Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

ДИПЛОМНА РОБОТА МАГІСТРА

Метод оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту
Назва теми

Галузь знань 12 – Інформаційні технології

Спеціальність 125 –Кібербезпека

ДРКб. 170151.21.01.02 ПЗ

Виконав: студент 2 курсу, група КБм-21-1 _____ Дацко Б.В.
Підпис

Керівник доц., д. т. н, професор кафедри КБ _____ Касянчук М.М.
Підпис

Нормоконтролер ст. викладач кафедри КБ _____ Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри КБ к.т.н., доц _____ Кльоц Ю.П.
Підпис

7. 12. 2022 2022р.

Хмельницький, 2022

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ПРОГРАМУВАННЯ ТА ЗАХИСТ КОМП`ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"1" 09 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дацко Богдан Вікторович

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту

Керівник роботи Касянчук Михайло Миколайович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

доктор технічних наук, професор

Затверджена наказом № 83 ректора університету додаток №25 від 01.07.2022

2. Строк подання студентом проєкту (роботи) на кафедру 20.11.2022

3. Вихідні дані до проекту (роботи) Підвищення результативності організації безпеки інформаційної системи через оцінювання ризиків із застосуванням штучного інтелекту.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Вступ. Дослідження щодо оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту. Математична модель методу. Алгоритмічна реалізація методу. Апробація методу. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Тема, мета магістерської, наукова новизна, практична значимість, публікації. Дослідження предметної області. Розробка математичної моделі методу. Алгоритмічна реалізація методу. Апробація методу. Висновки.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завданн
Нормоконтроль	Мостовий С.В. Старший викладач кафедри Кб		

7. Дата видачі завдання «01» липня 2022р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	30.06.2022	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	2.09.2022	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	6.09.2022	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	22.09.2022	
5	Робота над науковою публікацією	2.10.2021	
6	Робота над розділом 3 – розробка алгоритмів і технологій, їх аналіз	15.10.2022	
7	Робота над розділом 4 – апробація запропонованих рішень	29.10.2022	
8	Узгодження отриманих; оформлення пояснювальної записки згідно вимог	5.11.2022	
9	Попередній захист роботи	25.11.2022	
10	Захист роботи на засіданні ЕК	6.12.2022	

Студент _____ Б.В. Дацко
Підпис Ініціали, прі

Керівник проекту (роботи) _____ М.М. Касян
Підпис Ініціали, прі

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту».

Автор роботи: студент групи КБм – 21 – 1 Дацко Б.В.

Керівник роботи: к.т.н., доц. Касянчук М.М.

Спеціальність: 125 – Кібербезпека

Галузь знань: 12 – Інформаційні технології

Пояснювальна записка: 115 с., 15 рис., 8 табл., 34 джерел.

Перелік ключових слів: кібербезпека, штучний інтелект, матриця помилок, фактори ризику, аномалії, машинне навчання.

Мета роботи - дослідження та визначення методів оцінки ризиків безпеки інформаційної системи із застосуванням штучного інтелекту.

ANNOTATION

Theme of thesis: "Method of assessing the security risks of the information system using artificial intelligence."

Author of the work: student of the KBm group - 21 - 1 Datsko B.V.

Head of work: Ph.D., associate. Kasyanchuk M.M.

Specialty: 125 – Cybersecurity

Field of knowledge: 12 - Information technologies

Explanatory note: 115 pp., 15 figures, 8 tables, 34 sources.

List of keywords: cyber security, artificial intelligence, error matrix, risk factors, anomalies, machine learning.

The purpose of the work - research and determination of methods for assessing information system security risks using artificial intelligence.

ЗМІСТ

ВСТУП

У сучасному світі, що характеризується високим рівнем невизначеності, для подолання актуальних криз та знецілення сталого розвитку вкрай важливим є впровадження ефективних ризик-орієнтованих підходів до корпоративного та державного управління. У той же час активний розвиток технологій штучного інтелекту та аналізу великих даних відриває для держави та бізнесу нові можливості оптимізації операційної та управлінської діяльності за рахунок цифровізації окремих процесів та цілих галузей. Тому актуальним та своєчасним є розгляд можливостей застосування технологій штучного інтелекту до такої галузі як оцінка ризиків.

Очевидно, що штучний інтелект і технології обробки великих даних вже практично невід'ємні елементи чергового витка еволюції ризик-менеджменту. Тривалий час точаться дискусії щодо практичного застосування штучного інтелекту, в тому числі в інформаційній безпеці, але коли зрілість цих продуктів дозволяє використовувати їх у корпоративних налаштуваннях, інструменти виходять на ринок, і точність роботи починає зростати. щоб виправдати їх секс. вартість, можливості зловмисника стають широкими. Настільки, що тільки використання цієї технології може їм ефективно протистояти. Сьогодні термін «штучний інтелект» (ШІ) міцно увійшов у повсякденне життя.

Хоча пристроям з елементами штучного інтелекту все ще не вистачає здатності розуміти проблеми та знаходити рішення, штучний інтелект вже випереджає людські здібності та можливості щодо зменшення помилок у оперативних завданнях та пошуку аномалій у різних процесах. ШІ відіграє важливу роль в оцінці помилок, які можуть зробити люди. Що стосується кібербезпеки, системи на основі штучного інтелекту обіцяють захистити організації від інтернет-загроз, ідентифікувати типи зловмисного програмного

забезпечення, забезпечити дотримання стандартів безпеки та допомогти розробити кращі стратегії запобігання атакам і відновлення.

За оцінками Gartner, витрати на інформаційну безпеку та системи управління ризиками зростуть до 174 мільярдів доларів у 2022 році, з яких близько 50 мільярдів доларів підуть на захист клієнтських систем. У 2023 році продажі хмарних платформ і додатків безпеки зростуть до 1,63 млрд доларів США, а продажі систем безпеки додатків зростуть до 4,5 млрд доларів США Ринок послуг у сфері інформаційної безпеки також зростає з 62 млрд. США минулого року до 66,9 мільярдів доларів.

Однак одними грошима проблему не вирішити. Більшість фахівців з інформаційної безпеки сьогодні зайняті аналізом журналів, запобіганням хакерським атакам, розслідуванням можливих випадків шахрайства тощо. Дефіцит персоналу гострий, тому індустрія безпеки все більше шукає рішення у сфері штучного інтелекту. За даними Marketsand Markets, ринок інструментів штучного інтелекту для кібербезпеки буде зростати в середньому на 23,3% у 2019-2026 роках, з $8,8 млрд до $38,2 млрд [2].

Кількість атак на інформаційні системи з кожним роком стрімко зростає. У той же час атаки стають все більш складними, а завдана шкода також зростає. Потенційні цілі тепер включають мережеву інфраструктуру, пристрої IoT і розумні домашні пристрої. «Класичні» антивірусні засоби не змогли впоратися з такими епідеміями, і з’явилися рішення на основі штучного інтелекту.

Незважаючи на те, що технології штучного інтелекту відрізняються від сучасних рішень кібербезпеки, вони потужніші, гнучкіші та здатні покращувати захист від зростаючої кількості превентивних кіберзагроз. Однак, незважаючи на глибокі зміни, які штучний інтелект привніс у сферу кібербезпеки, задіяні системи ще не готові повністю адаптуватися до середовища та змінити свій стан. На сьогодні ШІ не є головною панацеєю безпеки. Коли людський інтелект має намір атакувати інтелектуальну систему безпеки, система зазнає збою. Водночас

це не означає, що ми не повинні використовувати для захисту методи штучного інтелекту. Натомість ми повинні знати його обмеження та правильно їх використовувати.

Незважаючи на деякі уявлення про потенційні можливості інструментів штучного інтелекту, їх використання залишається здебільшого епізодичним і несистематичним. Наразі в кібербезпеці відсутня загальна концепція впровадження штучного інтелекту, найважливіші методи штучного інтелекту, які можна використовувати в кібербезпеці, не визначені, а також роль, яку ці методи можуть відігравати (особливо в машинному навчанні, інтелектуальному аналізі даних, глибокому навчанні та експертні системи) для захисту організацій у кіберпросторі. Тому метою даної роботи є аналіз та систематизація методів застосування основних технологій штучного інтелекту у сфері кібербезпеки [34].

Проведене дослідження та аналіз робіт в даній області обумовлює актуальність дослідження щодо методу оцінки ризиків безпеки інформаційної системи із застосуванням штучного інтелекту.

Об’єкт дослідження - штучний інтелект в кібербезпеці.

Предмет дослідження - методи оцінювання ризиків безпеки інформаційної системи.

Мета дослідження полягає у визначенні методів оцінки ризиків безпеки інформаційної системи із застосуванням штучного інтелекту.

Завдання дослідження наступні:

1. Здійснити аналіз методів оцінювання ризиків безпеки інформаційної системи, систем штучного інтелекту в системах захисту інформації, системи штучного інтелекту для моделювання загроз безпеки інформаційної системи.

2. Охарактеризувати моделі кіберзагроз в системах захисту інформації (статистичну модель, кластерний аналіз, модель кінцевих автоматів, марківська

модель, метод «теорії ігор», метод використання нейронних мереж, переваги та недоліки евристичних методів), дослідити метод машинного навчання, поняття та класифікація алгоритмів кластеризації методів машинного навчання.

3. Провести оцінку ризиків безпеки інформаційної системи, визначити керування ризиками з використанням методу штучного інтелекту, визначити метод оцінювання ризиків безпеки інформаційної системи із застосуванням системи штучного інтелекту.

4. Дослідити використання методу оцінювання ризиків інформаційних систем в кібербезпеці, використання методу оцінювання ризиків інформаційних систем при виявленні атак і способів їх подолання, дати рекомендації щодо попередження ризиків інформаційних систем з використанням системи штучного інтелекту.

Методи дослідження. Для вирішення поставлених задач в роботі використовуються методи випадкових процесів і теорія ймовірності, математичної статистики, методів чисельного аналізу, інтелектуального аналізу даних, комбінаторики та машинного навчання.

Практична цінність роботи полягає в розширенні знань про використання штучного інтелекту в кібербезпеці, а саме реалізація методу оцінки ризиків інформаційної системи.

Достовірність результатів дослідження підтверджується конкретною постановкою задачі, результатами моделювання, конкретним використанням математичного апарату та апробацією отриманих результатів. Отримані в ході виконання дослідження дані не суперечать отриманим раніше даним, які описані в літературі іншим автором.

Структура роботи. Магістерська робота складається із вступу, чотирьох розділів, висновків після кожного з них, загального висновку, списку використаних джерел.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ РЕАЛІЗАЦІЇ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Аналіз методів оцінювання ризиків безпеки інформаційної системи

Навіщо слід досліджувати ризики у сфері інформаційної безпеки (ІБ) і що це може дати під час розробки системи забезпечення ІБ інформаційної системи (ІВ)?

Для будь-якого проекту, що вимагає фінансових витрат на його реалізацію, дуже бажано вже на початковій стадії визначити, що ми вважатимемо ознакою завершення роботи і як оцінюватимемо результати проекту. Для завдань, пов'язаних із забезпеченням ІБ, це більш ніж актуально. Адже витрати на забезпечення високого рівня безпеки можуть бути невиправданими. Фактично постає питання: який рівень захисту має бути у системи, що розглядається? Для відповіді на це питання в процесі створення ІБ можна використовувати два підходи (рис 1.1.)

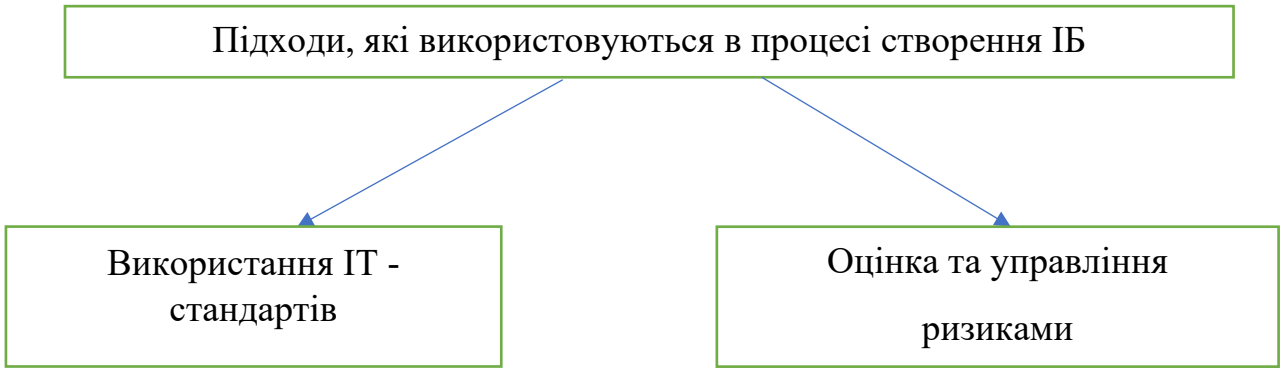


Рис 1.1. Підходи, що використовуються для реалізації інформаційної безпеки

Перший зосереджений на основних IT-стандартах або іншому наборі вимог. Таким чином, критерієм досягнення цілей області безпеки є задоволення заданого набору вимог. Критерій ефективності — найменша загальна вартість для задоволення заданих функціональних вимог. Однак рівень безпеки, необхідний у цих документах, не завжди чітко визначений, що ускладнює визначення ефективного рівня безпеки ІБ [1].

Другий підхід пов'язаний з оцінкою та управлінням ризиками. Спочатку це випливало з принципу «розумної адекватності», застосованого до постачання інформаційних систем. Принцип описується набором тверджень:

• Неможливо створити абсолютно непереборний захист;

• Необхідність досягнення балансу між вартістю захисту та досягнутим ефектом;

• Вартість засобів захисту не повинна перевищувати вартість інформації, що захищається;

• Ціна, яку сплачує порушник за несанкціонований доступ до інформації, має перевищувати ефект, який він отримує від такого доступу.

Ризиком у сфері ІБ називається потенційна можливість зазнати збитків через порушення безпеки інформаційної системи (ІВ).

Найбільш детально процес аналізу ризиків описується у [7]. При аналізі ризиків розглядається ІС у її вихідному стані, оцінюється розмір очікуваних втрат від інцидентів, пов'язаних із інформаційною безпекою за певний період. Після цього, робиться оцінка того, як запропоновані засоби та заходи безпеки впливають на зниження ризиків, і скільки вони коштують.

«Походження» філософії управління ризиками відбулося в 70-х роках, коли була розроблена повністю перекриваюча модель безпеки (або модель Клементса-Гоффмана).

Модель Клементса-Гоффмана дуже «ідеалістична» у своїй початковій формі, але саме в аналізі моделі виникає проблема оцінки загроз.

Модель побудована на припущенні, що система безпеки повинна мати принаймні один спосіб захисту зловмисника на кожному можливому шляху впливу ІБ (рис 1.2.).

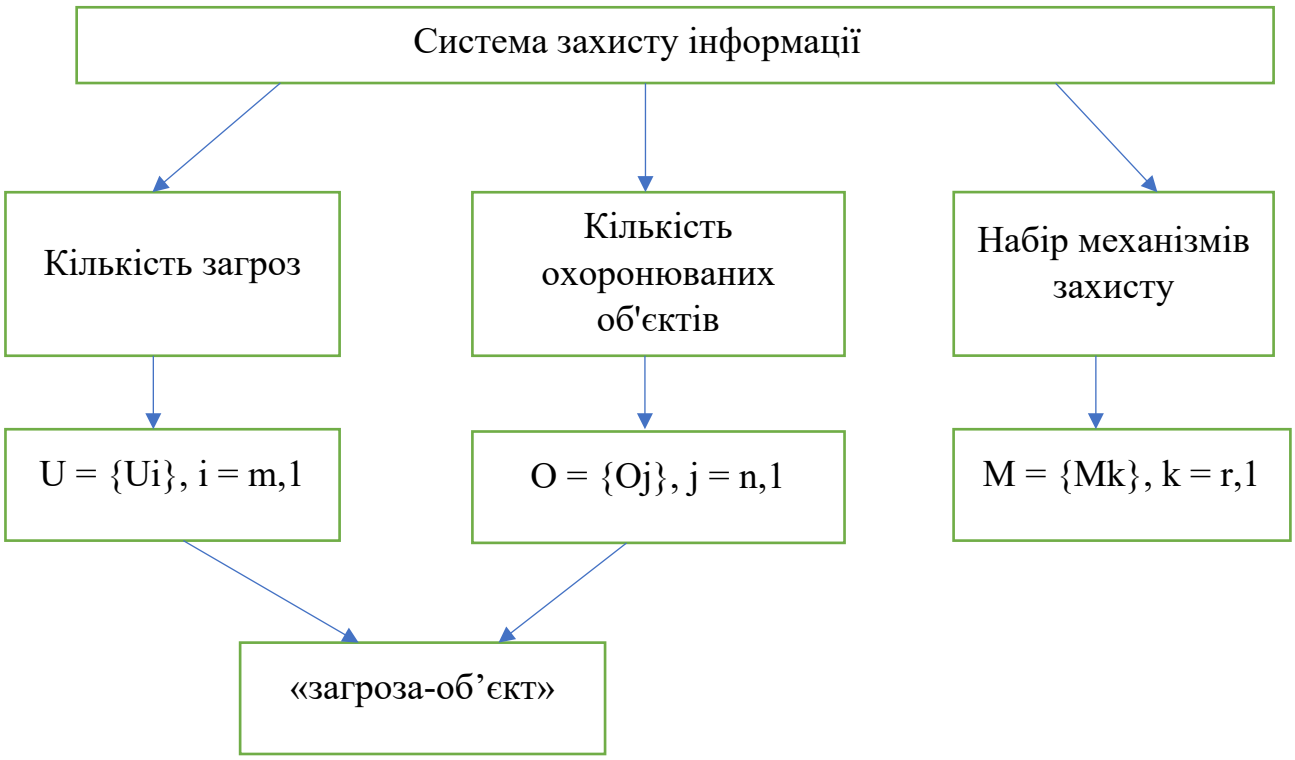


Рис 1.2. Групи систем захисту інформації

Слід зазначити, що зв’язок між загрозами та об’єктами не обов’язково є взаємозв’язком один-до-одного – загроза може поширюватися на будь-яку кількість об’єктів, і об’єкт може бути вразливим до кількох загроз.

Мета захисту полягає в тому, щоб охопити кожну дугу на графі та встановити бар’єри доступу на цьому шляху. Загальна постановка задачі така: набір засобів захисту M забезпечує захист набору об’єктів O від набору загроз U. В ідеалі кожен засіб mk має характеризувати деяке ребро <Ui, Oj> у зазначеному графі.

Застосовують набір захисних засобів M, щоб перетворити дводольний граф у тридольний граф.

У захищеній системі всі ребра представляються як <Ui, Mk> і <Mk, Oj>. При цьому один і той же засіб захисту може перекривати більше однієї загрози та захищати більше одного об'єкта.

Вводиться поняття "система з повним перекриттям" - це система, в якій є засоби захисту на кожний можливий шлях проникнення (рис 1.3.) [4].

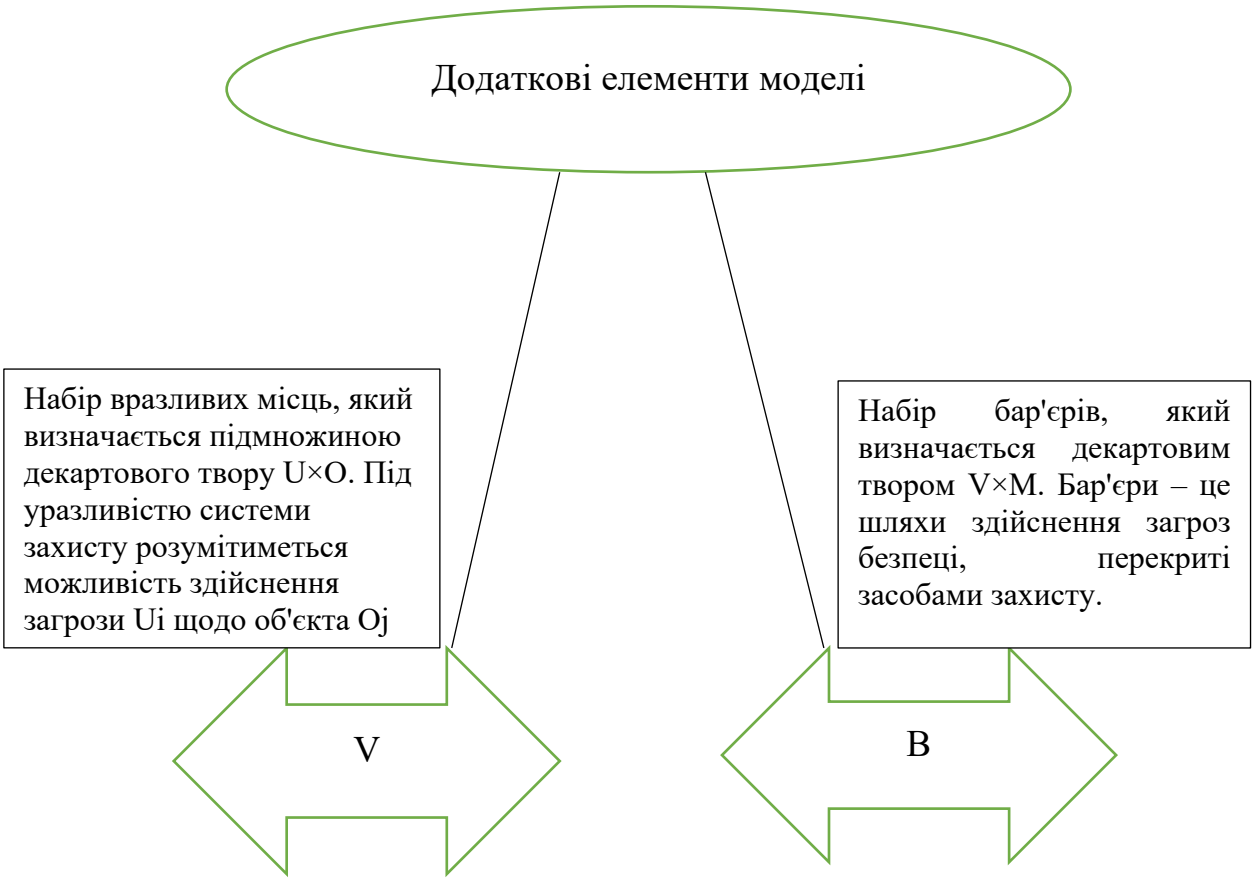


Рис 1.3. Запровадження додаткових елементів моделі

Отримуємо п'ятидольний граф (рис 1.4.)

Рис 1.4. Рівні захисту системи

Тепер, якщо кожній дузі графа поставити у відповідність ваговий коефіцієнт, то є можливість кількісно визначити рівень захисту системи.

Зазначимо, що ця модель має «утопічний» характер. У ній не враховується вартість впроваджуваних засобів захисту, а також співвідношення цієї вартості до можливих втрат при реалізації конкретної загрози. Враховуючи, що у нас завжди існують не тільки як матеріальні, так і тимчасові обмеження при створенні системи забезпечення ІБ, побудувати систему з повним перекриттям неможливо.

Також пошук усіх можливих впливів зловмисника на об'єкт часто не може бути здійснений. Адже, крім відомих способів здійснення загрози в майбутньому, можуть виникнути і нові. Таким чином, якщо забезпечити захист абсолютно від усіх загроз неможливо, то постає питання вибору тих загроз, від яких ми захищатимемо систему.

Нарешті, кожен бар'єр захисту насправді забезпечує лише певний ступінь опірності загрозам безпеці. Міцність бар'єру характеризується величиною залишкового ризику Ri.

Саме тут ми стикаємося із необхідністю аналізу ступеня захисту об'єкта від певної загрози. Оскільки загрози ризику виникнення загрози повністю позбутися не можна, пропонуються певні способи обробки ризику (зниження, усунення, перенесення чи прийняття) [24].

Таким чином, при побудові системи інформаційної безпеки постає проблема визначення ступеня захисту від загроз безпеки. Для цього нам необхідно певним чином ранжувати загрози залежно від ступеня небезпеки та виробити заходи щодо їх обробки.

1.2 Аналіз систем штучного інтелекту в системах захисту інформації

По-перше, давайте дамо кілька актуальних визначень кількох термінів, пов’язаних зі ШІ.

Системи ШІ виконують завдання, подібні до природного інтелекту, наприклад навчання та прийняття рішень.

Нейронна мережа - це набір взаємопов'язаних штучних нейронів, призначених для виконання основних математичних операцій. Він також має можливості навчання за допомогою машинного навчання.

Машинне навчання або англійською Machine learning — це технологія, яка використовує дані для розробки алгоритмів. Це форма штучного інтелекту, яка не дотримується жодних правил на основі конкретної інформації. Машини використовують системи машинного навчання, щоб вивчати свої системи за допомогою наборів даних, наданих особою, яка їх навчає. Цей процес називається початковим навчанням, а потім – прийняттям рішень після навчання системи [27] (таблиця 1.1).

Таблиця 1.1.

Підходи до машинного навчання

Вид навчання	Опис навчання
Навчання під наглядом	Форма машинного навчання, яка використовує позначені набори даних, наприклад тварин або людей із заданими характеристиками. Ці набори даних надходять або від людини, або від навчальної вибірки, яку називають «вчителем». Потім необхідно розробити запрограмований алгоритм, щоб надати відповіді на питання з подібними характеристиками.
Навчання без нагляду	Включає виявлення зв’язків між різними наборами даних шляхом аналізу інформації, отриманої з властивостей об’єктів. Цей метод не передбачає надання відповідей на певний набір запитань і не використовує мічені набори даних.
Контрольоване навчання	Вимагає збору даних із мітками, також відомих як навчальний набір. Однак придбання якісного тренувального набору коштує дорого та довго. Напівконтрольоване навчання поєднує невелику кількість позначених наборів даних із великою кількістю непозначених. Передбачається, що цей підхід буде економічно ефективнішим і швидшим, ніж традиційні методи, оскільки він поєднує як позначені, так і непідготовлені дані [25].
Навчання з підкріпленням	Конкретний приклад навчання, керованого вчителем. У цьому випадку вчитель є навколишнім середовищем, яке забезпечує зворотний зв'язок з інформаційною системою на основі рішень, прийнятих інформаційною системою.
Глибоке навчання	Форма машинного навчання, яка використовує штучні нейронні мережі з кількома рівнями для моделювання людського мозку та обробки мови, аудіо та візуальних зображень. В даний час машинний зір використовується в системах безпеки, контролю руху і пасажирів. Він також використовується в голосових помічниках, таких як «Siri» або «Alice», які можуть обробляти мову та розпізнавати текст. Крім того, ці програми можуть розпізнавати зображення та розуміти природну мову.

Додаткові методи використання машинного навчання включають байєсовські мережі, ланцюги Маркова та посилення градієнта.

Великі дані — це велика кількість структурованих і неструктурованих даних, представлених у цифровій формі, яка має характеристики великої кількості, швидкості та різноманітності. Для обробки великих даних можна використовувати спеціалізовані програмні засоби, такі як Apache Hadoop/Storm/Spark, Kaggle і СУБД NoSQL. Вважається, що для додавання бізнес-цінності при використанні великих даних необхідно перейти від різних даних до структурованої інформації, а також попередніх знань (інформації) [2].

Оброблені, структуровані та позначені набори даних, отримані з пов'язаних масивів великих даних, є одним із необхідних (і найцінніших) компонентів машинного навчання в сучасних системах.

Глибокий аналіз даних (data mining) - побудова та вилучення корисної інформації з неоднорідних і неструктурованих великих обсягів даних, включаючи великі дані [1].

Нечітка логіка – використання вільних правил та нечітких відповідей для вирішення проблем у системах штучного інтелекту та нейронних мережах. Його можна використовувати для моделювання людської логіки, наприклад, під час звуження або розширення результатів пошуку відповідей на запитання на основі контексту.

Розглянувши основні визначення та принципи, перейдемо до питання практичного застосування систем ШІ в кібербезпеці. Є дві основні причини для використання ШІ в ІБ – необхідність швидкого реагування у разі кіберінциденту та відсутність кваліфікованих експертів з кібербезпеки. Насправді в сьогоднішніх реаліях складно наповнити штатні плани кваліфікованими фахівцями ІБ з необхідним досвідом, а масштабні інциденти ІБ можуть розвиватися стрімко: рахунки часто вимірюються хвилинами.

Без регулярних 24-годинних змін аналітиків ІБ та системи, яка працюватиме автономно для реагування на кіберінциденти, важко забезпечити високоякісний захист у неробочий час [11].

Крім того, зловмисники можуть застосувати тактику відволікання перед атакою, наприклад, розпочати DDoS-атаку або активне сканування мережі, щоб відвернути увагу кіберекспертів. У цьому випадку допоможе система реагування на кіберінциденти на основі ШІ, яка може обробляти велику кількість інцидентів ІБ одночасно, автоматизувати щоденні операції аналітиків ІБ і швидко реагувати на інциденти без втручання людини. Наприклад, у нашому рішенні Security Vision IRP/SOAR широко використовуються механізми штучного інтелекту та машинного навчання: навчена на раніше вирішених інцидентах платформа сама запропонує відповідні відповіді аналітикам на основі типу кіберінциденту та його властивостей. найкраща група реагування буде призначена з числа колег, які володіють найбільш відповідними знаннями, і в разі виявлення нетипового підозрілого інциденту система сама створить відповідний інцидент і повідомить про це співробітників відділу ІБ.

Рішення IRP/SOAR Security Vision використовує алгоритми для прогнозованого реагування на кіберподії: навчена система дозволяє передбачати вектори атак та їх подальший розвиток у вашій інфраструктурі, показувати тенденції, потім автоматично блокувати шкідливу поведінку та надавати рекомендації аналітикам SOC.

Системи захисту на основі штучного інтелекту необхідні для виявлення аномалій у великій кількості інцидентів інформаційної безпеки, наприклад, шляхом аналізу журналів CSI, даних із систем SIEM або рішень SOAR. Ця інформація разом із даними про події ІБ, які були оброблені та закриті, стане високоякісним набором даних із мітками, на якому систему можна буде легко навчити [23].

Класичні системи аналізу відхилень зазвичай побудовані на певних правилах, попередньо встановлених оператором: наприклад, перевищення певного обсягу трафіку, певна кількість невдалих спроб аутентифікації, певна кількість послідовних активацій SHI.

Системи на основі штучного інтелекту зможуть приймати рішення самостійно, незалежно від правил, раніше створених співробітниками ІБ, які могли втратити свою актуальність і не враховували зміни в ІТ-інфраструктурі. Виявлення аномалій може допомогти захистити дані користувачів - наприклад, служби онлайн-банкінгу можуть збирати та аналізувати дані про моделі активності клієнтів (підписи, шаблони), щоб швидко ідентифікувати скомпрометовані облікові записи [11].

Наприклад, якщо минулого року користувач підключався до сервісу з російської IP-адреси та використовував браузер Internet Explorer у робочий час у будні дні, під час підключення з Китаю за допомогою браузера Mozilla Firefox у нічний час обліковий запис може бути тимчасово заблоковано для реєстрації користувачеві та відправлені на службу. Вони надсилають сповіщення.

Фінансові установи також можуть використовувати системи машинного навчання та штучного інтелекту для оцінки (балів) позичальників, аналізу фінансових ризиків і використання систем боротьби з шахрайством. Ще один спосіб використання систем штучного інтелекту в кібербезпеці – це робота з інсайдерськими злочинцями: знаючи типову поведінку користувачів, система може надсилати сповіщення аналітикам ІБ про значні зміни в моделях роботи співробітників (відвідування підозрілих веб-сайтів, відхід на тривалий час). час) робота на комп’ютері, зміна кола спілкування під час спілкування в месенджері компанії тощо).

Системи безпеки, оснащені комп’ютерним зором і обробкою голосу, зможуть оперативно повідомляти охоронцям про спробу пройти через перехід

сторонніх осіб або співробітників про використання чужої перепустки, використовувати веб-камери для аналізу робочої діяльності співробітників і оцінювати правильність телефонного спілкування [10].

У той же час не варто забувати, що системи на основі штучного інтелекту також використовуються кіберзлочинцями: відомі методи шахрайства використовують глибокі фейки (створення реального віртуального образу людини), щоб обдурити системи боротьби з шахрайством, підроблені голоси родичів жертв, шахрайські дзвінки, запити на грошові перекази, фішинг і розкрадання за допомогою телефонної технології IVR.

Зловмисне програмне забезпечення також використовує елементи штучного інтелекту, що дозволяє зловмисникам швидше підвищувати свої привілеї, переміщатися по корпоративних мережах, а потім знаходити та викрадати цікаві для них дані.

Таким чином, технології, доступні громадськості, можуть бути використані як на благо, так і на шкоду, а це означає, що можна і необхідно використовувати найсучасніші засоби захисту та методи боротьби з такими високопідготовленими кіберзлочинцями.

1.3 Системи штучного інтелекту для моделювання загроз безпеки інформаційної системи

Сучасний світ вимагає інформаційної безпеки для захисту своїх систем від зміни даних, втрати даних і комп’ютерної інфільтрації. Окремі особи та компанії хочуть захистити свою інформацію від цих загроз. Кібербезпека також важлива в автоматизованих системах; це допомагає протистояти загрозам.

Багато організацій купують десятки продуктів безпеки. Це вказує на те, що, незважаючи на збільшення витрат на безпеку, порушення безпеки тривають без зупинки чи сповільнення.

Ефективній системі кібербезпеки потрібен час, щоб виявити атаки та вирішити їх. AI можна використовувати для прискорення цього процесу шляхом автоматичного виявлення та видалення загроз. ШІ — це технологія, яку можна використовувати в кібербезпеці; просто експертам потрібно трохи більше часу, щоб це реалізувати.

Інструменти на основі штучного інтелекту відповідають багатьом потребам у сфері кібербезпеки [16].

Паролі можуть бути зламані, що може призвести до несанкціонованого доступу до важливих ділових чи державних даних або інформації користувача. Замість використання біометричної автентифікації, яка захищена від злому паролів, користувачі повинні використовувати інші методи ідентифікації. Біометричні функції значно безпечніші порівняно зі сканерами пальців і долонь, оскільки вони сканують мозок або вену долоні. Коли користувачі вирішують пов’язати свої біометричні дані з паролем, це ускладнює злом їхніх даних.

Звичайні системи кібербезпеки не здатні виявляти всі типи зловмисного програмного забезпечення одночасно. Крім того, хакери ускладнили свої зусилля, впровадивши нове шкідливе програмне забезпечення. Необхідно використовувати вдосконалені інструменти безпеки для вирішення будь-яких складних загроз. Ці інструменти використовують вдосконалені алгоритми та шаблони коду, які постійно оновлюються за допомогою штучного інтелекту. Це тому, що звичайні інструменти безпеки не можуть легко виявити ці загрози. Розуміння проходження сайту, мікроповедінки зловмисного програмного забезпечення та будь-якої шкідливої діяльності допомагає приймати рішення завдяки поєднанню штучного інтелекту та машинного навчання [14].

Щоб боротися з будь-якими загрозами та запобігати їм, система штучного інтелекту повинна мати можливість точно виявляти загрози в режимі реального часу. Якщо система штучного інтелекту не може точно виявляти загрози в реальному часі, тоді система марна. Коли команда хакерів атакує систему з різних точок, штучний інтелект автоматично з'єднує крапки та пропонує контрзаходи. Це тому, що ШІ знає, що хакери з різних точок атакуватимуть одну точку системи одночасно. Програми AI використовують інтелектуальну аналітику, яка швидше та ефективніше розпізнає та усуває порушення безпеки. Наприклад, якщо програма ШІ виявляє шкідливий файл на диску, вона зазвичай переміщує файл в ізольовану частину диска.

Дані можуть бути перехоплені в мережах завдяки динамічній автентифікації. Системи штучного інтелекту забезпечують безпечну альтернативу традиційним методам автентифікації, оскільки вони можуть отримувати віддалений доступ до систем. Це викликає занепокоєння, коли віддалені користувачі системи скомпрометовані. Дані збираються та аналізуються системами штучного інтелекту під час віддаленого доступу до даних. Це стосується поведінки користувача, а також його пристрою та програми. Це створює глобальне середовище автентифікації в реальному часі, яке змінює привілеї доступу на основі місцезнаходження користувача або мережі [20].

Для прийняття рішень інженери використовують дані, тенденції та статистику. Машини не можуть мислити чи уявляти так, як люди — лише люди мають творче мислення та уяву. Однак інженерам для прийняття рішень потрібна допомога даних, тенденцій і розуміння.

Витрачення часу на вивчення та обробку значущих даних робить будь-яку ризиковану роботу практично неможливою в одну мить.

Компанії можуть автоматизувати безпеку без втручання людини, створюючи безпечні програми за допомогою ШІ.

Безперервний аналіз поведінки користувача на додаток до аналітики, що прогнозує, зменшує втручання інженера для захисту систем від серії атак. Зекономлений час можна інвестувати у творчі та плідні починання [3].

Тим не менш, системи штучного інтелекту навчаються і керуються людьми, і в деяких місцях потреба в людських інженерах є обов'язковою, оскільки вони здатні виходити за рамки аномалій, які машини не можуть виявити, і підтвердити, що передбачувана атака є справжньою.

1.4 Висновки

При створенні проектів, пов'язаних з інформаційною безпекою, ці критерії життєво важливі. Зрештою, неможливо виправдати витрати, пов’язані із забезпеченням безпеки організації, якщо вони не виправдані. Люди цікавляться, який рівень захисту повинна мати система. Вони можуть вибирати між двома підходами під час створення систем ідей.

Забезпечення безпеки проекту вимагає дотримання певних стандартів у сфері ІТ. Ці стандарти визначають, що має бути включено в проект. Використовуючи цю інформацію, кожен критерій зосереджується на досягненні певного стандарту. Оскільки ці документи не стосуються безпеки, визначення належного рівня захисту є складним процесом. Натомість слід зосередитися на вартості виконання функціональних вимог. Загальною мірою ефективності є середня вартість транзакції, яку можна знайти, поділивши загальну вартість на кількість виконаних функціональних вимог.

В управлінні ризиками використовується другий підхід для управління оцінками ризиків. Ідея цього підходу походить від ідеї «розумної достатності» при розгляді послуг ІБ.

Щоб правильно оцінити рівень загрози безпеці, нам потрібно ранжувати кожну загрозу на основі її передбачуваної небезпеки. Це вимагає розробки методу обробки кожної загрози, щоб визначити ступінь захисту від кожної з них.

Експерти з кібербезпеки користуються великим попитом через необхідність швидкого реагування в разі кібератаки. Також мало кваліфікованих спеціалістів з ІБ з досвідом; це пояснюється тим, що великомасштабні інциденти ІБ можуть розвиватися швидко, а рахунки можна виміряти за лічені хвилини. Частково це пов’язано з обмеженою кількістю людей, здатних зайняти посади спеціалістів.

Важко забезпечити надійну цілодобову безпеку, коли системі потрібно автоматично працювати автономно, щоб реагувати на кіберінциденти, а аналітикам ІБ потрібно працювати в регулярні зміни.

Зловмисники можуть використовувати методи відволікання напередодні атаки, такі як запуск DDoS-атаки або сканування активної мережі цілі. Це дозволяє їм відволікати кіберекспертів і не дати їм помітити майбутні атаки. Система реагування на кіберінциденти на основі ШІ, яка автоматизує щоденний аналіз ІБ та операції; забезпечує автоматичне реагування без втручання людини; і обробляє велику кількість одночасних інцидентів, що значно допоможе слідчим.

РОЗДІЛ 2. МОДЕЛЬ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІЗ ЗАСТОСУВАННЯМ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

2.1 Моделі кіберзагроз в системах захисту інформації

Згідно з аналізом літератури щодо систем виявлення та аналізу кіберзагроз, наведені вище методи, як правило, не мають достатніх математичних описів. В основному вони формалізовані у вигляді методів і функцій виявлення кіберзагроз, інструментальних засобів попередження та виявлення кіберзагроз. Проблема боротьби із загрозами комп'ютерної мережі не знайшла самостійного відображення в сучасній літературі, тому аналіз розглянутих методів проведено на відомих методах виявлення та аналізу мережевих загроз. Методи виявлення та аналізу несанкціонованого впливу на ресурси інформаційної системи можна розділити на (рисунок 2.1).

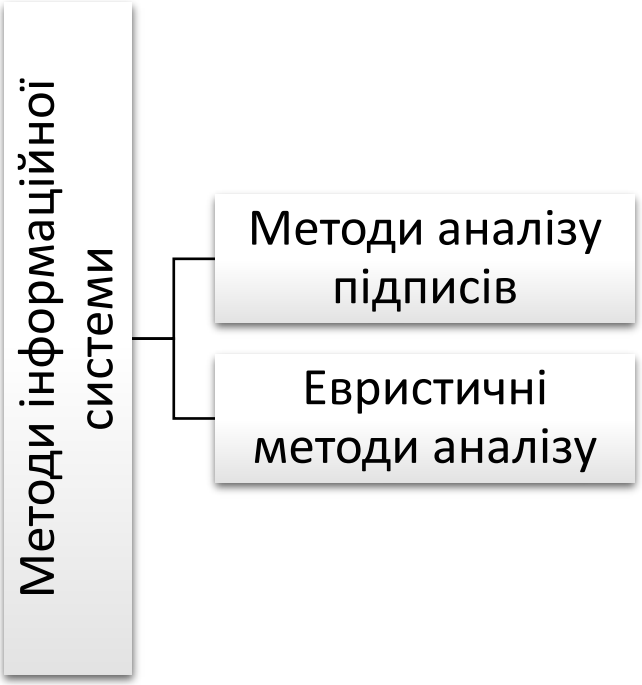


Рис 2.1. Методи інформаційної системи

До останніх відносять статистичні моделі (імовірнісні моделі, моделі кластерного аналізу), моделі кінцевих автоматів, марковські моделі, моделі на основі нейронних мереж, моделі на основі генної інженерії.

Сигнатури використовуються для аналізу кіберзагроз на основі контролю програм і даних, послідовностей символів, подій у мережі та бази даних сигнатур кіберзагроз. В якості вихідних даних для цих методів використовується інформація з системних журналів, баз даних і ключові слова мережевого трафіку. Крім того, загальне та спеціалізоване програмне забезпечення можна аналізувати на ознаки загроз. На жаль, методи аналізу сигнатур мають серйозний недолік: нові модифіковані загрози неможливо виявити без оновлення бази даних сигнатур мережевих загроз. Крім того, ці методи потребують дуже мало обчислювальної потужності. Це робить їх дуже надійними та забезпечує високу ефективність впровадження циклів технічного контролю ІТ. Ще одна перевага полягає в тому, що вони не вимагають суворої формалізації ключових слів у мережевому трафіку [5].

Методи, розроблені для виявлення кіберзагроз, які ще ніхто не ідентифікував, використовують евристику. Їхній метод роботи зосереджений на виявленні ненормальної поведінки ІС, яка відхиляється від типової. Після виявлення аномалії вони можуть приймати рішення щодо можливих кіберзагроз. Евристичний аналіз у мережах використовує ознаки загроз комп’ютерної мережі, такі як незвичні стеки протоколів, які використовуються для запиту інформації, і довгі пакети. Вони також шукають незвичайні масові запити даних і нестандартний розподіл символів у пакетах.

Правила обробки даних і вимоги захисту інформації повинні бути зрозумілі перед застосуванням методів евристичного аналізу. Також необхідно оновити процедури обробки даних, а також краще зрозуміти правила обробки даних і вимоги захисту інформації.

2.1.1.Статистична модель

Моніторинг аномалій у мережі IS зосереджується на статистичному аналізі з використанням попередньо визначеної моделі нормальної поведінки. Цей підхід визначає аномалії шляхом порівняння поточного мережевого трафіку IS із вимогами шаблону.

Відсутність надійної інформації ускладнює людям прийняття рішень без урахування якісних даних. Відсутність обчислювальних моделей робить прийняття рішень ще більш складним. Ось чому людям потрібно покладатися на експертні думки та статистичні моделі, які поєднують дані експериментів із теорією ймовірностей (рис 2.2.).

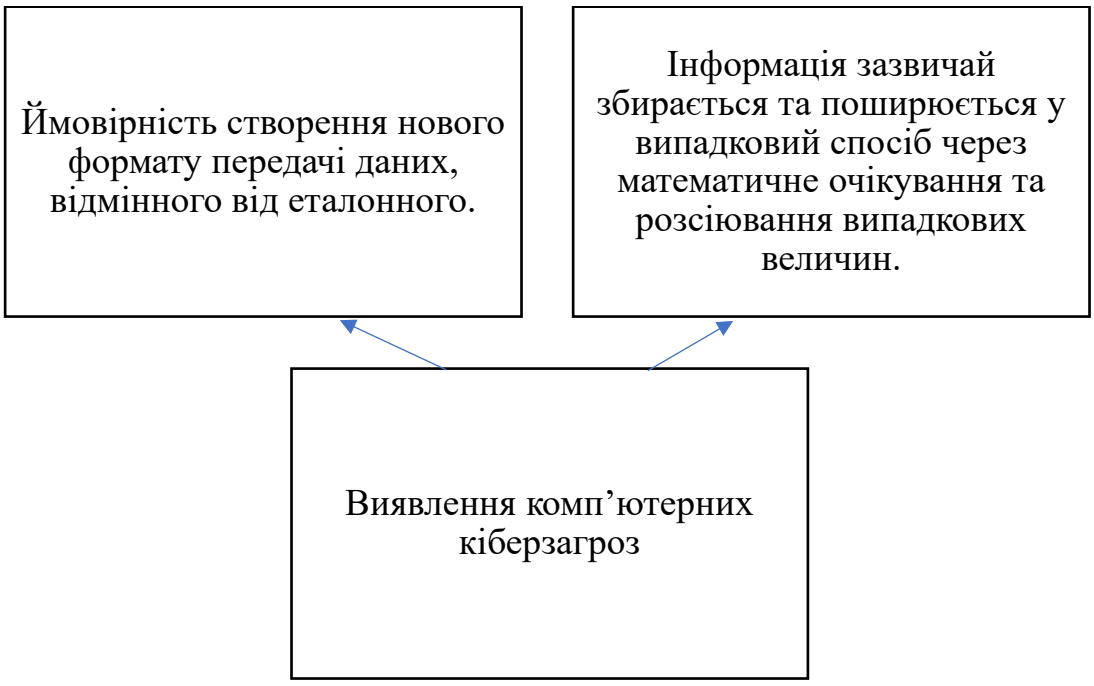


Рис.2.2. Виявлення кіберзагроз

Статистичний аналіз корисний для аналізу невеликої частини комп’ютерних кіберзагроз. Однак він має труднощі з виявленням аномалій і вторгнень через маніпуляції даними. Через це статистичні методи не можуть точно виявити всі типи загроз. Однією з причин, чому ці методи не працюють

належним чином, є те, що їм важко впоратися з величезною кількістю даних, які вони аналізують. Іншою проблемою цих методів є велика кількість неправдивої інформації, яка надсилається через «сміттєві» повідомлення.

Важливо використовувати статистичні моделі, щоб визначити, чи кіберзагрози відхиляються від норми. Тому необхідно створити чіткі вказівки та перевірити ключові слова під час розрахунку статистики на різних рівнях передачі даних. За оцінками, приблизно 40% усіх виявлених загроз є помилковими спрацьовуваннями [33].

2.1.2.Кластерний аналіз

Аналіз кіберзагроз використовує два етапи алгоритму. Перший аналізує кластери даних, утворені аномальною поведінкою ІС на нижчому рівні протоколів передачі даних. Другий аналізує кластери даних, утворені вищими рівнями використання протоколу. На основі цього аналізу моделі кластерного аналізу визначають класифікатори, які вказують на основні компоненти кіберзагроз. Ці моделі використовують ці класифікатори для обчислення відстані між кластерами даних і визначення наявності чи відсутності кіберзагроз в організації.

Створення кластерів регулярної та аномальної поведінки системи вимагає другого етапу. У цій частині отримані кластери порівнюються з кластерами звичайної поведінки. Кластеризація пакетів на основі заголовків без аналізу їх вмісту є середнім способом виявлення кіберзагроз, коли вторгнення відбуваються лише за заголовками пакетів передачі даних. Щоб отримати достовірні дані за допомогою моделі кластерного аналізу, потрібно проаналізувати кілька системних журналів ІС у порядку ідентифікації та автентифікації ІС, реєстрації користувача, збою системи, доступу до

обчислювальних ресурсів: аудит, реєстрація, ресурс, що спричиняє затримки. під час прийняття рішення. Ця затримка часто перешкоджає використанню моделей кластерного аналізу в квазіреалістичних системах масштабу часу [31].

2.1.3.Модель кінцевих автоматів

Обмін інформацією між людиною та інформаційною системою представлений кінцевим автоматом, який моделює протоколи передачі даних. Вивчаючи цю модель, кіберзагрози виявляються за допомогою підходу інформаційної машини стану. Кожен стан має вхідні дані, внутрішні стани та вихідні дані. Вважається, що ІС розпізнає нормальні стани системи та переходи, перемикаючись між ними. Будь-які зміни в системі, які виходять за рамки звичайного, вважаються ненормальними та потенційно небезпечними.

Основною перевагою моделі є простота визначення критеріїв класифікації ІБ. Оскільки він враховує лише невелику кількість переходів між станами, він точно відображає характер обробки даних у реальному часі через мережеві протоколи. Недоліки моделі включають необхідність створення багатьох складних експертних правил для аналізу аномальних і необхідних змін стану з метою класифікації кіберзагроз. Крім того, модель потрібно оновити, щоб включити нові правила переходу. Експертні правила оцінки станів ІС взаємопов'язані з характеристиками мережевих протоколів передачі даних [30].

2.1.4.Марківська модель

Ланцюги Маркова визначають ймовірність переходу з одного стану в інший. Ця інформація використовується для створення ланцюга Маркова

системи, яка нормально функціонує. Потім виміряні дані використовуються як навчальні дані моделі Маркова. Для пошуку аномалій поряд із функціями розподілу ймовірності ненормальної та нормальної роботи використовується ланцюг Маркова. Ця модель ефективна для пошуку аномалій, виявлених за допомогою системних викликів з операційної системи. Це також вимагає використання додаткової статистики в системах квазіреального часу, які обчислюють час аналогічним чином.

Так, марківська модель загрози безпеки системи захисту інформації представлена у вигляді процесів з дискретним станом і безперервним часовим проміжком для орграфа загрози інформаційній безпеці. Створюється за допомогою загрози двох атак:

- в першій використовуються загрози першої і другої уразливості;
- в другій використовуються загрози першої і третьої уразливості.

Тут система з відмовами і відновленнями характеристики безпеки, граф системи станів випадкових процесів представлений на рисунку 2.3

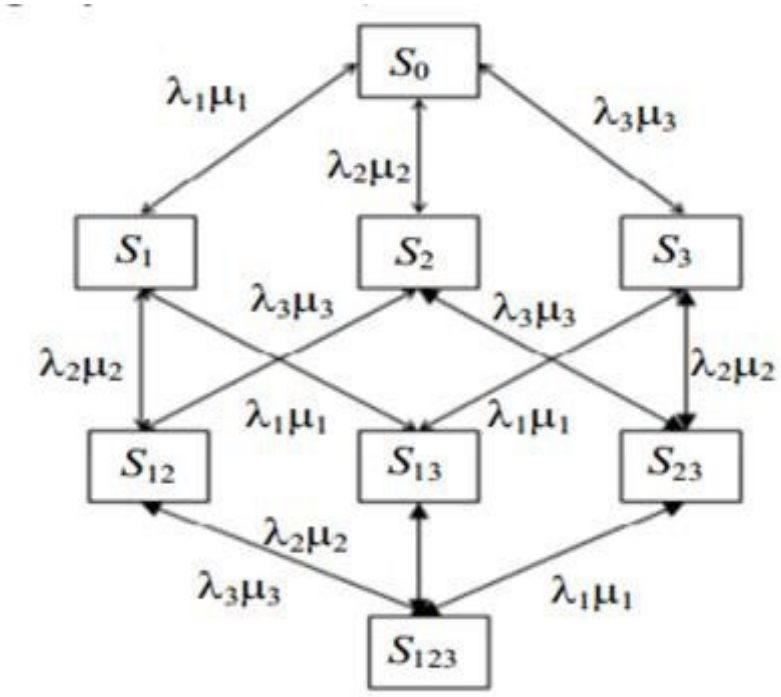


Рис. 2.3. Марківська модель загрози інформаційної безпеки

Згідно цієї схеми, S0 – початковий стан системи, S1 – в системі виявлена і не усунена одна із загроз, S2 – в системі виявлені і не усунені дві загрози, S3 – в системі виявлені і не усунені всі три загрози.

На підставі даного графа відбувається моделювання залежності загроз за ступенем їх вразливості. Завдяки використанню даної моделі, будується система диференціальних рівнянь Колмогорова для ймовірностей станів. При вирішенні якої, розраховується ймовірність того, наскільки готова інформаційна система до безпечної експлуатації. Тут обґрунтовується коректність використання марківських процесів моделювання характеристик безпеки інформації, виявляються відмінності в постановці і вирішенні задач моделювання комплексної системи захисту інформаційної системи [21].

2.1.5.Метод «теорії ігор»

Крім марківської моделі оптимізації комплексної системи захисту інформації важлива роль відводиться і методологічного апарату теорії ігор, яка передбачає наявність покупця і продавця, взаємозв'язок між якими визначена у вигляді платіжної матриці (табл. 2.2).

Таблиця 2.2.

Загальний вигляд платіжної матриці статистичної гри

	S1	S2	…	Sj
A1	w11	w12	…	w1j
A2	w21	w22	…	w2j
…	…	…	…	…
Ai	wi1	wi2	…	wij

В даному випадку рядок матриці буде виглядати так: A1, A2 ..., Ai - це стратегія особи приймаючої рішення, а стовпці матриць S1, S2, ..., Sj - відображають стан навколишнього середовища, wij =i =j - очікувана нагорода при використанні тієї чи іншої стратегії А в разі знаходження середовища в стані Sj.

Для того, щоб прийняти вірне рішення, в основному управління здійснюють на підставі критерію Вальда і критерію Гурвіца. Завдяки критерію Вальда здійснюється вибір так званої, обережною стратегії в сторону песимістичного плану. Тобто, для кожного прийнятого рішення вибирають найгіршу ситуацію з пошуком гарантованого максимального ефекту.

На підставі цього обраний варіант повністю виключає ризик небажаного варіанту подій.

Коли застосовується критерій Вальда, то рішення здійснюється за наступним сценарієм:

- виявляються можливості зовнішнього прояву нічого невідомого природного стану Sj;
- проводиться облік прояви того чи іншого зовнішнього стану Sj;
- рішення використовується одноразово з виключенням будь-якого було ризику [34].

2.1.6.Метод використання нейронних мереж

Початкова класифікація аномалій за методами виявлення кіберзагроз через нейронні мережі виконується за допомогою ІС. Ці методи використовують ідентифікацію нормальної поведінки системи на основі функції розподілу

пакетів даних — разом із навчанням нейронної мережі та аналізом подій на основі вибірки, яка використовується під час навчання.

Аномальне відхилення в IS вказує на те, що впевненість нейронної мережі у своїх рішеннях нижче встановленого порогу. Це вказує на те, що в мережі існує аномалія, що ускладнює виявлення кіберзагроз. Це пояснюється тим, що для навчання алгоритмів для належної роботи на нормальних нейронах потрібен час, що сповільнює процес виявлення. Нейронна мережа також надзвичайно складна, і її важко навчити, якщо вона не знає, що таке кіберзагрози.

Щоб використовувати нейро-нечітку мережу для оцінки ризиків інформаційної безпеки, необхідно визначити, які дані слід подавати на вхід системи. З визначення ризику інформаційної безпеки слід, що величина ризику R є функція від потенційно можливого збитку (вартості інформації, ресурсу або активу) A, загрози інформаційній безпеці T і уразливості інформаційної системи [16].

Таким чином, вхідними факторами будуть служити експертні оцінки трьох нечітких змінних («загроза», «збиток», «вразливість»), описаних лінгвістичними терм-множини {дуже низький, низький, середній, високий, дуже високий} (табл. 2.3).

Крім експертних оцінок, додатково слід використовувати і дані системи виявлення вторгнень, антивірусів, міжмережевих екранів про потенційно небезпечної активності, загальний рівень мережевої активності і навантаження на ту чи іншу ділянку автоматизованої системи.

Таблиця 2.3.

Стани загроз

Рівні шкали	Загрози	Збиток	Уразливість
1	2	3	4
Дуже низький	Подія практично ніколи не відбувається	Незначні втрати матеріальних засобів та ресурсів, які швидко заповнюються, або незначний вплив на репутацію	Уразливість, якою можна знехтувати
Низький	Подія відбувається рідко	Більш помітні втрати матеріальних активів, більш істотний вплив на репутацію або ущемлення інтересів	Незначна уразливість, що яку легко усунути
Середній	Подія можлива тільки при певному збігові обставин	Достатні втрати матеріальних активів або ресурсів або достатній шкоди репутації та інтересам	Помірна вразливість
Високий	Велика ймовірність, що подія настане при організації атаки	Значної шкоди репутації та інтересам, що може становити загрозу для продовження діяльності	Серйозна вразливість, ліквідація якої можлива, але повязана з витратами
Дуже високий	Подія вірогідніше настане під час атаки	Руйнівні наслідки і неможливість ведення діяльності	Критична вразливість, яка ставить під сумнів можливість її усунення

В результаті на виході системи буде отримана оцінка рівня ризику інформаційної безпеки [16].

В цьому випадку шкала вимірювання рівень інформаційних ризиків буде виглядати наступним чином:

- можна знехтувати низький - ризиком можна знехтувати;
- дуже низький - необхідно визначити, чи існує необхідність у коригувальних діях, або є можливість прийняти цей ризик;
- низький - рівень ризику дозволяє працювати, але є передумови до порушення нормальної роботи;
- нижче середнього - необхідно розробити і застосувати план корегуючих дій протягом прийнятного періоду часу;
- помірний - рівень ризику не дозволяє стабільно працювати, є нагальна необхідність у коригувальних діях, що змінюють режим роботи в сторону зменшення ризику;
- вище середнього - система може продовжувати роботу, але коригувальний план дій необхідно застосувати якомога швидше;
- високий - рівень ризику такий, що бізнес-процеси знаходяться в нестійкому стані;
- дуже високий - необхідно негайно вжити заходів щодо зменшення ризику;
- критичний - рівень ризику дуже великий і є неприпустимим для організації, що вимагає припинення експлуатації системи і прийняття радикальних заходів щодо зменшення ризику [14].

Розглянемо приклад застосування нейро-нечіткої мережі для оцінки інформаційних ризиків в автоматизованій системі. Для наочності на рис. вказані три вхідні змінні (загрози, збитки, уразливості). Виходом є ризик інформаційної безпеки.

Блок, позначений на схемі як NNclass (шар L1) (рис. 2.5), призначений для вирішення завдання кластеризації, тобто завдання функцій належності вхідних даних п'яти нечітким класами.

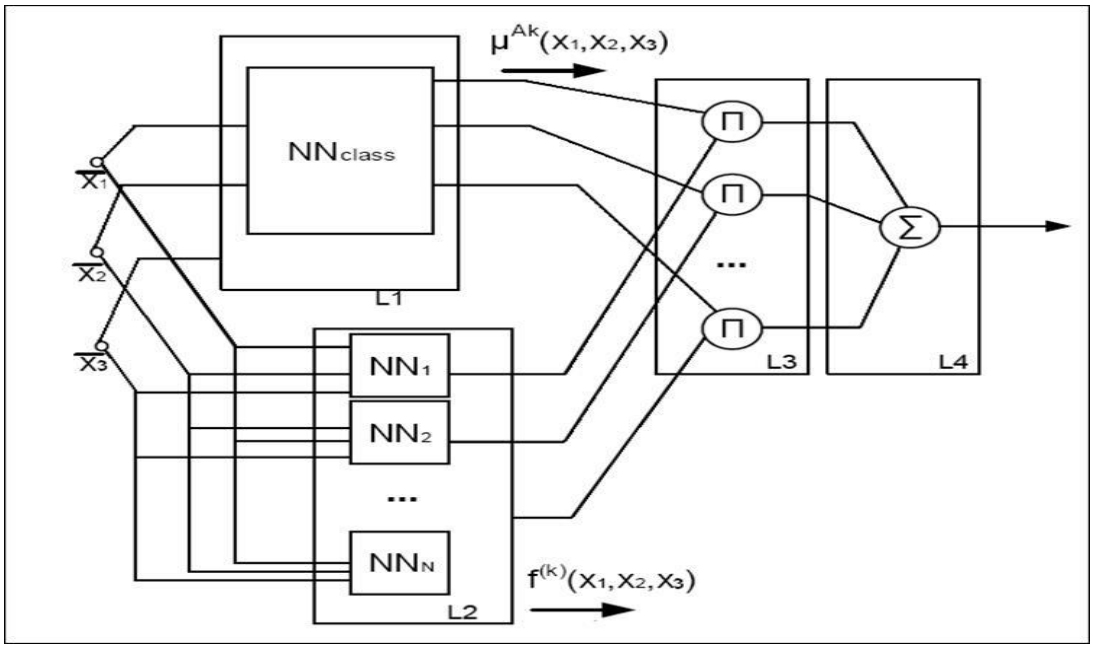


Рис. 2.5. Нейро-нечітка мережа для оцінки інформаційних ризиків в АС

Застосування нейронних мереж для оцінки кіберзагроз дозволяє вирішити проблему явної неповноти інформації про складові ризику і їх неоднозначних властивостей. При застосуванні нейронних мереж відсутня необхідність створення детальної моделі автоматизованої системи для здійснення аналізу інформаційних ризиків. Система дозволяє агрегувати дані з різних джерел і добре пристосована для ітераційного безперервного аналізу ризиків інформаційної безпеки [19]

2.1.7.Переваги та недоліки евристичних методів

Таким чином, перевагою методів виявлення аномальних відхилень є можливість аналізу динамічних процесів функціонування ІС і виявлення в них нових типів кіберзагроз. Методи дають можливість апріорного розпізнавання аномалій шляхом систематичного сканування вразливих місць.

До недоліків цих методів можна віднести необхідність збільшення навантаження на трафік в мережі, складність реалізації і більш низька вірогідність виявлення комп'ютерних кіберзагроз в порівнянні з сигнатурним аналізом.

Обмеженням методів виявлення та аналізу кіберзагроз є необхідність детальної інформації про застосування протоколів (стеків протоколів) передачі даних в ІС на всіх рівнях еталонної моделі взаємодії відкритих систем [7].

2.2 Машинне навчання

Машинне навчання являє собою підрозділ штучного інтелекту, що стоїть на стику таких дисциплін, як математика, статистика, теорія ймовірностей, теорія графів і вивчає алгоритми, які здатні самостійно навчатися на основі досвіду (рис. 2.6).

Рис. 2.6. Класифікація методів машинного навчання

При навчанні з учителем для кожного прецеденту задана пара «ситуація, рішення». Завдання такого навчання полягає в пошуку залежно прийнятого рішення від заданої ситуації і побудові алгоритму, здатного прийняти на вхід опис ситуації, а на виході передбачити для неї рішення.

При навчанні без учителя на вхід подаються тільки описи об'єктів без прийнятого рішення по цій ситуації, а завдання полягає в пошуку залежностей між представленими об'єктами.

Часткове навчання є проміжною ланкою між навчанням з учителем і без учителя, так як кожен прецедент задається парою «ситуація, рішення», однак відповіді відомі лише для частини цих ситуацій.

Існують різні алгоритми машинного навчання, на основі яких будується модель системи. Багато в чому вибір відповідного алгоритму залежить від характеристик набору даних, таких як обсяг, структура і якість. Також на вибір алгоритму впливає бажаний результат (двокласова або багатокласова класифікація, регресія або фільтрація викидів), необхідна точність передбачення і час, необхідний для навчання моделі [21].

При навчанні з підкріпленням не існує «правильних відповідей» для кожної ситуації, алгоритм шукає оптимальну стратегію поведінки, спираючись на реакцію зовнішнього середовища.

Регресійна модель

Як правило, для передбачення значень змінної використовується регресійний аналіз. Його мета - розробити статистичну модель, що дозволяє прогнозувати значення залежної змінної, або відгуку, за значеннями, принаймні однієї, незалежної, або пояснює, змінної.

Для ілюстрації залежності між змінними X і Y використовувалася діаграма розкиду. На ній значення змінної X відкладалися по горизонтальній осі, а

значення змінної Y - по вертикальній. Залежність між двома змінними може бути різною: від найпростішої до вкрай складної [26].

Труднощі, пов'язані з регресійним аналізом (рис 2.7):

Рис 2.7. Проблеми регресійного аналізу

Критерій згоди «χ2-квадрат Пірсона»

Розподіл χ3 використовується для перевірки узгодженості набору даних з фіксованим розподілом ймовірностей. У критерії згоди частоти, що належать певній категорії, порівнюються з частотами, які є теоретично очікуваними, якби дані дійсно мали зазначений розподіл.

Перевірка за допомогою критерію згоди χ 3 виконується в кілька етапів. По-перше, визначається конкретний розподіл ймовірностей, яке порівнюється з вихідними даними. По-друге, висувається гіпотеза про параметри обраного розподілу ймовірностей (наприклад, про її математичне сподівання) або проводиться їх оцінка. По-третє, на основі теоретичного розподілу визначається теоретична ймовірність, відповідна кожної категорії. На закінчення, для

перевірки узгодженості даних і розподілу застосовується тестова $\chi 3$ – статистика.

Критерій χ 3 для перевірки гіпотези від дисперсії або стандартного відхилення вважається класичною параметричної процедурою. При перевірці гіпотези про дисперсії генеральної сукупності або стандартного відхилення передбачається, що вихідні дані мають нормальний розподіл. Нажаль, $\chi 3$ - критерій досить чутливий до порушення цих припущень (тобто цей критерій не є стійким). Отже, якщо генеральна сукупність не має нормального розподілу, особливо, коли обсяг вибірки невеликий, точність критерію може значно знизитися [29].

Класифікація на основі Байєсівського підходу

Байєсівський підхід до класифікації заснований на теоремі, яка стверджує, що якщо щільності розподілу кожного з класів відомі, то шуканий алгоритм можна виписати в явному аналітичному вигляді. Більш того, цей алгоритм оптимальний, тобто володіє мінімальною ймовірністю помилок.

На практиці щільності розподілу класів, як правило, не відомі. Їх доводиться оцінювати (відновлювати) за навчальною вибіркою. В результаті байесовский алгоритм перестає бути оптимальним, так як відновити щільність по вибірці можна тільки з деякою погрішністю. Чим коротше вибірка, тим вище шанси підігнати розподіл під конкретні дані і зіткнутися з ефектом перенавчання.

Байєсівський підхід до класифікації є одним з найстаріших, але до сих пір зберігає міцні позиції в теорії розпізнавання. Він лежить в основі багатьох досить вдалих алгоритмів класифікації. До числа байесовских методів класифікації відносяться:

- Наївний байесовский класифікатор;
- Лінійний дискримінант Фішера;

- Квадратичний дискримінант;
- Метод парзеновского вікна;
- Метод радіальних базисних функцій (RBF);
- Логістична регресія [29].

Наївний байесівський класифікатор (naïve Bayes) - спеціальний окремий випадок байєсівського класифікатора , заснований на додатковому припущенні, що об'єкти $x \in X$ описуються n статистично незалежними ознаками.

$$x \equiv (\xi 1, \ldots, \xi n) \equiv (\mathrm{f1}(x), \ldots, \mathrm{f}n(x))$$

Припущення про незалежність означає, що функції правдоподібності класів представимо у вигляді:

$$\mathrm{py}(x) = \mathrm{py1}(\xi 1) \cdot \ldots \cdot \mathrm{pyn}(\xi n)$$

де pyj(ξj)- щільність розподілу значень j-го ознаки для класу Припущення про незалежність істотно спрощує завдання, тому що оцінити одновимірних щільності набагато легше, ніж одномірну щільність. На жаль, воно вкрай рідко виконується на практиці, звідси і назва методу.

Наївний байесівський класифікатор може бути як параметричних, так і непараметричним, в залежності від того, яким методом відновлюються одномірні щільності.

Основні переваги наївного байєсівського класифікатора - простота реалізації і низькі обчислювальні витрати при навчанні та класифікації. У тих рідкісних випадках, коли ознаки дійсно незалежні (або майже незалежні), наївний байесівський класифікатор (майже) оптимальний.

Основний його недолік - відносно низька якість класифікації в більшості реальних задач. Найчастіше він використовується або як примітивний еталон для порівняння різних моделей алгоритмів, або як елементарний будівельний блок в алгоритмічних композиціях [26].

2.3 Поняття та класифікація алгоритмів кластеризації методів машинного навчання

Класифікація — це дія поділу набору об’єктів на окремі групи. Навпаки, кластеризація — це процес поділу об’єктів на кластери, які визначаються під час роботи алгоритму. Різні групи в схемі класифікації повинні бути максимально подібними і містити «схожі» об’єкти.

У загальному вигляді кластерний аналіз використовує наступні етапи прогресії.

1. Вибір групи подібних предметів.
2. Змінні, що використовуються для оцінки суб'єктів вибірки, повинні бути визначені та нормалізовані, якщо необхідно.
3. Ступінь подібності об'єктів обчислюється за допомогою чисел.
4. Аналіз об’єктів на групи за допомогою методів кластерного аналізу призвів до того, що схожі об’єкти утворили кластери.
5. Подання результатів аналізу.

Додатковий аналіз метрик і методів дає найкращі результати. Цього можна досягти шляхом налаштування вибраного показника та методу групування.

Подібність об’єктів визначається за допомогою набору числових значень, наприклад, чийсь зріст/вага. Однак існують методи, які також кількісно визначають якісні ознаки. Під час обчислення відстані між двома векторами всі компоненти необхідно нормалізувати, щоб їхні значення були еквівалентними. Цей процес регулює всі значення в діапазоні від -1 до 1 або від 0 до 1. Після нормалізації ми можемо виконувати будь-які обчислення, які забажаємо [14].

Метрики для вимірювання подібності включають відстань, яка є сприйманим проміжком між двома об’єктами. Існує багато метрик для вимірювання цієї відстані між різними парами об’єктів.

Евклідова відстань є найпоширенішим способом вимірювання відстані в нашому просторі. Він використовується для вимірювання відстаней у багатовимірному просторі з акцентом на геометричні відстані.

Вага додається до віддалених об’єктів, що робить Евклідов квадрат ефективним для визначення ваги.

Відстань між двома кварталами міст на Манхеттені вимірюється шляхом усереднення різниць у координатах адрес. Цей метод дає ті самі результати, що й звичайні обчислення відстані під час обліку викидів. Однак він усуває ефект екстремальних відмінностей через відсутність квадратичних вимірювань.

Під час обчислення відстані Чебишева між двома об’єктами корисно розглядати кожну координату як окремий фактор, що розрізняє.

Відстань у градусах від певного кута використовується для вимірювання різниці ваги між об’єктами різних розмірів. Для цього вимірювання використовується наступна формула.

Дослідник визначає використовувану систему вимірювання завдяки величезним відмінностям у кластеризації даних, які спостерігаються в різних системах [21].

Алгоритми комп’ютерної кластеризації бувають двох основних видів.

З плоскою та ієрархічною організацією.

Ієрархічні алгоритми поділяють дані на підмножини, які є різними та незалежними. Натомість вони створюють систему вкладених підрозділів, створюючи ієрархії, які поділяють дані. Наприклад, плоский алгоритм може

розділити великий набір даних на один кластер, тоді як ієрархічний алгоритм може організувати його на кілька незалежних груп.

Ясно і неоднозначно.

Алгоритми, які точно відповідають кожному об’єкту вибірки номеру кластера, або які не мають пересічних алгоритмів, вважаються нечіткими або середніми. Алгоритми, які є середніми для зв’язків між об’єктами вибірки та номерами кластерів, називаються нечіткими. Ці алгоритми призначають кожному об’єкту набір значень і ймовірностей, пов’язаних із його зв’язком із кластерами.

Додавання кількох груп разом для створення єдиної згуртованої групи.

При об’єднанні кластерів з ієрархічними алгоритмами необхідно вирішити, як виміряти «відстань» між кожним кластером. Існує кілька показників для досягнення цього подвигу.

Використовуючи одинарні зв’язки, найближчі вузли є рівноправними.

Цей підхід фокусується на відстані між кластерами, враховуючи найближчих сусідів різнорідних груп. Це призводить до ланцюжків згрупованих кластерів як наступного кроку.

Найбільша відстань між будь-якими двома будинками вважається «повним зв’язком».

Цей метод визначає відстань між кластерами, знаходячи найдальші точки між усіма об’єктами, що містяться в різних кластерах. Він ґрунтується на тому, що різні групи об’єктів не мають спільного між собою простору. Цей метод ефективний при застосуванні до кластерів неправильної форми або типів груп, які не є ланцюгами. Однак це погано працює, якщо тип природної групи схожий на ланцюг або витягнутий.

Незважені попарні середні обчислення включають усі точки даних, незалежно від їх ваги.

Цей метод на основі даних вимірює середню відстань між кожною парою об’єктів у кожному кластері. Він ефективно визначає відстань між групами об’єктів, які утворюють ланцюги або кластери з більш ніж двома членами.

Середньозважене значення розраховується за допомогою суми двох окремих середніх значень.

Зважені середні значення створюються за допомогою того ж процесу, що й незважені попарні середні, за винятком того, що враховується кількість об’єктів, які містяться в кожному кластері. Цей метод можна використовувати, коли припускаються різні розміри кластерів [25].

Метод незваженого центроїда передбачає визначення місцезнаходження центру маси об’єкта.

Відстань між двома центрами кластерів використовується як міра їх відстані один від одного.

Практикується за допомогою використання зважених центроїдів або центральної точки.

На додаток до попередніх обчислень цей метод включає ваги для врахування різниці між розмірами кластерів. Як правило, він вважається кращим за попередній метод, якщо підозрюються або присутні значні відмінності в розмірах кластерів.

Замість використання кластерних методів деякі ієрархічні алгоритми використовують концепцію порогу. Порогові алгоритми зазвичай використовуються для створення початкових сукупностей. Вони природно ділять набір даних на кілька окремих груп або кластерів. Одним із популярних типів порогових алгоритмів є FOREL (формальний елемент), який є прикладом

евристичного методу класифікації, заснованого на концепції об’єднання об’єктів у зонах високої концентрації. Це математичне рівняння визначає таксони, отримані в певному радіусі. Менші радіуси дають більше таксонів. Це пояснюється тим, що математично розраховані кулі мають сферичну форму [4].

Без вчителя нейронні мережі, такі як Кохонен, навчаються вирішувати нові завдання. Вони кластеризують дані, прогнозують властивості та зменшують розмірність даних. Ці мережеві архітектури можуть навіть виконувати багато завдань одночасно, навіть без «майстра», який би вказував їм, що робити далі.

Раніше розглянуті архітектури нейронних мереж навчалися з учителем на вибірках даних, що включають безліч прикладів, що складаються з відповідних один одному пар вхідних і вихідних векторів. При цьому вихідні значення брали безпосередню участь в налаштуванні вагових коефіцієнтів. У нейронних мережах Кохонена вихідні вектора в навчальній вибірці можуть бути, але можуть бути і відсутніми, і, в будь-якому випадку, вони не беруть участі в процесі навчання. Тобто виходи не використовуються в якості орієнтирів при корекції синапсів. Саме тому даний принцип настройки нейронної мережі називається самонавчанням.

У розглянутій архітектурі сигнал поширюється від входів до виходів в прямому напрямку. Структура нейронної мережі містить єдиний шар нейронів (шар Кохонена) без коефіцієнтів зміщення. Загальна кількість вагових коефіцієнтів розраховується як добуток. Кількість нейронів дорівнює кількості кластерів, серед яких відбувається початкове розподіл і подальше перерозподіл навчальних прикладів. Кількість вхідних змінних нейронної мережі дорівнює числу ознак, що характеризують об'єкт дослідження і на основі яких відбувається віднесення його до одного з кластерів [14].

Слід розрізняти власне самонавчання і самоорганізацію нейронної мережі Кохонена. При звичайному самонавчанні мережа має строго фіксовану

структуру, тобто кількість нейронів, що не змінюються протягом усього життєвого циклу. При самоорганізованій мережі, навпаки, не має постійної структури. Залежно від знайденого відстані до нейрона-переможця, або цей нейрон використовується для кластеризації прикладу, або для поданого на входи прикладу створюється новий кластер з відповідними йому ваговими коефіцієнтами. Крім того, в процесі самоорганізації структури мережі Кохонена окремі нейрони можуть виключатися з неї (рис. 2.8).

Для життєвого циклу нейронних мереж даної архітектури характерні три основні стадії життєвого циклу: навчання, кластерний аналіз та практичне використання [11].

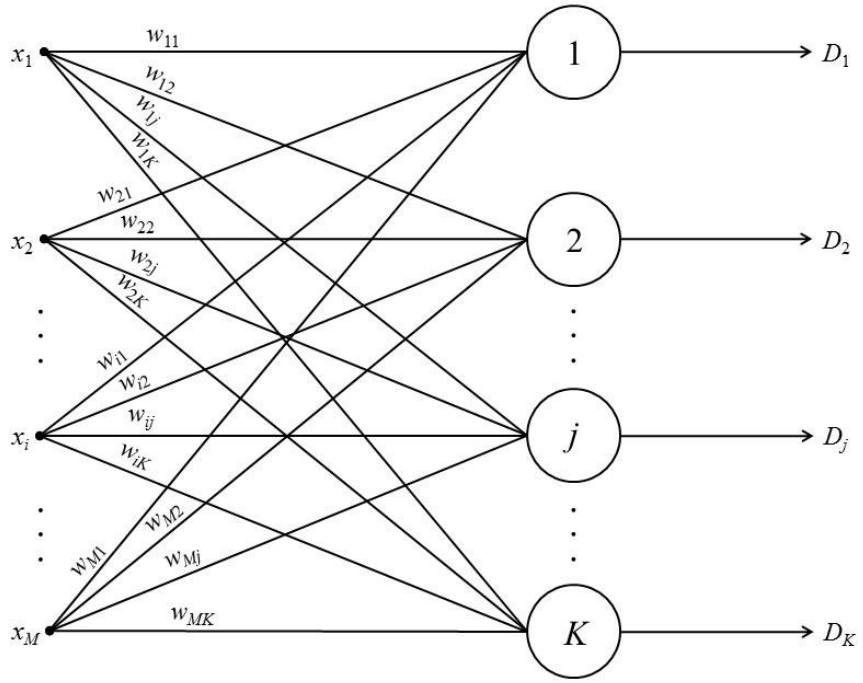


Рис. 2.8. Загальна структура нейронної мережі Кохонена. Нормалізація вхідних змінних виконується в межах [-1, 1] або [0, 1].

Алгоритм навчання мережі Кохонена включає етапи, склад яких залежить від типу структури: постійної (самонавчальна мережу) або змінною (самоорганізовану мережу). Для самонавчання послідовно виконуються:

1. Задання структури мережі (кількості нейронів шару Кохонена). Випадкова ініціалізація вагових коефіцієнтів значеннями, що задовольняють одному з наступних обмежень при нормалізації вихідної вибірки в межах [-1, 1] та [0, 1].

2. Подача на входи мережі випадкового навчального прикладу поточного навчання і розрахунок евклідових відстаней від вхідного вектора до центрів всіх кластерів. За найменшому з значень Rj вибирається нейрон-переможець j, в найбільшою мірою близький за значеннями з вхідним вектором. Для обраного нейрона (і тільки для нього) виконується корекція вагових коефіцієнтів.

Цикл повторюється з кроку 3 до виконання одного або декількох умов закінчення:

- вичерпано заданий гранична кількість епох навчання;
- не відбулося значного зміни вагових коефіцієнтів в межах заданої точності протягом останньої доби навчання;
- вичерпано заданий граничний фізичний час навчання.

Коефіцієнт швидкості навчання може здаватися незмінним за межі [0, 1] або змінним значенням, поступово зменшується від циклу до циклу [20].

У разі самоорганізації мережі Кохонена алгоритм зазнає певних змін. Здається критичну відстань Rкр, відповідне максимально допустимому евклидову відстані між входами прикладу і вагами нейрона- переможця. Початкова структура не містить нейронів. При подачі на входи мережі самого першого прикладу навчальної вибірки створюється перший нейрон з ваговими коефіцієнтами, рівними поданням вхідним значенням.

На входи мережі подається новий випадково обраний приклад поточної епохи навчання, розраховуються евклідові відстані від прикладу до центру кожного кластера по співвідношенню і визначається нейрон- переможець з найменшим з них Rmin.

Якщо виконується умова Rmin ≤ Rкр, проводиться корекція вагових коефіцієнтів відповідного нейрона-переможця по співвідношенню (4), в іншому випадку в структуру мережі додається новий нейрон, вагові коефіцієнти якого приймаються чисельно рівними вхідним значенням поданого прикладу.

Процедура повторюється з п.3. Якщо протягом останньої доби навчання будь-які кластери залишилися не задіяними, відповідні нейрони виключаються зі структури мережі Кохонена.

Обчислення закінчуються, якщо виконується одна з умов, прописані в алгоритмі самонавчання мережі фіксованого структури.

Ще одна модифікація алгоритмів самонавчання і самоорганізації передбачає корекцію вагових коефіцієнтів не тільки нейрона-переможці, а й усіх інших нейронів. Для цього слід використовувати коефіцієнт швидкості навчання, регресний зі збільшенням відстані до центру кластера [19].

Як значення Rкр можна розраховувати середнє відстань для кожного кластера при поточному пред'явленні навчального прикладу. Параметр β рекомендується вибирати рівним 3,0 ± 0,5.

Як правило, практично під час використання самоорганізації нейронної мережі Кохонена доводиться стикатися ще з однією проблемою. З одного боку, якісь кластери можуть містити занадто маленька кількість прикладів, що призводить до складнощів у наступному узагальненні інформації. З іншого боку, деякі кластери можуть виявитися занадто великими, тобто містити дуже багато прикладів. В цьому випадку для регулювання розміру кластера і вирішення проблеми його переповненості можна задати в якості додаткового параметра граничне число прикладів, які формують кластер Nпр. Якщо в якийсь момент виявляється, що новий приклад повинен бути віднесений до кластеру, розмір якого вже максимальний, приймається рішення про створення іншого кластера, центр якого буде представляти собою вектор змінних одного з Nпр+1 прикладів

кластера (включаючи новий) найбільш віддаленого від центру даного кластера [6].

До навченої нейронної мережі застосовується процедура кластерного аналізу - процедури опису властивостей кластера на основі аналізу кількісного і якісного складів прикладів, які сформували його. Слід враховувати, що опис кластерів може базуватися не тільки на значеннях вхідних змінних навчальної вибірки, а й на значеннях змінних, які не брали участі у формуванні кластерів. Зокрема, в опис можуть входити дані про середні значення таких змінних серед всіх прикладів, які сформували кластер. Крім того, доцільно для кожного кластера мати дані про середньоквадратичному відхиленні або дисперсії по кожній змінній.

При практичному використанні нейронної мережі Кохонена новий приклад подається на її вхід і відноситься до одного з існуючих кластерів, або робиться висновок про неможливість такого віднесення (при великій відстані до центру найближчого кластера). Якщо вибір кластера відбувся, його опис, отримане в результаті кластерного аналізу, і відповідні кластеру рішення повинні поширюватися в тому числі на поданий приклад.

Практичне використання мережі Кохонена полегшується за рахунок візуалізації результатів кластеризації. В результаті самонавчання (самоорганізації) мережі виходить набір кластерів, кожен з яких характеризується своїм центром (значеннями вагових коефіцієнтів відповідного нейрона) і кількістю навчальних прикладів, які сформували його. Чи не складає ніяких труднощів визначити евклідова відстань між центрами всіх можливих пар кластерів і графічно зобразити їх на так званій карті Кохонена - двовимірної графічної структурі, що дозволяє судити не тільки про розміри і положення кожного окремо взятого кластера, а й про близькість один до одного і взаємне розташування окремих кластерів.

Метод k-means - це спеціальний алгоритм кластеризації, що має на увазі, що у нас є масив даних, які ми хочемо згрупувати в кластери, а точніше – в k кластерів [17].

Вхідними даними в методі k-means є тільки матриця наших X. Як правило, ми формуємо її так, щоб кожен рядок представляла окремий приклад (зразок), а кожен стовпець - окремий ознака або, користуючись термінами з статистики, фактор. Зазвичай ми говоримо, що є N прикладів і D ознак, так що X є матрицею розмірності NxD.

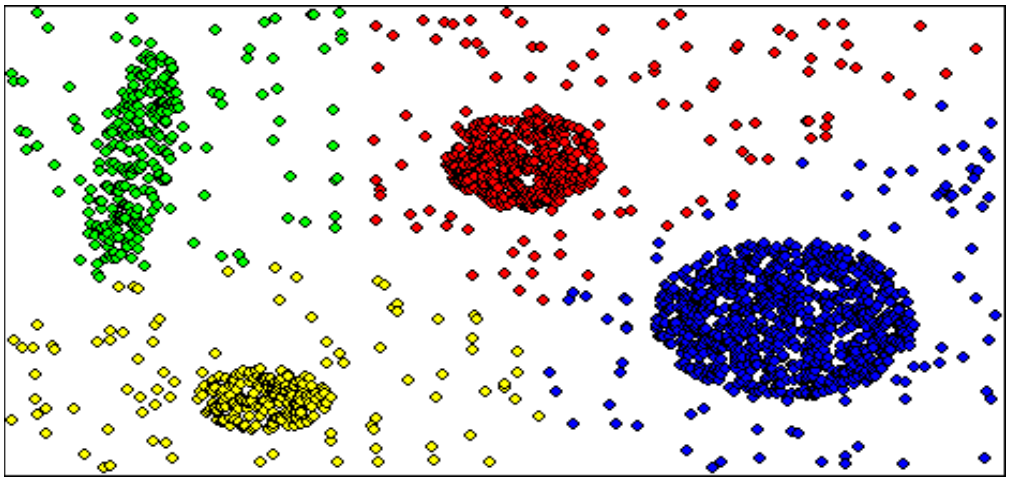
В алгоритмі методу k-means є два основних етапи:

1. Спочатку ми вибираємо k різних центрів кластерів - як правило, це просто випадкові точки в наборі даних.
2. Потім ми переходимо до нашого основного циклу, який також складається з двох етапів.

- Перший - це вибір, до якого з кластерів належить кожна точка з X. Для цього ми беремо кожен приклад і вибираємо кластер, чий центр ближче всього. Не забувайте, що спочатку ми вибираємо центри випадковим чином.
- Другий етап - заново обчислити кожен центр кластера, ґрунтуючись на безлічі точок, які до нього приписані. Для цього беруться всі відповідні приклади і обчислюється їх середнє значення, звідси і назва методу - «метод k-means». Все це робиться до тих пір, поки алгоритм не зійде, тобто поки не припиниться зміна в розподілі точок по кластерам або в координатах центрів кластерів. Як правило, це відбувається дуже швидко - в районі від 5 до 14 проходів циклу. Це сильно відрізняється від градієнтного спуску в глибокому навчанні, де можуть пройти тисячі ітерацій, поки не відбудеться сходження [15].

Розглянемо наочний приклад роботи методу k-середній (рис. 2.9). На першому етапі ми приписуємо центри кластерів m1 і m3 до випадкових точках X. На наступному етапі - що є першим етапом основного циклу - ми вибираємо, до якого з кластерів належить кожна точка. Так, на малюнку дві точки зліва належать до кластеру 1, а дві точки праворуч - до кластеру 3. На наступному етапі перераховуємо середні значення m1 і m3. Тоді m1 виходить середнім значенням двох точок зліва, оскільки вони належать цьому кластеру.

Рис. 2.9. Результат класифікації методами k-means



Все, алгоритм зійшовся, оскільки більше не може бути змін до присвоєння даних до кластерів і, отже, в значеннях m1 і m3.

Кластеризація є однієї з найбільш важливих завдань Data Mining. В даний час розроблено велику кількість методів і алгоритмів кластеризації але, на жаль, не всі вони можуть ефективно працювати з великими масивами даних, тому подальші дослідження в цьому напрямку пов'язані з подоланням цієї проблеми. Одним з широко відомих в аналітичному співтоваристві алгоритмів кластеризації, що дозволяють ефективно працювати з великими обсягами даних, є EM-алгоритм. Його назва походить від слів "expectation- maximization", що перекладається як "очікування-максимізація". Це пов'язано з тим, що кожна ітерація містить два кроки - обчислення математичних очікувань (expectation) і максимізацію (maximisation).

Em — це алгоритм, який використовує запобіжну модель для оцінки параметрів багатовимірного нормального розподілу. Припущення, що лежить в основі алгоритму Em, полягає в тому, що спостережувані дані можна моделювати за допомогою лінійної комбінації багатофакторних нормальних розподілів. Мета полягає в тому, щоб оцінити параметри розподілу, які максимізують логарифм правдоподібності, що використовується як якість моделі. Це тому, що передбачається, що кожен кластер має певний закон розподілу, зокрема нормальний розподіл. Враховуючи це припущення, можна визначити очікуване значення та дисперсію розподілу, які обидва відповідають закону розподілу. Ці дані в кращому випадку є «нехарактерними» порівняно з тим, коли вони виникають природним шляхом [34].

Ми вважаємо, що кожне спостереження можна віднести до кількох кластерів з різними ймовірностями. Після цього ми повинні використовувати ймовірності спостережень належності до кожного кластера, щоб «вписати» кожен розподіл у дані. Потім ми можемо визначити найбільш імовірний кластер, до якого належить кожне спостереження. Очевидно, що спостерігачі повинні віднести спостереження до групи з найвищою ймовірністю (рис 2.10).

Переваги ЕМ-алгоритму	Потужна статистична основа.
	Лінійне збільшення складності при зростанні обсягу даних.
	Можливість побудови бажаного числа кластерів.
	Швидка збіжність при вдалій ініціалізації.
	Стійкість до шумів та перепустками в даних.

Рис 2.10. Переваги EM-алгоритму

Алгоритм має кілька недоліків. Його припущення щодо нормальних вимірювань даних не завжди точні. Конвергенція може зайняти деякий час, якщо ініціалізація не вдається. Це може спричинити зупинку алгоритму на локальному мінімумі. Таким чином можна отримати квазіоптимальні рішення.

EM передбачає, що змішані нормальні розподіли поєднують дані лінійним способом.

Дані повинні відповідати суміші багатофакторних нормальних розподілів для кількох змінних q.

EM додає більше даних до суміші, доки модель не досягне достатньо точного результату. Потім він припиняє покращувати рішення та обчислює остаточні результати. Подібно до кластеризації, EM визначає відстані між розподілами ймовірностей. Мірою в даному випадку є монотонно збільшується статистична величина, звана логарифмічною правдоподібністю. Метою алгоритму є оцінка середніх значень C, коваріацій R і ваг суміші W для функції розподілу ймовірності, описаної вище. Параметри, оцінені алгоритмом, зберігаються в таблиці 2.3.

Слід зазначити, що одна з популярних алгоритмів кластеризації k-means є окремим випадком алгоритму EM, коли W і R постійні (табл. 2.3).

Таблиця 2.3.

Параметри, оцінені алгоритмом EM

Матриця	**Розмір**	**Містить**
C	q×k	Математичні очікування, μ
R	q×q	Коваріації, Σ
W	k×1	Ваги, wi

Алгоритм часто може знайти рішення, яке виглядає близьким до оптимального, навіть після вибору початкового наближення з низьким рівнем успіху. Ця проблема спричинена тим, що алгоритм застрягає в локальному оптимумі, що ускладнює вибір початкової моделі.

Алгоритм може працювати з двома режимами роботи. Перший режим завантажує лише частину даних і намагається побудувати з ними модель. Якщо це вдається, алгоритм завершує свою роботу. В іншому випадку завантажується та обробляється наступна порція. Цей процес повторюється, поки алгоритм не дасть прийнятних результатів або не буде оброблено всі дані. Останній режим дозволяє завантажувати всі дані одночасно. Для цього потрібно більше оперативної пам’яті, ніж для другого режиму, який завантажує дані у наданому порядку [32].

Для визначення ефективності K-Mesos був проведений експеримент. Розмір вибірки було обрано так, щоб представляти ширшу картину, представлена на рис. 2.11.

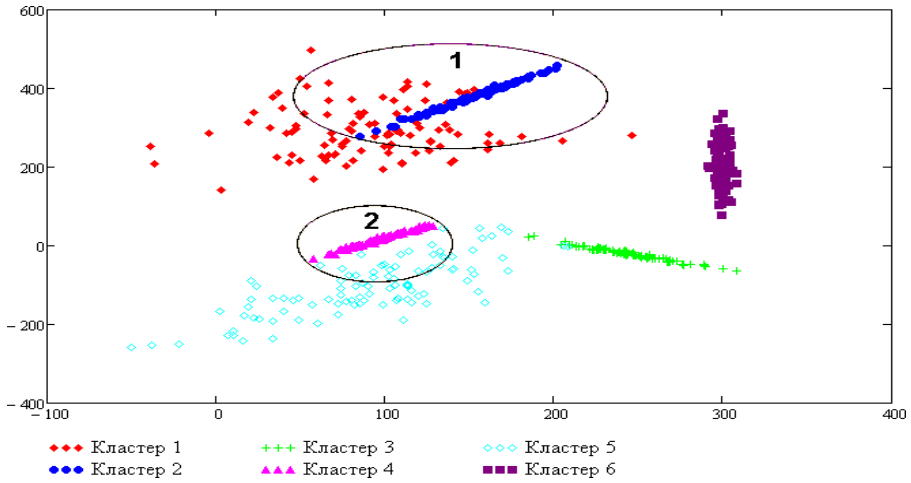


Рис. 2.11. Вихідні кластери

Зверніть увагу, що вихідний набір даних не є простим з точки зору завдання кластеризації, оскільки є явне перекриття кластерів (області 1 і 3). В

області 1 перекриваються кластери 1 і 3, а в області 3 кластери 4 і 5. Кластери 3 і 6 розташовані відокремлено і, як очікується, будуть легко розділено.

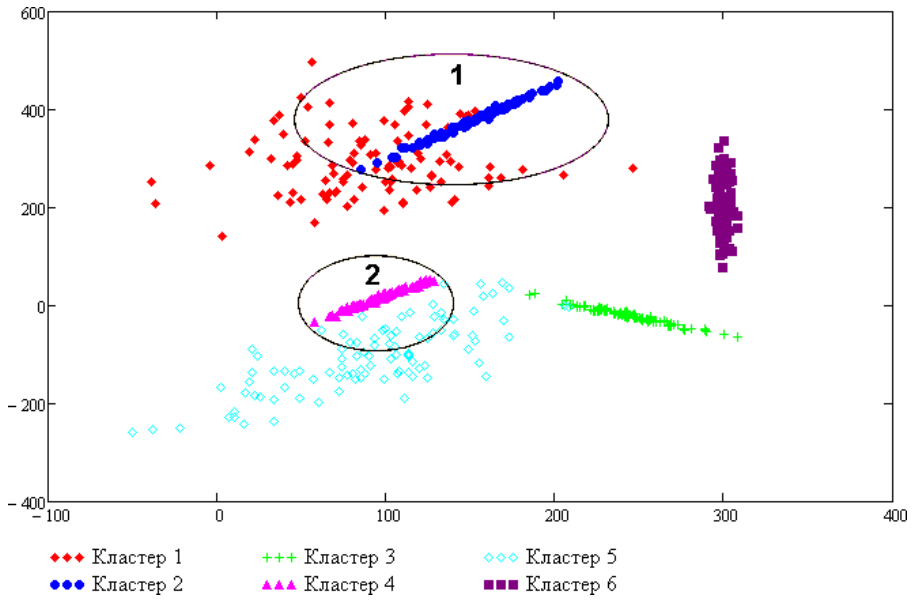


Рис. 2.11. Вихідні кластери

Для алгоритму k - means особливі труднощі повинні виникнути в місцях перекриття кластерів (рис. 2.12). Дане припущення підтверджується результатами.

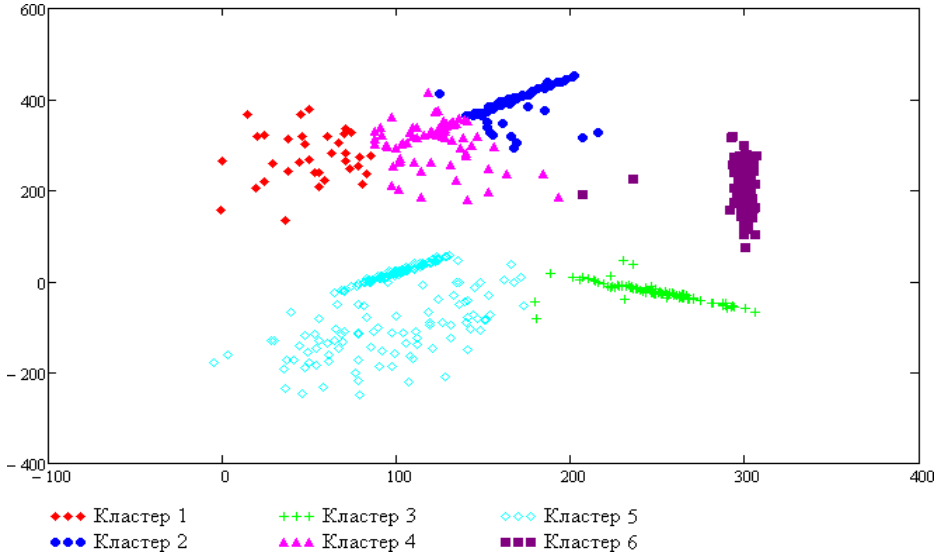


Рис. 2.12. Результати кластеризації k- means

У місцях перекриття кластерів спостерігається найбільше число помилок. У той же час відокремлені кластери 3 і 6 були розпізнані алгоритмом k - means без помилок. Як можна побачити на малюнку рис. 2.13, алгоритм EM вельми успішно виявив перекриваються кластери, хоча й майже не розпізнав кластер 6.

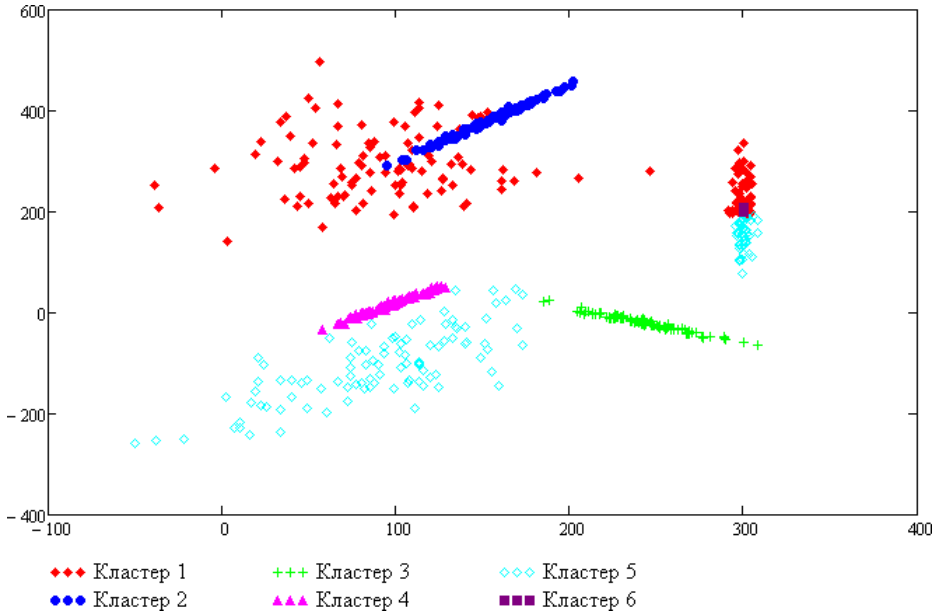


Рис. 2.13. Результати кластеризації EM

Таким чином, можна зробити висновок, що алгоритм k - means може мати перевагу при роботі з відокремленими кластерами, але повністю програє алгоритму EM при наявності їх перекриття.

2.4 Висновки

Проблема боротьби із загрозами комп'ютерної мережі не знайшла самостійного відображення в сучасній літературі, тому аналіз розглянутих методів проведено на відомих методах виявлення та аналізу мережевих загроз. Моніторинг аномалій у мережі IS зосереджується на статистичному аналізі з використанням попередньо визначеної моделі нормальної поведінки. Цей підхід

визначає аномалії шляхом порівняння поточного мережевого трафіку IS із вимогами шаблону.

Моделі кластерного аналізу визначають класифікатори, які вказують на основні компоненти кіберзагроз. Ці моделі використовують ці класифікатори для обчислення відстані між кластерами даних і визначення наявності чи відсутності кіберзагроз в організації.

Основною перевагою моделі кінцевих астоматів є простота визначення критеріїв класифікації ІБ. Оскільки він враховує лише невелику кількість переходів між станами, він точно відображає характер обробки даних у реальному часі через мережеві протоколи.

Марківська модель ефективна для пошуку аномалій, виявлених за допомогою системних викликів з операційної системи. Це також вимагає використання додаткової статистики в системах квазіреального часу, які обчислюють час аналогічним чином. Теорія ігор передбачає наявність покупця і продавця, взаємозв'язок між якими визначена у вигляді платіжної матриці.

Початкова класифікація аномалій за методами виявлення кіберзагроз через нейронні мережі виконується за допомогою ІС. Ці методи використовують ідентифікацію нормальної поведінки системи на основі функції розподілу пакетів даних — разом із навчанням нейронної мережі та аналізом подій на основі вибірки, яка використовується під час навчання.

Машинне навчання являє собою підрозділ штучного інтелекту, що стоїть на стику таких дисциплін, як математика, статистика, теорія ймовірностей, теорія графів і вивчає алгоритми, які здатні самостійно навчатися на основі досвіду.

Класифікація — це дія поділу набору об’єктів на окремі групи. Навпаки, кластеризація — це процес поділу об’єктів на кластери, які визначаються під час

роботи алгоритму. Різні групи в схемі класифікації повинні бути максимально подібними і містити «схожі» об’єкти.

РОЗДІЛ 3. МЕТОД ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІЗ ЗАСТОСУВАННЯМ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

3.1 Оцінка ризиків безпеки інформаційної системи

Ризик-менеджмент – досить зріла дисципліна. Існують як національні стандарти з управління ризиками, так і міжнародні стандарти — «ISO Guide 73» (визначає термінологічний апарат ризикменеджмента), «ISO 31000» (містить принципи та рекомендації в галузі управління ризиками), «ISO 31010» (описує технології оцінки ризику).

На процесному рівні у ризик-менеджменті виділяються такі аспекти:

- обмін інформацією та консультування - група процесів, спрямованих на підвищення обізнаності зацікавлених сторін та розуміння ними ризику для підтримки прийняття рішень;
- визначення сфери застосування, середовища та критеріїв - процеси адаптації ризик-менеджменту до специфіки організації:
- оцінка ризику - систематичні ітеративні процеси ідентифікації, аналізу та порівняльної оцінки ризиків;
- обробка ризику - процеси визначення та вибору можливих варіантів обробки ризиків, а також прийняття пов'язаних з цим управлінських рішень;
- моніторинг та перегляд - безперервні процеси підвищення якості та ефективності ризикменеджменту;
- документування та звітність - підтримуючі процеси, що полягають у формалізації ризик-менеджменту та результатів його застосування [1].

«Стандарти оцінки ризиків» містять рекомендації щодо використання технологій та методів для кожного з перерахованих аспектів ризик-

менеджменту. Рекомендовані методи спираються переважно на експертну оцінку, а отже вимагають значних трудовитрат на реалізацію та залежать від людського фактору, що у свою чергу створює похідні ризики внесення систематичних дефектів в механізми ризик-менеджменту, зумовлені хибними чи необ'єктивними думками задіяних експертів. Варто також відзначити, що вкрай важлива роль в успішному застосуванні пропонованих класичних технологій відводиться процесам збирання з різноманітних джерел, обробки, структурування та передачі великих обсягів інформації, а також систематизації знань, що виникають за результатами ризик-менеджменту.

З наведених вище результатів розгляду стандартів оцінки ризиків випливають деякі ідеї щодо вдосконалення процесів ризик-менеджменту. По-перше, доцільною і очевидною є можливість застосування математичних моделей штучного інтелекту в ключових завданнях оцінки ризиків, таких як ідентифікація та виявлення нових типів ризиків, а також оцінка ймовірності настання ризиків і величини ймовірних наслідків при їх настанні. По-друге, практично всі процеси управління ризиками можуть бути вбудовані інтелектуальні інформаційні системи, засновані на онтології предметної області. Впровадження таких систем дозволяє створити умови підвищення ефективності та якості формалізації знань у сфері застосування ризик-менеджменту [3].

Завдання оцінки ймовірності настання ризику може розглядатися як окремий випадок класифікації і вирішуватися за допомогою моделей штучного інтелекту, що дозволяють визначати ймовірність приналежності об'єкта до того чи іншого класу. Класифікація відноситься до завдань навчання з учителем, де навчальна вибірка складається з множини X, що містить ознаки об'єктів, і відповідної множини У, що містить мітки класів, до яких належать дані об'єкти.

У загальному вигляді задача класифікації є побудовою алгоритму відображення множини X у множину У, здатного зіставити довільний об'єкт з відповідними мітками класе.

Таким чином, завдання оцінки ймовірності настання ризику зводиться до завдання бінарної класифікації. Як вибірку даних для навчання класифікаційної моделі використовуються накопичені історичні масиви інформації про зафіксовані факти настання ризиків у минулому, а також про характеристики суб'єктів та об'єктів, що мають відношення до ризиків [18].

Навчена на таких даних класифікаційна модель визначає ймовірність настання ризику певного типу в майбутньому за сукупністю характеристик суб'єктів та об'єктів, що належать до ситуації, що оцінюється. При цьому ймовірність настання ризику фактично є ймовірністю приналежності об'єкта до класу А, де А клас наявності ризику, а В - клас відсутності ризику.

Якщо необхідно визначати ймовірність настання кількох типів ризиків, можливе застосування двох способів:

- застосування моделі мультикласової класифікації (коли кожен об'єкт з множини X може відноситися одночасно до кількох класів);
- застосування кількох бінарних класифікаторів, кожен із яких максимально адаптований для найбільш точної оцінки одного конкретного типу ризику.

У випадках, коли ризики різнорідні за своєю природою та залежать від різного набору ознак, найбільш ефективним є спосіб навчання кількох бінарних класифікаторів (для кожного типу ризику) з подальшим обчисленням інтегральної оцінки ймовірності настання ризику [22].

Для балансування навчальної вибірки може бути використаний метод «under - sampling», що ґрунтується на вибірковому виключенні навчального набору даних об'єктів переважаючого класу, або метод «over-sampling», що

базується на генерації синтетичних об'єктів мінорних класів та їх додаванні в навчальний набір даних.

Як було зазначено вище, при навчанні класифікаторів на незбалансованих вибірках необхідно використовувати релевантні метрики якості моделей, що формуються. Наприклад, така метрика оцінки як «точність» (accuracy), може оцінювати якість моделі більш ніж 99% навіть у випадках, коли формовані класифікатором прогнози про належність об'єктів до мінорного класу здебільшого є помилковими. Тому коректніше використовувати більш інформативні метрики оцінки якості класифікаторів, наприклад, такі як метрика «збалансована точність» («balanced accuracu»), що оцінює частку коректних відповідей моделі з урахуванням дисбалансу класів у вибірці, метрика точності «precision», метрика повноти «recall» та метрика «F-міра» - середнє гармонійне значення точності та повноти [17].

Крім того, відстеження балансу часток хибнопозитивних і хибнонегативних передбачень дозволяє налаштувати модель під специфіку конкретного прикладного завдання оцінки ймовірності настання ризиків. Так, наприклад, у деяких завданнях велика кількість хибнопозитивних спрацьовувань може нести в собі певні фінансові витрати, при тому, що рідкісна хибна оцінка ризику є не настільки критичною. І, навпаки, у таких завданнях як, наприклад, оцінка ризику в медичній діагностиці, моделі налаштовуються відповідно до максимальної обережності для виключення (мінімізації) потенційних перепусток небезпечних (несучих ризик) об'єктів.

Ще однією особливістю, яку необхідно враховувати, є можливість випадкових та навмисних, зумовлених людським фактором помилок під час фіксації в історичному масиві даних фактів настання ризиків. Найбільшу проблему тут є ситуації, коли з метою навмисного приховування факту настання ризику (порушення) об'єкт відзначається людиною (оператором) як об'єкт без

ризику. Це призводить до ситуації прихованих не ідентифікованих ризиків. В історичному масиві накопичується спотворена недостовірна інформація, що суттєво знижує якість моделей оцінки ймовірності настання ризиків, що навчаються на даному масиві.

Одним із ефективних заходів щодо нівелювання даного фактора є підхід до автоматизованої ідентифікації нових типів ризиків через виявлення аномалій. Аномальні об'єкти можуть виключатися з навчальної вибірки для класифікаторів за відомими (ідентифікованими) типами ризиків або для однорідних груп (кластерів) виявлених аномалій як потенційно нових типів ризиків можуть навчатися окремі класифікатори (у другому варіанті результати ідентифікації нових типів ризиків фактично є додатковою розміткою набору даних навчання класифікаційних моделей) [16].

3.2 Керування ризиками з використанням методу штучного інтелекту

Ідентифікація ризиків - це ітеративний процес пошуку нових типів ризиків та профілювання їх основних характеристик для подальшої смислової інтерпретації, аналізу та обробки.

З погляду штучного інтелекту, завдання ідентифікації ризиків може вирішуватися як завдання пошуку аномалій в історичних масивах даних про діяльність, що стосується галузі застосування ризик-менеджменту. Аномальні спостереження в таких даних можуть пояснюватися в тому числі наявністю взаємозв'язків та взаємодій між об'єктами та суб'єктами діяльності, що вже призводять до наступу прихованих (ще не ідентифікованих) ризикових ситуацій та відповідних наслідків, або є потенційними джерелами виникнення таких ситуацій у майбутньому.

Підходи до ризик-менеджменту, засновані на використанні методів пошуку аномалій, активно розвиваються і застосовуються, наприклад, при виявленні шахрайських дій в онлайн-платежах, при управлінні ризиками інвестиційних портфелів та при виявленні мережевих атак.

Було сформульовано комплексний підхід до автоматизованої ідентифікації нових типів ризиків, що ґрунтується на методах пошуку аномалій. Пропонований підхід складається з трьох основних етапів:

- виявлення аномалій в історичному масиві даних;
- поділ виявлених аномалій на однорідні кластери:
- профілювання кластерів аномалій як потенційно нових типів ризиків [4].

Для виділення аномалій можуть використовуватися різні методи інтелектуального аналізу, в результаті застосування яких виявляються рідкісні об'єкти або події, які значно відрізняються від більшості об'єктів, що спостерігаються.

Окремо дані методи мають слабкі систематичні переваги одного методу над іншими, також їх ефективність залежить від набору навчальних даних. Отже, оптимальний підхід до виявлення аномалій повинен поєднувати різні комбінації відомих методів. У рамках аналізованого підходу пропонується використовувати ансамблювання методом голосування наступних найефективніших методів пошуку аномалій:

- методу трьох сигм;
- методу еліпсоїдальної апроксимації;
- методу локального рівня викиду;
- методу ізолюючого лісу.

Для формування однорідних кластерів аномалій пропонується використати кластерний аналіз, що реалізується за допомогою інтелектуальних алгоритмів машинного навчання без учителя [18].

Оскільки в задачі поділу аномалій на однорідні групи немає апріорно відомої кількості кластерів та розподілу за кластерами, для вибору кращого методу кластерного аналізу та налаштування його параметрів можуть використовуватися внутрішні метрики якості кластеризації: силует, індекс Девіса-Болдуїна, індекс Калинського-Харабаша.

Профілювання кластерів аномалій полягає в описі характерних ознак, що виділяють цю групу аномалій з інших груп. Для профілювання кожного аномального кластера виконуються кроки:

- виділення індикаторів кластера аномалій методами кореляційного аналізу;
- розрахунок показників розподілу кількісних індикаторів кластера (середні, квантили, мінімальні та максимальні значення);
- розрахунок частот розподілу категоріальних індикаторів кластеру.

Розроблений профіль аномального кластера являє собою сутність, що описує потенційно новий тип ризику і призначену для подальших процедур смислової інтерпретації, валідації на нових даних, включення до типології ризик-менеджменту предметної галузі та вбудовування в прийняті організацією процеси оцінки ризику [22].

3.3 Метод оцінювання ризиків безпеки інформаційної системи із застосуванням системи штучного інтелекту

Для оцінки ймовірності настання ризику можна використовувати як «класичні методи» машинного навчання, і глибокі нейронні мережі. Оптимальна архітектура нейронної мережі у разі підбирається відповідно до природи даних із навчальної вибірки: з метою оцінки ймовірності настання ризику можна використовувати як пов'язані нейронні мережі, таки, наприклад, згорткові чи рекурентні.

Детальний розгляд архітектур нейронних мереж та моделей машинного навчання, придатних для вирішення подібних завдань, виходить за межі цієї статті. Перерахуємо лише найпоширеніші та застосовні моделі класифікаторів, що дозволяють визначити не лише належність оцінюваного об'єкта до класу ризику, а й ймовірність приналежності до цього класу:

- логістична регресія;
- найближчі сусіди;
- вирішальні дерева;
- випадковий ліс:
- градієнтний бустинг [11].

Практика показує, що ефективність перерахованих моделей класифікації залежить від специфіки конкретної задачі, що вирішується, і природи даних. Тому в більшості випадків доцільно навчати декілька різних моделей з різними конфігураціями, а вибір найбільш оптимальної моделі та її гіперпараметрів робити за метрикою якості, отриманої на тестовій вибірці даних.

На сьогоднішній день застосування моделей штучного інтелекту для оцінки ймовірності настання ризиків найбільше поширене в наступних сферах.

Фінанси. Моделі штучного інтелекту успішно застосовуються для вирішення завдань кредитного скорингу. Також інтелектуальні моделі успішно

застосовуються для аналізу фінансових транзакцій на предмет шахрайства та оцінки страхових ризиків.

Охорона здоров'я. Моделі штучного інтелекту дозволяють прогнозувати ймовірність ризику виникнення та загострення захворювань, а також супутніх їм заходів, таких як незапланована повторна госпіталізація, що призводить до зниження рівня догляду за пацієнтами та перевантаження системи охорони здоров'я.

Державне управління. Як приклад застосування методів штучного інтелекту для управління ризиками у сфері державного управління можна навести модель автоматизованої оцінки ризику державних контрактів, спрямовану на підвищення ефективності державних закупівель та оптимізацію бюджетних видатків.

Освіта. В освітній сфері застосування методів штучного інтелекту також може бути досить різноманітним та застосовуватись, наприклад, для аналізу ймовірності ризику відрахування студента або незадовільних результатів академічної успішності.

Безпека. Інтелектуальні моделі можуть використовуватися для виявлення адміністративних та кримінальних правопорушень та їх своєчасного запобігання [25].

Резюмуючи вищевикладене, можна сказати, що методи штучного інтелекту застосовні у завданнях оцінки ймовірності настання ризиків і мають потенціал більш ефективного та якісного (порівняно з класичними технологіями) вирішення цих завдань за рахунок зниження навантаження на експертів та зниження впливу людського фактора на процес та результат оцінки ризиків.

Величина можливих наслідків при настанні ризику зазвичай може бути виражена кількісними значеннями, які залежить від низки чинників,

характеризуючих сам ризик, і навіть стан взаємопов'язаних із нею процесів, об'єктів і суб'єктів у момент виникнення ризику. Тому завдання оцінки величини ймовірних наслідків при настанні ризику може розглядатися як окремий випадок завдання регресії і вирішуватися з використанням відповідних моделей штучного інтелекту. Регресія, як і класифікація, відноситься до завдань навчання з учителем, де навчальна вибірка складається з множини X, що містить ознаки об'єктів, і відповідної множини, що містить речові числа. У загальному вигляді завдання регресії є побудовою алгоритму відображення множини X на множину У, здатного зіставити довільний об'єкт із речовим числом.

Стосовно розглянутої задачі у множині X навчальної вибірки для побудови регреслонної моделі містяться факти настання ризиків у минулому, а також значення ознак, що характеризують ризики, що відбулися. Безліч У містить значення величин, кількісно характеризують поспедства настав ризику (наприклад, суму збитків і витрат організації, суму нарахованих штрафів).

Також завдання регресії можна розглядати як завдання кількісного розрахунку ризику менш конкретному сенсі, коли потрібно непросто розрахувати можливі матеріальні витрати. а провести прогнозування значення, що відбиває рівень будь-якої величини чи ступінь ризику. В даному випадку часто потрібно проводити додаткову інтерпретацію отриманих висновків моделі - зіставляти прогнозні значення з деякими критеріями ризик-категорування, прийнятими в галузі діяльності організації. Як правило, такі критерії формуються на основі спеціальних експертних оцінок та закріплюються у галузевих документах (нормативних актах, стандартах, рекомендаціях).

Регресійні моделі можуть поєднуватись із розглянутими вище за текстом класифікаційними моделями оцінки ймовірності настання ризиків. Система штучного інтелекту, що використовує і класифікацію, і регресію, може

формувати інтегральну оцінку ризику, що складається з ймовірності його настання та кількісної оцінки величини можливих наслідків.

Аналогічно оцінці ймовірності настання ризику із застосуванням класифікаторів, для оцінки ймовірних наслідків при настанні ризику можуть використовуватись як «класичні методи» машинного навчання (наприклад, лінійна регресія, метод найближчих сусідів, вирішальні дерева, випадковий ліс, градієнтний бустіні) таки глибокі нейронні.

Розглянутий підхід вже знаходить ефективне застосування, наприклад, у медицині та фінансах. В галузі медицини регресійні моделі можуть використовуватися для прогнозування значень медичних показників, зміною яких супроводжується виникнення того чи іншого захворювання. У фінансовій сфері регтресійні методи можуть бути використані при побудові систем, що протнозують збитки у матеріальному еквіваленті для задач мікрозкономічного та макроекономічного моделювання [9].

Застосування інтелектуальних систем на основі онтології предметної галузі «Стандартні процеси ризик-менеджменту» вимагають ухвалення своєгрімових рішень, заснованих на повних, достовірних та актуальних даних із різних джерел, у тому числі з внутрішніх інформаційних систем організації, інформаційних систем партнерів, державних інформаційних систем.

Ці джерела різноманітні. Їх склад і структура інформації, що передається, підтверджені динамічним змінам під впливом різних факторів, включаючи фактори розвитку організації. На ці джерела дані спираються розглянуті вище інтелектуальні моделі оцінки ризиків.

Тому вкрай важливими в галузі ризик-менеджмента є завдання інтеграції різнорідної інформації, її ефективної систематизації та формалізації. Як методологічний фундамент вирішення цих завдань можливе використання

онтології — формалізованого опису предметної галузі діяльності, що входить до сфери застосування ризик-менеджменту. На даний момент бачиться кілька найбільш перспективних напрямків застосування засобів онтології:

- формування моделі предметної галузі, що визначає термінологічний апарат, логічні та фізичні моделі даних, а також підтримує надійні механізми актуалізації та валідації з використанням засобів онтології;
- створення та ведення формалізованих правил застосування інтелектуальних моделей оцінки різних тилів ризиків до різних об'єктів та суб'єктів діяльності залежно від їх характеристик;
- створення та ведення формалізованих правил навчання моделей оцінки конкретних типів ризиків, включаючи правила відбору даних із різних, визначених у фізичній моделі, джерел для формування навчальних вибір, правила попередньої обробки цих даних, переліки застосовних математичних алгоритмів [16].

3.4 Висновки

Завдання оцінки ймовірності настання ризику може розглядатися як окремий випадок класифікації і вирішуватися за допомогою моделей штучного інтелекту, що дозволяють визначати ймовірність приналежності об'єкта до того чи іншого класу. Класифікація відноситься до завдань навчання з учителем, де навчальна вибірка складається з множини X, що містить ознаки об'єктів, і відповідної множини У, що містить мітки класів, до яких належать дані об'єкти.

У загальному вигляді задача класифікації є побудовою алгоритму відображення множини X у множину У, здатного зіставити довільний об'єкт з відповідними мітками класе.

Ідентифікація ризиків - це ітеративний процес пошуку нових типів ризиків та профілювання їх основних характеристик для подальшої смислової інтерпретації, аналізу та обробки.

З погляду штучного інтелекту, завдання ідентифікації ризиків може вирішуватися як завдання пошуку аномалій в історичних масивах даних про діяльність, що стосується галузі застосування ризик-менеджменту. Аномальні спостереження в таких даних можуть пояснюватися в тому числі наявністю взаємозв'язків та взаємодій між об'єктами та суб'єктами діяльності, що вже призводять до наступу прихованих (ще не ідентифікованих) ризикових ситуацій та відповідних наслідків, або є потенційними джерелами виникнення таких ситуацій у майбутньому.

Для оцінки ймовірності настання ризику можна використовувати як «класичні методи» машинного навчання, і глибокі нейронні мережі. Оптимальна архітектура нейронної мережі у разі підбирається відповідно до природи даних із навчальної вибірки: з метою оцінки ймовірності настання ризику можна використовувати як пов'язані нейронні мережі, таки, наприклад, згорткові чи рекурентні.

РОЗДІЛ 4. ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДІ ВИРІШЕННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

4.1 Використання методу оцінювання ризиків інформаційних систем в кібербезпеці

Ми вивчимо три найпопулярніші методи оцінки ризиків ІБ, які використовує KMZ SSI. Ми з’ясуємо, які з них ефективні, а які ні, розбивши їх на частини та вивчивши сильні та слабкі сторони кожного методу. Це метод 4 оцінки NIST 800-30, метод 5 CRAMM і метод 6 OCTAVE.

Методологія оцінки ризиків NIST визначена в спеціальній публікації NIST 800-30 Посібник з управління ризиками систем інформаційних технологій. Це один із найпопулярніших і широко використовуваних методів оцінки управління ризиками. NIST 800-30 визначає два основні параметри для оцінки: потенційний збиток і ймовірність реалізації загрози. Це також відомий як метод оцінки ризику NIST.

Системи управління ризиками виконують практичну функцію інформування про інтеграцію інформаційних технологій у повсякденні операції.

Методологія оцінки ризиків, наведена в Спеціальній Рекомендації 800-30, охоплює широкий спектр завдань, пов'язаних зі стратегіями управління ризиками, і є основою для розробки вашої власної системи управління ризиками. Проте представлений процес оцінки ризику ІБ, який представлений у формі таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку та ймовірності можливої події. При цьому значення кожної змінної, особливо ризику, оцінюється за трирівневою шкалою. Такий «жорсткий» механізм отримання оцінок ризику значною мірою обмежує точність результатів, забезпечуючи їх ефективність і відтворюваність [7]. Алгоритм цієї методики зображено на рис. 4.1.

Рисунок 4.1 Алгоритм методики управління ризиками

Використання даної методики передбачає наступні етапи:

- опис характеристик системи;
- ідентифікувати загрози;
- визначити вразливі місця;
- проаналізувати наявні засоби/заходи захисту;
- визначити значення ймовірності;
- аналіз впливу;
- визначити величину ризику;
- вибір засобів/заходів захисту;
- запишіть отримані результати [26].

Метод аналізу та управління ризиками ССТА, також відомий як метод CRAMM, був створений Центральним комп'ютерним і телекомунікаційним агентством Великої Британії за дорученням британського уряду. Після

впровадження урядом Великобританії в 1985 році ця технологія стала національним стандартом. З тих пір багато організацій у комерційному секторі прийняли цей метод. Компанія Insight Consulting Limited створила та підтримує програмний продукт, що реалізує метод CRAMM. Протягом цього періоду CRAMM кардинально вплинув на світ.

Підхід CRAMM поєднує як кількісні, так і якісні методи оцінки ризику. Це загальний метод, який можуть використовувати державні та комерційні організації будь-якого розміру. Для різних типів організацій існують різні версії програмного забезпечення CRAMM. Ці конфігураційні файли змінюються залежно від цільового призначення програмного забезпечення. CRAMM має комерційну та державну версії. Державна версія цього профілю також підтримує аудит на відповідність стандартам US ITSEC («Помаранчева книга»)[8].

Використання методології CRAMM може допомогти бізнесу економічно виправдати витрати на підтримку інформаційної безпеки та безперервності бізнесу. Економічно ефективна стратегія управління ризиками ІБ може зменшити витрати, уникаючи непотрібних витрат.

Після розгляду першого питання, яке запитує, чи достатньо основних інструментів, що відповідають традиційним функціям ІБ, необхідно виконати другий етап. Тут розглядаються різні варіанти для більш глибокого аналізу. Для оцінки ризику підхід CRAMM використовує дані, зібрані на перших двох етапах. Також використовується чек-лист, запитання для співбесіди та звіти, підготовлені на третьому етапі. Ця структура розбиває кожен крок на конкретні етапи: оцінка ризиків, встановлення заходів і створення звітів. Алгоритм методики CRAMM подано на рис. 4.2 [29].

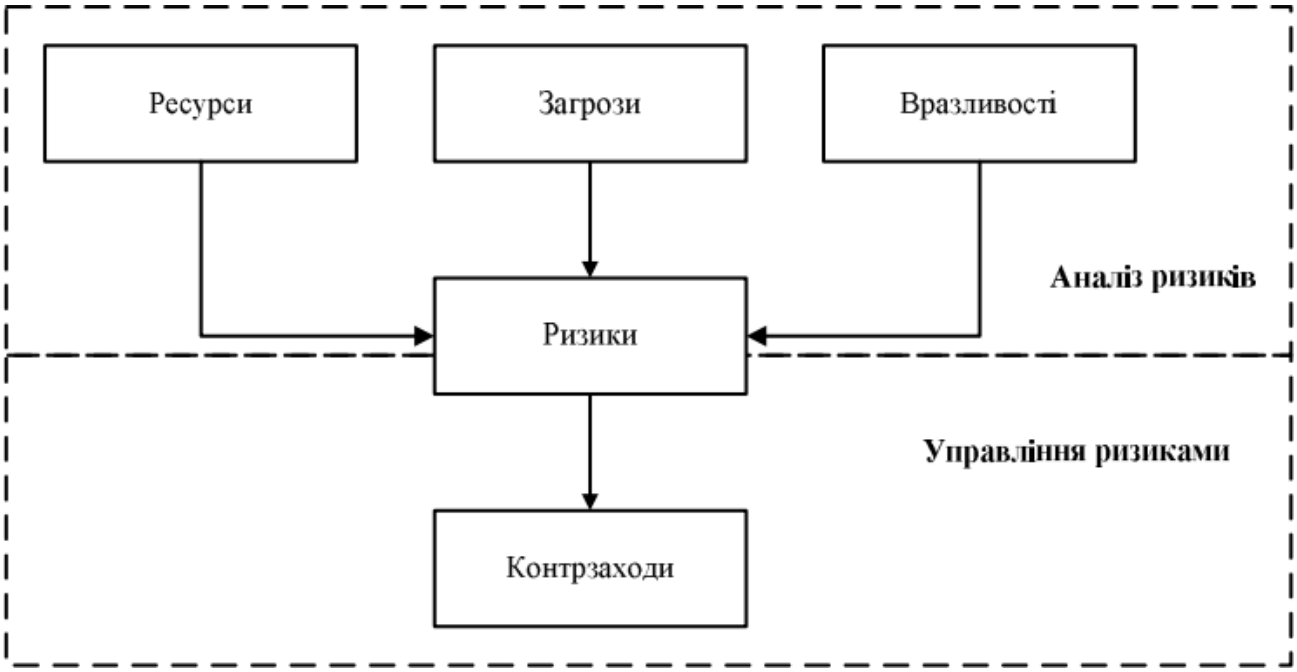


Рисунок 4.2 Алгоритм методики управління ризиками CRAM

Методика OCTAVE (Operational Critical Threat, Asset and Vulnerability Assessment) була розроблена в Університеті Карнегі-Меллона (США) і передбачає оцінку критичності загроз, активів і вразливостей.

Цей метод використовується в усьому світі для проведення оцінки ризиків інформаційних систем і впровадження процесів управління ризиками в усій компанії. Існує багато модифікацій методу, призначених для організацій різного розміру та сфери діяльності [9].

Суть підходу OCTAVE полягає в серії належним чином організованих внутрішніх семінарів для оцінки ризиків. Оцінка ризиків здійснюється в три етапи, яким передує комплекс підготовчих заходів: узгодження розкладу семінару, розподіл ролей, планування та координація дій учасників команди проекту [19].

Практичні семінари є відправною точкою для створення оцінки загроз. Ці семінари створюють профілі загроз, які включають інвентаризацію та оцінку активів, а також інформацію про відповідні закони та нормативні акти. Потім

семінар визначає загрози та оцінює їхню ймовірність. Далі – визначення системи організаційних заходів системи захисту інформації.

На другому етапі технарі оцінюють серйозність вразливості своєї організації, щоб виявити будь-які небезпеки, що насуваються. Цей другий етап передбачає виявлення вразливостей у їхніх системах і їх серйозності.

Третій етап оцінки інформаційної безпеки передбачає пошук уразливостей, виявлених у попередніх оцінках. Потім вони планують варіанти пом’якшення загроз інформаційній безпеці. Вони також розраховують ймовірність і величину шкоди, завданої впровадженням загроз інформаційної системи. Нарешті, вони працюють над розробкою засобів захисту інформаційних систем і стратегій зменшення ризиків. Обсяг ризику визначається як середньорічний збиток компанії через впровадження загроз інформаційним системам [30].

Алгоритм цієї методики зображено на рис. 4.3.

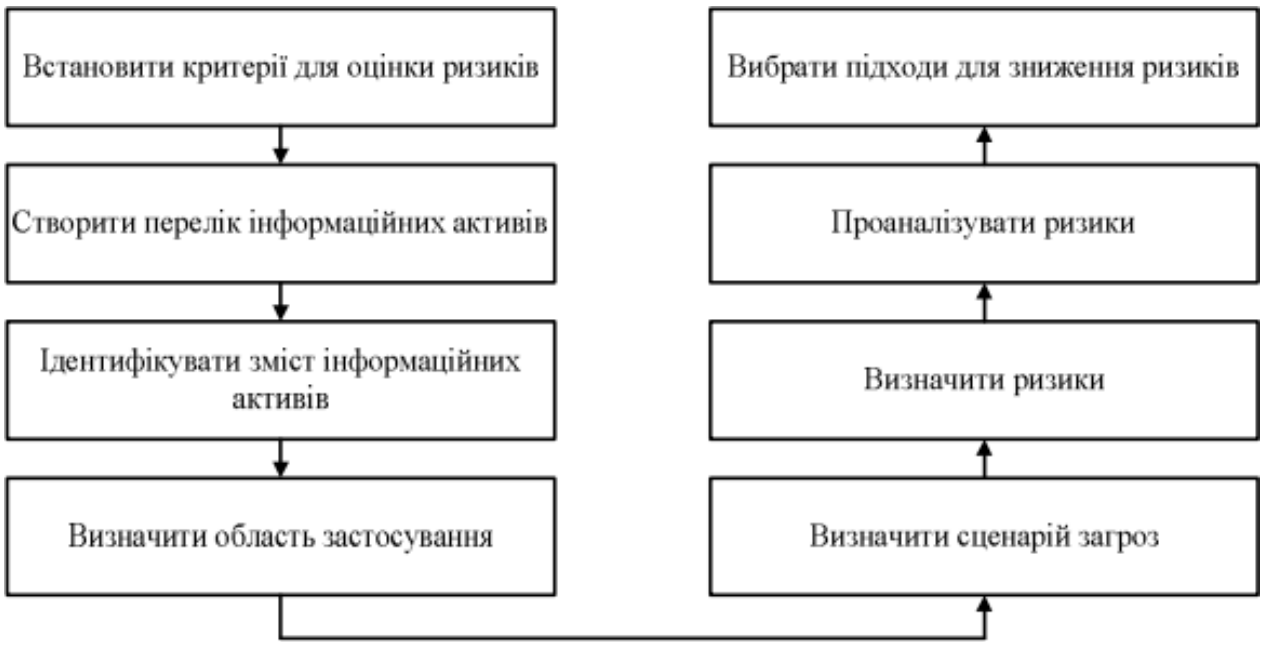


Рисунок 4.3Алгоритм методики управління ризиками OCTAVE

Тому, коротко охарактеризувавши три найпоширеніші методи управління ризиками у сфері інформаційної безпеки [8, 10, 11] та проаналізувавши основні характеристики цих методів, автори виділяють основні переваги та недоліки вищевказаних методів. Їх подано у вигляді табл. 4.1.

Таблиця 4.1

Переваги та недоліки методик з управління ризиками ІБ

Методика	Переваги	Недоліки
NIST	порівняно проста в реалізації; – придатна для підприємств різного розміру; детально описує всі можливі ризики для інформаційних активів; припускає використання як способів зниження ризиків всіх можливих варіантів (зниження, прийняття, перенесення, уникнення ризику); існує автоматизоване програмне забезпечення, що реалізовує принципи методики; йому властива відносна легкість та зручність використання.	довготривалий процес аналізу; розроблена для використання у федеральних організаціях США; оцінювання ризиків проводиться за трирівневою шкалою, що істотно обмежує можливості методики загалом.

CRAMM	є універсальною і підходить для організацій як державного, так та комерційного сектору; використовує кількісні і якісні способи оцінки ризиків; – розроблені комерційні програмні продукти, що реалізовують положення CRAMM;	використання методики потребує спеціальної підготовки і високої кваліфікації спеціаліста; довготривалий процес аналізу; програмний інструментарій генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці; не дає змоги створювати власні шаблони звітів або модифікувати наявні; припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як “уникнення” або “прийняття”, не розглядаються.
OCTAVE	швидко впроваджується; – можливе застосування для організацій різного розміру та галузей зайнятості; є комерційні програмні продукти, що реалізовують положення методики; високий рівень гнучкості.	не дає кількісної оцінки ризиків; припускає використання як способів зниження ризиків лише його зниження і прийняття.

У контексті забезпечення безперервності роботи СМС у МОЗ, що є тривалим і ресурсомістким процесом, аналіз ризиків ІБ, які можуть становити загрозу для безперервності діяльності СМС, є лише одним із багатьох етапів, які необхідно успішно пройти. завершено. Тому важливо мати можливість швидко і відносно легко управляти ризиками ІБ, які входять до сфери впливу

функціональної безперервності СІЗ МОЗ. Таким чином, на основі проведеного аналізу автори статті дійшли висновку, що в контексті забезпечення безперервності діяльності МОЗ найкращі варіанти вибору методів управління IT-ризиками, особливо адаптації та через логіку мінімізації їх сильних і слабких сторін Комбінації для покращення відомих методів. [11]

4.2 Використання методу оцінювання ризиків інформаційних систем при виявленні атак і способів їх подолання

Управління інформаційною безпекою має велике значення для будь-якої організації, яка у своїй діяльності використовує сучасні технології збирання, зберігання та обробки інформації. Невід'ємною частиною цього процесу є оцінка ризиків інформаційної безпеки, яку необхідно періодично проводити з метою ефективного впровадження заходів щодо управління інформаційною безпекою, обліку нових загроз та вразливостей, а також змін у вимогах та пріоритетах діяльності організації.

В даний час для оцінки ризиків інформаційної безпеки використовується безліч різних методів та засобів. У них пропонуються різні способи зіставлення можливої шкоди в результаті інцидентів інформаційної безпеки з ймовірністю реалізації загроз та отримання відповідних висновків, пропонуються різні шкали вимірювання рівня ризику. При цьому в дослідженнях, які вивчають та порівнюють ефективність цих методів у різних умовах, не береться до уваги важливий факт.

Оцінка інформаційних ризиків, незважаючи на наявні специфічні для неї нюанси в різних сферах діяльності, є упорядкованим процесом, що складається з одних і тих же етапів, на кожному з яких можуть бути застосовані свої методи

та засоби. Тому першочергову увагу в дослідженнях такого роду слід приділяти не результативності методів взагалі, а їх ефективності на тому чи іншому етапі, можливостям їх поєднань та комбінацій, способам переходу від одного методу до іншого (таблиця 4.2.) [18].

Таблиця 4.2.

Фактори ризику інформаційної безпеки та їх складові

Фактори ризику	Складники факторів
Загрози (X1)	Природні агрози (X11)
	Антропогенні (людські) загрози (X12)
Збитки (X2)	Збитки конфіденційності (X21)
	Збитки цілісності (X22)
	Збитки доступності (X23)
Вразливість (X3)	Технічні вразливості (X31)
	Уразливості в управлінні (X32)
Контрміри(X4)	Існуючі контрзаходи(X41)
	Необхідні контрзаходи (X42)

Цей процес та його етапи аналогічні для будь-яких організацій, незалежно від сфери їхньої діяльності, масштабів, рівня організаційної зрілості [3]. Проте всі ці етапи вирішують конкретні завдання та мають специфічні особливості, тому для оцінки інформаційних ризиків необхідно на різних етапах застосовувати різні механізми їх реалізації. Далі будуть розглянуті цілі та завдання кожного з етапів та методи, які слід використовувати при їх здійсненні.

На етапі аналізу потоків даних в інформаційній системі будується модель інформаційної системи, визначається призначення її елементів та підсистем та

взаємозв'язку між ними, а також маршрути циркулюючих потоків інформації. Мета даного етапу – виявити недоліки, «вузькі місця» в інформаційній системі, які мають значення для інформаційної безпеки. Отже, модель системи має бути наочною та зручною для аналізу. Такі властивості мають функціональні моделі, що будуються за допомогою методів структурного аналізу у графічній формі з змістовним описом, що дозволяє аналізувати діаграми. Наприклад, у роботі [14] розглядається реалізація цього етапу за допомогою методології DFD. У роботах [5, 16] наведено приклад аналізу інформаційних потоків у віртуальних інфраструктурах охорони здоров'я на основі методології IDEF0.

На наступному етапі вирішується завдання оцінки 3 факторів ризику – X1, X2 та X3. Методи, що вирішують завдання оцінки, можна розділити на кількісні та якісні, які відрізняються у виборі шкали виміру – числової та лінгвістичної відповідно. Кожна з цих груп методів має свої переваги та недоліки (табл. 4.3.) [22].

Таблиця 4.3.

Переваги та недоліки кількісних та якісних методів

Методи оцінки	Кількісні методи	Якісні методи
Переваги	Дозволяють чисельно оцінити необхідні параметри. Реалізують аналіз витрат та прибутку при виборі захисту. Надають більш точне відображення значень, що шукаються.	Дозволяють визначити галузі критичних рівнів у короткий час та без значних витрат. Дозволяють оцінювати відносно легко та дешево.

Недоліки	Кількісні заходи залежать від обсягу і точності шкали вимірювання, що використовується. Результати оцінки можуть бути неточними і вводити в оману. Повинні бути доповнені якісним описом. Оцінка, що проводиться із застосуванням цих методів, як правило, дорожча, потребує більшого досвіду та сучасного інструментарію.	Не дозволяють визначити ймовірності та результати з використанням числових коефіцієнтів. Аналіз витрат і вигод при виборі захисту складніший. Отримані результати мають загальний, наближений характер.

Звести перелічені недоліки до мінімуму дозволяє комбінація кількісних та якісних методів – використання шкали числових коефіцієнтів спільно з лінгвістичним описом окремих інтервалів (рівнів). Тому саме такі змішані методи слід використовувати як на даному, так і на наступному етапі – при оцінці існуючих заходів безпеки.

Особливістю цих етапів є те, що оцінити фактори ризику (по суті, вхідні дані для оцінки самого ризику) можна лише експертно. Особливо це стосується оцінки можливої шкоди, що включає такий складний, неоднозначний і суб'єктивний процес, як визначення вартості інформаційних активів і ресурсів. При оцінці інших факторів як допоміжна інформація експерти можуть використовувати результати аналізу потоків даних в інформаційній системі, отримані на першому етапі, і накопичені статистичні дані (якщо такі є) про загрози, уразливості та ефективність існуючих заходів безпеки. Ще однією важливою проблемою є вибір механізмів проведення експертного опитування. Шкала оцінки вибирається експертами довільно, і в різних дослідженнях існують абсолютно різні висновки щодо ефективності використання тих чи інших шкал. Також існує необхідність забезпечення адекватності та узгодженості експертних думок. В роботі проведено порівняльний аналіз експертних методів, який

показав, що найбільшу адекватність та узгодженість забезпечують метод Дельфі та використання коефіцієнта конкордації [18].

При цьому зроблено висновок, що метод конкордації має меншу громіздкість за тієї ж ефективності, що й метод Дельфі. Коефіцієнт конкордації W лежить в інтервалі [0, 1]. Чим ближче значення коефіцієнта до одиниці, тим більший рівень узгодженості експертних думок. Зазвичай мінімально допустиме значення коефіцієнта конкордації становить 0,4. Тому за досить узгодженого результату $W \geq 0,4$.

Також для забезпечення адекватності експертних думок можна використовувати розв'язання задачі лінійного програмування симплекс-методом, де ймовірності реалізації загрози інформаційної безпеки (x1), нанесення найвищої можливої шкоди (x2) та використання вразливості інформаційної системи (x3) - повинні бути в інтервалі [0, 1].

Наступний етап – оцінка ризику. Для нього статистичні дані та експертні оцінки недостатні. Тут необхідні складні математичні розрахунки, які б обробляли дані про фактори ризику X1, X2, X3 і X4, які отримують від експертів на попередніх етапах. Такі можливості мають методи, що використовують лементи штучного інтелекту (табл. 4.4.) [18].

При цьому найбільшою ефективністю в оцінці інформаційних ризиків мають гібридні моделі, що поєднують кілька методів штучного інтелекту, оскільки вони враховують як числові значення факторів ризику, так і якісні дані, які отримують від експертів. Наприклад, у роботі [9] представлений модуль нечіткого виведення на основі нейронних мереж для динамічного ітеративного аналізу інформаційних ризиків, а в роботі [10] – нейронечітка мережа, що оцінює рівень інформаційних ризиків за 3 змінними в середовище програмного комплексу MATLAB. Етап оцінки ризику повторюється до тих пір, поки рівень

залишкового ризику, зниженого в результаті впровадження контрзаходів, не буде прийнятним.

Окремим етапом йде економічна оцінка захисту інформації, метою якої є розрахунок співвідношень ризику інформаційної безпеки, витрат на контрзаходи та вигод, одержуваних від їх впровадження. Особливістю цієї оцінки є те, що вона має бути виражена суворо у кількісній формі, причому у фінансовому еквіваленті. Для цього також існує кілька методів (табл. 4) [13].

Залежно від рівня ризику та оцінки економічних витрат на його зниження реалізується завершальний етап – управління ризиками. Існує 4 типові методи його реалізації:

- мінімізація ризику (виконання дій для зменшення ймовірності та/або негативних наслідків, пов'язаних із ризиком);
- прийняття ризику (готовність організації завдати шкоди від конкретного ризику у разі, якщо його рівень вважається прийнятним);
- ухилення від ризику (відмова від залучення в ризиковану ситуацію або дію, що запобігає її виникненню);
- передача ризику (перенесення відповідальності за ризик на треті особи).

Таблиця 4.4.

Інтелектуальні підходи до оцінки ризиків інформаційної безпеки

Категорія	Деякі підходи
	Багатошаровий перцептрон Метод зворотного розповсюдження помилки

Нейронні сіті	Нейронна мережа радіально-базових функцій Ймовірнісна нейронна мережа Самоорганізована конкуренція
Навчальний вектор	Метод опорних векторів
М'які обчислення	Наближені множини «Сірі стосунки» Генетичний алгоритм Нечіткі множини
Гібридні моделі	Байєсівська нечітка мережа Нейронечітка мережа Нечітко-наближені множини Нечіткий метод аналізу ієрархій Нечіткий метод аналізу мереж «Сіра ієрархічна модель» Нейронна мережа з генетичним алгоритмом

Виявлено, що при оцінці ризиків інформаційної безпеки слід використовувати не один універсальний метод, а комбінувати методи та засоби на різних етапах цього процесу: DFD або IDEF0 – на етапі аналізу потоків даних в інформаційній системі, експертне опитування з методами Дельфі , конкордації або симплекс-методом – на етапі оцінки факторів ризику, методи штучного інтелекту, особливо гібридні моделі – на етапі оцінки ризику, відповідні математичні методи – на етапі економічної оцінки захисту інформації та мінімізація, прийняття, передання або ухилення від ризику – на етапі реалізації управління ризиками.

4.3 Рекомендації щодо попередження ризиків інформаційних систем з використанням системи штучного інтелекту

Для попередження ризиків інформаційних систем дуже важливо проведити перевірку на наявність загроз. Це виконується за допомогою наступних методів.

- Матриця помилок (або матриця неточностей, англ. Confusion matrix)

Перед переходом до самих метрик необхідно ввести важливу концепцію для опису цих метрик в термінах помилок класифікації - confusion matrix (матриця помилок). Припустимо, що у нас є два класи y = {0,1} і алгоритм, який пророкує (передбачає) приналежність кожного об'єкта одному з цих класів. Розглянемо приклад. Нехай система захисту мережі використовує систему класифікації для виявлення атаки: нормальна робота мережі чи аномальна (наявність атаки). При цьому у першому випадку система і далі нормально працює, а у другому – видається сигнал аномальної роботи. Таким чином, виявлення неадекватної (аномальної) роботи мережі (y = 1) можна розглядати як "сигнал тривоги", що повідомляє про можливі ризики.

Будь-який реальний класифікатор робить помилки. У нашому випадку таких помилок може бути дві:

1. Нормальна ситуація у мережі за даними трафіка розпізнається моделлю як аномальна. Даний випадок можна трактувати як "помилкову тривогу".
2. Аномальна ситуація розпізнається як нормальна і ніяких дій по захисту від атаки не відбувається. Даний випадок можна розглядати як "пропуск цілі".

Неважко помітити, що ці помилки нерівноцінні по зв'язаних з ними наслідками. У разі "помилкової тривоги" втрати складуть тільки марно потрачений час та ресурси на протидію неіснуючій загрозі. У разі "пропуску цілі"

можна втратити набагато більше (інформацію, роботу мережі та інше, це залежить від виду атаки). Тому системі захисту важливіше не допустити "пропуск цілі", ніж "помилкову тривогу" [17].

Оскільки з точки зору логіки завдання виявлення аномалій нам важливіше правильно розпізнати аномалію (атаку) з міткою y = 1, ніж помилитися в розпізнаванні нормальної роботи мережі, будемо називати відповідний результат класифікації позитивним (аномалія чи атака виявлені вірно), а протилежний - негативним (аномалії чи атаки немає y = 0). Тоді можливі наступні чотири результати класифікації:

1. True Positive (TP) – наявність атаки класифікована як наявна атака, тобто позитивний клас розпізнано як позитивний. Спостереження, для яких це має місце називаються істинно-позитивними.
2. True Negative (TN) – нормальна робота мережі класифікована як нормальна робота без аномалій, тобто негативний клас розпізнано як негативний. Спостереження, яких це має місце, називаються істинно негативними.
3. False Positive (FP) – нормальна робота мережі класифікована як аномальна, тобто мала місце помилка, в результаті якої негативний клас був розпізнаний як позитивний. Спостереження, для яких було отримано такий результат класифікації, називаються помилково-позитивними, а помилка класифікації називається помилкою I роду.
4. False Negative (FN) – атака чи аномальна робота мережі розпізнана як нормальна, тобто мала місце помилка, в результаті якої позитивний клас був розпізнаний як негативний. Спостереження, для яких було отримано такий результат класифікації, називаються помилково-негативними, а помилка класифікації називається помилкою II роду [22].

Таким чином, помилка I роду, або хибно-позитивний результат класифікації, має місце, коли негативне спостереження розпізнано моделлю як позитивне. Помилкою II роду, або хибно-негативних результатом класифікації, називають випадок, коли позитивне спостереження розпізнано як негативне. Пояснимо це за допомогою матриці помилок класифікації:

	y = 1	y = 0
a (x) = 1	Істинно-позитивний (True Positive - TP)	Помилково-позитивний (False Positive - FP)
a (x) = 0	Помилково-негативний (False Negative - FN)	Істинно-негативний (True Negative – TN)

Тут a(x) - це відповідь алгоритму при конкретній ситуації, а y - справжня мітка класу для цієї ситуації. Таким чином, помилки класифікації бувають двох видів: False Negative (FN) і False Positive (FP). P означає що класифікатор визначає клас об'єкта як позитивний (N - негативний). T означає що клас передбачений правильно (відповідно F - неправильно). Кожен рядок в матриці помилок представляє прогнозований клас, а кожен стовпець - фактичний клас.

Тобто у загальному випадку, матриця неточностей - це матриця розміром N на N, де N – кількість класів, яка представляє собою табличне представлення прогнозованих і фактичних значень для кожного можливого класу.

Матриця помилок, одна з наважливіших речей, на яку потрібно дивитися при оцінці моделі класифікації. Це матриця, яка візуалізує кількість фактичних екземплярів класу в порівнянні з прогнозованими екземплярами класу. Таке подання дозволяє нам швидко побачити кількість правильних і неправильних прогнозів для кожної категорії.

На основі цієї матриці будується ряд інших характеристик. Розглянемо кожну з них більш детально [27].

Акуратністю називається пропорція точних прогнозів по відношенню до загальної кількості прогнозів, тобто це ймовірність того, що клас буде передбачений правильно (4.1).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

Тобто, accuracy - частка правильних відповідей алгоритму:

Хоча акуратність є швидким та інформативним індикатором продуктивності моделі, ми не можемо покладатися виключно на неї. Це пов'язано з тим, що вона приховує наявність зсуву в моделі, що є звичайним явищем, якщо набір даних незбалансований, тобто негативних моментів значно більше, ніж позитивних, або навпаки. Тобто, ця метрика марна в задачах з нерівними класами, що як варіант можна виправити за допомогою алгоритмів семпліювання. Семпліювання (англ. Data sampling) - метод коригування навчальної вибірки з метою балансування розподілу класів у вихідному наборі даних. Розглянемо це на простому прикладі.

Припустимо, ми хочемо оцінити роботу спам-фільтра пошти. У нас є 100 НЕ-спам листів, 90 з яких наш класифікатор визначив вірно (True Negative = 90, False Positive = 10), і 10 спам-листів, 5 з яких класифікатор також визначив вірно (True Positive = 5, False Negative = 5). Тоді accuracy:

$$Accuracy = \frac{5 + 90}{5 + 90 + 10 + 5} = 86{,}4$$

Але якщо ми просто будемо передбачати, що всі листи Не-спам, то отримаємо більш високу акуратність:

$$Accuracy = \frac{0 + 100}{0 + 100 + 0 + 10} = 90{,}9$$

При цьому, наша модель абсолютно не володіє ніякою прогностичною силою, оскільки спочатку ми хотіли визначати листи зі спамом. Подолати це нам допоможе перехід із загальної для всіх класів метрики до окремимих показників якості класів [12].

Точністю називається частка правильних відповідей моделі в межах класу - це частка об'єктів, що дійсно належать даному класу, щодо всіх об'єктів які система віднесла до цього класу.

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

Саме введення precision не дозволяє нам записувати всі об'єкти в один клас, так як в цьому випадку ми отримуємо зростання рівня False Positive [7].

Повнота - це частка істинно позитивних класифікацій. Повнота показує, яку частку об'єктів, що реально належать до позитивного класу, ми передбачили вірно. Або ж іншими словами: це частка варіантів, класифікованих як позитивні, які насправді виявилися позитивними.

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

Повнота (recall) демонструє здатність алгоритму виявляти даний клас взагалі.

Маючи матрицю помилок, дуже просто можна обчислити точність і повноту для кожного класу. Точність (precision) дорівнює відношенню відповідного діагонального елемента матриці і суми всього рядка класу. Повнота (recall) - відношенню діагонального елемента матриці і суми всього стовпчика класу. Оскільки класів може бути багато (не обов’язково два), то формально:

$$Precision_{\text{c}} = \frac{A_{c,c}}{\sum_{i=1}^{n} A_{c,i}}$$

$$Recall_{\text{c}} = \frac{A_{c,c}}{\sum_{i=1}^{n} A_{i,c}}$$

Тобто, результуюча точність класифікатора розраховується як середнє арифметичне його точності по всіх класах. Те ж саме з повнотою [18].

Precision і recall не залежить від співвідношення класів (на відміну від accuracy) і тому можуть бути застосовні в умовах незбалансованих вибірок. Часто в реальній практиці стоїть завдання знайти оптимальний (для замовника) баланс між цими двома метриками. Зрозуміло що чим вище точність і повнота, тим краще. Але в реальному житті максимальна точність і повнота недосяжні одночасно і доводиться шукати якийсь баланс. Тому, хотілося б мати якусь метрику яка об'єднувала б у собі інформацію про точність та повноту нашого алгоритму. У цьому випадку нам буде простіше приймати рішення про те, яку реалізацію запускати у виробництво (у кого більше той і крутіше). Саме такою метрикою є F-міра [29].

F-міра є гармонійним середнім між точністю і повнотою. Вона прагне до нуля, якщо точність або повнота прагне до нуля.

$$F = \frac{2 \times precision \times recall}{precision + recall} \tag{4}$$

Дана формула надає однакову вагу точності і повноти, тому F-міра буде падати однаково при зменшенні і точності і повноти. Можливо розрахувати F-

міру надавши різну вагу точності і повноті, якщо ви свідомо віддаєте пріоритет одній з цих метрик при розробці алгоритму:

$$F_\beta = \frac{(1+\beta^2) \times precision \times recall}{(\beta^2 \times precision) + recall} \quad (5)$$

де β приймає значення в діапазоні 0 <β <1 якщо ви хочете віддати пріоритет точності, а при β> 1 пріоритет віддається повноті. При β = 1 формула зводиться до попередньої і ви отримуєте збалансовану F-міру (також її називають F1) (рис.4.4.,4.5.,4.6.).

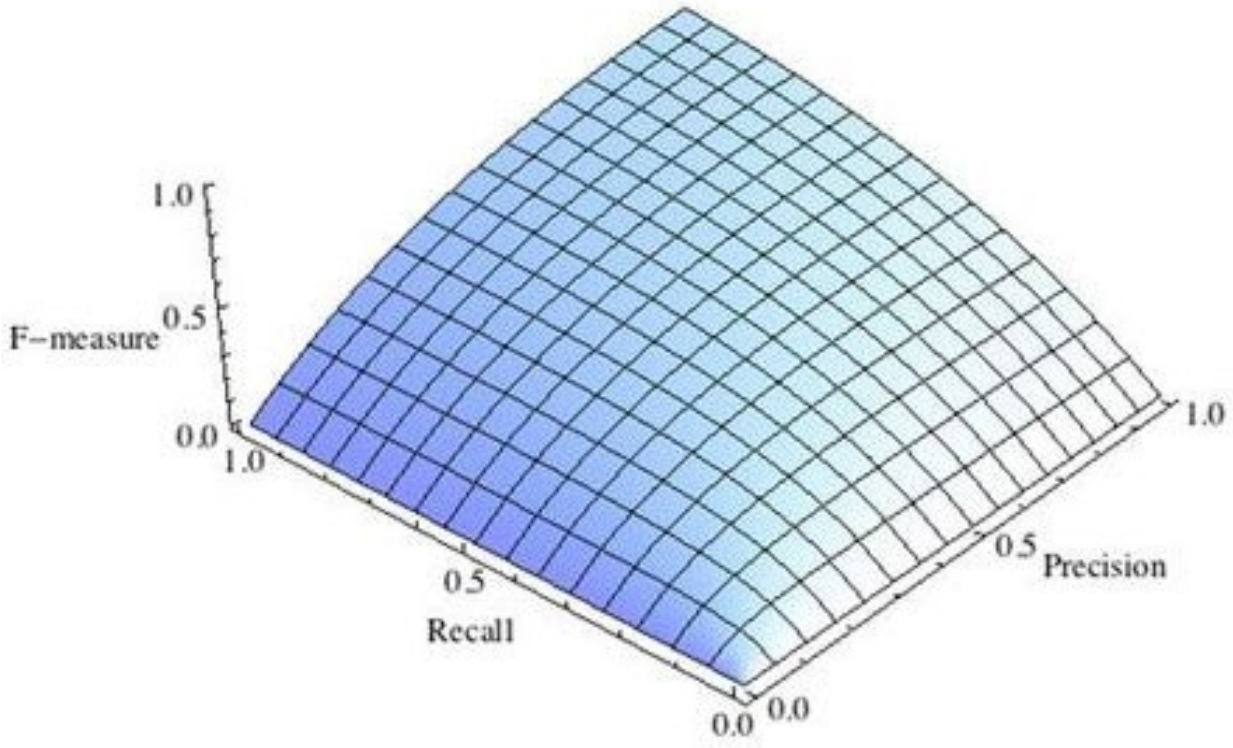


Рис.4.4. Збалансована F-міра, β=1

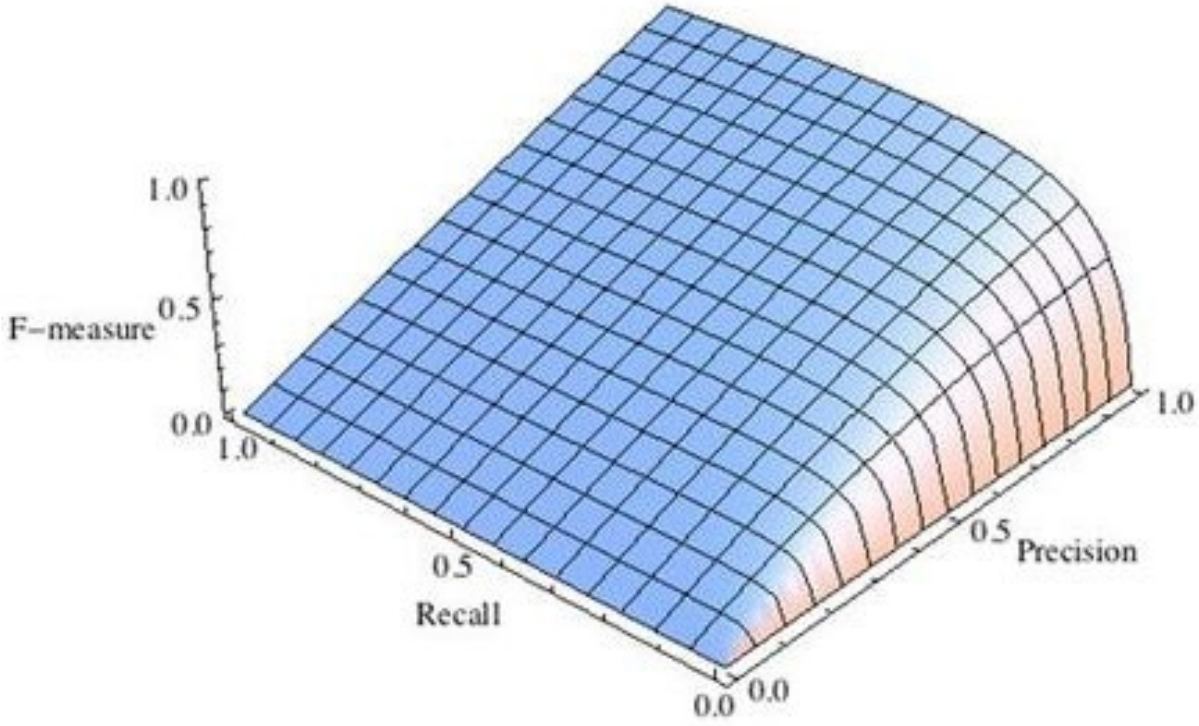


Рис.4.5. F-міра з приоритетом точності, β2=1/4

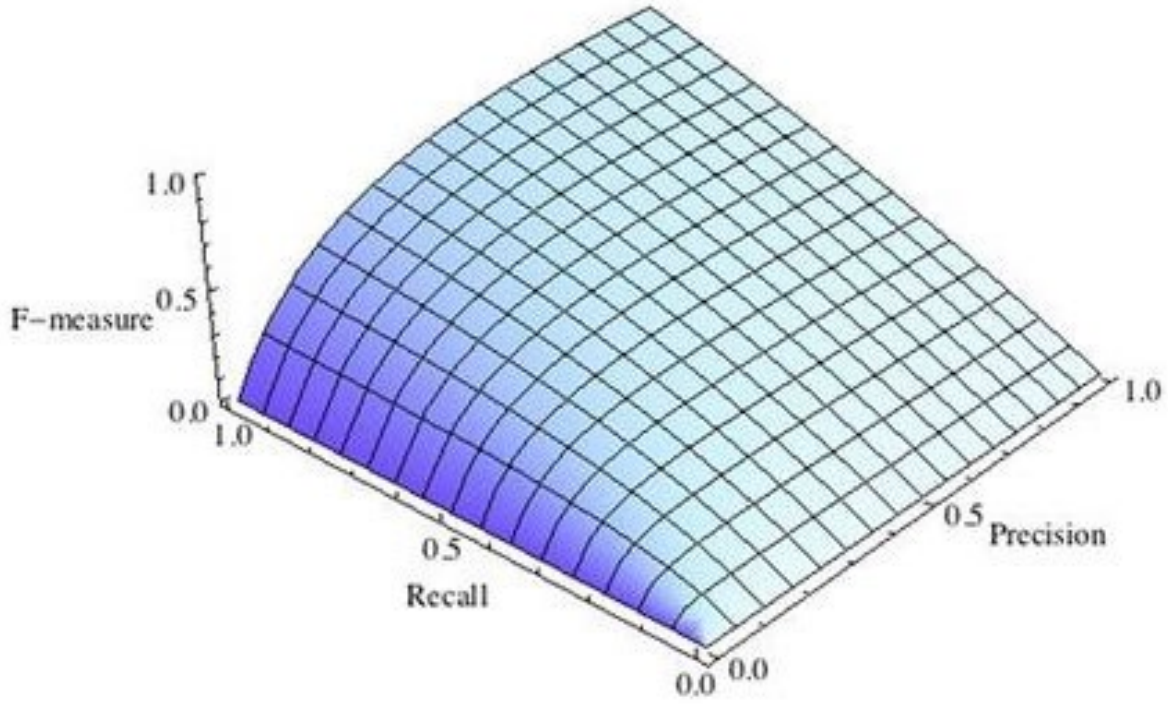


Рис.4.6. F-міра с пріоритетом повноти, β2=2

F-міра досягає максимуму при максимальній повноті і точності, і близька до нуля, якщо один з аргументів близький до нуля.

G-F-міра є хорошим кандидатом на формальну метрику оцінки якості класифікатора. Вона зводить до одного числа дві інші основоположні метрики: точність і повноту. Маючи "F-міру" набагато простіше відповісти на питання: "змінився алгоритм в кращу сторону чи ні?"

H-Крива робочих характеристик (англ. Receiver Operating Characteristics curve). Використовується для аналізу поведінки класифікаторів при різних порогових значеннях. Дозволяє розглянути всі порогові значення для даного класифікатора. Показує частку хибно позитивних прикладів (англ. False positive rate, FPR) в порівнянні з часткою істинно позитивних прикладів (англ. True positive rate, TPR).

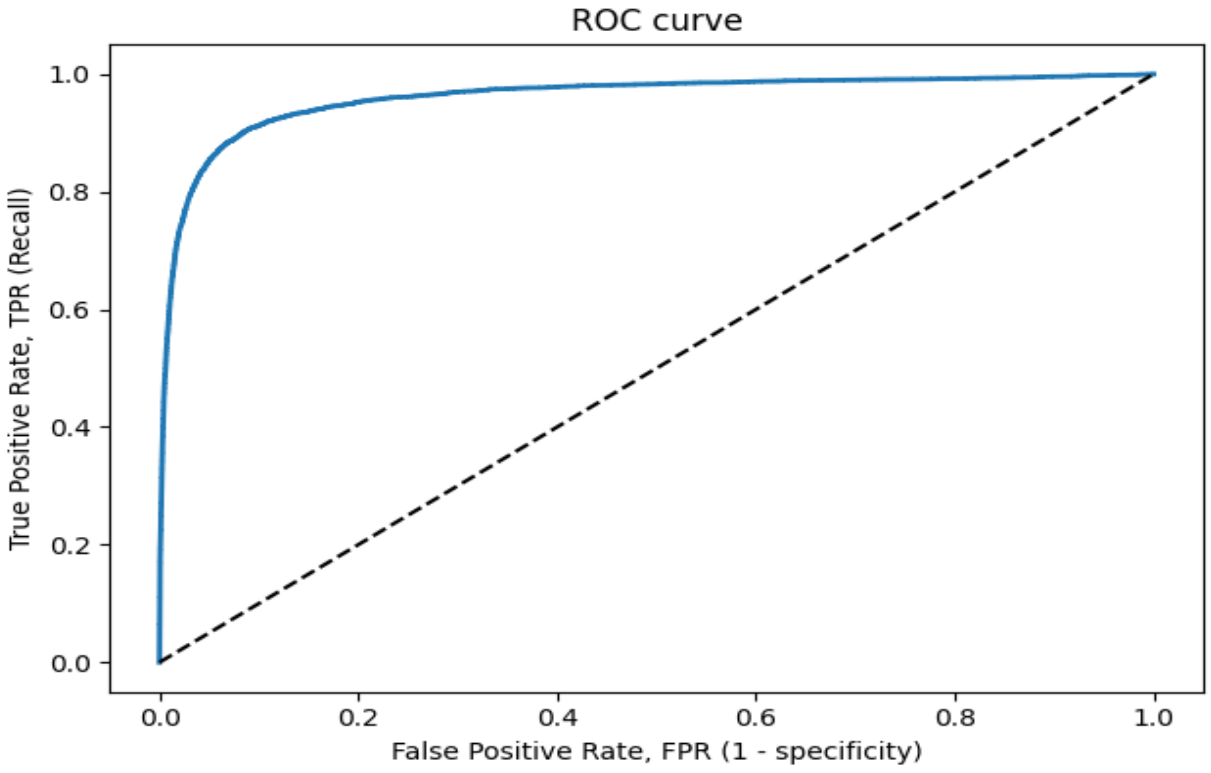


Рисунок 4.7.–ROC-крива

$$TPR = \frac{TP}{TP + FN} = Recall \quad (6)$$

$$FPR = \frac{FP}{FP + TN} \quad (7)$$

Частка FPR - це пропорція негативних зразків, які були некоректно класифіковані як позитивні.

$$FPR = 1 - TNR$$

де TNR - частка істинно негативних класифікацій (англ. Trie Negative Rate), що представляє собою пропорцію негативних зразків, які були коректно класифіковані як негативні.

Частка TNR також називається специфічністю (англ. Specificity). Отже, ROC-крива зображає чутливість (англ. Sensitivity), тобто повноту, в порівнянні з різницею 1 - specificity.

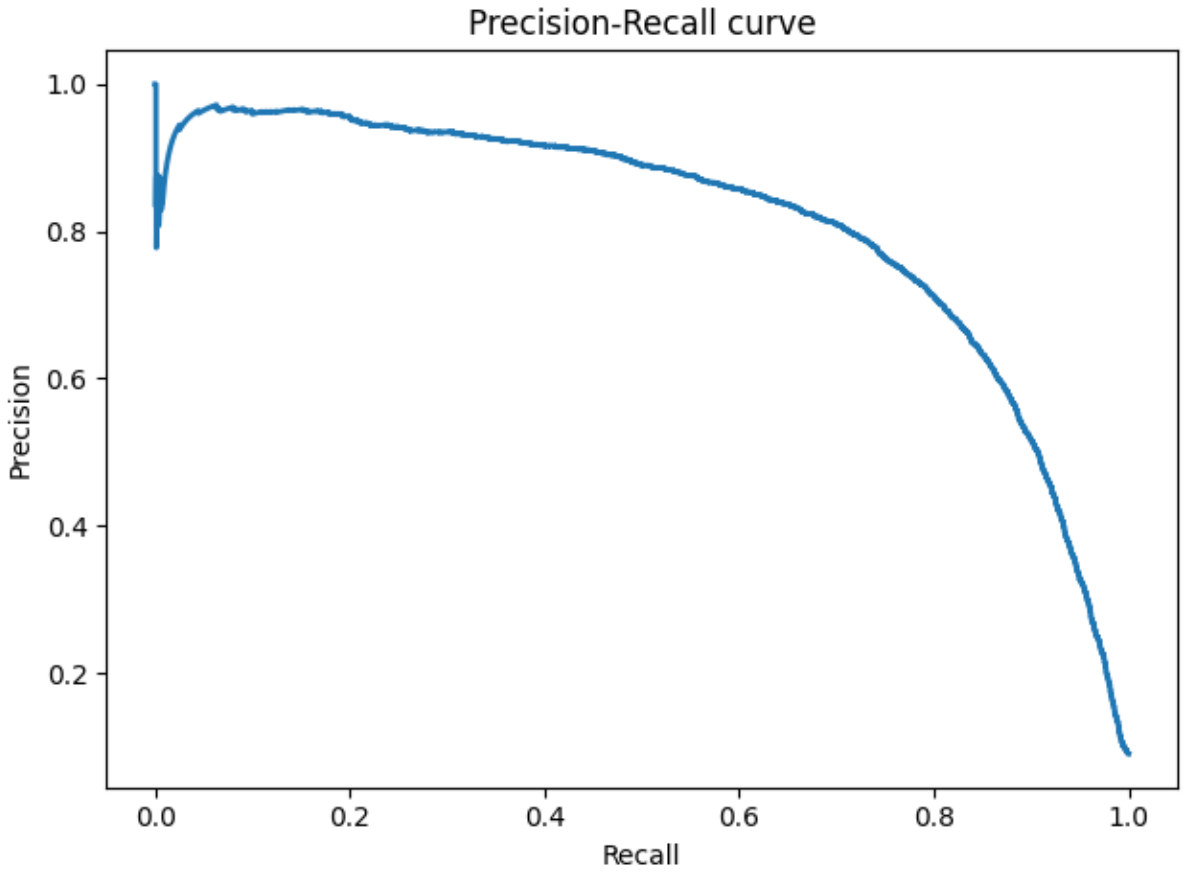
Пряма лінія по діагоналі представляє ROC-криву чисто випадкового класифікатора. Хороший класифікатор тримається від зазначеної лінії настільки далеко, наскільки це можливо (прагнучи до лівого верхнього кута).

Один із способів порівняння класифікаторів передбачає вимір площі під кривою (англ. Area Under the Curve - AUC). Бездоганний класифікатор матиме площу під ROC-кривою (ROC-AUC), що дорівнює 1, тоді як чисто випадковий класифікатор - площу 0.5.

Графік ROC допомагає прийняти рішення про те, де встановити поріг класифікації, щоб максимізувати істинно позитивний рівень або мінімізувати псевдопозитивний показник, що в кінцевому підсумку є бізнес-рішенням.

Чутливість до співвідношення класів. Розглянемо задачу виділення математичних статей з безлічі наукових статей. Припустимо, що за все мається 1.000.100 статей, з яких лише 100 належать до математики. Якщо нам вдасться побудувати алгоритм a(x), що ідеально вирішує завдання, то його TPR буде дорівнює одиниці, а FPR - нулю. Розглянемо тепер поганий алгоритм, що дає позитивну відповідь на 95 математичних і 50.000 нематематичних статтях. Такий алгоритм абсолютно даремний, але при цьому має TPR = 0.95 і FPR = 0.05, що вкрай близько до показників ідеального алгоритму. Таким чином, якщо позитивний клас істотно менше за розміром, то AUC-ROC може давати неадекватну оцінку якості роботи алгоритму, оскільки вимірює частку невірно прийнятих об'єктів щодо загального числа негативних. Так, алгоритм b(x), що поміщає 100 релевантних документів на позиції з 50.001-й по 50.101-ю, матиме AUC-ROC 0.95 [14].

Позбутися від зазначеної проблеми з незбалансованими класами можна, перейшовши від ROC-кривої до Precison-recall (PR) PR-кривої. Вона визначається аналогічно до ROC-кривої, тільки по осях відкладаються НЕ FPR і TPR, а повнота (по осі абсцис) і точність (по осі ординат). Критерієм якості сімейства алгоритмів виступає площа під PR-кривою (англ. Area Under the Curve - AUC-PR).



Задача виконуваності формул у теоріях (SMT - Satisfiability modulo theories) представляє собою узагальнений варіант задачі визначення виконуваності булевих формул.

SMT-формула - це формула в деякій формальній логіці, яка включає функції і предикатні символи. Ці функції та символи можуть мати певну інтерпретацію. В багатьох задачах необхідно визначити, чи є формула виконуваною чи ні. На відміну від задачі про виконуваність булевих формул, замість булевих змінних SMT-формула може містити довільні змінні, а предикати - це булеві функції від цих змінних. Стандартна задача SAT – знаходити множину змінних, які, підставлені у булеві вирази, дадуть в результаті “true”.

За рядом досліджень показано, що тестування програмного забезпечення може зводитися до завдання виконуваності булевих формул (SAT) і виконуваності формул в теоріях (SMT) [17].

Алгоритми можуть бути представлені у вигляді певних булевих формул, при обмеженнях на можливі комбінації вхідних параметрів.

Сучасні SAT-розв'язники здатні обробляти формули з сотнями тисяч змінних, що показує їх перспективність для використання у великій кількості задач. Розв'язники SMT теж є дуже потужними, зокрема Barcelogic, CVC, MathSAT, Yices і Z3, створені для найбільш поширених логік (теорій).

В сучасних умовах, при наявності потужного програмно-апаратного забезпечення для обчислень SAT-розв'язники можуть використовуватись для аналізу програмного забезпечення.

Основні застосування SAT/SMT в сфері безпеки програмного забезпечення:

- Статичний аналіз на вразливості програмного коду;
- Створення експлойтів (для задач тестування);
- Вивчення захисту від копіювання, дослідження та модифікації;
- Аналіз непротиречивості та повноти політики безпеки, формальна верифікація відсутності вразливостей протоколів, програмного забезпечення тощо [18].

Однією із проблем, яка виникає при застосуванні розв'язника, є генерація обмежень. На вхід розв'язника необхідно подавати обмеження на стани та вхідні параметри, одначе, задати такі обмеження для реальних систем є досить складною задачею, яка інколи не має точного розв'язку. Це накладає обмеження на істинність відповідей, які може надати розв'язник.

SMT дозволяє більш природно моделювати властивості коду, ніж SAT при розв’язанні задач аналізу програмних застосунків.

Розв'язники SMT можуть використовуватись в якості «чорного ящика», на вхід якого подається задача, сформульована у вигляді булевого виразу, а на вихід видається відповідь на подану задачу.

Не менш важливою є перевірка програмного коду.

Питання статичного аналізу програм пов’язані із існуючими досить давно питаннями оптимізації компіляторів. Статичний аналіз використовується для аналізу бінарних файлів, а також, з іншого боку, і вихідного коду на наявність вразливостей. Статичний аналіз може використовуватись як для пошуку механічних помилок, так і для пошуку вразливостей програмного коду.

Оптимізаційні компілятори повинні знати характеристики компільованої програми, щоби в результаті згенерувати ефективний код. Такими властивостями можуть бути [19]:

1. Наявність шматків “мертвого коду”, наприклад, функцій, які не викликаються з main. Якщо так, код піддається оптимізації за рахунок винищення таких шматків.
2. Наявність виразів всередині циклів, значення яких залишається сталим. Якщо так, код піддається оптимізації за рахунок виносу подібних виразів за межі циклу.
3. Залежність змінної від вхідних даних програми. За умови відсутності залежності, значення змінної можна попередньо обчислити під час компіляції.
4. Діапазони змін значень змінних. При цьому можна керувати вибором представлення змінної під час виконання.

5. Наявність покажчиків на несуміжні структури даних у пам'яті. Це може бути підставою для паралельної обробки відповідних фрагментів програми.

Найуспішніші інструменти аналізу, розроблені для виявлення помилок (або перевірки відсутності помилок), спрямовані на загальні властивості коректності, які застосовуються до більшості або всіх програм, написаних на певних мовах програмування. В деяких мовах програмування, зокрема C, існує ряд типових слабкостей, які можуть призводити до критичних уразливостей безпеки. У більш безпечних мовах, таких як Java, такі помилки, як правило, менш серйозні, але вони все одно можуть спричинити збої програм.

Прикладами таких властивостей є:

1. Чи існує вхід, який веде до нульового покажчика розмежування, ділення на нуль або переповнення арифметики?
2. Чи всі змінні ініціалізовані перед їх читанням?
3. Чи завжди доступ до масивів здійснюється в їх межах? 4. Чи можуть існувати покажчики на звільнену пам’ять? 5. Чи завершується програма на кожному введенні?

Інші властивості правильності залежать від специфікацій, наданих програмістом для окремих програм (або бібліотек), наприклад, чи всі твердження гарантовано матимуть успіх? Твердження виражають специфічні властивості коректностіпрограми, які передбачається мати у всіх виконаннях.

В програмному забезпеченні на основі мобільних платформ та веб-застосунків дуже важливі властивості перевірок потоків інформації:

1. Чи сприймає ПЗ запити користувачів до операцій файлової системи без належної фільтрації та перевірки, що призводить до порушень конфіденційності та цілісності.
2. Чи надається доступ невповноваженим користувачам до інформації з обмеженим доступом, внаслідок помилок проектування ПЗ. Це є порушеннями конфіденційності.

В ПЗ, яке забезпечує розпаралелювання, розподілення обчислень та ПЗ на основі моделей виконання, керованих подіями, необхідно знати поведінкові особливості ПЗ:

1. Чи присутня обробка даних у швидкісному режимі, режимі реального часу? Чи різні потоки можуть використовувати спільні ресурси без належної синхронізації?
2. Чи може програма (або частини програми) зайти в глухий кут? Це питання виникає для багатопотокових програм, які використовують блокування для синхронізації.
3. Сучасні інтегровані середовища розробки проводять різні види аналізу програм для підтримки налагодження, рефакторингу та розуміння програм. Сюди входять такі питання, як: Які функції можливо викликати в певному рядку, або навпаки, звідки можна викликати певну функцію; на яких кроках програми змінній може бути присвоєне поточне значення; чи може значення однієї змінної впливати на значення іншої змінної? Під час налагодження такі питання виникають в процесі пошуку помилок.
4. Які типи значень може мати змінна x? Такі питання характерні для нетипізованих мов програмування, наприклад OCaml, JavaScript або Python.

Доведення безпечностіпевного протоколу, перевірка безпечності політики безпеки, безпечності певного алгоритму функціонування програми

виконується методами формальної верифікації. Основними методами верифікації програми є доведення теорем , абстрактна інтерпретація та перевірка моделі. Ці задачі теж можуть виконуватись із використанням SAT/SMT розв’язників.

Задача тестування програмного забезпечення може зводитися до завдання виконуваності булевих формул (SAT) і виконуваності формул в теоріях (SMT).

Застосування SAT/SMT - розв’язників для статичної перевірки коду здійснюється у фреймворку Triton. Triton призначений для реалізації підходу конколічного виконання (з англ. concolic execution framework), реалізований як Pintool - засіб аналізу програмного забезпечення для платформ Windows та Linux.

Taint-аналіз дозволяє поширити по програмі помічені дані. Дане завдання є ключовим для інформаційної безпеки, оскільки саме за допомогою розповсюдження помічених даних виявляються уразливості, пов'язані з ін’єкціями даних (SQL- ін’єкції, міжсайтовий скриптинг, підробка файлового шляху і так далі), а також з витоком конфіденційних даних (небезпечні дії з паролем, небезпечна передача даних).

Приклади задач кібербезпеки, які можна реалізувати за допомогою механізмів використаних в цьому фреймворку:

1. Аналіз слідів конкретних даних – вміст регістрів та значення пам'яті в кожній точці програми;
2. Символьне виконання - символьне вираження регістрів та пам'яті в кожній точці програми;
3. Виконання символьного фаззингу; 4. Генерація та вирішення обмежень;
4. Регістри виконання та модифікація пам’яті ;

5. Повторне відтворення слідів дій безпосередньо в пам’яті. Частково в цих задачах можуть бути задіяні і SAT/SMT –солвери.

Taint-аналіз може надавати інформацію про те, якими регістрами та адресами пам'яті користувач оперує в кожній точці програми. Цей вид аналізу допомагає налаштувати символьні змінні (символьна змінна - це по суті область пам'яті, якою користувач може керувати), обмежує механізм символьного виконання відповідною частиною коду. У кожній інструкції гілки ми безпосередньо знаємо, чи може користувач пройти обидві гілки (це в основному використовується для покриття коду). Мета цього аналізу -визначити чи є регістр або пам’ять поміченими. Тоді як метою символьного механізму є побудова символьних виразів на основі семантики інструкцій. Ці підходи допомагають здійснити мету механізму розв’язника - створити модель виразу (умову шляху).

За допомогою штучного інтелекту можна вирішувати ряд задач щодо політики безпеки комп’ютерних мереж [19].

Якщо у нас є досить складна мережа, завжди актуальною задачею залишається, чи є ця мережа захищеною проти певного вида атак чи ні. Для розв’язання цієї задачі можна використовувати логічний граф атак, вершини якого представляють собою такі види: a) вершина, що відповідає привілеям (права користувача, ftp, rsh і т.д.); b) вершина, що відповідає потенційній можливості використанню експлойта на хості, оскільки хост містить вразливості; c) вершина, що відповідає налаштуванням конфігурації, що протидіють атаці (правила файрволу, IDS-конфігурація, тощо).

За допомогою інструментів типа MulVAL є можливим побудувати відповідний граф для мережі. MulVAL – це інструмент аналізу безпеки, який, враховуючи початкові конфігурації мережі (машини, активні служби, доступність між хостами тощо) та базу даних відомих вразливостей, може визначити всі потенційні шляхи атак, за допомогою яких зловмисник може

використовувати систему. Вхідними даними для аналізу є конфігурація хоста, конфігурація мережі, дані про користувачів мережі, модель взаємодії всіх компонентів та політика захисту мережі.

Граф атаки в мережі може бути представлений у вигляді булевої формули. Ця формула може бути подана на вхід SMT- розв'язника, при відповідних обмеженнях, які характеризують особливості функціонування мережі. Розв'язник може надати відповіді на питання реалізованості атаки в мережі із заданою конфігурацією, питання непротиречивості та достатності існуючих правил, засобів політики безпеки. Однак, врахування всіх можливих факторів успішності атаки при створенні математичної логічної моделі є складною задачею, яка потребує високої кваліфікації.

4.4 Висновки

Методологія оцінки ризиків NIST визначена в спеціальній публікації NIST 800-30 Посібник з управління ризиками систем інформаційних технологій. Це один із найпопулярніших і широко використовуваних методів оцінки управління ризиками. NIST 800-30 визначає два основні параметри для оцінки: потенційний збиток і ймовірність реалізації загрози. Це також відомий як метод оцінки ризику NIST.

Системи управління ризиками виконують практичну функцію інформування про інтеграцію інформаційних технологій у повсякденні операції.

Підхід CRAMM поєднує як кількісні, так і якісні методи оцінки ризику. Це загальний метод, який можуть використовувати державні та комерційні організації будь-якого розміру. Для різних типів організацій існують різні версії програмного забезпечення CRAMM. Ці конфігураційні файли змінюються

залежно від цільового призначення програмного забезпечення. CRAMM має комерційну та державну версії. Державна версія цього профілю також підтримує аудит на відповідність стандартам US ITSEC («Помаранчева книга»)[8].

Методика OCTAVE (Operational Critical Threat, Asset and Vulnerability Assessment) була розроблена в Університеті Карнегі-Меллона (США) і передбачає оцінку критичності загроз, активів і вразливостей.

Цей метод використовується в усьому світі для проведення оцінки ризиків інформаційних систем і впровадження процесів управління ризиками в усій компанії. Існує багато модифікацій методу, призначених для організацій різного розміру та сфери діяльності [9].

В даний час для оцінки ризиків інформаційної безпеки використовується безліч різних методів та засобів. У них пропонуються різні способи зіставлення можливої шкоди в результаті інцидентів інформаційної безпеки з ймовірністю реалізації загроз та отримання відповідних висновків, пропонуються різні шкали вимірювання рівня ризику. При цьому в дослідженнях, які вивчають та порівнюють ефективність цих методів у різних умовах, не береться до уваги важливий факт.

Оцінка інформаційних ризиків, незважаючи на наявні специфічні для неї нюанси в різних сферах діяльності, є упорядкованим процесом, що складається з одних і тих же етапів, на кожному з яких можуть бути застосовані свої методи та засоби. Тому першочергову увагу в дослідженнях такого роду слід приділяти не результативності методів взагалі, а їх ефективності на тому чи іншому етапі, можливостям їх поєднань та комбінацій, способам переходу від одного методу до іншого.

ВИСНОВКИ

Конкретні критерії встановлюють стандарт, якому повинен відповідати кожен проект. Ці стандарти визначають, що має бути включено в проект, щоб зробити його безпечним. Кожен стандарт стосується конкретної мети, якої необхідно досягти. Основні заходи безпеки не потребують спеціального навчання. Натомість людям слід враховувати вартість виконання функціональних вимог, щоб вибрати рівень захисту. Середня вартість виконання транзакцій є відповідною базовою лінією. Люди можуть знайти це, поділивши загальну вартість на кількість виконаних функціональних вимог.

Оцінка ризику вимагає двох методів управління ризиком. Один випливає з ідеї «розумної достатності» при розгляді послуг ІБ.

Щоб правильно оцінити рівень загрози безпеці, ми повинні ранжувати кожну з них на основі її передбачуваної небезпеки. Цей процес вимагає розробки методу обробки кожної загрози для визначення ступеня захисту від них.

Через високий попит на експертів з кібербезпеки існує дефіцит фахівців із досвідом роботи з ІБ. Це пояснюється тим, що великомасштабні інциденти ІБ можуть розвинутися швидко, а рахунки можна оцінити за лічені хвилини. Спеціалізовані робочі місця важко заповнити через обмежену кількість здатних людей. Наразі аналітики ІБ повинні працювати регулярними змінами, щоб підтримувати надійну безпеку 24/7. Це пов’язано з тим, що їхня автономна система безпеки повинна мати можливість реагувати на кібератаки. Крім того, зловмисники можуть використовувати різні методи перед нападом, щоб відвернути увагу жертви. Це може включати запуск DDoS-атаки або сканування активної мережі жертви. Це розроблено, щоб допомогти слідчим шляхом автоматичного аналізу інцидентів і виконання завдань без втручання людини.

Він також може обробляти багато одночасних інцидентів, що дозволяє кіберекспертам відволіктися та не дати їм помітити майбутні атаки.

Сучасної літератури, присвяченої проблемі боротьби з загрозами комп'ютерної мережі, на сьогодні немає. Це означає, що для аналізу розглянутих методів використовуються сучасні методи виявлення та аналізу мережевих загроз. Підходи, зосереджені на моніторингу мережі ІБ, використовують статистичний аналіз для виявлення аномалій. Це робиться шляхом порівняння поточного мережевого трафіку з вимогами визначеного шаблону.

Кіберзагрози можна розділити на різні кластери за допомогою математичних моделей, які називаються кластерним аналізом. Ці моделі класифікують основні частини кіберзагрози та вказують її віддаленість від інших кластерів даних. Ця інформація використовується для визначення наявності кіберзагрози в організації.

Оскільки модель кінцевої стоми враховує лише кілька переходів між станами, вона точно показує поточний стан обробки даних через мережеві протоколи. Головною перевагою цієї моделі є її простота при визначенні критеріїв класифікації ІБ.

Моделі Маркова добре працюють під час пошуку аномалій, виявлених системними викликами операційної системи. Вони також вимагають використання додаткової статистики в системах квазіреального часу, які обчислюють час подібним чином. Теорія ігор передбачає наявність покупця і продавця; їх зв'язок розраховується в платіжній матриці.

Класифікація аномалій за допомогою таких методів, як виявлення кіберзагроз за допомогою нейронних мереж, вимагає використання IS. Це пояснюється тим, що функції розподілу пакетів даних допомагають їм ідентифікувати нормальну поведінку системи за допомогою навчання нейронної

мережі та аналізу подій на основі зразка, який використовується під час навчання.

Алгоритми самонавчання походять із вивчення таких предметів, як теорія графів, теорія ймовірностей, статистика та математика. Одним із прикладів цього є машинне навчання, яке знаходиться на перетині цих дисциплін.

Штучний інтелект можна використовувати для визначення класифікації для певного ризику. Це робиться через оцінку ймовірності та вирішення конкретного підвипадку класифікації. У класифікаційних завданнях учням надаються мітки та навчальні приклади, які вписуються в X і Y. Y — це мітка класу, тоді як X — це окремі ознаки об’єкта.

Будь-який процес класифікації повинен створити алгоритм, який відображає набір X на набір Y і зіставляє будь-який об’єкт із класифікаціями, знайденими в Y.

Щоб ідентифікувати ризики, необхідно проаналізувати та інтерпретувати їх основні ознаки за допомогою ітераційного процесу.

Управління ризиками та штучний інтелект тісно пов’язані. Досягнення штучного інтелекту можливо шляхом аналізу наборів даних історичних ризиків у певній галузі застосування. Шляхом пошуку аномалій у цих даних управління ризиками може визначити потенційні ризикові ситуації, ризики та їхні можливі наслідки. Це пояснюється тим, що аналіз ризиків шукає зв’язки та взаємодії між суб’єктами та об’єктами в даних. Аналіз ризиків також виявляє потенційні джерела майбутніх потенційних ризиків.

Як класичні методи, так і глибокі нейронні мережі можуть оцінити ймовірність виникнення ризику. Щоб визначити ймовірність виникнення ризику, вибирається оптимальна архітектура нейронної мережі для даних. Це можна зробити за допомогою обох пов’язаних нейронних мереж, наприклад

рекурентної або згорткової. Наприклад, це можна використовувати для оцінки ймовірності ризику, пов’язаного з підключеною нейронною мережею, яка використовує штучний інтелект.

Посібник з управління ризиками систем інформаційних технологій NIST, опублікований NIST SP800-30, є популярним і широко використовуваним методом оцінки управління ризиками. NIST 800-30 встановлює два основні критерії для визначення потенціалу загрози та ймовірності пошкодження даного об’єкта. Це називається методом оцінки ризику NIST.

Системи управління ризиками допомагають повсякденним операціям інтегрувати інформаційні технології, надаючи практичну інформацію.

Підхід CRAMM поєднує як кількісні, так і якісні методи оцінки ризику. Це загальний метод, який можуть використовувати державні та комерційні організації будь-якого розміру. Для різних типів організацій існують різні версії програмного забезпечення CRAMM. Ці конфігураційні файли змінюються залежно від цільового призначення програмного забезпечення. CRAMM має комерційну та державну версії. Державна версія цього профілю також підтримує аудит на відповідність стандартам US ITSEC («Помаранчева книга»)[8].

Методика OCTAVE (Operational Critical Threat, Asset and Vulnerability Assessment) була розроблена в Університеті Карнегі-Меллона (США) і передбачає оцінку критичності загроз, активів і вразливостей.

Цей метод використовується в усьому світі для проведення оцінки ризиків інформаційних систем і впровадження процесів управління ризиками в усій компанії. Існує багато модифікацій методу, призначених для організацій різного розміру та сфери діяльності [9].

В даний час для оцінки ризиків інформаційної безпеки використовується безліч різних методів та засобів. У них пропонуються різні способи зіставлення

можливої шкоди в результаті інцидентів інформаційної безпеки з ймовірністю реалізації загроз та отримання відповідних висновків, пропонуються різні шкали вимірювання рівня ризику. При цьому в дослідженнях, які вивчають та порівнюють ефективність цих методів у різних умовах, не береться до уваги важливий факт.

Оцінка інформаційних ризиків, незважаючи на наявні специфічні для неї нюанси в різних сферах діяльності, є упорядкованим процесом, що складається з одних і тих же етапів, на кожному з яких можуть бути застосовані свої методи та засоби. Тому першочергову увагу в дослідженнях такого роду слід приділяти не результативності методів взагалі, а їх ефективності на тому чи іншому етапі, можливостям їх поєднань та комбінацій, способам переходу від одного методу до іншого.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Биковська Д. Г. Визначення мережевих атак з використанням методів штучного інтелекту : дипломна робота на здобуття кваліфікаційного ступеня магістра : спец. 125 – кібербезпека / наук. керівник В. М. Пахомова ; Дніпров. нац. ун-т залізн. трансп. ім. акад. В. А. Лазаряна. Дніпро, 2020. 81 с.
2. Гладка Ю. А. Аналіз застосування технологій штучного інтелекту в кібербезпеці / Ю.А. Гладка, Є. О. Назаренко //Наукові праці Третьої міжнар. наук.-практ. конф.«Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 25–26 січня 2021 р.(Київ, Україна).–К.: НУХТ, 2021.–181 с.
3. Гончар С. Ф. Метод оцінювання ризиків кібербезпеки інформаційних систем SMART GRID / С.Ф.Гончар //Вчені записки ТНУ імені ВІ Вернадського. Серія: Технічні науки 31.70. - 2020. С. 97-101.
4. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. – Київ: ДП "УкрНДНЦ", 200.335. – 60 с.
5. Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій (Guide for Conducting Risk Assessments. National Institute of Standards and Technology) [Текст]. – Gaithersburg: National Institute of Standards and Technology, 200.332. – 95 с.
6. Кожокар В. Структурні закономірності еволюціонування метаморфного шкідливого ПЗ/ Кожокар В.Ю., Стьопочкіна І.В. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.- 2017, №1(33).-С.52-57.

7. Кожокар В.Ю.. Виявлення спільних закономірностей у зразках метаморфного шкідливого ПЗ на основі статичних характеристик./Кожокар В.Ю., Стьопочкіна І.В .// XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених “Теоретичні і прикладні проблеми фізики, математики та інформатики” 25-27 травня 2017, т.2.

8. Кушнарьов В.В. Національна система кібербезпеки України: виклики та кіберзагрози // *Р*едакційна колегія. - 2022. - №29

9. Методи штучного інтелекту в кібербезпеці [Електронний ресурс] : навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: І.В. Стьопочкіна, О.М. Новіков. – Електронні текстові дані (1 файл: 19,9 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022 – 82 с.

10. Осадчий В. И. Искусственный интеллект и алгоритмы машинного обучения для оценки достоверности научной статьи в Scopus: опыт переводчика : [презентация]. University Library at a New Stage of Social Communications Development : матеріали VII Міжнар. конф., (м. Дніпро, 06.10–07.10.2022 р.). Дніпро, 2022. URL: http://conflib.diit.edu.ua/Conf_univ_Library_2022/paper/view/26788.

11. Пахомова В. М. Дослідження двох підходів до виявлення мережних атак із використанням нейромережної технології/ Пахомова В. М., Коннов М. С.// Наука та прогрес транспорту. 2020. № 3(87). С. 81-93. DOI: 10.15802/stp2020/208233

12. Пахомова В. М. Можливості розвитку комп’ютерних мереж у автоматизованих системах залізничного транспорту: монографія / Пахомова В. М. Дніпро: Дніпропетр. нац. ун-т залізн. трансп. ім. акад. В. Лазаряна. - 2015. - 207 с.

13. Пахомова В. М. Теорія проектування комп’ютерних мереж: методичні вказівки до виконання курсового проект /Пахомова В. М. Дніпровск. нац. ун-т залізн. трансп. ім. акад. В. Лазаряна. - 2019. -60 с.

14. Прищепенко Я. С. Комп'ютерна кібербезпека з використинням штучного інтелекту //Diss. ФОП Петров ВВ, 2021.

15. Прямухіна О. М. Напрямки застосування технологій штучного інтелекту/Прямухіна О.М., Потапова А.Н // Прикладні аспекти сучасних міждисциплінарних досліджень. - 2021. С. 111-113.

16. Радутний ОЕ Кримінально-правові аспекти кібербезпеки ризикової діяльності під керуванням штучного інтелекту/ОЕ Радутний//Кібербезпека в Україні: правові та організаційні питання: матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 17 листопада 2017 р.).–Одеса: Одеський державний університет внутрішніх справ, 2017. С. 45-47., 2017.

17. Риндич Є. В. Особливості створення мережевої системи виявлення вторгнень у комп’ютерні системи /Риндич Є. В., Зайцев В. В., Коняши С. В., Усов Я. Ю. // Математичні машини і системи. - 2018. - № 3. - С. 89-96.

18. Скачек Л. М. Цінінсть інформації в інформаційній безпеці [Текст] / Л. М. Скачек. // Інформаційна безпека. – 200.333. – №0.33(9). – С. 352–354.

19. Соколовська А. А.Протидії штучного інтелекту кіберзагрозам / Соколовська А. А., А. О. Плакса, and Я. Ю. Усов. -2019.

20. Солдатова М.О. Перспективи використання штучного інтелекту в кібербезпеці / М.О.Солдатова // The 9 th International scientific and practical conference “Innovations and prospects of world science”(April 28-30, 2022) Perfect Publishing, Vancouver, Canada. 2022. 724 p.. 2022.

21. Терейковський І. Вдосконалення алгоритму навчання багатошарового перспетрону, призначеного для розпізнавання мережевих атак/І.Терейковський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». - 2012. - № 2. - 6 с.

22. Устенко С.В. Система управління кібербезпеки банків з використанням засобів штучного інтелекту / Устенко С.В. Остапович Т. В. - 2020.

23. Федоренко О.А. Використання технологій штучного інтелекту для виявлення та припинення кіберзагроз/ О.А. Федоренко. - 2021.

24. Цяпа С. М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах /С.М.Цяпа // Інформація і право. -2021. № 2 (37). С. 51-59.

25. Шевченко А.С. Аналіз застосування штучних нейронних мереж у задачах виявлення кіберзагроз/ Шевченко А.С, Самойлов І.В, Пономарьов О.А, Науменко О.Г // Збірник наукових праць ВІТІ0 2238, № 60 С. 363–368.

26. Шостак О. С. Застосування штучного інтелекту у забезпеченні безпеки даних / О.С.Шостак// Реалізація наукового потенціалу студента вищої школи: виклики, перспективи, напрями. -2021. -354 с.

27. Яровенко Г. М. Перспективи застосування технології блокчейн у системах забезпечення кібербезпеки банків / Яровенко Г. М., В. О. Ковач // Підприємництво та інновації. - 2020. -№ 12.С. 206-214.

28. Amit I., Matherly J., Hewlett W., Xu Z., Meshi Y., Weinberger Y. (2018) 'Machine Learning in Cyber-Security – Problems, Challenges and Data Sets', The AAAI-19 Workshop on Engineering Dependable and Secure Machine Learning Systems, 8 p.

29. Cyber risk in retail: Protecting the retail business to secure tomorrow's growth [Електронний ресурс]. – 200.337 – Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/us-risk-200.337-retail-cyber-risk-report-04070.335.pdf

30. Cyber security concerns in the retail sector [Електронний ресурс]. – 200.337 с.

31. Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust [Електронний ресурс] // Symantec White Paper. – 200.335. – Режим доступу до ресурсу: https://www.symantec.com/content/dam/symantec/docs/white-papers/cybersecurity-retail-en.pdf.

32. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [Текст] / R. A.Caralli, J. F. Stevens, L. R. Young, L. R. Wilson.– Бостон: Університет Карнегі-Меллон, 2007. – 354 с.

33. Security trends in the retail industry [Електронний ресурс]. – 2009. - 336 с. – Режим доступу до ресурса: https://www.ibm.com/downloads/cas/DO8MZRV9

34. Tsukerman E. (2019) Machine Learning for Cybersecurity Cookbook [e-book], Birmingham: Packt Publishing, 348 p.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту

Автор: Дацко Богдан Вікторович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Касянчук Михайло Миколайович, д.т.н, професор
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 88,2%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 94%.

Згідно з Положенням про дотримання академічної доброчесності в Хмельницькому національному університеті (http://www.khnu.km.ua/root/files/01/10/03/0005.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 80-100 %, визнається роботою з достатньою унікальністю тексту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 11.8%, з яких 8% є збігами з одним джерелом, зумовленими проведенням аналізу існуючих рішень з запозиченням матеріалу з цього джерела,наявністю типових фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.
2. Інші три збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань.

Керівник роботи _____ М. М. Касянчук

Завідувач кафедри КбКСМ _____ Ю. П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Магістр Дацко Богдан Вікторович

Тема: Метод оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту

Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека денної форми навчання

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень 12 ; кількість сторінок записки 115;

1. Короткий зміст ДР та прийнятих рішень В рамках роботи проведено дослідження та розробка оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту. В роботі поставлено і вирішено задачі: здійснити аналіз методів оцінювання ризиків безпеки інформаційної системи, систем штучного інтелекту в системах захисту інформації, системи штучного інтелекту для моделювання загроз безпеки інформаційної системи; охарактеризувати моделі кіберзагроз в системах захисту інформації (статистичну модель, кластерний аналіз, модель кінцевих автоматів, марківська модель, метод «теорії ігор», метод використання нейронних мереж, переваги та недоліки евристичних методів), дослідити метод машинного навчання, поняття та класифікація алгоритмів кластеризації методів машинного навчання; провести оцінку ризиків безпеки інформаційної системи, визначити керування ризиками з використанням методу штучного інтелекту, визначити метод оцінювання ризиків безпеки інформаційної системи із застосуванням системи штучного інтелекту; дослідити використання методу оцінювання ризиків інформаційних систем в кібербезпеці, використання методу оцінювання ризиків інформаційних систем при виявленні атак і способів їх подолання, дати рекомендації щодо попередження ризиків інформаційних систем з використанням системи штучного інтелекту.

2. Висновок про відповідність М Р завданню Магістерська робота у достатній мірі відповідає поставленому завданню як у теоретичній і практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми дослідження; її зв'язок із науковими програмами, планами, темами та формулюється мета і основні завдання дослідження. У першому розділі було проведено аналіз методів оцінювання ризиків безпеки інформаційної системи та систем штучного інтелекту при реалізації заходів інформаційної безпеки. У другому розділі описано модель оцінювання ризиків безпеки інформаційної системи із застосуванням системи штучного інтелекту. У третьому розділі уточнено метод оцінювання ризиків безпеки інформаційної системи із застосуванням системи штучного інтелекту. У четвертому розділі роботи практичне застосування методів вирішення ризиків безпеки інформаційної системи.

4. Позитивні сторони проекту полягають в розширенні знань про використання штучного інтелекту в кібербезпеці, а саме реалізація методу оцінки ризиків інформаційної системи

5. Негативні сторони проекту : У роботі недостатньо приділено увагу формулюванню визначень понятійного апарату дослідницької роботи, математичної та експерементальних моделей. Робота носить більше аналітичний характер і не має чітко визначених практичних результатів

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми дипломної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам .

7. Відгук про роботу в цілому В загальному дипломна робота заслуговує позитивної оцінки.

8. Інші зауваження

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що дипломна робота заслуговує оцінки «задовільно ».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Гідченко Сергій Костянтинович, д.т.н., завідувач кафедри телекомунікаційних медійних та інтелектуальних технологій

« 7 » 12 2022 . (підпис)

ХНУ. Зам. 54, тир. 6000, 2022.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Дацко Богдана Вікторовича
ПІБ здобувача вищої освіти
студента ФІТ, 2 курсу, групи КБм-21-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

5.12.2022
дата

підпис

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 6.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 7%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 109162 Название: Метод оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту Добавлено в БД: 2022-12-09 Авторы: Дацко Б.В. Руководители: Касянчук М.М. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	146555	1126	10600 (7%)	104 (9%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1013253196

Дата перевірки:
09.12.2022 10:23:11 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
09.12.2022 10:26:19 EET

ID користувача:
100008300

Назва документа: **Магістерська Дацко КБ**

Кількість сторінок: **111** Кількість слів: **20622** Кількість символів: **162303** Розмір файлу: **1,012.29 KB** ID файлу: **1013011666**

11.8%
Схожість

Найбільша схожість: **8.08%** з Інтернет-джерелом (https://learn.ztu.edu.ua/pluginfile.php/200479/mod_resource/content/.

11.6% Джерела з Інтернету	83	Сторінка 113
0.69% Джерела з Бібліотеки	10	Сторінка 114

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	33

challenges for search based software testing. *8th International Conference on Software Testing, Verification and Validation (ICST)*. IEEE, 2015. P. 1-12.

9. Does the fault reside in a stack trace? Assisting crash localization by predicting crashing fault residence / Yongfeng Gu and ets. *Journal of Systems and Software*. 2019. № 148. P. 88-104.

ДАЦКО Богдан,
студент групи КБм-21-1,
ПАХАР Олександр,
студент групи КБм-21-1,
Хмельницький національний університет
Науковий керівник: ***ЧЕШУН В.М.****, канд. техн. наук, доцент,*
доцент кафедри кібербезпеки

УМОВИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ КРИПТОГРАФІЧНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Сучасна криптографія надає всі необхідні алгоритми, методи й засоби, які дозволяють побудувати систему захисту, витрати на злом якої такі, що в супротивника з обмеженими фінансовими й технічними можливостями для одержання інформації, що його цікавить, залишаються тільки два варіанти – використання або людського фактору, або особливостей конкретної реалізації криптоалгоритмів і криптопротоколів [1]. Саме такий висновок можна зробити, аналізуючи приклади реальних успішних атак на криптосистеми. Відомі лише одиничні випадки злому з використанням винятково математичних методів. У той же час, різних прикладів зломів реальних систем так багато, що їхнім аналізом змушені займатися цілі компанії, найбільш відома з яких Counterpane Systems Б. Шнайера [2].

Система захисту в цілому не може бути надійнішою окремих її компонентів. Іншими словами, для того, щоб перебороти систему захисту, досить зламати або використати для злому найненадійніший з її компонентів. Типові помилки користувачів, що порушують безпеку системи захисту [1; 2], наступні:

– надання свого секретного пароля колегам по роботі для вирішення невідкладних завдань під час відсутності власника пароля;

– повторне використання секретних паролів у несекретних системах;

– генерація паролів самими користувачами, вибір паролів за критерієм зручності запам’ятовування;

– несвоєчасне інформування про компрометацію ключової інформації, наприклад, про втрату смарт-карт.

Одержують поширення атаки типу відмова в обслуговуванні (denial of service) [2], що провокують користувача відключати систему захисту, при вирішенні невідкладних завдань. Можна виділити наступні причини ненадійності криптосистем, пов’язані з особливостями їхньої реалізації:

– застосування нестійких криптоалгоритмів;

– неправильне застосування криптоалгоритмів;

– помилки в реалізації криптоалгоритмів.

У деяких випадках, особливо в системах реального часу, застосування стійких алгоритмів принципово неможливе через їх низьку швидкодію й тому вимушено використовуються менш стійкі, але швидкі криптоалгоритми [3].

Багато якісних криптографічних засобів підпадають під дію експортних обмежень, що штучно знижують якість цих засобів [2]. Наприклад, у США заборонений експорт симетричних криптоалгоритмів з довжиною ключа більше 56 біт. Всі програмні засоби, зроблені в США й легально експортовані за кордон, забезпечують ослаблений криптографічний захист. Аналогічна ситуація має місце й у Європі. Так, наприклад, існує дві версії алгоритму потокового шифрування A5 (стандарт GSM) – надійна A5/1 і істотно менш стійка A5/2 для поставок у країни, що розвиваються.

Багато розроблювачів ПЗ включають у свої продукти власні криптографічні алгоритми, самовпевнено вважаючи себе фахівцями, забуваючи, що сучасна криптографія, заснована на глибоких дослідженнях у таких розділах математики, як вища алгебра, теорія чисел, теорія інформації, теорія складності обчислень та ін. Якщо розроблювачі роблять ставку на власні методи, шанси зломщиків, навіть у випадку повної відсутності на початковому етапі інформації про використаний алгоритм, багаторазово зростають.

Основними помилками при застосуванні криптографічних алгоритмів [3; 4] є: недостатня довжина ключа, неякісна процедура керування ключами, неякісний генератор ПВЧ або неправильна його ініціалізація; використання криптографічних алгоритмів не за призначенням (наприклад зберігання паролів у зашифрованому, а не в хешованому вигляді, і використання на практиці моделі довірчих відносин, відмінної від тої, на яку проектувалася система).

Помилки в реалізації криптоалгоритмів як причина ненадійності криптосистем у силу своєї нетривіальності й різноманіття вимагає окремого розгляду, тому обмежимося лише коротким перерахуванням основних проблем.

Надійна система захисту повинна вміти оперативно виявляти несанкціоновані дії для мінімізації можливого збитку. У випадку виявлення ушкоджень у системі повинні включатися ефективні процедури відновлення зруйнованих елементів. Система не повинна втратити живучість навіть у випадку проведення успішної атаки на неї. Причини наявності більшості «дір» (або люків) у ПЗ, тобто не описаних у документації можливостей роботи з ними, очевидні: безпам’ятність розроблювачів, які в процесі налагодження продукту створюють тимчасові механізми, що полегшують її проведення (наприклад, за рахунок прямого доступу до відлагоджуваних частин програми). По закінченні налагодження частина «дір» прибирається, а про частину розроблювачі благополучно забувають або залишають їх свідомо, особливо в ранніх версіях продукту, коли в майбутньому досить імовірна його доробка.

«Діри» можуть бути наслідком застосування технології розробки програм «зверху вниз», коли програміст відразу приступає до написання керуючої програми, заміняючи передбачувані в майбутньому підпрограми «заглушками», що імітують реальні підпрограми або просто позначають місце їхнього майбутнього приєднання. Дуже часто ці «заглушки» залишаються в кінцевій

версії програми – або знову ж через безпам'ятність, або розраховуючи на майбутню модифікацію продукту, або, наприклад, якщо в процесі розробки з'ясовується, що якась підпрограма не потрібна, а видалити заглушку неможливо. У випадку виявлення такої заглушки зловмисник може скористатися нею для підключення до програми своєї підпрограми, що працює аж ніяк не в інтересах законного користувача. Третє джерело «дір» – неправильна обробка (або її відсутність) яких-небудь нестандартних ситуацій, які можуть мати місце при роботі програми: невизначене уведення, помилки користувачів, збої і т.п. У цьому випадку супротивник може штучно викликати в системі появу такої нестандартної ситуації, щоб виконати потрібні йому дії. Наприклад, він може викликати аварійне завершення програми, що працює в привілейованому режимі, щоб, перехопивши керування, залишитися в цьому привілейованому режимі. Нарешті, відомі випадки, коли люк у ПЗ або апаратурі – перший крок до атаки системи безпеки. Розроблювач навмисне залишає його в кінцевому продукті, щоб у майбутньому, наприклад, мати можливість модифікувати інформацію непомітно для законного користувача, розшифровувати її, не знаючи ключа тощо.

Апаратуру легше фізично захистити від проникнення ззовні. Криптомодулі можуть поміщатися в особливі контейнери, які унеможливлюють зміну алгоритму функціонування. Інтегральні схеми можуть покриватися спеціальним хімічним складом, при цьому будь-яка спроба подолання захисного шару приводить до самознищення їх внутрішньої логічної структури. Проте відомі випадки виявлення й апаратних закладок. Крім того, виникає проблема захисту від екзотичних атак, застосовних до реалізацій в smart-картах, тимчасового аналізу й аналізу споживаної потужності. Ці атаки засновані на використанні того факту, що різні операції, виконувані на мікропроцесорі, вимагають різного часу, а також приводять до різного споживання потужності. Загальна ідея цих атак у тому, що, аналізуючи тимчасові характеристики алгоритму (час відповіді) або споживання потужності, ми можемо скласти картину виконання різних операцій і навіть приблизно обчислити їхні аргументи.

Приблизний аналіз уразливості різних операцій з погляду тимчасових характеристик дає наступні результати:

- пошук за таблицями – невразливий для тимчасових атак;
- фіксовані зсуви – невразливі для тимчасових атак;
- булеві операції – невразливі для тимчасових атак;
- додавання/віднімання – важко захистити від тимчасових атак;
- множення/ділення – найбільш уразливі для тимчасових атак операції.

Стійкість до атак, спрямованих не на криптоалгоритм, а на його реалізацію, також необхідно враховувати. Захищеність стосовно часового аналізу можна підвищити введенням додаткових затримок. Більш складною є проблема захисту від аналізу потужності, але її можна вирішити декількома шляхами: балансуванням алгоритму (рівномірний розподіл різних операцій по коду), введенням спеціальних «шумових» операцій або вибором іншого процесора.

Останнім часом одержали поширення атаки на апаратуру криптосистем,

засновані на аналізі електромагнітного випромінювання й інших побічних джерел інформації [4]. Одержують поширення також «біологічні» за суттю методи злому, що розглядають криптосистеми як складні об'єкти, певним чином реагуючі на зовнішні подразники [3]. Атаки подібного роду засновані на аналізі поводження системи після випадкових або навмисних збоїв у роботі.

Незважаючи на успіхи сучасної криптографії, завдання побудови надійної системи криптографічного захисту комплексне, воно значно складніше, ніж здається на перший погляд. Надійна система захисту може бути побудована тільки з урахуванням всіх перерахованих факторів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тарнавський Ю. А. Технології захисту інформації : підручник. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.

2. Грицак А. В. Методи побудови ефективних криптографічних функцій гешування : дис. … канд. техн. наук : 05.13.21. Київ, 2020. 128 с.

3. Кушнерик О. О., Джулій В. М. Дослідження та класифікація основних типів загрозливих програм. *Інтелектуальний потенціал – 2018* : збірник наукових праць молодих науковців і студентів. Хмельницький, 2018. Ч. 3. С. 67-70.

4. Комаров М. Ю. Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури : дис. … канд. техн. наук : 05.13.05. Київ, 2021. 171 с.

ЗАКРУЖЕЦЬКИЙ Євгеній,
студент групи ІПЗм-31,
Університет економіки і підприємництва
Науковий керівник: ***ЧЕШУН В.М.****, канд. техн. наук, доцент,*
доцент кафедри вищої математики та інформатики

ЛОГІКА ВИСЛОВЛЮВАНЬ І ФУНКЦІЙ ЛОГІЧНИХ ЕЛЕМЕНТІВ

На сьогоднішній день в термінології, що використовується при описі функцій логічних елементів різними авторами, відслідковується неоднозначність. Так, зокрема, елемент кон'юнкції (логічного множення) визначають як елемент «І» [1; 2] або елемент «ТА» [3]. Це обґрунтовується, як правило, тим, що ці слова в українській мові є рівноправними і рівнозначними. Елемент інверсії (логічного заперечення) визначають як елемент «НЕ» [1] або елемент «НІ» [2; 3], що в українській мові є відображенням різновидів заперечення.

Зазначимо, що проблема неоднозначності термінології виникла, в основному, завдяки необдуманому використанню програм-перекладачів з російської мови на українську. В той же час, правила правопису української мови, на яких базуються (до речі, не завжди вдало) програми-перекладачі, не завжди підходять для застосування в математичній логіці, адже ця наука не припускає двозначності трактування висловлювань.