безпеки.*

REFERENCE

Todorika S.Y. "Evaluation of the effectiveness of penetration testing in critical infrastructures: risk analysis and recommendations".

Qualification work in the specialty 125 "Cybersecurity and Information Protection", level of education second "Bachelor", field of knowledge 12 "Information Technology" - State University of Information and Communication Technologies: Kyiv, 2024.

The qualification work carried out a thorough analysis of the standard, in particular: forms of information security (IS) assessment measures; stages of IS assessment; methods of analysis and testing used in the assessment of IS; forms and sequence of penetration testing; vulnerabilities to be tested; recommended tools for analysis and testing, which are given in. The conclusions about the strengths and weaknesses of the standard are made. Recommendations for using the standard in the development of an industry draft penetration testing standard are provided.

The paper consists of an introduction, three chapters, conclusions, a list of references: 60p., 6 figures, 14 tables, and a 35 source. The introduction substantiates the relevance of the topic and formulates the research objectives.

Object of research - processes of ensuring information security in information systems of critical infrastructures.

The subject of research is methods and algorithms for assessing the risks of successfully implemented targeted computer attacks on information systems of critical infrastructures.

Purpose - to develop a method for managing the risks of information security of critical infrastructure information systems in the face of targeted computer attacks.

Research methods - methods of fuzzy set theory, probability theory.

Field of application - information security at the object of information activity.

Keywords: *automated control systems, risks to the information security system, assets.*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КІІ – критична інформаційна інфраструктура

ІС– інформаційна система

ОІД – об'єкт інформаційної діяльності

КІ – критична інфраструктура

ЦКА – цільова комп'ютерна атака

ПКІ – підприємство критичної інфраструктури

ПЗ– програмне забезпечення

НСД – несанкціонований доступ

ІБ – інформаційна безпека

ІР – інформаційні ризики

БД – бази даних

ВСТУП

Актуальність теми. Як відомо, критична інформаційна інфраструктура (надалі - КІІ) є відкритою системою, яка забезпечує взаємодію зі сполученими інформаційними системами. Це призводить до спроможності реалізувати віддалений деструктивний інформаційний вплив з боку зловмисників. При цьому тривалість підготовки та сама реалізація деструктивного інформаційного впливу на КІІ може здійснюватися протягом тривалого часу [1].

Втрата працездатності КІІ не проявляється миттєво у вигляді стрибкоподібного процесу, а є наслідком зниження якості основних показників її функціонування та їх виходу за межі допусків. Процес зміни показників, що характеризують якість функціонування, займає деякий проміжок часу, який визначається вихідними значеннями показників, а також різними факторами, що впливають [2].

Сьогодні завдання інформаційної безпеки об'єктів критичної інфраструктури є одним з головних завдань. Водночас поточні завдання аудиту інформаційної безпеки об'єктів критичної інфраструктури, як правило, обмежуються перевіркою їх на відповідність вимогам з ІБ з боку керівних документів. Однак за такого підходу до аудиту, найчастіше, залишається незрозумілою захищеність цих об'єктів від існуючих кібератак хакерів. Для об'єктивної перевірки такої захищеності над об'єктами проводиться процедура тестування, а саме - тестуванню на проникнення. Вказівки щодо проведення такого тестування, наприклад, містяться в рекомендаціях НБУ щодо перевірки ІБ банківських систем. Однак, стримуючим фактором у проведенні тестування на проникнення українських об'єктів критичної інфраструктури є відсутність єдиного вітчизняного стандарту проведення такого тестування.

Таким чином, постає завдання підтримання КІІ в працездатному стані впродовж деякого часу, необхідного для проведення заходів щодо нейтралізації негативних наслідків впливу. Відмову КІІ слід визначати як подію, що полягає у виході параметрів її функціонування за встановлені межі, тобто відбувається накопичення несправності, відмова розповсюджується в часі [2,3]. Склад і обсяг заходів щодо підвищення стійкості КІІ до деструктивних впливів і нейтралізації загроз інформаційній безпеці базується не тільки на оцінці поточного стану КІІ, а й на прогнозі їхньої зміни на деякий відрізок часу, необхідний для вжиття відповідних заходів. При цьому проблему забезпечення безпеки функціонування КІІ в умовах деструктивного інформаційного впливу слід розглядати в комплексі із забезпеченням її технічної надійності та безпеки [1,2,3].

Об`єкт дослідження. процеси забезпечення інформаційної безпеки в інформаційних системах критичних інфраструктур.

Предмет дослідження. Методи та алгоритми розрахунку ризиків інформаційної безпеки на інформаційну систему критичної інфраструктури.

Метою даної роботи є розробка методу керування ризиками інформаційної безпеки інформаційних систем критичної інфраструктури в умовах цільових комп'ютерних атак.

Методи дослідження. методи теорії ймовірності та теорії випадкових процесів, методи нечітких множин, теорія графів.

РОЗДІЛ 1 АНАЛІЗ РИЗИКІВ, ЯКІ ПОРОДЖУЮТЬ УРАЗЛИВОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Уразливість інформаційних систем критичної інфраструктури та загрози їм

Під ***аналізом вразливостей*** будемо розуміти множину процесів, які спрямовані на дослідження елементів інформаційної системи (ІС) на наявність довільних загроз, уразливих вузлів (точок) та наявність при цьому ризиків потенційного несанкціонованого проникнення зловмисників в ІС.

Під ***уразливістю*** будемо розуміти слабкий компонент ІС, яка функціонує на об'єкті інформаційної діяльності (ОІД). Критична інфраструктура (КІ) є одним з прикладів ОІД. Під ***загрозою інформаційній системі*** (ЗІС) будемо розуміти спроможність негативного впливу зловмисником, який може спричинити компрометацію службової, комерційної, конфіденційної та таємної інформації. З урахуванням введених означень, в такому аналізі фігурує третя особа, під якою розуміють зловмисника, який, виявивши вразливість ІС , здійснює цільову комп'ютерну атаку (ЦКА) на ІС.

Наявність вразливостей призводить до негативного знаку в роботі всього підприємства критичної інфраструктури (ПКІ), оскільки це призводить до порушення роботи ПКІ, що в свою чергу може призвести до дуже негативних наслідків на державному рівні за рахунок спрощення роботу зловмисників з нанесення шкоди і дає змогу третім особам отримати доступ до конфіденційної інформацію, до спотворення інформації та блокуванню доступу до інформації (відмова в обслуговуванні).

Джерело загрози може мати як випадкову природу так і бути детермінованим (навмисним).

В даній роботі ми не розглядаємо техногенні та природні чинники, які також є загрозами.

У кожної загрози є свій банк вразливостей, за допомогою яких зловмисник може реалізувати свою мету.

В професійній діяльності фахівців з кібербезпеки широко застосовується процес тестування на проникнення (пентест), за результатом якого кожній уразливості присвоюється певний клас небезпеки. Ця оцінка не є суб'єктивною, вона ґрунтується методиках, які отримали якісного практичного застосування. На основі таких методик прийнято класифікувати й оцінювати вразливості ІС.

Варто відмітити, що існує різниця між уразливостю та загрозою. Загрози в інформаційній безпеці (ІБ) уявляють собою потенційні небезпеки, які можуть виникнути в ІС, при умові, що хакер (зловмисник) використовує її вразливості для кібератак (цільових комп'ютерних атак). На рисунку 1.1 представлено всі загрози, які існують в ІС.

Рисунок 1.1. Загрози, які існують в інформаційних системах

Число вразливостей дуже велике і з часом їх кількість тільки зростає. Уразливості - це певні дефекти в програмному забезпеченні (ПЗ), вади в обладнанні, в заходах із забезпечення безпеки ПКІ з погляду людського чинника (доступи, перепустки), що надають зловмиснику можливість здійснювати в ІС

несанкціонований доступ (НСД). Сама вразливість швидко виникає, якщо ІБ відсутня або є достатньо слабкою.

Виявивши вразливість, зловмисник, який здійснює кібератаку отримує можливість реалізувати загрозу. Те, що дає можливість використовувати вразливості, називається джерелом загрози (**threat agent**). Таким джерелом є хакер або несумлінний або помилковий працівник, через якого стався витік конфіденційної інформації або той хто пошкодив файли. Також загрозою є процес, який забезпечує доступ до даних в обхід політики безпеки або обставини непереборної сили (землетрус, який зруйнував будівлю).

На рисунку 1.2 представлено можливий прояв уразливостей.

Рисунок 1.2. Прояв уразливостей

1.2. Класифікація загроз інформаційним системам і аналіз інформаційних ризиків

Сучасні системи, які функціонують в критичних інфраструктурах визначаються наявністю такої складової, як інформаційна система (ІС). В сучасному часі вимагається в умовах обмеженої можливості фінансування, проектування та розроблення ІС потребує враховувати захищеність таких ІС від ризиків.

Згідно класичного означення ризику - це комбінація ймовірності події та її наслідків [4].

Серед множини існуючих ризиків українські та зарубіжні автори виокремлюють операційний ризик відповідно до Базель II [5], що визначається ризиком прямих або непрямих втрат, джерелами яких можуть бути хибні або не відповідні роботі КІ внутрішні процеси, кадрові ресурси та системи або зовнішні впливи. Наслідком виникнення вказаних зовнішніх впливів є порушення достовірності, повноти та актуальності інформації, яка акумулюється та обробляється.

Отже, *інформаційний ризик* (ІР) можна розглядати як вид операційного ризику, що виникає внаслідок неадекватних та хибних внутрішніх процесів, дій працівників або зовнішніх впливів, джерелом яких є інформаційні активи підприємства - матеріальні та нематеріальні об'єкти. В групі стандартів ISO27001 [6] відзначається, що *IP* - це потенційна можливість того, що загроза використовує вразливість активу або групи активів, завдаючи шкоди підприємству або установі.

Сам ризик породжує інцидент інформаційної безпеки – це одне або декілька інцидентів, які призводять до несанкціонованого доступу до конфіденційної або таємної інформації, або до модифікації інформації, що обробляється в ІС КІ, або

блокуванню доступу до інформації що при певному значенні ймовірності призводить до порушення технологічних процесів в КІ.

Отже, для здійснення аналізу ІР, необхідно визначити самі об'єкти КІ та їх вразливості, на які спрямовані кібератаки, для успішної їх реалізації.

Вектори ІР спрямовані на інформацію, мережеве ПЗ, системне ПЗ та прикладне ПЗ, персональні комп'ютери, накопичувальні та друкувальні пристрої, мережеві сервери, шлюзи, інтерфейси, сервіси, які є основними активами КІ, які забезпечують отримання, обробку та передачу інформації В ІС КІ. В таблиці 1.1 представлено основні активи ПКІ, відповідна уразливість та наявність існуючих при цьому загроз.

Таблиця 1.1. Активи, їх уразливість та наявність загроз

Актив	Уразливість	Загроза
Конфіденційна інформація та конфіденційна база даних	Не достатня якість навчання в галузі інформаційної безпеки	Проблемні ситуації в технічній підтримці
	Не достатня якість навчання в галузі інформаційної безпеки	Помилки або халатність користувачів
	Рівень складності інтерфейсу користувачів в ІС	
	Відсутність моніторингу доступу до системного та прикладного ПО	Несанкціонований доступ до ПО з метою його використання
	Відсутність правил коректного використання засобів комунікацій та процесу передачі службової інформації	Несанкціоноване використання мережевого обладнання
	Відсутність правил обмеженого доступу до інформації, що обробляється	Несанкціонований доступ до службової, конфіденційної та таємної інформації
	Хибний розподіл доступу до інформації	
	Відсутність контролю прав доступу до інформації та відсутній сам аналіз щодо доступу	

Таблиця 1.1. (продовження)

Актив	Уразливість	Загроза
	Відсутність або проведення не в повному обсязі тестування ПЗ	
	Відсутність захисту мобільного комп'ютерного обладнання	
	Відсутність мотивації у персоналу або наявність у нього невдоволення	Зловживання засобами обробки інформації
	Відсутність процедур резервного копіювання	Втрата або крадіжка інформації
	Відсутність політик чистих столів та чистих екранів	
	Неконтрольоване копіювання	
	Не вірне керування паролями	Не легітимне використання облікового запису
	Недостатній захист криптографічних ключів	Розкриття інформації
Програмне забезпечення	Недостатня освіта в галузі ІБ Не якісна документація корпоративних додатків	Помилки в технічному обслуговувані
	Відсутність механізму оновлення ПЗ, яке використовується для захисту від шкідливого ПЗ	Вірусне інфікування, шкідливе ПЗ
	Неконтрольоване завантаження та використання ПЗ	
	Неадекватне керування мережею	Перевантаження трафіка
	Незрозумілі та неповні специфікації для розробників	Збій ПЗ
	Добре відомі дефекти в ПЗ	Використання ПЗ не авторизованими користувачами
	Відсутність контролю вхідних та вихідних даних	Системні помилки
	Неконтрольоване використання безкоштовного або зламаного ПЗ в корпоративних додатках	Юридична відповідальність

Таблиця 1.1. (продовження)

Актив	Уразливість	Загроза
	Невдосконалена політика в галузі застосування криптографії	
	Неадекватний контроль змін	Збій системи безпеки
	Відсутність доведення відправки та отримання інформації	Ухиляння від відповідальності
	Відсутність розділення на тестові та робочі екземпляри систем	Несанкціонована модифікація систем
Обладнання	Неадекватне та не охайне використання механізмів контролю доступу на ОІД	Зловмисне заподіяння шкоди
	Незахищене зберігання	Крадіжка
	Розміщення в зоні, яка може бути затопленою	Затоплення
	Не дотримання вимог пожежної безпеки	Пожар
	Відсутність періодичної заміни обладнання	Знос засобів зберігання інформації
	Не вдале встановлення, недостатній супровід засобів захисту інформації	Помилка в процесі супроводження
	Схильність обладнання до вологості, накопичення пилу	Запилення
	Схильність обладнання до перепадів температури	Порушення температурного режиму

Під аналізом інформаційних ризиків будемо розуміти процес комплексного оцінювання захищеності ІС параметрами, які відображають кількісну та якісну їх складові. Однією з основних завдань аналізу інформаційних ризиків є оцінка вартості збитків, які виникають в умовах того чи іншого ризиків. На теперішній час не існує єдиної методики такого оцінювання., так як відсутній достатній обсяг статистичних даних для визначення закону розподілу ймовірності успішної реалізації певної загрози, а також відсутня однозначність в оцінці вартості як матеріального так і нематеріального інформаційного ресурсу.

Виходячи з вищевикладеного і з аналізу відповідних джерел, можна стверджувати, що самими поширеними методами в оцінці ІР є якісні методи, які засновані на експертних оцінках. Однак це ускладнює можливості моделювання ризикового профілю та не призводить до об'єктивного висновку.

Таким чином, для проведення аналізу ризиків та надання відповідних рекомендацій сформулюємо умови, при яких відбувається вплив на ІР.

1. Критичність наслідків при якій є спроможність здійснити вимірювання збитку при фіксованій вартості ресурсу у відсотках. При отриманих статистичних даних в даній роботі, запропоновано чотири рівня, які представлено в таблиці 1.2.

Таблиця 1.2. Рівні критичності наслідків при фіксованій вартості ресурсу

Критичність наслідків у %	**Рівень критичності**	**Позначення лінгвістичної змінної**
≤10	Низький	SM
11 – 30	Середній	MD
31 – 80	Граничний	LM
> 80	Катастрофічний	KT

При цьому в показник критичність наслідків входять наступні складові:

* ***Трудовитрати*** – вартість заходів для відновлення наслідків, до яких привів інцидент. Ця сума залежить від вартості наслідку від одного інциденту та кількості інцидентів за період, який досліджується. Трудовитрати на відновлення наслідків від одного інциденту складаються з трудовитрат на здійснення діагностування, створення відповідної документації, здійснення відповідних виправлень.

* ***Матеріальні збитки***, включаючи ***репутаційні***.

2. Оцінка ймовірності успішної реалізації кібератаки при наявності відповідної загрози аранжується за шкалою п'яти лінгвістичних змінних, а саме *WL* - дуже мала, *SM* - мала, *MD* - середня, *H* - висока, *WH* - дуже висока. Всі ці ідентифікатори залежать від рівня вразливості ресурсу проти загрози та ефективності тестування на проникнення в КІ.

- При цьому, визначення ймовірності згідно запропонованої шкали лінгвістичних змінних залежить від уразливості на вході або на виході самої ІС. При цьому маємо три лінгвістичні змінні, а саме: *Low* - низький, *Middle* - середній і *High* - високий.

- Частка інцидентів, спровокованих загрозою і таких, що спричинили шкоду, у загальній кількості інцидентів, спровокованих цією загрозою, за минулий період. Шкала включає значення *VeryLow* - дуже низький ($\leq 19\%$), *LowI* - низький ($20\% - 39\%$), *MiddleI* - середній ($40\% - 60\%$), *HighI* - високий ($61\% - 80\%$) і *VeryHighI* - дуже високий ($\geq 81\%$).

1.3. Постановка технічного завдання, що розв'язується в кваліфікаційній роботі

На основі проведеного аналізу інформаційних ризиків підприємств критичної інфраструктури відкритим залишається питання визначення закону розподілу ймовірності успішної реалізації кібератак при наявності уразливості, яка визначається на основі тестування на проникнення. Таке тестування дає можливість зібрати банк статистичних даних для аналізу з одного боку уразливих точок ІС КІ, а з іншого боку створити паспорт кібератак у відповідності уразливі точці.

При можливості мати такий закон розподілу можна миттєво визначати можливі загрози та запобігти втратам, які можуть виникнути при успішній реалізації кібератак.

Отже, технічне завдання в даній роботі полягає в побудові функцій належності за лінгвістичними змінними, які відповідають критичним наслідкам, наявним загрозам, якісному визначенню ймовірності при наявності загроз, та інцидентів, які спровоковані загрозами для побудови закону розподілу втрат при реалізації кібератаки на ІС КІ.

Дане припущення дає можливість сформувати відповідні рекомендації для підвищення рівня інформаційної безпеки в інформаційних системах підприємств критичних інфраструктур.

Висновки до першого розділу

В першому розділі було здійснено огляд уразливості інформаційних систем підприємств критичної інфраструктури та проаналізовані загрози інформаційній безпеці, які при цьому виникають. Було також структурно визначено прояв самих цих загроз.

Було розкрито поняття інформаційного ризику та проаналізовано сутність самого ризику, який виникає в інформаційній системі підприємств критичних інфраструктур.

У зв'язку з наявністю інформаційних ризиків було введено:

- поняття критичного наслідку, який було аранжовано чотирма лінгвістичними змінними;
- якісна оцінка ймовірності успішної реалізації кібератак, яку було аранжовано п'ятьма лінгвістичними змінними;
- частка інцидентів, спровокована загрозою, аранжованою п'ятьма лінгвістичними змінними.

Виходячи з трьох вище введених понять, було визначено якісна оцінка ймовірності загрози від уразливості на вході та на виході самої інформаційної системи, яку аранжовано трьома лінгвістичними змінними.

Також, в цьому розділі було сформульовано технічне завдання, що розв'язується в даній кваліфікаційній роботі.

РОЗДІЛ 2. ОЦІНКА СТІЙКОСТІ ДО КІБЕРАТАК ПРИ ТЕСТУВАННІ НА ПРОНИКНЕННЯ

2.1. Вплив кібератак на функції керування та моніторингу інформаційних систем критичної інфраструктури

Завдання забезпечення стійкості функціонуванням керування та моніторингу ІС висувають системні вимоги до якості інформації, яка обробляється протягом формування керуючих впливів на технологічний процес критичної інфраструктури. При цьому велике значення відіграє функціональна повнота, надійність роботи компонентів системи надходження, передавання й оброблення інформації та ПЗ.

Впровадження цифрових компонентів у систему оперативно-диспетчерського керування (ОДК) фізичними процесами КІ на основі різноманітних інформаційних потоків, породжує в ІС кіберзагрози. Кібератаки, а також спеціально розроблене шкідливе ПЗ, такі як *Stuxnet*, *BlackEnergy*, *Crash Override* та *Trisis/Trident*, спрямовані на виведення з ладу систем ОДК [7]. Це призводить не тільки до ризиків кібербезпеки [8,9] системи ОДК, а до необхідності забезпечення стійкості до кібератак в разі успішної їх реалізації.

Стійка система керування - це система, яка підтримує обізнаність про стан і прийнятний рівень нормального функціонування ІС у відповідь на порушення, включаючи загрози, які виникають несподівано або зловмисно [10].

Одночасно при забезпеченні заходів для забезпечення ІБ, які спрямовані на запобігання збоїв для забезпечення конфіденційності, цілісності та доступності інформації [11,12], забезпечення стійкості до кібератак спрямоване на проведення головних операцій, підтримання критичних рівнів функцій керування та оперативне відновлення [13-15]. Стійкість до кібератак особливо актуальна для системи ОДК, оскільки наслідками кіберзбоїв можуть бути відмови функціональних компонентів систем керування [16]. В таблиці 2.1 представлено загрози, які виникають при

надходженні різноманітної інформації на ІС критичних інфраструктур та наслідки, які впливають на функції оперативного керування на ІС.

Таблиця 2.1. Вплив кібератак на функції оперативного керування ІС КІ

Загрози	Порушення функцій оперативного керування
Атаки, спрямовані на впровадження хибних даних	Створення хибних керуючих впливів (КВ). Втр номінального значення частоти, робочої напру Обмеженість або повна втрата спостерігання. Хи команди керування. Хибні параметри нарушен забезпечать вплив на операції розподілу та передавання
Атаки синхронізації часу (spoofing-атаки)	Хибний моніторинг поточного режиму, який призводи до помилок щодо контролю та інформаційному захис Втрата контролю частоти, напруги. Хибна інформа щодо наявності несправності та самої точки, де во виникла. Розсіювання команд на відключення/реаліза інтелектуальних засобів.
DoS. DDoS – атаки (відмова в обслуговуванні)	Запізнення керування. Здійснення хибних керуючих впливів. Втрата контролю над частотою, напругою. Блокування сигналу, який забезпечує керування. Обмеження або втрата спостереження.
Атаки повторного відновлення	Запізнення керування. Обмеження або втрата спостереження. Не коректний контроль над частотою, напругою.
Цільові атаки	Всі, що в попередніх випадках.
Шкідливе ПЗ	Хибне виконання керуючого впливу. Хибне спрацюва апаратних та програмних засобів. Втрата контролю частотою, над напругою.

Умовна міра стійкості - це адаптивна здатність або здатність реагувати на загрозу і підтримувати прийнятну функціональність. Стійка система має знижувати ризики кібербезпеки та запобігати тяжким наслідкам кібератак. Звідси, під час оцінювання стійкості до кібератак системи ОДК пропонується враховувати ризик кібербезпеки, що дає змогу оцінити ймовірність виникнення події та наслідки, які можуть виникнути в разі виникнення кібератаки [17].

Існує висока потреба в оцінці показника стійкості до кібератак системи ОДК, що відображає поведінку системи при порушеннях кібербезпеки.

В даному розділі подано структуру системи ОДК, визначено вразливі до кібератак компоненти та представлено означення стійкості до кібератак на ІС КІ.

2.2. Стійкість керуючої складової інформаційної системи критичної інфраструктури

Стійкість до кібератак – це спроможність системи забезпечувати захист від інцидентів кібератак та здатність підтримувати прийнятний рівень продуктивності завдяки підтримці критичної функціональності та оперативному відновленню якості послуг до рівня, що передував інциденту [21].

В процесі дослідження проблем забезпечення стійкості до кібератак системи ОДК в роботі [22] представлено ієрархічну структуру, яка включає в себе наступні складові:

- регіональне диспетчерське керування;

- головне диспетчерське керування - центральне диспетчерське керування.

Головними функціями оперативно-диспетчерського керування на різних рівнях ієрархії є:

- оперативний контроль та керування об'єктами КІ;

- моніторинг надійності КІ;

- оптимізація режимів КІ;

- аналіз даних моніторингу в режимі $on-line$ - прогнозування навантажень та втрат потужності;

- регулювання частоти, пере струмів активної потужності;

- оцінювання та прогнозування стану об'єктів КІ, пропускної спроможності мереж тощо.

Компонентами системи ОДК є вимірювальні підсистеми, підсистеми передавання даних, підсистеми оброблення даних, підсистеми синхронізації часу, які входять до систем $SCADA/EMS$, що призначені для підтримки дій диспетчерського персоналу під час оперативного керування, та $WAMS$, яка забезпечує можливості моніторингу, керування та контролю ІС КІ [23]. Кіберінциденти можуть виникнути в будь-якому з описаних компонентів системи ОДК та призвести до порушення функцій керування.

Головними характеристиками, якими повинна володіти система керування для підтримки власної функціональності на прийнятному рівні при кібератаках, є:

- можливість пом'якшувати і пригнічувати негативн наслідки кібератаки;

- можливість реагувати та адаптуватися;

- можливість відновлення.

Стан уразливості виникає при зниженні кібербезпеки системи керування та характеризується зниженням поглинаючих властивостей системи, що призводить до підвищення ризику небезпечних в результаті успішно реалізованих кібератак. Таким чином, під час дослідження проблеми стійкості до кібератак ІС КІ за результатами аналізу можливих

збоїв, які порушують функціональність системи, призводить до зниження надійності її компонентів [24].

В результаті кібератак на будь-який компонент ІС КІ можливі наступні сценарії:

- інформаційні відмови;

- відмови апаратного забезпечення;

- відмови програмного забезпечення;

- відмови взаємодії апаратного та програмного забезпечення.

Інформаційні відмови можуть виникнути внаслідок спотворення, втрати та затримки інформаційних потоків, що використовуються під час керування ІС, під час кібератак на віддалені пристрої телемеханіки *RTU*, диспетчерські пункти керування *MTU*, людино-машинний інтерфейс *HMI* системи *SCADA*, а також пристрої синхронізованих векторних вимірювань *PMU*, концентратори векторних даних *PDC* на всіх рівнях диспетчерського керування, глобальні навігаційні супутникові системи *GPS* / *ГЛОНАС* (GNSS - Global Navigation Satellite Systems), сервери часу *TS* (TS - Time Server) системи *WAMS*, а також мережі передачі даних.

Відмови апаратного та програмного забезпечення, а також їхньої взаємодії [25], впливають на надійність цифрових пристроїв, таких як *PMU* або *PDC*, мережі передавання даних [26].

Для підтримки системи стійкості до кібератак системи ОДК суттєвим є забезпечення надійності реалізацій функцій керування, зумовленої надійністю даних, апаратною складовою, надійністю ПЗ та надійністю самої мережі.

2.3. Модель стійкості від кібератак інформаційної системи при тестуванні на проникнення

Порогова функціональність системи ОДК - це мінімальний очікуваний рівень, який має підтримуватися нею в разі кібератаки. Деякі додатки, що використовуються під час керування ІС КІ, можна віднести до категорії критично важливих - їхня відмова може завдати шкоди технологічній частині КІ. На стійкість від кібератак системи ОДК впливає її здатність пом'якшувати наслідки кібератаки і, тим самим, знижувати ризик кібербезпеки ІС КІ. Повернення системи в нормальний стан означає здатність системи до адаптації та відновлення. Таким чином, забезпечення стійкості до кібератак залежить від рівня кібербезпеки, швидкості відгуку і відновлення, як це представлено на рисунку 2.1.

Рисунок 2.1. Фактори забезпечення стійкості до кібератак

Звідси, показник стійкості до кібератак ІС КІ можна описати нечіткою моделлю

$$L = L_1 \ X \ L_2 \ X \ L_3, \tag{2.1}$$

де L_1- лінгвістична змінна «Кібербезпека ІС КІ», L_2 - лінгвістична змінна «Оклик (відповідь) ОДК на кібератаку», L_3 - лінгвістична змінна «Відновлення системи ОДК».

В таблицях 2.2 – 2.5 представлено можливі порушення функцій оперативного керування ОДК при успішної реалізації кібератак.

Таблиця 2.2. Рівні ризиків, які виникають при порушенні функцій оперативного керування ОДК

Рівень/діапазон	Опис
Дуже низький VL,[0;0.04]	Можливість очікування того, що подія, яка полягає в загрозі буде мати не значний негативний вплив на оперативне керування
Низький L,[0.05;0.2]	Небезпечна подія може мати обмежений негативний вплив на оперативне керування, наслідки для функціонування мають локальний характер
Середній M,[0.21;0.79]	Небезпечна подія може здійснити негативний вплив на оперативне керування
Високий H,[0.8;0.95]	Небезпечна подія може мати безпечні або катастрофічні наслідки ля функціонування ІС КІ
Критично високий CH,[0.96;1]	Небезпечна подія може мати багаточисельні небезпечні або катастрофічні негативні події для функціонування ІС КІ

Таблиця 2.3. Рівні відгуків, які виникають при порушенні функцій оперативного керування ОДК

Рівень/діапазон	Опис
Низький L,[0;0.24]	Система ОДК не якісно адаптується та чутливо реагує в умовах кібератак з урахуванням заходів з активного та пасивного захисту від кібератак, відмічається низька функціональність, можливі відмови компонентів, втрата деяких функцій оперативного управління та значні помилки у функціонуванні системи. При цьому інтенсивність відмов висока, що зумовлює низьку ймовірність безвідмовної роботи.
M,[0.25;0.79]	Адаптації системи ОДК відбувається при використанні активного захисту від несприятливих наслідків кібератак. Як реакція системи на кібератаку можливі збої (само відновлювані) у функціональності системи ОДК. Інтенсивність відмов не призводить до значних помилок у функціонуванні системи ОДК.
Високий H,[0.8;0.95]	Адаптація та реагування системи ОДК під час кібератак відбувається без відмов, відмічається прийнятна функціональність системи оперативно-диспетчерського управління, що зумовлює високу ймовірність безвідмовної роботи.

Таблиця 2.4. Рівні відновлення, які виникають при порушенні функцій оперативного керування ОДК

Рівень/діапазон	Опис
Низький L,[0;0.24]	Інтенсивність відновлення та ймовірність відновлення низька. Середній час відновлення здатності системи ОДК до виконання i-ї функції після відмови може призвести до помилок і значних затримок керування.
M,[0.25;0.79]	Інтенсивність відновлення середня. Середній час відновлення здатності системи ОДК до виконання функцій після відмови не призводить до значних помилок і затримок управління.
Високий H,[0.8;0.95]	Інтенсивність відновлення дозволяє виконання всіх функцій оперативного керування в режимі реального часу. Імовірність відновлення висока.

Таблиця 2.5. Рівні стійкості до кібератак які виникають при порушенні функцій оперативного керування ОДК

Рівень/діапазон	Опис
Низький L,[0;0.24]	Реалізація функцій оперативного управління в умовах кібератак низька. Небезпека виникнення в системі ОДК відмов і збоїв висока. Поєднання відмов компонентів з відповідними помилками функціональності системи керування може призвести до значних порушень функціонування ІС КІ.
M,[0.25;0.79]	У результаті кібератак можливі незначні збої та помилки в управлінні, які можна усунути і які не чинять критичного впливу на функціональність системи ОДК. Реалізація функцій оперативного керування здійснюється в необхідному обсязі і не призводить до порушень функціонування ІС КІ.
Високий H,[0.8;0.95]	Вплив кібератак не призводить до відмов і збоїв системи ОДК. Спрацьовують усі заходи щодо забезпечення стійкості до кібератак. Функціональність системи керування висока.

Рівні вхідних лінгвістичних змінних L_1, L_2 і L_3 визначають рівень вихідної лінгвістичної змінної L на основі розробленої ієрархічної нечіткої системи.

Враховуючи вплив кібератак, які порушують функції оперативного керування, як це представлено в таблиці 2.1, стає суттєвим створити умови для достатньо швидких відгуків та відновленню системи керування, які можуть бути параметризовані мінімальною інтенсивністю відмов λ_s та найбільшій інтенсивності відновлення системи μ_s і які визначаються наступним чином

$$\lambda_s = \left(\overline{\theta}\right)^{-1}, \tag{2.2}$$

де $\overline{\theta}$ - середнє напрацювання системи на відмову.

$$\mu_s = \left(\overline{\tau}\right)^{-1}, \tag{2.3}$$

де $\overline{\tau}$ - середній час відновлення системи [27].

Рівень стійкості до кібератак системи ОДК можна розглядати як її здатність здійснювати пом'якшення наслідків кібератак, інакше кажучи, прийнятним рівнем кібербезпеки, а також ймовірністю безвідмовної роботи $P_{L_{21}}$ та ймовірності відновлення системи ОДК P_{L_3} в умовах кібератак. Ці ймовірності визначаються наступним чином

$$P_{L_2} = e^{-\lambda_s t}, \tag{2.4}$$

$$P_{L_3} = 1 - e^{\mu_s t}. \tag{2.5}$$

Застосовуючи представлені міркування, представимо алгоритм оцінки стійкості до кібератак системи ОДК ІС КІ в умовах кібератак.

З урахуванням факторів забезпечення стійкості до кібератак, представлених на рисунку 2.1 алгоритм оцінки стійкості до кібератак складається з наступних етапів:

1. оцінка рівня ризику кібербезпеки L_4 [24].

2. Оцінювання рівня кібербезпеки як показника пом'якшення придушення при реалізованій кібератаки:

$$L_1 = 1 - L_4, \tag{2.6}$$

3. Оцінка рівня відгуку L_2 при порушенні кібербезпеки.

4. Оцінка рівня відновлення L_3 при порушенні кібербезпеки.

5.Оцінка показника стійкості до кібератак L.

Усі фактори, як і стійкість до кібератак, описуються лінгвістичними змінними, для кожного з них визначено терм-множини в таблицях 2.2 – 2.5 з відповідним семантичним описом з урахуванням даних, представлених в таблиці 2.1.

Для визначення показника стійкості до кібератак системи ОДК ІС КІ відповідно моделі (2.1) розроблено ієрархічну нечітку систему, в якій закладено системи нечіткого логічного виведення *FISi* , що представлена на рис. 2.2.

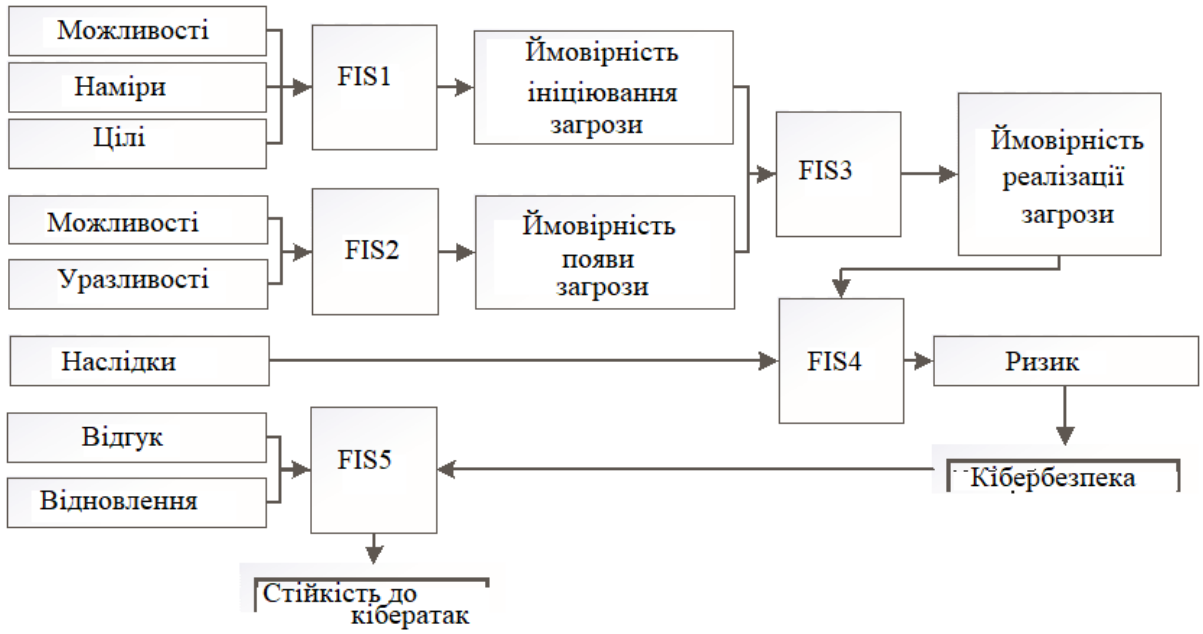

Рисунок 2.2. Оцінка стійкості до кібератак ІС КІ

Для отримання оцінки стійкості до кібератак системи ОДК ІС КІ розглянуто руйнівну подію у вигляді *DoS* -атаки на систему передачі даних.

Значення вхідних лінгвістичних змінних факторів, що визначають рівень ризику кібербезпеки системи ОДК, наведено в таблиці 2.6.

Таблиця 2.6. Вхідні лінгвістичні змінні, які визначають рівень ризику

Фактори	DoS-атака
Можливості	0.8
Наміри	0.81
Цілі	0.65
Уразливості	0.72
Наслідки	0.89

Під час порушення кібербезпеки умовно задано інтенсивність відмови системи $\lambda_s = 0.002$, інтенсивність відновлення системи $\mu_s = 0.5$, тривалість роботи системи $t = 100$ *годин*.

На основі алгоритму оцінки ризику керування ІС КІ отримано показник ризику $R_4 = 0.64$ (рівень ризику - середній). Згідно з (2.6) визначено значення показника кібербезпеки $R_1 = 0.36$ (рівень кібербезпеки - середній).

Для визначення показників відгуку і відновлення визначено ймовірність безвідмовної роботи системи і ймовірність відновлення за формулами (2.4) і (2.5): $P_{L_2} = 0.82$ - високий рівень відгуку, $P_{L_3} = 1$ - високий рівень відновлення.

Звідки, показник стійкості до кібератак $L = 0.84$, що визначає високий рівень функціональності системи ОДК, незважаючи на порушення кібербезпеки

Висновки до другого розділу

1. В даному розділі розглянуто проблему забезпечення стійкості до кібератак системи ОДК ІС КІ.

2. Проведено аналіз причин порушення стійкості до кібератак та наслідків, до яких можуть призвести руйнівні події внаслідок кібератак.

3.Показано, що такі чинники, як кібербезпека, відгук і відновлення системи забезпечують стійкість до кібератак. З урахуванням цього запропоновано нечітку модель стійкості до кібератак системи ОДК ІС КІ.

4.Розроблено алгоритм оцінювання показників стійкості до кібератак системи ОДК ІС КІ, використання якого на практиці дасть змогу, надалі, розробити ефективні заходи як щодо забезпечення стійкості до кібератак, так і щодо зниження ризиків кібербезпеки системи ОДК ІС КІ.

РОЗДІЛ 3. МОДЕЛІ РИЗИКІВ НАПАДУ НА ІНФОРМАЦІЮ

3.1. Аналіз ризиків для визначення параметрів моделі

Важливими параметрами є ефективність керування ІБ та рівень зрілості підприємства щодо сприйняття завдання інформаційної безпеки. В таблиці 3.1 представлено співставлення оцінки зрілості згідно даних університету *Carnegien Mellon*

Таблиця 3.1. Співставлення оцінки зрілості

Рівень зрілості	Критерії рівня зрілості
1	Відсутнє формальне визначення проблеми
2	Проблема розв'язується на базі поступового практичного впровадження. Завдання відносно ефективності захисту не є зрозумілим у зв'язку з відсутністю суттєвих порушень
3	Часткове дотримання стандартам та рекомендаціям. Увага приділяється процесам документування
4	Актуальні питання вимірювання параметрів, які визначають режим ІБ. Застосування кількісних методів аналізу ризиків
5	Ставляться та розв'язуються різні варіанти оптимізаційних задач в галузі ІБ

Організації з високою ефективністю мають 3, 4, 5 рівні зрілості. Крім того, аналітиками компанії *PwC* виявлено, що підвищення рівня зрілості дає істотне поліпшення результатів проектів, так як тридцять відсотків компаній поліпшили свої результати більш ніж на двадцять п'ять відсотків [28].

Граничні значення у всіх цих випадках підбираються для кожного випадку відповідно особистим властивостям.

Оцінювання очікуваних втрат від конкретної загрози, з огляду на застосування експертних оцінок і шкал, що містять лінгвістичні змінні, може бути здійснено за допомогою теорії нечітких множин.

Використання теорії нечітких множин при дослідженнях ризиків необхідно виділяти наступні параметри: стійкість до застосування в динаміці об'єктивних та суб'єктивних даних, а також спроможність реалізації завершеного, з точки зору цілісності, підходу щодо оцінки ризиків за рахунок включення особливих та організаційних факторів (рисунок 3.1).

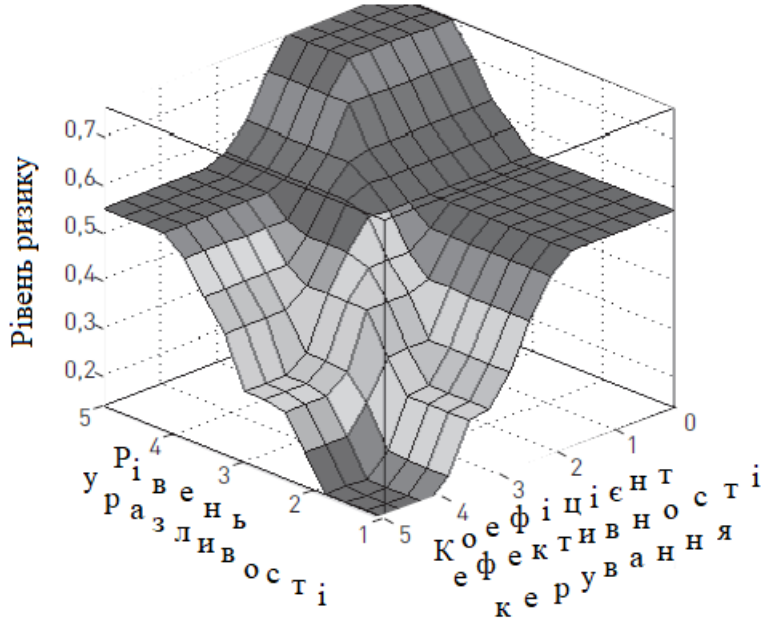

Рисунок 3.1. Розподіл рівня ризику при залежностях коефіцієнта ефективності керування та рівня уразливості

3.2. Визначення функції належності лінгвістичних змінних

Задамо описані вище чинники, що впливають на рівень ризику, як універсальні передумови $X = \{x_1, x_2, ..., x_n\}$. За множину проявів ризику приймемо $Y = \{y_1, y_2, y_3, y_4\}$, що позначають: y_1 - низький рівень ризику, y_2-середній рівень ризику, y_3- високий рівень ризику, y_4- дуже високий рівень ризику. При цьому результуючий параметр ризику характеризуватиметься наступними компонентами:

- лінгвістичною змінною $R(x)$, $x \in [0;1]$;

- *терм – множиною* значень лінгвістичної змінної, що складається зі значень {*низький, середній, високий, дуже високий*}.

Для кожного з компонентів *терм – множини* визначається нечітка множина, компонентами якої є значення нечіткої змінної, приналежність яких до множини визначається функцією належності. Аналітичний вигляд функції належності для значень рівня ризику подано в таблиці 3.2.

Таблиця 3.2. Аналітичне представлення функції належності лінгвістичної змінної $R(x)$.

ТЕРМ R_i, $i = \overline{1,4}$	**Функція належності нечіткої множини** R_i
R_1 - низький рівень ризику	$\mu_1(x) = \begin{cases} 1, x \le 0{,}2 \\ -11x + 2.5, 0.2 < x \le 0.3 \\ 0, x > 0.3 \end{cases}$
R_2 - середній рівень ризику	$\mu_2(x) = \begin{cases} 0, x \le 0.2 \\ 11x + 3, 0.2 < x \le 0.3 \\ 1, 0.3 < x \le 0.5 \\ -11x + 8.5, 0.5 < x \le 0.6 \\ 0, x \ge 0.6 \end{cases}$
R_3 - високий рівень ризику	$\mu_3(x) = \begin{cases} 0, x \le 0.5 \\ 11x + 4.5, 0.5 < x \le 0.6 \\ 1, 0.6 < x \le 0.8 \\ -11x + 7.5, 0.8 < x \le 0.9 \\ 0, x \ge 0.9 \end{cases}$
R_4 - дуже високий рівень ризику	$\mu_4(x) = \begin{cases} 1, x \le 0{,}8 \\ 11x + 5.5, 0.8 < x \le 0.9 \\ 1, x > 0.9 \end{cases}$

Функція належності уявляє собою суб'єктивну міру, яка визначається експертами для визначення меж значень у шкалі.

Залежність появи того чи іншого значення ризику визначається комбінацією чинників ризику, яка описується системою правил: ***ЯКЩО ... ТО***. Ці залежності визначено в таблиці 3.3 та 3.4.

Таблиця 3.3. Залежність ймовірності загрози від незалежних від неї факторів

ЯКЩО	***Застосування***			***ТО***	***Ймовірність***
	Ефективність керування	**Уразливість процесів**	**Відсоток інцидентів**		
ЯКЩО	**1**	Висока	0-20	**ТО**	Висока
	2	Висока	0-20		Висока
	3	Середня	0-20		Середня
	4	Низька	0-20		Дуже низька
	5	Низька	0-20		Дуже низька
	6	Висока	80-100		Дуже низька
	7	Висока	80-100		Дуже низька
	8	Середня	80-100		Висока
	9	Низька	80-100		Низька
	10	Низька	80-100		Низька

Після цього здійснюється визначення ризику залежно від рівнів імовірності та ступеня негативності наслідків, як це представлено в таблиці 3.5.

Аналіз сформульованих залежностей у середовищі *Maple* підтверджує коректність формування шкали рівня ризику. У подальшому математичний апарат *Maple* можна застосовувати для пошуку локальних екстремумів цільової функції об'єкту в реальному режимі часу.

Таблиця 3.4. Залежність ступеня негативності наслідків від величина втрат на їх відновлення

ЯКЩО	***Застосування***			***ТО***	***Ступінь негативності наслідків***
	Трудовтрати	**Матеріальні втрати**	**Репутаційні втрати**		
Якщо	Дуже високі	Низькі	Високі	То	Критична
	Високі	Високі	Високі		Катастрофічна
	Середні	Низькі	Високі		Критична
	Низькі	Низькі	Високі		Критична
	Дуже низькі	Низькі	Високі		Критична
	Дуже високі	Середні	Низькі		Критична
	Середні	Середні	Низькі		Помірна
	Низькі	Середні	Низькі		Помірна
	Дуже низькі	Середні	Низькі		Помірна
	Дуже високі	Високі	Середні		Катастрофічна

Таблиця 3.5. Класифікатор оцінки ризиків як функція від ймовірності ступеня негативності наслідків появи інциденту

Ймовірність	**Ступінь негативності наслідків**			
	катастрофічний	**критичний**	**помірний**	**низький**
Дуже висока	Дуже висока	Дуже висока	Висока	Середня
Висока	Дуже висока	Висока	Середня	Низька
Середня	Висока	Висока	Середня	Низька
Низька	Висока	Середня	Низька	Низька
Дуже низька	Висока	Низька	Низька	Низька

В якості вихідних даних розглянемо проект, вартість якого складає один мільйон гривень при наявності ста співробітників, серед яких 90 осіб є користувачами комп'ютерів. При цьому термін планування складає три роки, а

рівень рентабельності складає десять відсотків. Документи компанії зберігаються в каталозі, до якого вільний доступ і файли розподілені в різних папках відповідно до структури організації та тематики. Доступ до папок обмежений утилітами операційної системи і не відстежується. Відповідно, особа, яка пропрацювала в компанії кілька років, може мати надлишкові права доступу, наприклад, після переведення в інший підрозділ або на іншу посаду.

Задача полягає в оцінці наслідків реалізації загрози несанкціонованого доступу до даних, якою можуть бути персональні дані, дані договорів за поточними проектами, інновації, поточні документи, що готуються компанією для участі в тендерах.

Втрати від реалізації загрози можна оцінити за операційними витратами та за допомогою експертних оцінок.

Нехай заробітна плата фахівця - 40000 гривень, для визначення, будемо вважати, що розрахунки заробітної плати не диференціюють, тоді денна вартість його може бути оцінена, як $P = \frac{40000}{22} \approx 1818.18\ грн.$

Максимальний збиток від інциденту, спричиненого несанкціонованим доступом до даних щодо поточних та потенційних проектів компанії, містить не тільки безпосередню вартість самого проекту, а й операційні витрати. Ці витрати складаються з трудовитрат на виправлення наслідків, а також матеріальних і репутаційних витрат. У цьому прикладі конфіденційна інформація стала відома компанії, яка є конкурентом, і яка виграла тендер. В цьому випадку упущеною вигодою є:

1) вартість проекту - один мільйон гривень;

2) вартість технічної підтримки становить приблизно двадцять відсотків, при умові, що компанія займається розробкою та впровадженням інформаційних технологій;

3) трудовитрати на підготовку концепції рішення, технічної та проектної документації. Введемо припущення, що підготовка пропонованого рішення велася протягом тридцяти робочих днів трьома фахівцями. У цьому разі трудовитрати будуть складати приблизно 16364 гривень, що не є великою сумою, і як порівняти із сумою упущеної вигоди, але також потребує врахування. Отже, втрати компанії становитимуть 1216363 гривень. Будемо вважати цю суму базовою N_j.

Оскільки ризик має ймовірнісну природу, то встановлювати детерміновану величину збитку не є резонним. Тому було запропоновано додатковий параметр $S_{j,m}$, який враховує ймовірнісну природу ризику і визначає за формулою (3.1) витрати, які виникають, якщо масштаб наслідків у десятки, сотні та у тисячі разів більший за наслідки стандартного інциденту [24].

$$EL_j = N_j\left(10S_{j,10} + 100S_{j,100} + 1000S_{j,1000} + 1 - \left(S_{j,10} - S_{j,100} - S_{j,1000}\right)\right). \quad (3.1)$$

Так як середня величина збитку від зареєстрованих витоків інформації в Україні за 2023 рік дорівнює 37,8 мільйонів гривень, то можна припустити, що витік інформації зі збитком, що дорівнює $12163630\,грн$, станеться з імовірністю 0,05, зі збитком, що дорівнює $12636300\,грн$ приблизно 0,01, а збиток, що дорівнює 1216363000, прямує до нуля. У цьому випадку втрати

компанії становитимуть 1858395 *грн.*. Це ймовірнісна оцінка збитків від одного витоку інформації [24].

На базі експертних висновків було визначено приблизну відносну кількість інцидентів, розподілених за видами наслідків α_{ij}. За статистичними даними у 2023 році в Україні було зареєстровано 105 витоків інформації, у США - понад 650 витоків. Очевидно, що навіть одного суттєвого витоку інформації достатньо, щоб завдати значної шкоди компанії.

Більшість із вихідних оцінок, зокрема ті, що стосуються ступеня негативності наслідків і ймовірностей виникнення інцидентів, можуть бути суб'єктивними, що не може не позначитися на точності оцінки ризику. Для надання розрахункам більшої точності. Результати імітаційного моделювання більшої точності оцінку ризику було виконано за допомогою методу Монте-Карло. Для цього прийнято, що ймовірність того, що кількість інцидентів більша або менша за раніше визначене число, дорівнює 0,5. Ці дані використовуються функцією біноміального розподілу випадкової величини для розрахунку майбутньої частоти появи інциденту.

Проведене імітаційне моделювання, що складалося з 1000 ітерацій, дало змогу з довірчою ймовірністю 0,955 зробити висновок, що ризик може становити 134416 *грн.*

В таблиці 3.6 представлено результати імітаційного моделювання з застосуванням метод Монте-Карло, а на рисунку 3.2 представлено залежність, також за результатами імітаційного моделювання, частоти появи інциденту певного виду і величини ризику, який виникає як наслідок.

Таблиця 3.6. Результати імітаційного моделювання

Втрати, грн.	Частота	Ймовврність, у %	Кумулятивна ймовірність у %
1 289	1	0,10	100,00
10 164	0	0,00	99,90
19 040	3	0,30	99,90
27 915	2	0,20	99,60
36 790	9	0,90	99,40
45 665	22	2,20	98,50
54 540	45	4,50	96,30
63 415	63	6,30	91,80
72 290	97	9,70	85,50
81 166	143	14,30	75,80
90 041	155	15,50	61,50
98 916	139	13,90	46,00
107 791	120	12,00	32,10
116 666	102	10,20	20,10
125 541	54	5,40	9,90
134 416	29	2,90	4,50
143 292	10	1,00	1,60
152 167	4	0,40	0,60
161 042	2	0,20	0,20
+	0	0,00	0,00
Всього	1000	100	

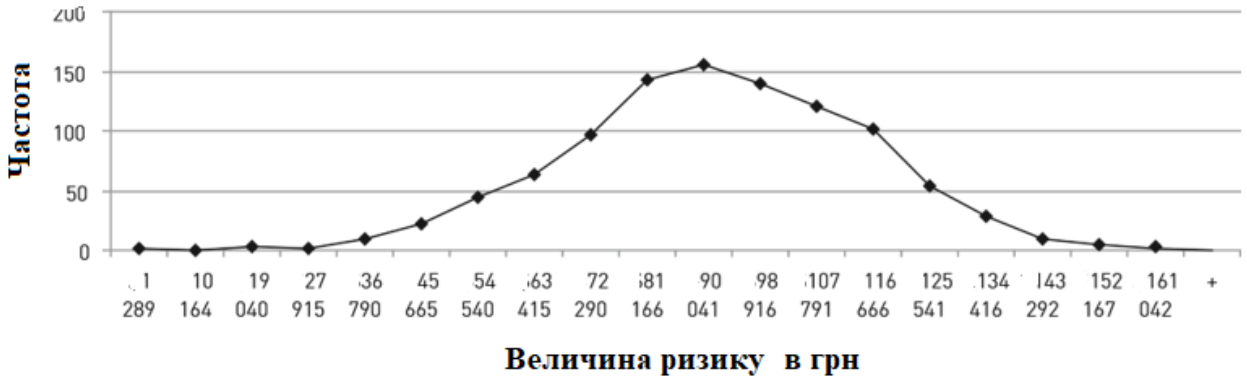

Рисунок 3.2. Залежність частоти появи інциденту певного виду і величини ризику, який виникає як наслідок.

3.3. Тестування на проникнення за стандартом *NIST SP* 800 – 115

Питання ІБ об'єктів та відповідних інформаційних ресурсів є одним з головних завдань сьогодення при створенні ІС довільного рівня складності і є актуальністю в подальшому на нескінченний термін. На теперішній час існує велика кількість систем та засобів, які якісно забезпечують ІБ і які базуються на програмних та технічних заходах, а в особливих випадках і комбінованими системами захисту. Зазвичай системи ІБ відповідного розробника є особливими і уявляють собою в певному випадку авторською розробкою. Як наслідок, варто розуміти, що у користувача відсутній доступ до таких систем. Однак, для забезпечення ефективного захисту застосовують формалізовані методи, такі як криптографічні. З точки зору надійності інформаційного захисту застосовують багаторівневий захист.

Таким з методів, який визначає якість інформаційного захисту є визначення відповідності технічного завдання щодо створення СЗ, яка реалізована відповідними функціями, які визначають характеристики експлуатації та відповідних вимог при цьому.

Крім того, існує і інший підхід, який базується на аналізі функціональної стійкості системи, яка визначає рівень якості системи ІБ.

Для визначення кількісного рівня захисту вводять основні та абсолютні параметри.

Відносна кількісна оцінка – це число, яке може визначати рейтинг, або категорію і яке потребує порівняння з іншими числами, які розглядаються як еталони. Ці числа визначаються експертами.

Головним критерієм якісної оцінки є корекція та похибка, яка є суб'єктивною за рахунок дій експертів.

Оцінка ІБ відповідно до *NIST SP* 800 – 115 - це процес визначення того, наскільки оцінюваний об'єкт відповідає критеріям забезпечення ІБ. Для цього рекомендується використовувати три типи заходів, спрямованих на оцінку ІБ:

1) аналіз - це процес експертизи, перевірки, вивчення та спостереження об'єкта оцінювання для розуміння його функціональності та ступеня захищеності;

2) тестування - це процес використання об'єкта оцінки в певних умовах для порівняння фактичної та очікуваної поведінки цього об'єкта (відповідає використанню способів тестування;

3) інтерв'ю - це процес проведення опитування окремих осіб або груп осіб усередині організації для полегшення розуміння функціональності оцінюваного об'єкта, а також для одержання додаткової інформації про систему (не є основним типом заходів оцінювання ІБ, а використовується додатково до двох вищевказаних, переважно спільно із заходами аналізу).

У стандарті *NIST SP* 800 – 115 розглядаються способи аналізу та способи технічного тестування ІБ, які можна використовувати для виявлення, перевірки та оцінювання технічних вразливостей, а також для допомоги організаціям у розумінні та поліпшенні стану ІБ їхніх об'єктів.

Оцінка ІБ, відповідно до стандарту *NIST SP* 800 – 115 , призначена для вирішення таких завдань:

1) забезпечити адекватність оцінки ІБ цільових об'єктів в інтересах зниження ризику проведення атак зловмисниками;

2) мінімізувати ризики порушення нормального функціонування об'єктів системи, що перевіряється під час проведення тестування на проникнення;

3) сформувати заходи щодо виявлення, аналізу та ліквідації виявлених вразливостей цільових об'єктів.

У стандарті *NIST SP* 800 – 115 процес оцінювання ІБ розбито на три основні етапи.

1) ***Планування***. Цей етап є критично важливим для успішної оцінки ІБ об'єкта, що тестується. На цьому етапі проводять збір інформації, необхідної для виконання тестування, як-от: об'єкти, які тестують, загрози та вразливості об'єктів, заходи забезпечення ІБ, які перевіряють, способи аналізу та оцінювання вразливостей, які використовують. Цей етап завершується розробкою плану тестування, в якому відображаються цілі та завдання тестування, області та об'єкти тестування, обмеження, виділені ресурси, способи, що використовуються, ролі та обов'язки аудиторів, очікувані результати і терміни.

2) ***Аналіз і перевірка вразливостей***. Основна мета цього етапу - виявити вразливості об'єктів, що тестуються, і перевірити можливість їхньої експлуатації в інтересах нанесення шкоди. На цьому етапі реалізуються способи аналізу та способи перевірки вразливостей, передбачені планом тестування. Результатом цього етапу є перелік актуальних вразливостей об'єктів та організаційних процесів.

3) ***Аналіз результатів оцінки ІБ і пост-тестові заходи***. Цей етап передбачає аналіз виявлених вразливостей, визначення основних причин їхньої появи, вироблення рекомендацій щодо усунення вразливостей. Усі ці аспекти включаються в підсумковий звіт за результатами тестування.

Існує безліч способів проведення оцінювання ІБ і перевірки безпеки, які можна використовувати для оцінювання стану цільових об'єктів, систем і

комп'ютерних мереж. У *NIST SP* 800 – 115 усі способи оцінювання ІБ згруповано в такі дві основні категорії:

1) Способи аналізу - це способи експертизи, перевірки, вивчення і спостереження, які використовуються для оцінки об'єктів, систем, додатків, мереж, політик і процедур для виявлення вразливостей, які, як правило, виконуються аудитором вручну. Ці способи містять у собі:

1.1) аналіз документації;

1.2) аналіз подій, зафіксованих в журналах;

1.3) аналіз наборів правил;

1.4) аналіз конфігурацій системи;

1.5) сканування мережі;

1.6) перевірку цілісності файлів.

2) Способи перевірки вразливостей - ці способи практично підтверджують наявність вразливостей у об'єктів, що перевіряються, і їх можна виконувати як вручну, так і з використанням спеціалізованих технічних засобів та ПЗ. Способи перевірки вразливостей в об'єктів включають у себе:

2.1) тестування паролів;

2.2) тестування на проникнення;

2.3) тестування безпеки додатків;

2.4) соціальну інженерію.

Для забезпечення високого ступеня повноти тестування рекомендується комбінувати різні способи в рамках відведених на тестування час, фінансові ресурси та компетенції персоналу.

У стандарті *NIST SP* 800 – 115 детально пояснюється суть і зміст різних вищевказаних способів, але не здійснюється уточнення, які способи слід використовувати за яких обставин. Що, з одного боку, є недоліком цього стандарту, з іншого боку, дає організаціям гнучкість у виборі та використанні конкретних способів.

Способи аналізу використовуються для пасивного вивчення об'єктів, систем, додатків, мереж, політик і процедур з метою виявлення вразливостей ІБ і, у своїй більшості, орієнтовані на перевірку та оцінку документів. За допомогою аналізу можна зібрати інформацію про систему в інтересах формування переліку об'єктів, що тестуються, і використовуваних способів перевірки вразливостей. Оскільки способи аналізу пасивні, їх використання несе мінімальний ризик для функціонування систем і мереж.

Аналіз документації дає змогу визначити, чи є технічні аспекти політик і процедур ІБ актуальними і чи справді забезпечують належний рівень ІБ. Як правило, внутрішні документи слугують основою для забезпечення безпеки організації. Необхідно перевірити на технічну точність і повноту процедур такі документи організації:

1) політики безпеки;

2) архітектуру та вимоги з безпеки;

3) типові робочі процедури забезпечення ІБ на робочих місцях;

4) плани безпеки системи та угоди про авторизацію;

5) плани та алгоритми реагування на інциденти.

Аналіз документації може виявити «*прогалини*» і слабкі місця, які можуть призвести до відсутності або неправильної реалізації заходів безпеки. Аудитори зазвичай перевіряють, чи відповідає документація організації стандартам і правилам і шукають політики, які є недосконалими або застарілими. Аналіз документації не гарантує, що заходи безпеки реалізовано належним чином, вони показують тільки те, що існують вказівки та інструкції для забезпечення певного рівня безпеки. Дотримання персоналом цих вказівок та інструкцій - це окреме питання, яке виходить за рамки аналізу документації.

Аналіз журналів подій, що фіксуються, дає змогу визначити, чи реєструють системи управління безпекою правильну інформацію і чи дотримується організація своїх політик управління журналами. Аудит журнальних подій дає змогу виявити такі проблеми, як неправильно налаштовані служби та засоби управління ІБ, факти НСД і спроби вторгнення.

Далі наведено приклади журналів і журнальованих подій різних об'єктів ІС, які можуть бути корисними під час проведення оцінки ІБ:

1) сервер аутентифікації або системні журнали можуть реєструвати успішні та невдалі спроби аутентифікації;

2) системні журнали можуть містити інформацію про запуск і завершення роботи операційної системи (ОС), служб, про встановлення неавторизованого ПЗ, доступ до файлів, зміни політики безпеки, зміни облікових записів (наприклад, створення і видалення облікового запису, призначення привілеїв облікового запису) і використання привілеїв;

3) журнали систем виявлення вторгнень *IDS* (*Instruction Detection System*) і систем запобігання вторгнень *IPS* (*Instruction Prevention System*), які можуть реєструвати факти зловмисних дій і неналежне використання привілеїв;

4) журнали брандмауерів і маршрутизаторів можуть містити дані про вихідні з'єднання, що вказують на зламані внутрішні пристрої. Крім того, вони можуть реєструвати спроби несанкціонованого підключення і неналежне використання мережевого обладнання;

5) журнали різних застосунків можуть відображати спроби несанкціонованого під'єднання, зміни облікових записів, використання привілеїв та інформацію про використання застосунку або бази даних.

6) журнали антивірусу можуть містити дані про події, невдалі спроби оновлення та інші ознаки застарілих сигнатур і ПЗ.

7) журнали безпеки *IDS / IPS* можуть містити інформацію про відомі вразливі місця у використовуваних операційних системах, службах і додатках.

Набір правил - це сукупність правил або сигнатур, з якими порівнюють мережевий трафік або активність системи для визначення, яку дію слід вжити системі. Аналіз наборів правил виконується для перевірки їхньої повноти та виявлення «*слабких місць*» у технічних і програмних засобах забезпечення ІБ з метою виявлення таких порушень ІБ, як вразливості комп'ютерних мереж, порушення політик безпеки, використання небезпечних або вразливих каналів зв'язку. Цей аналіз також може виявити недоліки, які негативно впливають на якість виконання набору правил.

Під час проведення аналізу доцільно перевірити набори правил мережевого та хост-брандмауера, набори правил *IDS / IPS*, а також списки управління доступом маршрутизатора.

Аналіз конфігурацій системи - це процес виявлення слабких місць у налаштуваннях та елементах управління конфігурацією безпеки системи. Він орієнтований на виявлення систем, які не налаштовані відповідно до політик безпеки або налаштовані так, що створюють загрозу порушення безпеки.

Даний тип перевірки по відношенню до операційної системи може виявити служби і додатки, які не використовуються, неправильні налаштування облікових записів і паролів користувачів, а також неправильні налаштування ведення журналів подій і резервного копіювання. Прикладами файлів конфігурації безпеки, які можна переглянути, є параметри політики безпеки операційної системи *Windows* і файли конфігурації безпеки операційної системи *Unix*, наприклад, у папці *etc*.

Оскільки аналіз конфігурацій системи вручну вимагає багато часу, рекомендується використовувати протокол автоматизації управління даними безпеки *SCAP* (*Security Content Automation Protocol*).

Сканування мережі - це пасивний спосіб дослідження, який відстежує мережевий зв'язок об'єктів, ідентифікує мережеві протоколи, які використовуються, і перевіряє заголовки пакетів і користувацьких даних, щоб виявити інформацію, що цікавить.

Цілі використання мережевого сканування:

1) захоплення і відтворення мережевого трафіку;

2) виконання пасивного аналізу мережі (наприклад, визначення активних пристроїв у мережі);

3) визначення операційної системи, додатків, служб і протоколів, включно з незахищеними і несанкціонованими протоколами;

4) виявлення несанкціонованих і невідповідних дій, таких як незашифрована передача конфіденційної інформації;

5) збір корисної інформації, такої як незашифровані імена користувачів і паролі.

Сканування мережі, відповідно до стандарту *NIST SP* 800 – 115, може включати в себе проведення таких заходів:

1) доступ і сканування дротової мережевої інфраструктури;

2) доступ і сканування бездротових мереж;

3) сканування можливості доступу до окремих комп'ютерних систем користувачів з використанням таких радіо інтерфейсів як *Wi – Fi* (*IEEE* 802.11).

Для проведення сканування мережі використовується спеціальне ПЗ - сніфер. У деяких випадках потрібне додаткове обладнання: мережевий концентратор, відгалужувач або комутатор із підтримкою технології віддзеркалення трафіку *SPAN* (*Switch Port Analyzer*), за якої трафік, що передається на всі інші порти комутатор, копіюється в порт, де встановлено сканер.

Організації можуть розгорнути мережеві сканери в декількох місцях:

1) по периметру системи для оцінки трафіку, що входить і виходить із мережі;

2) за брандмауерами, щоб переконатися, що набори правил точно фільтрують трафік;

3) за системами *IDS* / *IPS*, щоб визначити, чи запускаються сигнатури і чи на них реагують належним чином;

4) перед критично важливою системою або додатком для оцінки його мережевої активності;

5) у певному сегменті мережі для перевірки зашифрованих протоколів.

Засоби перевірки цілісності файлів дають змогу визначити, чи були змінені системні файли об'єктів, обчислюючи і зберігаючи контрольну суму для кожного захищеного файлу, а також створюючи базу даних (БД) контрольних сум файлів. Збережені контрольні суми пізніше перераховуються для порівняння їхнього поточного значення з раніше збереженим значенням, що дає змогу визначити факт порушення цілісності файлу та ідентифікує зміни файлу.

Незважаючи на те, що перевірка цілісності файлів не вимагає високого ступеня взаємодії з людиною, її слід використовувати обережно, щоб гарантувати її ефективність. Перевірка цілісності файлів найефективніша, коли системні файли ОС порівнюються з еталонною БД, створеною з використанням завідомо безпечної системи - це дає змогу гарантувати, що еталонна БД не була побудована з використанням скомпрометованих файлів. Еталонна БД має зберігатися в автономному режимі, щоб зловмисники не зламали цю БД і не змогли змінити контрольні суми файлів. Крім того, оскільки виправлення та інші оновлення змінюють файли, БД контрольних сум слід підтримувати в актуальному стані.

Тестування паролів - це процес відновлення паролів із хешів паролів, що зберігаються в системі. Зазвичай цей процес виконується під час аудиту системи для виявлення облікових записів зі слабкими паролями.

Злом паролів виконується для хеш функцій, які або перехоплюються мережевим аналізатором трафіку під час передавання мережею, або витягуються з комп'ютерної системи, що зазвичай вимагає доступу на рівні адміністратора або фізичного доступу до цільової системи. Щойно ці хеші отримано, спеціалізоване ПЗ на кшталт «*зломщик паролей*» генерує додаткові хеші, доки не буде знайдено збіг або доки аудитор не зупинить спробу злому.

Цей спосіб тестування може бути використаний для перевірки вимог до рівня складності пароля, виключення використання типових фраз або паролів за замовчуванням. Якщо в організації діє політика закінчення терміну дії пароля, цей спосіб перевірки може використовуватися з інтервалами, що збігаються з передбачуваним терміном дії пароля. Використання цього способу контролю паролів, що виконується в автономному режимі, практично не впливає на швидкодію системи або мережі, а переваги цієї операції включають перевірку як політики паролів організації, так і перевірку її відповідності вимогам ІБ.

Висновки до третього розділу

1. Викладений вище метод пропонує імітаційне моделювання як спосіб підвищення точності оцінки. Однак надання будь-яких чисельних значень частоти виникнення інцидентів не позбавлене суб'єктивності. Це дає підстави для використання «*розмитих*» лінгвістичних значень, оскільки під час аналізу причин і наслідків інциденту аналітик може краще визначити порядок наслідків, ніж його точну, чисельну оцінку. В умовах невизначеності застосовуються підходи, засновані на

«*розмитих*», якісних оцінках рівнів загроз і вразливостей. Властива їм суб'єктивність, вочевидь, знижується збільшенням кількості респондентів і кількості запитань в використовуваних опитувальниках.

2. Аналіз стандарту *NIST SP* 800 – 115 засвідчив, що за своєю шириною та глибиною охоплення питань проведення тестування його доцільно використовувати під час розроблення вітчизняного стандарту тестування на проникнення.
3. Перевагами стандарту *NIST SP* 800 – 115 є те, що стандарт охоплює у сферу оцінювання ІБ не лише питання проведення тестування, а й питання аналізу документації організації, політик забезпечення безпеки, а також питання використання способів соціальної інженерії та їхній вплив на підсумковий рівень безпеки організації. Саме ці переваги доцільно запозичити з *NIST SP* 800 – 115 під час розроблення вітчизняного проекту стандарту тестування на проникнення.
4. У *NIST SP* 800 – 115 не розглядаються питання фізичного доступу до інформаційної інфраструктури організації та способи перевірки її безпеки. *NIST SP* 800 – 115 містить доволі застарілий набір інструментарію тестування, який, на погляд автора, програє в повноті та ефективності програмним засобам у складі останніх дистрибутивів *Kali Linux*. Ці недоліки показують, що під час розроблення відповідних питань вітчизняного стандарту на проникнення доцільно використовувати інші методики та стандарти, відмінні від *NIST SP* 800 – 115.

ВИСНОВКИ

1. В результаті проведеного дослідження було встановлено, що математичний апарат нечітких множин є достатньо потужним засобом для оцінки ефективності тестування інформаційної системи критичних інфраструктур в процесі тестування на проникнення, так як дає можливість за рахунок побудови функції належності визначати закони розподілу ймовірностей загроз ІБ.
2. За допомогою лінгвістичних змінних існує можливість створювати комбінації для якісної оцінки трудових втрат, матеріальних втрат та репутаційних втрат, які виникають в умовах існуючих зовнішніх кібератак на ІС КІ.
3. Завдяки функції належності і лінгвістичним змінним створюється шкала, яка дає можливість і експертам створювати відповідні характеристики, які є параметрами, що виступають в ролі індикаторів рівня інформаційного захисту та інформаційної безпеки інформаційних систем, які забезпечують реалізацію технологічного процесу критичних інфраструктур.
4. За допомогою технології *NIST SP* 800 – 115, яка визначає етапи тестування на проникнення і методам нечітких множин, які представлено в даній роботі, існує можливість інтегровано аналізувати ризики, які виникають в полі інформаційної безпеки функціонування критичних інфраструктур.
5. Інтеграція теорії нечітких множин і *NIST SP* 800 – 115 дає можливість запобігти негативним наслідкам, які можуть виникнути в результаті успішної реалізації зовнішнього деструктивного інциденту, вектор якого направлено на крадіжку конфіденційної інформації, або на модифікацію даних для некоректної роботи самої інформаційної системи або на відмову в обслуговуванні інформаційної системи. Такі наслідки можуть призвести до аварійних або катастрофічних ситуацій, що не допустимо в роботі критичної інфраструктури.
6. Сформульоване в розділі 1.3 технічне завдання в даній роботі виконано і поставлена мета реалізована в повному обсязі.

СПИСОК ВИКОРИСТАНИХ ДЖЕЗРЕЛ

1. Мухін В.Є. Ризик-орієнтована інформаційна безпека: монографія / В.Є. Мухін. – К.: НТУУ «КПІ», 2011. – 292 с.
2. Самандула В.В. Застосування методів внутрішніх точок в задачах кібербезпеки інтелектуальних систем енергетики / В.В. Самандула, М.М. Луценко // Сучасний захист інформації №2 (46), 2021. С. 53-58.
3. Шуклін Г.В. Методика забезпечення стійкості інформаційного напрямку за умов інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю / Г.В. Шуклін, Є.В. Бондаренко // Зв'язок №2, 2023. С. 10-20.
4. Керування ризиком: Словник термінів (ISO Guide 73:2009) ДСТУ ISO Guide 73:2013. *Офіційне видання*. Київ, Мінекономрозвитку України, 2014.Електроннийресурс:https://khoda.gov.ua/image/catalog/files/dstu%2073.pdf
5. Коваль С. Базель II: аналіз основних положень та можливості їх впровадження в Україні / Світлана Коваль // Світ фінансів.-2008.-Вип. 4. – С.104-111.Електроннийресурс: http://dspace.tneu.edu.ua/handle/316497/26515
6. https://www.klubok.net/Downloads-index-req-viewdownloaddetails-lid-291.html
7. N. Jacobs, S. Hossain-McKenzie and E. Vugrin. Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example. 2018 Resilience Week (RWS). 2018, pp. 38-46. DOI: 10.1109/RWEEK.2018.8473549.
8. M. Touhiduzzaman, S. N. G. Gourisetti, C. Eppinger and A. Somani. A Review of Cybersecurity Risk and Consequences for Critical Infrastructure. 2019 Resilience Week (RWS). 2019, pp. 7-13. DOI: 10.1109/RWS47064.2019.8971975.
9. I. Zografopoulos, J. Ospina, X. Liu and C. Konstantinou. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources,

Metrics, and Case Studies. IEEE Access. 2021, vol. 9, pp. 29775-29818. DOI: 10.1109/ACCESS.2021.3058403.

10. J. Zuo, Z. Guo, J. Gan and Y. Lu. Enhancing Continuous Service of Information Systems Based on Cyber Resilience. 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC). 2021, pp. 535-542. DOI: 10.1109/DSC53577.2021.00085.
11. Shady S. Refaat, Omar Ellabban, Sertac Bayhan, Haitham Abu-Rub, Frede Blaabjerg, Miroslav M. Begovic. Smart Grid Information Security. Smart Grid and Enabling Technologies, IEEE. 2021, pp.229-248. DOI: 10.1002/9781119422464.ch9.
12. E. U. Haq, H. Xu, L. Pan and M. I. Khattak. Smart Grid Security: Threats and Solutions. 2017 13th International Conference on Semantics, Knowledge and Grids (SKG). 2017, pp. 188-193. DOI: 10.1109/SKG.2017.00039.
13. I. Friedberg, K. McLaughlin and P. Smith. A cyber-physical resilience metric for smart grids. 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). 2017, pp. 1-5. DOI: 10.1109/ISGT.2017.8086065.
14. A. S. Musleh, H. M. Khalid, S. M. Muyeen and A. Al-Durra. A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications. IEEE Systems Journal. March 2019, vol. 13, no. 1, pp. 710-719. DOI: 10.1109/JSYST.2017.2741483.
15. S. Hopkins, E. Kalaimannan and C. S. John. Cyber Resilience using State Estimation Updates Based on Cyber Attack Matrix Classification. 2020 IEEE Kansas Power and Energy Conference (KPEC). 2020, pp. 1-6. DOI: 10.1109/KPEC47870.2020.9167652.
16. A. Ashok, M. Govindarasu and J. Wang. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. In Proceedings of the IEEE. July 2017, vol. 105, no. 7, pp. 1389-1407. DOI: 10.1109/JPROC.2017.2686394.

17. M. A. Haque, S. Shetty, B. Krishnappa. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019, pp. 273-281. DOI: 10.1109/BigDataSecurity-HPSCIDS.2019.00058.
18. Jia Guo, Yifei Wang, Chuangxin Guo, Shufeng Dong and Baijian Wen. Cyber-Physical Power System (CPPS) reliability assessment considering cyber attacks against monitoring functions. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741899.
19. Diptendu Sinha Roy, Cherukuri Murthy, Dusmanta Kumar Mohanta. Reliability analysis of phasor measurement unit incorporating hardware and software interaction failures. Generation Transmission & Distribution IET. 2015, vol. 9, no. 2, pp. 164-171. DOI: 10.1049/ iet-gtd.2014.0115.
20. Tong, Q., Yang, M., & Zinetullina, A. A Dynamic Bayesian Network-based approach to Resilience Assessment of Engineered Systems. Journal of Loss Prevention. Process Industries. 2020. 104152. DOI: 10.1016/j.jlp.2020.104152.
21. M. A. Haque, S. Shetty, B. Krishnappa. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019, pp. 273-281. DOI: 10.1109/BigDataSecurity-HPSCIDS.2019.00058.
22. Kolosok I.N., Gurina L.A. Povyshenie kiberbezopasnosti intellektual’nyh energeticheskih sistem metodami ocenivaniya sostoyaniya // Voprosy kiberbezopasnosti [Cybersecurity issues], 2018, № 3(27), pp. 63-69. DOI: 10.21681/2311-3456-2018-3-63-69.

23. Zhukov A.V., Saczuk E.I., Dubinin D.M., Opalev O.L., Utkin D.N. Voprosy` primeneniya texnologii sinxronizirovanny`x vektorny`x izmerenij dlya zadach monitoringa e`kspluatacionnogo sostoyaniya e`lektrooborudovaniya // E`nergetik [Energetik], 2017. № 9, pp. 3-8.
24. Jia Guo, Yifei Wang, Chuangxin Guo, Shufeng Dong and Baijian Wen. Cyber-Physical Power System (CPPS) reliability assessment considering cyber attacks against monitoring functions. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741899.
25. Diptendu Sinha Roy, Cherukuri Murthy, Dusmanta Kumar Mohanta. Reliability analysis of phasor measurement unit incorporating hardware and software interaction failures. Generation Transmission & Distribution IET. 2015, vol. 9, no. 2, pp. 164-171. DOI: 10.1049/ iet-gtd.2014.0115.
26. Uspenskij M.I. Sostavlyayushchie nadezhnosti informacionnoj seti sistemy monitoringa perekhodnyh rezhimov // Metodicheskie voprosy issledovaniya nadezhnosti bol’shih sistem energetiki [Methodological problems reliability study of large energy systems], 2020, pp. 370-379.
27. Tong, Q., Yang, M., & Zinetullina, A. A Dynamic Bayesian Network-based approach to Resilience Assessment of Engineered Systems. Journal of Loss Prevention. Process Industries. 2020. 104152. DOI:10.1016/j.jlp.2020.104152.
28. SAE J1739:2000 Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery.
29. Isabel L. Nunes and Mario Simóes-Marques. Applications of Fuzzy Logic in Risk Assessment — The RA_X Case // Centre of Technologies & Systems and Faculdade de Cieˆncias e Tecnologia, Universidade Nova de Lisboa, Portuguese Navy, Portugal, 2012.

30. Shang K. , Hossen Z.Applying Fuzzy Logic to Risk Assessment and Decision-Making // Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries. November 2013.
31. Boc K. , Vaculik J. , Vidrikova D. Fuzzy approach to risk analysis and its advantages against the qualitative approach // Proceedings of the 12th International Conference “Reliability and Statistics in Transportation and Communication” // Transport and Telecommunication Institute, Lomonosova 1, LV-1019, Riga, Latvia.
32. Мужанова Т.М. Організаційне забезпечення інформаційної безпеки підприємства: основні засади / Т.М. Мужанова // Сучасний захист інформації. – 2016. №2. – С. 78-82.
33. Корченко О.Г. Стаціонарні системи виявлення і попередження кібератак в інтересах кіберзахисту та кіберконтррозвідки (на прикладі США) / О.Г. Корченко, І.В. Логінов, С.О. Скворцов // Ukrainian Scientific Journal of Information Security. – 2019. Vol. 25. Issue.1. - P.5-12.
34. Pokoradi L. Fuzzy logic-based risk assessment. URL: http:// www.zmka.hu/docs/Volume1/Issue1/pdf/04poko.pdf
35. The Security Risk Management Guide. Microsoft Corporation, 2006. http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.