Міністерство освіти і науки україни
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 «Кібербезпека»*
(код і назва напряму підготовки)

освітній рівень ***магістр***
(назва освітнього рівня)

Кваліфікація
(код і назва кваліфікації)

на тему: Розробка елементів системи підтримки прийняття рішень про захищеність інформаційних систем

Виконавець: студент 2 **курсу, групи** КБм-11

(підпис) **Гречко Вікторія Володимирівна** (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Бабенко Т.В.		
Рецензент			
Нормоконтроль			

КИЇВ
2021

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації
_____ Лукова-Чуйко Н.В.
«____» _____ 2021 року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 «Кібербезпека»*
(код і назва спеціальності)

студентці ***КБм-21*** ***Гречко Вікторії Володимирівні***
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи *Розробка елементів системи підтримки прийняття рішень про захищеність інформаційних систем*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 2 від 08.10.2020

2. ВИХІДНІ ДАНІ ДО РОБОТИ

Об'єкт досліджень *процес оцінювання рівня захищеності інформаційної системи.*

Предмет досліджень *елементи системи підтримки й прийняття рішень щодо захищеності інформаційних систем.*

Мета *розробка інтелектуальних моделей оцінки зрілості процесів системи управління інформаційної безпеки*

Вихідні дані для проведення роботи

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *вперше розроблено модель зрілості процесів СУІБ відповідно до вимог та рекомендацій стандартів ISO/IEC 27001:2017 та ISO/IEC 27001:2017 з використанням апарату нейронних мереж прямого поширення сигналу та зворотнього поширення похибки.*

Практична цінність *полягає у розроблених інтелектуальних моделях оцінки зрілості процесів СУІБ, які можуть бути застосовані як елементи СППР, що дозволить скоротити часові та фінансові витрати ресурси підприємства на проведення оцінки захищеності ІС.*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	12.10.2020 – 18.10.2020
Аналіз літератури	19.10.2020 – 10.12.2020
Виконання порівняльного аналізу моделей зрілості у сфері ІБ	21.12.2020 – 12.01.2021
Визначення базової парадигми моделі оцінювання	13.01.2021 – 26.01.2021
Розробка алгоритму попередньої підготовки даних	27.01.2021 – 20.02.2021
Підготовка даних для моделювання	21.02.2021 – 10.04.2021
Синтез моделі зрілості СУІБ з визначенням відповідності досліджуваної ІС на відповідність вимогам стандарту ISO/IEC 27001:2017 з використанням технологій штучного інтелекту та її навчання;	11.04.2021 – 16.04.2021
Аналіз адекватності розробленої моделі	17.04.2021 – 07.05.2021
Оформлення пояснювальної записки	08.05.2021 – 10.05.2021
Підготовка до захисту дипломної роботи	11.05.2021 – 17.05.2021

5. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект

Соціальний ефект _____

_____

7. ДОДАТКОВІ ВИМОГИ

_____

_____

_____

Завдання видав	_____	Т.В. Бабенко _____
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	В.В. Гречко _____
	(підпис)	(ініціали, прізвище)

Дата видачі завдання:_____

Термін подання дипломної роботи до ЕК _____

ЗМІСТ

ВСТУП

Діяльність будь-якого підприємства спрямована, в першу чергу, на отримання прибутку. На досягненні цієї мети сфокусовані основні бізнес-процеси організації. Також існує ряд підтримуючих процесів, до яких відносяться інформаційні технології (ІТ) та інформаційна безпека (ІБ), які спрямовані на забезпечення інфраструктури для функціонування основних процесів. Логічно припустити, що керівництво підприємства зацікавлене в тому, щоб процеси всередині організації були їм підконтрольні, функціонували так, як були задумані, а кількість помилок або зловмисних дій з боку співробітників організації, бізнес-партнерів, а також інших сторін, залучених в бізнес-процеси організації, була мінімальною.

Постановка завдання щодо впровадження та просування будь-якого процесу управління в організації повинна відповідати рівню організаційного та технологічного розвитку підприємства, і зокрема, процесів забезпечення ІБ. Вибір інструментів управління також залежить від організаційних рішень, прийнятих на основі прийнятності ризиків, варіантів управління ризиками та загального підходу до управління ризиками відповідно до національних та міжнародних норм. Вимоги до реалізації заходів з безпеки повинні формулюватися з урахуванням рівня зрілості цих процесів в конкретній організації.

Тому дуже важливим моментом є вибір організацією власних інструментів управління та вимог безпеки. Є три основні джерела для їх визначення:

1. Оцінка ризиків на основі загальної бізнес-стратегії та цілей організації;
2. Правові, нормативні, договірні або законодавчі вимоги;
3. Принципи, цілі та вимоги до бізнесу щодо обробки, обробки, зберігання, передачі та архівування інформації.

Для визначення стадії організаційного та технологічного розвитку організації та її процесів у світовій практиці існує поняття «модель зрілості».

Модель зрілості можливостей кібербезпеки забезпечує орієнтир, за допомогою якого організація може оцінити поточний рівень зрілості своїх практик, процесів та встановити цілі та пріоритети для вдосконалення кібербезпеки

Метою даної роботи є розробити інтелектуальні моделі оцінки зрілості процесів системи управління ІБ (СУІБ), які можуть бути застосовані як елементи системи підтримки прийняття рішень (СППР), що дозволить скоротити часові та фінансові витрати ресурсів підприємств на проведення оцінки захищеності ІС.

Для достягнення поставленої мети у роботі необхідно виконати низку завдань:

1. Виконати порівняльний аналіз моделей зрілості у сфері ІБ;
2. Визначення базової парадигми моделі оцінювання;
3. Розробка алгоритму попередньої підготовки даних;
4. Підготовка даних для моделювання;
5. Синтезувати модель зрілості СУІБ з визначенням відповідності досліджуваної ІС на відповідність вимогам стандарту ISO/IEC 27001:2017 з використанням технологій штучного інтелекту та здійснити її навчання;
6. Провести аналіз адекватності розробленої моделі.

Об’єктом даної роботи є процес оцінювання рівня захищеності (ІС).

Предметом дослідження виступають елементи СППР щодо захищеності ІС.

У рамках даного дослідження були використані наступні методи: вивчення та аналіз наукової літератури; системний і порівняльний аналіз; моделювання; методи штучного інтелекту, системний аналіз, статистичні методи .

Наукова новизна дослідження в тому, що:

- вперше розроблено модель зрілості процесів СУІБ відповідно до вимог та рекомендацій стандартів ISO/IEC 27001:2017 та ISO/IEC

27001:2017 з використанням апарату нейронних мереж прямого поширення сигналу та зворотнього поширення похибки, що дозволяє знизити навантаження на експерта за рахунок автоматизації розв'язуваних їм завдань.

Практична значущість роботи полягає в тому, що результати можуть бути застосувані в діяльності конкретної установи для вдосконалення системи оцінювання захищеності ІС; запропонований метод дозволяє автоматизувати рішення задач, оцінювання відповідності ІС вимогам безпеки та прийняття рішення щодо його використання, що покладаються на експерта.

Апробація роботи. Основні положення та результати роботи були представлені в наступних виданнях: IEEE 5th World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4 2021, London), VII International conference on Information Technology and Interactions (IT&I-2020, Kyiv), IEEE International Scientific-Practical Conference on Problems of Infocommunications, Science and Technology (PIC S&T 2019, Kyiv)

Структура та об’єм роботи. Дана робота складається включає в себе вступ, 3 розділи, висновок, список літератури. Загальний обсяг роботи 101 сторінка.

РОЗДІЛ 1
АНАЛІЗ ЛІТЕРАТУРНИХ ДАНИХ І ПОСТАНОВКА ПРОБЛЕМИ ДОСЛІДЖЕННЯ

1.1. Сучасні підходи до забезпечення інформаційної безпеки

Діяльність будь-якого підприємства спрямована, в першу чергу, на отримання прибутку. На досягненні цієї мети сфокусовані основні бізнес-процеси організації. Логічно припустити, що керівництво підприємства зацікавлене в тому, щоб процеси всередині організації були їм підконтрольні, функціонували так, як були задумані, а кількість загроз та помилок були мінімальними, адже у разі успішної реалізації загроз можливий виток, пошкодження або неправомірна модифікація інформації, що може призвести до фінансових і репутаційних збитків.

Під загрозами будемо розуміти потенційну небезпеку для інформації або системи. Загрозою є наявність певної уразливості, яка може бути використана проти компанії або людини. При цьому те, що дає можливість використання уразливості, називається джерелом загрози.

Уразливість – це недолік в програмному забезпеченні, устаткуванні або процедурі, який може надати зловмиснику можливість доступу до комп'ютера або мережі, а отже і до інформаційних ресурсів компанії.

Ризик – це вірогідність того, що джерело загрози скористається уразливістю, що приведе до негативної дії на бізнес [1]. Ризик можна розрахувати як добуток виникнення загрози (очікувані події / рік) та збитку у визначеній валюті. Існують різні типи збитків:

- Іміджевий - наприклад, коли партнери в ланцюгу постачання мали витік інформації про приватних клієнтів.

- Нормативні штрафи - цей вид збитків може виникнути, наприклад, коли лікарня не виконує вимоги федерального Закону про переносимість та підзвітність медичного страхування (HIPAA), і конфіденційність інформації про пацієнтів зменшується.
- Виробничі втрати через порушення цілісності IT-ресурсів, що підтримують виробництво. Існує також важливе питання, яке слід врахувати при моделюванні загроз.

Актив – це інформація або ресурси, які потребують захисту.

Дія – це щось, що призводить до втрат у зв'язку з діями джерела загрози. Уразливості впливають на компанію, призводячи до можливості нанесення їй збитку.

Для забезпечення належного рівня захисту власних активів підприємство реалізує контрзаходи. Контрзаходи – це такі заходи, впровадження яких дозволяє понизити рівень потенційного ризику, а отже збитків.

На рис. 1 представлений взаємозв’язок даних визначень.

Рисунок 1.1 - Ризик-орієнтований підход у побудові СУІБ

Типи контрзаходів можуть значно відрізнятися. Деякі контрзаходи покликані обмежити фізичний доступ. Сюди входять системи введення паролів, сканування сітківки або відбитків пальців та озброєні охоронці. Інші контрзаходи призначені для блокування доступу та/або захисту конфіденційності даних в мережах, що обслуговують організацію. Сюди можуть входити фаерволи, шифрування даних, антивіруси та сканери на шпигунське програмне забезпечення. Крім того, деякі контрзаходи розроблені для швидкого відновлення у разі успішного вторгнення, наприклад, резервне копіювання.

Підвищення ефективності оперативного та стратегічного управління розвитку інформаційних систем, вимагає спеціалізованого аналітичного апарату для прийняття управлінських рішень [1]. Особливістю предметної області даної проблеми є складність її формалізації, наявність невизначеностей, пов’язаних з неповнотою даних, циклічність та сезонність досліджуваних процесів, наявність значної кількості взаємопов’язаних, а не лише кількісних, але також якісні показники, що їх описують.

Тому для успішного забезпечення інформаційних ресурсів необхідно не тільки результативно управляти функціональними ресурсами, а й створювати ефективні системи управління інформаційної безпеки (СУІБ). Оскільки об’єкти управління – СУІБ є досить складними організаційно-технічними структурами, що функціонують в умовах невизначеності, ефективне управління подібними системами повинно базуватися на інтеллектуальних системах підтримки прийняття рішень в питаннях ІБ та КБ.

Одним з варіантів вирішення даної проблеми є застосування систем підтримки рішень (СПР) з управління КБ на основі інтелектуальних інформаційних технологій (ІІТ).

1.2. Теоретичні засади розробки системи підтримки прийняття рішень про захищеність ІС

За оцінкою Gartner, витрати на системи інформаційної безпеки і управління ризиками у 2022-му році збільшаться до $ 174 млрд, з них приблизно $ 50 млрд будуть спрямовані на захист клієнтських систем. Продажі хмарних платформ і додатків для забезпечення безпеки виростуть до $ 1,63 млрд в 2023-му році, а систем забезпечення безпеки додатків до $ 4,5 млрд. Зростає і ринок послуг в області інформаційної безпеки, за останній рік він збільшився з $ 62 млрд до $ 66,9 млрд. Однак самі по собі гроші не можуть вирішити питання. Більшість фахівців з інформаційної безпеки сьогодні перевантажені аналізом журналів, запобіганням спроб злому, розслідуванням можливих випадків шахрайства і т.д. Дефіцит кадрів великий, тому в індустрії безпеки все з більшою надією дивляться на рішення в області штучного інтелекту. За оцінкою MarketsandMarkets, в 2019-2026 рр. зростання ринку засобів ШІ для забезпечення кібербезпеки буде рости в середньому на 23,3% в рік, з $ 8,8 млрд до $ 38,2 млрд

Зростання кількості кіберзагроз ОБІ викликало сплеск досліджень в області розробки математичних моделей для СПР [3, 4] та експертних систем (ЕС) [5, 6] з питань інформаційної безпеки та захисту інформаці. Аналіз літературних джерел показав, що в основному пропоновані моделі не доведені до працездатних програмних продуктів і демонструються виключно як формальні математичні моделі.

Поточні звіти про кібербезпеку спонукають до розробки нових технологій, які можуть збільшити розуміння людиною та здатність приймати рішення для створення обізнаності про ситуацію в кіберсередовищах [7].

Тим не менше, багато існуючих інструментів та підходів до безпеки зосереджені на рівні системи та додатків[8]. З цієї причини аналітикам безпеки потрібні більш сучасні систематичні методи кількісної оцінки мережевих вразливостей, прогнозування ризику атаки та потенційних

наслідків, оцінки належних дій для мінімізації збитків бізнесу та забезпечення успіху місії у ворожому середовищі. Як наслідок, показники безпеки мають головне значення для поінформованості про безпеку в контексті, координованого захисту мережі та аналізу забезпечення місії. Вони можуть забезпечити краще розуміння адекватності засобів контролю безпеки та допомогти аналітикам з питань безпеки ефективно визначити, на які найважливіші активи слід зосередити свої обмежені ресурси для забезпечення успіху місії [9].

В роботах [10, 11] зазначено, що існуючі стандарти в області менеджменту ІБ не формують конкретних підходів до управління кібербезпекою ОБІ, а це ускладнює процедури проектування працездатних програмних продуктів, які дозволяють адекватно оцінювати ступінь захищеності ОБІ.

Проведення аналізу сучасних методів та засобів забезпечення кібербезпеки є дуже трудомістким та часто неефективним через різні сфери використання. В зв’язку з цим стає актуальним перехід до методів та засобів з використанням інтелектуальних технологій через їх адаптивність та здатність діяти зі слабоструктурованими и погано формалізованими даними.

Сучасні системи підтримки прийняття рішення виникли як природний розвиток і продовження управлінських інформаційних систем. СППР є інструментом, що допомагає особам, що приймають рішення (ОПР) вирішувати багатокритеріальні управлінські задачі та приймати рішення на основні моделей, в тому числі з використанням слабоструктурованих або неструктрурованих вхідних даних.

Зміст СППР визначається змістом задач, на вирішення яких вона спрямована, вхідними даними базами знань та рівнем можливостей та знань користувачів. Однак важливо зауважити, що СППР лише підтримують ОПР, а не замінюють, вироблення рішень. СППР у загальному випадку властиві наступні характеристики:

- здатність оперування слабоструктурованими рішеннями;

- розрахована на ОПР різної кваліфікації;
- здатність бути використаною як для групового, так для індивідуального використання;
- підтрика послідовних та взаємозалежних рішень;
- можливість вибору різних методів для вирішення задач;
- гнучкість та масштабованість;
- адаптивність;
- та легке використання;
- покращення ефективності прийняття рішень;
- підтримка моделювання;
- підтримка баз знань.

У роботах [3, 12-14] обґрунтовано доцільність оснащення СППР функціональними модулями з метою підвищення ефективності прийняття рішень та раціонального планування складу систем ЗІ. Однак, практичне застосування подібних модулів не наведено.

Окремим напрямом досліджень є розробка систем інтелектуальної підтримки прийняття рішень (СІППР) [14, 15] з підтримкою засобів автоматизованої оцінки ризиків [16] і інтеграцією програмних комплексів управління ризиками ІБ і КБ [17]. У роботі [18] відзначається, що СУІБ, в яких реалізовані інтелектуальні технології реагування на події, пов’язані з порушенням ІБ, є продуктами приватних компаній, при цьому замовник у більшості випад ків не володіє інформацією стосовно методів та моделей формування керуючих впливів у системах [19].

Інтелектуальна система підтримки прийняття рішень (IDSS) - це система підтримки прийняття рішень, яка широко використовує методи штучного інтелекту (ШІ). «Системи, засновані на знаннях» (KBS) і «інтелектуальні системи» використовувалися з початку 1980-х років для опису компонентів систем управління. Вважається, що система підтримки прийняття рішень виникла у Клайда Холсапла і Ендрю Вінстона в кінці 1970-

х років. Приклади спеціалізованих інтелектуальних систем підтримки прийняття рішень включають гнучкі виробничі системи, інтелектуальні системи підтримки прийняття маркетингових рішень і системи медичної діагностики [20]

СППР складаються з наступних компонентів: інтерфейс користувача, база знань, модуль управління даними, модуль управління моделями [21]. Схематичне зображення структури СППР зображено на рис. 2.

Інтерфейс - це компонент, який забезпечує зв'язок між користувачем і системою підтримки прийняття рішень. Правильний дизайн цього компонента дійсно важливий, тому що він єдиний, з ким користувач має справу.

Модуль управління даними є підсистемою комп'ютерної системи підтримки прийняття рішень і має ряд власних складових:

- база даних інтегрованої системи підтримки прийняття рішень, яка включає дані, витягнуті з внутрішніх і зовнішніх джерел; дані, які можуть зберігатися в базі даних або можуть бути доступні тільки тоді, коли це корисно;
- система управління базами даних; база даних може бути реляційної або багатовимірної;
- словник даних, що має на увазі каталог, що містить всі визначення даних бази даних; він використовується на етапі визначення процесу прийняття рішень;
- інструменти запитів, які передбачають наявність мов для запитів до баз даних.

Модуль управління моделлю складається з наступних компонентів:

- модельна база, яка містить кількісні моделі, які дають системі можливість аналізувати і знаходити рішення проблем;
- модуль управління модельної базою, призначена для створення нових моделей з використанням мов програмування;

- словник моделей, що містить визначення моделей і іншу інформацію, пов'язану з ними;
- модуль створення, виконання та інтеграції моделей, який буде інтерпретувати інструкції користувача відповідно моделями і перенесе їх у систему управління цими моделями.

Завдяки безперервного зв'язку між системою і об'єктом управління здійснюється безперервний моніторинг його параметрів і як можна більш раннє виявлення несприятливих тенденцій і відхилень в його стані. Відповідні інформаційно-аналітичні компоненти системи здійснюють збір, зберігання і обробку оперативної інформації про стан об'єкта і відбуваються в ньому процесах. Вона необхідна для прийняття оперативних рішень, при відхиленні поточних значень контрольованих параметрів від встановлених їх номінальних (або робочих) значень.

Рисунок1.2 - Елементи СППР

Існує п'ять типів СППР [22]:

1. Системи запиту статусу. Різні аспекти ситуації прийняття рішень контролюють різні рішення в оперативному управлінні, а деякі - в керівництві середньої ланки. Він не потребує будь-яких обчислень, аналізу і т. д. Якщо статус відомий, рішення приймається автоматично.

2. Система аналізу даних. Різні системи прийняття рішень включають використання порівняльного аналізу, а потім використовують формулу або алгоритм. Ці процеси не структуровані в природі.

Для розробки системи аналізу даних потрібні прості інструменти обробки даних і бізнес-правила. Прикладами такої системи можуть бути система інвентаризації персоналу, аналіз грошових потоків і т. Д.

3. Інформаційно-аналітична система. Спочатку аналізуються дані, а потім відбувається генерація інформаційних звітів. У звітах можуть зустрічатися різні типи винятків, так як вони використовуються для оцінки ситуації. Прикладами такої системи можуть бути аналізи продажів, дебіторської заборгованості і т. Д.

4. Система бухгалтерського обліку. Використання таких систем не є необхідним, але може використовуватися для контролю або відстеження різних аспектів бізнесу або функції. Ці системи враховують такі предмети, як готівкові гроші, інвентар та персонал.

5. Модель на основі системи. Діє як модель стимулювання або модель оптимізації для прийняття рішень. Ці рішення, як правило, приймаються один раз і часто допомагають під час операції або діяльності.

Прикладами такої системи можуть бути: асортимент продукції, правила планування роботи і т. Д.

У роботах [23, 24] показано, що недоліками багатьох СПР та ЕС в області ІБ, є:

- Інформаційне перевантаження: комп'ютеризована система прийняття рішень може іноді приводити до інформаційного перевантаження оскільки аналізує всі аспекти проблеми, ставить користувача перед

дилемою - що слід враховувати, а що ні. Не кожен шматок інформації необхідний при прийнятті рішень. Але коли він присутній, особі, що приймає рішення, важко ігнорувати інформацію, яка не є пріоритетною. Постає також необхідність наявності експертів високої кваліфікації.

- Занадто сильна залежність від СППР. Щоб швидше і простіше було приймати повсякденні рішення, системи підтримки прийняття рішень інтегровані в бізнес. Найчастіше виникає тенденція надто сильно залежати від комп'ютеризованого прийняття рішень. Очевидно, що зміщення фокусу відбувається і особи, які приймають рішення, можуть і далі не відточувати свої навички через надмірну залежність від СППР.
- Девальвація суб'єктивності: система підтримки прийняття рішень сприяє раціональному прийняттю рішень, пропонуючи альтернативи на основі об'єктивності. Хоча обмежена раціональність або обмежена ірраціональність грають вирішальну роль в ухваленні рішень, суб'єктивність не може і не повинна бути відкинута. СППР сприяє об'єктивності і знижує суб'єктивність, яка може мати серйозний вплив на бізнес.
- Надмірна увага до прийняття рішень. Очевидно, що основна увага при прийнятті рішень на комп'ютері приділяється постійному розгляду всіх аспектів проблеми які можуть бути зайвими в багатьох ситуаціях. Вкрай важливо навчити користувачів для забезпечення ефективного і раціонального використання коштів СППР.
- Вартість розробки. Вартість прийняття рішень зменшується після установки системи підтримки прийняття рішень. Але розробка і впровадження СППР вимагає величезних грошових вкладень. Налаштування може залучити більш високу вартість. Якщо бюджет

обмежений, можна не отримати індивідуальний СППР, відповідний конкретним потребам.

У той час як велика кількість організацій вже включили СППР в процес прийняття бізнес-рішень, багато хто все ще не можуть інтегрувати його. Причини можуть бути наступні [24]:

- Вихід із зони комфорту. Йдеться про потребу додаткових зусиль, відмову від традиційних практик.
- Страх впровадження нових технологій. Люди бояться проходити навчання, брати участь в семінарах, спрямованих на надання функціональних навичок.

Процес прийняття рішень, на сьогоднішній день, складний, він підтримується комп'ютеризованими системами і включає в себе наступні кроки:

1. Визначення проблеми – це важливий етап, що надає ОПР, базу, на якій вони можуть будувати припущення, збирати й аналізувати дані і оцінювати альтернативи.
    a. Визначення проблеми починається з визнання того, що проблема існує. Проблема існує, коли:
        - є різниця між очікуваним і доставленим;
        - існує відхилення від звичайного;
        - вжиті заходи не виправдані.
    b. СППР визначає проблему і складності, пов'язані з зіставленням результатів.
    c. Визначення ОПР. Залежно від характеру проблеми, її відправляють потрібній людині. Погано структурована проблема перейде до вищого керівництва, складна проблема - менеджерам, а повторювані будуть відправлені працівникові на нижчому ієрархічному рівні.

2. Збір інформації. Як тільки проблема відправлена потрібній людині, яка зацікавлена людина може почати збір даних і виявлення чинників, що впливають на ситуацію. Без СППР збір і аналіз даних займе дуже багато часу. СППР може обробити тонни даних всього за кілька секунд.
3. Оцінка альтернатив і рішення. Ця стадія включає в себе аналіз всіх можливих напрямків дій і визначення найбільш підходящого з них шляхом оцінки плюсів і мінусів кожної альтернативи. СППР допомагає в обґрунтуванні конкретного вибору.
4. Впровадження та контроль. Як тільки рішення прийнято, необхідно йти далі. Реалізація вимагає планування. Моніторинг також важливий для визначення корисності конкретного рішення для досягнення цілей. Це може зажадати деяких коригувань або привести до нової проблеми. В останньому випадку, можливо, доведеться повторити весь процес.

З огляду на потенціал застосування в СУІБ СПР, які реалізують запобіжну стратегію кіберзахисту ОБІ, представляється актуальною задача по розробці методів, моделей та прикладного ПЗ прийнятних до практичного застосування в СІППР. Зокрема, ці дослідження є актуальними у напрямку інтелектуальної підтримки рішень з планування раціонального складу СЗІ, оцінки і прогнозування ризику порушення ІБ та КБ, а також, управління ЗІ в умовах невизначеності потенційних впливів з боку кіберзлочинців.

1.3. Використання моделей зрілості в ході оцінювання рівня захищеності ІС

Для визначення стадії організаційного та технологічного розвитку організації та її процесів у світовій практиці існує поняття «модель зрілості».

У світі відомо розроблено багато моделей зрілості, в тому числі в галузі кібербезпеки. У багатьох випадках вони розробляються державними

структурами для вирішення конкретних задач з подальною метою набуття статусу національного або міжнародного стандарту.

Модель зрілості можливостей кібербезпеки забезпечує орієнтир, за допомогою якого організація може оцінити поточний рівень зрілості своїх практик, процесів та встановити цілі та пріоритети для вдосконалення кібербезпеки [48]. В основі моделі зрілості можливостей (Capability Maturity Model, CMM) лежить процесний підхід. Одною з перших розроблених моделей даного виду була модель, розроблена Інститутом програмного забезпечення (Software Engineering Institute, SEI) в середині 1980-х років.

Моделі зрілості можливостей кібербезпеки зазвичай структуровані наступним чином:

- сфери: яким чином об'єднані загальні поняття організаційних процесів;
- цілі та показники: під цілями маються на увазі бажані значення показників, які мають бути набуті у кожній із сфер моделі, а показники допомагають у візуалізації прогресу щодо досягнення цілей.
- Рівні зрілості: це результат оцінки виконання цілей та вимірювання показників у сферах організації. Значення рівня зрілості коливається від початкового рівня, коли організація, можливо, тільки почала почала розглядати питання кібербезпеки, до динамічного порівняння, коли організація здатна швидко адаптуватися до змін у сфері кібербезпеки щодо загроз, вразливостей, ризиків, економічної стратегії або зміни організації потреби.

В ході даної роботи було проведено систематичний оглял літератури у спорідненій тематиці та були визначені найбільш популярні моделі зрілості можливостей кібербезпеки, а саме: SSE-CMM (System Security Engineering Capability Maturity Model) [26], C2M2 (Cybersecurity Capability Maturity

Model) [27], CCSMM (Community Cyber Security Maturity Model) [29] та NICE (National Initiative for Cybersecurity Education – Capability Maturity Model) [29].

Менш популярними моделями зрілості можливостей кібербезпеки є: ISM3 (Information Security Management Maturity Model) [30] та COBIT (Control Objectives for Information and related Technology) [31]. ISM3 - це модель, яка управляє показниками інформаційної безпеки, які допомагають підтримувати організацію на прийнятному рівні ризику, хоча вона пристосована до конкретних потреб, таких як кібербезпека; однак основна увага приділяється інформаційній безпеці, а не кібербезпеці. COBIT - це модель, яка не повністю розглядає питання кібербезпеки, але зосереджена на управлінні IT. Так само не були включені моделі, які не використовувались у дослідницьких дослідженнях або не мали відповідної згадки.

Підкреслимо, що ISO / IEC 27001 містить вказівки щодо створення системи управління інформаційною безпекою в компанії, однак вона не враховувалась у результатах систематичного огляду, оскільки вона не пропонує власне модель зрілості [44].

Наприклад, в стандарті ISO 27001:2017 існують вимоги до наявності в організації процедури аналізу ризиків. Завжди виникає питання, як же виконати ці вимоги, в якому обсязі і на якому рівні деталізації для різних за величиною компаній. Дуже часто менеджери з інформаційної безпеки звертають увагу саме на розмір організації і майже ніколи на рівень її організаційного та технологічного розвитку. Відповідь на це питання допоможе дати модель зрілості, на основі оцінки рівня зрілості процесів інформаційної безпеки підприємства.

1.4. Штучний інтелект в задачах кібербезпеки

Чим швидше можна виявити порушення цілісності даних, тим менші витрати на їх відновлення [32]. Постійне збільшення часу на усунення

порушень пов‘язане зі збільшенням тяжкості зловмисних нападів, які зазнали більшість компаній. Автоматизація безпеки та інтелектуальні засоби, що забезпечують контроль у ситуаційному центрі безпеки, можуть допомогти поліпшити здатність організації зменшити збитки, спричинені порушеннями[33].

Згідно з [34], більшість завдань забезпечення кібербезпеки відноситься до слабоструктурованих і складно формалізованих. Особливостями таких завдань є [34]:

- ускладнена можливість отримання об’єктивної та неупередженої інформації про досліджувану ІС для прийняття адекватних рушень;
- неоднозначність вихідних даних та багатоваріантність процесу аналізу та прийняття рішень;
- необхідність коригування і введення додаткової інформації в процес пошуку рішень, інтерактивний (людино-машинний, діалоговий) характер логічного висновку рішень;
- необхідність прийняття рішень в жорстких часових обмеженнях.

Наведені вище чинники підштовхують відмовитися від традиційних алгоритмічних методів і моделей прийняття рішень і управління та перейти до створення та використання інтелектуальних технологій через їх адаптивність, гнучкість та можливість оперування зі слабкоструктурованими або неструктурованими даними. До переліку задач, які можуть бути вирішені за допомогою інтелектуальних технологій відноситься безперервний моніторинг подій, технічна діагностика ІС, прогнозування змін технічного стану об'єкта в часі, оперативне втручання в хід процесів, а також планування необхідних відновлювальних заходів.

Штучний інтелект (ШІ) — механізм прийняття рішень, схожий на реальний механізм прийняття рішень людиною, смодульований за допомогою деяких алгоритмів[35].

ШІ у кібербезпеці – це достатньо широка область знань, яка потенційно може використовуватись в організаціях для зменшення ризиків та збільшення доходу, виявлення кіберзагроз та шахрайства [35]. Серед функцій ШІ, які можна використовувати для розробки інтелектуальної системи, можна виділити наступні [35-40]:

- Символьна обробка, яка не є алгоритмічним методом вирішення проблеми;
- Евристика, яка є інтуїтивним знанням або практичним правилом, витягнутим з досвіду;
- Висновок, який включає в себе можливості міркування, здатні побудувати знання більш високого рівня з існуючої евристики (з фактів і правил, що використовують евристику або інші пошукові підходи);
- Машинне навчання, що дозволяє системі регулювати свою поведінку і реагувати на зміни зовнішнього середовища (наприклад, індуктивний навчання, штучні нейронні мережі і генетичні алгоритми і т. д.).

ШІ все більше впливає на повсякденне життя людей і відіграє ключову роль у цифровій трансформації завдяки своїм автоматизованим можливостям прийняття рішень. Переваги цієї технології, що розвивається, значні, але й стурбованість. Таким чином, необхідно підкреслити роль кібербезпеки у встановленні надійного та розгортання надійного ШІ [35-40]:

1. Кібербезпека для ШІ: відсутність надійності та вразливості моделей та алгоритмів ШІ, атаки на кіберфізичні системи, що працюють на основі штучного інтелекту, маніпулювання даними, що використовуються в системах штучного інтелекту, отруєння даними, зміни навколишнього середовища, що спричиняють зміни у внутрішній природі даних, перевірка процесів навчання та оцінки ефективності, захист даних / конфіденційність у контексті систем ШІ тощо.

2. ШІ для підтримки кібербезпеки: ШІ, що використовується як інструмент / засіб для створення вдосконаленої кібербезпеки шляхом розробки більш ефективних засобів контролю безпеки (наприклад, активні брандмауери, розумний антивірус, розвідка кіберзагроз, інтелектуальна криміналістика, сканування електронної пошти, адаптивні пісочниці, автоматизований аналіз шкідливого програмного забезпечення, автоматизований кіберзахист тощо) реагування на кіберзлочини.

3. Зловмисне використання ШІ: зловмисне використання ШІ для створення більш складних типів атак, напр. Шкідливе програмне забезпечення на базі штучного інтелекту, вдосконалена соціальна інженерія, створення підроблених акаунтів соціальних медіа на основі штучного інтелекту, DDoS-атаки з доповненням штучного інтелекту, моделі для створення підроблених даних, злом паролів, тощо. Ця категорія включає як атаки, орієнтовані на штучний інтелект підриву існуючих систем ШІ з метою зміни їх можливостей), а також атак, що підтримуються ШІ (тих, що включають методи, засновані на ШІ, спрямовані на підвищення ефективності традиційних атак).

Методи штучного інтелекту можуть допомогти вирішити численні обмеження сучасних інструментів кібербезпеки завдяки їх масштабованості та адаптивності в роботі пристроїв [41]. Виявлення вторгнень, аналіз шкідливих програм, аналіз загроз безпеці [42], виявлення кібератак [43], аномалій [44] та інші[45-46] проблеми кібербезпеки можна вирішити за допомогою штучного інтелекту та глибокого навчання. Зокрема, багатошарові мережі на основі перцептрону (MLP) [47].

Кожна модель навчання повинна основуватися на певному алгоритмові [47].

На рисунку 3 наведена детальна інформація по кожному з існуючих алгоритмів побудови моделей машинного навчання і їх роботи.

Наведемо приклади використання даних моделей: для створення спам-фільтрів для виявлення фішингу використовують метод Баєса, що класифікує

нормальні і спам повідомлення. В основі даного методу лежить теорія ймовірності і статистичний аналіз [45].

Для виявлення Інтернет шахрайства використовуються нейронні мережі та системи підтримки рішень щодо шахрайства [43].

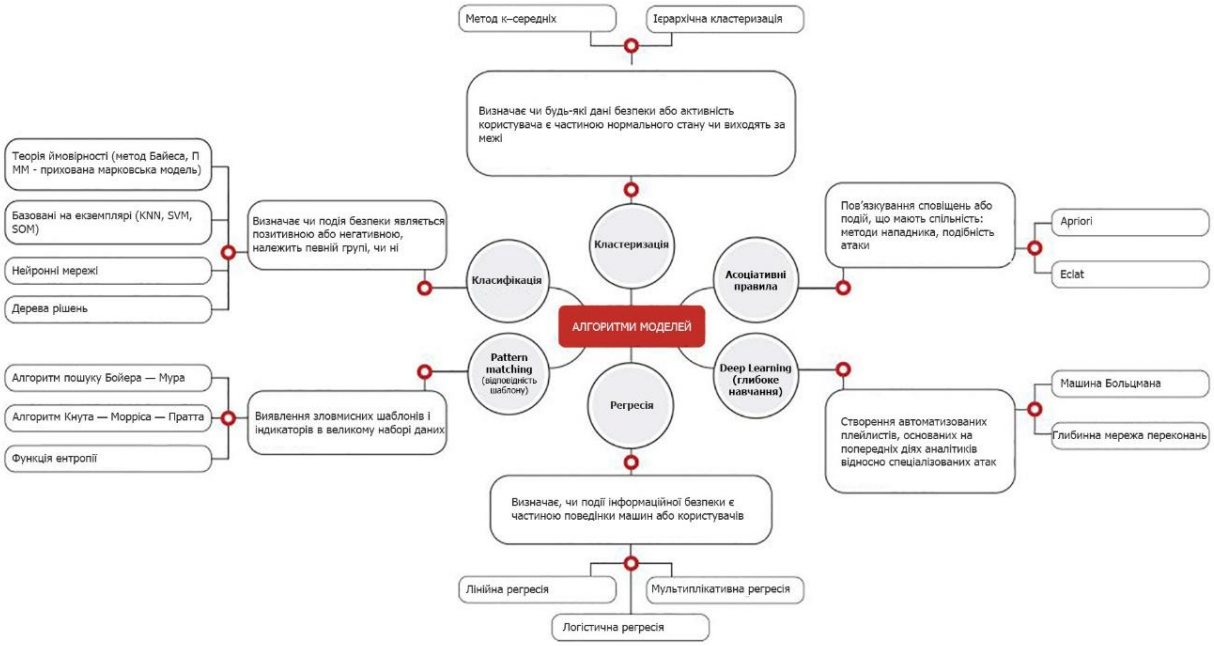


Рисунок 1.2 - Існуючі алгоритми моделей машинного навчання

Для виявлення інсайдерських загроз, таких як порушення розмежування доступу користувачів або витоку даних, використовуються методи кластеризації.

Боти можуть бути виявлені за допомогою функцій ентропії, що застосовуються до результатів взаємодії машина - машина.

Асоціативний аналіз може виявити групи нападників, які використовують примітивні (загальновідомі) методи нападу в мережі

Для успішного ведення бізнесу компанія повинна вміти прогнозувати можливі події безпеки, успішно протидіяти загрозам, аналізувати всі ризики. Це є вищою сходинкою побудови інтелектуальних систем [41]. Для цього використовуються наступні методи аналізу, наведені на Рисунку 4.

Описова аналітика (Descriptive Analytics): огляд минулого - корисна тому, що вона дозволяють нам вчитися на минулих моделях поведінки та розуміти, як вони можуть вплинути на майбутні результати.

Інтелектуальна аналітика (Predictive Analytics). Розуміння майбутнього - дає оцінку про ймовірність майбутнього результату. Важливо пам'ятати, що жоден статистичний алгоритм не може «прогнозувати» майбутнє з 100% впевненістю. Компанії використовують цю статистику для прогнозування того, що може трапитися в майбутньому.

Рисунок 1.3 - методи аналітики

Прескриптивна аналітика (Prescriptive Analytics): поради щодо можливих результатів - дозволяє користувачам "прописати" ряд різних можливих дій і спрямувати їх на вирішення. Прескриптивна аналітика намагається кількісно оцінити вплив майбутніх рішень, щоб дати поради щодо можливих результатів, перш ніж рішення дійсно буде зроблено. У найкращому разі, прескриптивна аналітика передбачає не тільки те, що станеться, а й чому це відбудеться.

Діагностична Аналітика (Diagnostic Analytics) - це форма передової аналітики, яка аналізує дані чи вміст, щоб відповісти на питання "Чому це сталося?"

Детективна аналітика (Detective Analytics) – базується на аналізі і виявлені ще невідомих практиці об’єктів, що можуть нести певну загрозу.

Багато які з нинішніх інструментів виявлення та аналітичних продуктів, таких як EDR та мережева криміналістика, є хорошими прикладами діагностичної та детективної аналітики. IBM Watson - це приклад прескриптивної аналітики, оскільки він збирає інформацію з глобальних джерел, і пред’являє її аналітику при роботі з інцидентом. Інструменти аналізу поведінки користувача можуть надати прогнозну аналітику на основі попередніх даних.

В інформаційній безпеці немає жодного єдиного методу чи механізму захисту, який зміг би захистити від всіх загроз. В теорії інформаційної аналітики така сама ситуація: наприклад, неможливо виявити всі види атак за допомогою одного лише методу.

Базова модель побудови інтелектуальної системи виявлення та ідентифікації подій кібербезпеки має наступний вигляд:

Рисунок 1.4 - Базова модель побудови інтелектуальної системи ідентифікації подій кібербезпеки

Висновки за розділом 1

Аналіз науково-технічних робіт в області розробки і систем підтримки рішень (СППР) з питань інформаційної безпеки (ІБ) дозволив сформулювати наступні висновки:

- існуючі пропрієтарні СППР по ІБ і кібербезпеки (КБ) мають закритий характер, і їх придбання пов'язано зі значними фінансовими витратами;

- існуючі некомерційні СППР щодо захисту інформації та кібербезпеки мають недостатню функціональність;

- в даний час незаповненою залишається ніша застосування СППР в завданнях, пов'язаних з розпізнаванням нових кіберзагроз та тривалих цільових кібератак, що не супроводжуються явними ознаками.

Модель зрілості використовується як інструмент вимірювання стану процесу на основі набору метрик, які являють собою певні характеристики. Оцінка цих метрик за певною шкалою дозволяє зрозуміти стан процесів організації, яка і буде характеризувати рівень зрілості. Після отримання оцінки зрілості можна виробити необхідні заходи для підвищення рівня зрілості процесів і організації в цілому.

Розглянуті моделі зрілості розроблені і застосовуються в основному в США та Європі. В Україні застосування таких моделей ускладнено в силу ряду причин. Зокрема, розвиток інформаційної безпеки в українських організаціях знаходиться на низькому рівні і часто вимоги, які розглядаються в зазначених моделях не реалізовані. Наприклад, моделі не враховую забезпеченість ресурсами для організації процесів інформаційної безпеки. Так само, розвиненість і стабільність процесів управління зарубіжних організацій і українських сильно відрізняється.

Наприклад, в стандарті ISO 27001:2017 існують вимоги до наявності в організації процедури аналізу ризиків. Завжди виникає питання, як же виконати ці вимоги, в якому обсязі і на якому рівні деталізації для різних за величиною компаній. Дуже часто менеджери з інформаційної безпеки звертають увагу саме на розмір організації і майже ніколи на рівень її організаційного та технологічного розвитку. Відповідь на це питання допоможе дати модель зрілості, на основі оцінки рівня зрілості процесів інформаційної безпеки підприємства.

Дослідники США, ЄС і Китаю є світовими лідерами в області розробки експертних систем з кібербезпеки, які будуються в основному на використанні штучних нейронних мереж (neural networks), машинному навчанні (machine learning) і методів data mining. Однак використання в Україні розроблених закордоном рішень ускладнюється через низку причин: закритістю методів і моделей, на яких базуються комерційні продукти, високою вартістю, відсутністю детальної науково-технічної документації, недостатньою адаптивностью до реальних об'єктів кіберзахисту, а, отже, і очікуваних результатів експлуатації

Виглядаючи по-різному стосовно сучасних рішень з кібербезпеки, методи ШІ надійні та більш гнучкі і здатні покращувати системи захисту від все більшої кількості випереджаючих кіберзагроз [40-47]. Разом з тим, незважаючи на інтенсивні зміни, які ШІ переніс у область кібербезпеки, відповідні системи ще не готові повністю адаптуватися до середовища, а також робити зміни у своєму стані. На сьогоднішній день ШІ ще не став основною панацеєю для безпеки.

Незважаючи на уявлення щодо потенційних можливостей засобів штучного інтелекту їх застосування залишається переважно епізодичним та несистематизованим. На даний час у кібербезпеці відсутня загальна концепція запровадження штучного інтелекту, не визначені найважливіші методи штучного інтелекту, які можуть бути використані у кібербезпеці, та не встановлено роль, яку можуть відігравати ці методи (особливо, що стосується машинного навчання, дата-майнінгу, глибокого навчання та експертних систем) для захисту організацій у кіберпросторі.

Відсутність великих масивів даних щодо кібератак є загальним викликом у дослідженнях з кібербезпеки. Часто це пояснюється вимогами щодо конфіденційності, коли компанії не бажають ділитися досвідом щодо атак, яких вони зазнали, але, разом з тим, база відомих загроз поступово все ж таки наповнюється, що дає можливість застосовувати методи глибокого

навчання. Основою для таких методів є великі і часто незбалансовані набори даних, які часто використовуються для ручної кластеризації.

Виходячи з проведеного аналізу джерел, для досягення мети було поставлено наступні задачі:

1. Виконати порівняльний аналіз моделей зрілості у сфері ІБ;
2. Визначення базової парадигми моделі оцінювання;
3. Розробка алгоритму попередньої підготовки даних;
4. Підготовка даних для моделювання;
5. Синтезувати модель зрілості СУІБ з визначенням відповідності досліджуваної ІС на відповідність вимогам стандарту ISO/IEC 27001:2017 з використанням технологій штучного інтелекту та здійснити її навчання;
6. Провести аналіз адекватності розробленої моделі.

РОЗДІЛ 2
РОЗРОБКА МОДЕЛІ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

В цьому розділі будуть вирішуватися наступні задачі:

1. Виконати порівняльний аналіз моделей зрілості у сфері ІБ;
2. Визначення базової парадигми моделі оцінювання;
3. Розробка алгоритму попередньої підготовки даних;
4. Підготовка даних для моделювання;
5. Синтезувати модель зрілості СУІБ з визначенням відповідності досліджуваної ІС на відповідність вимогам стандарту ISO/IEC 27001:2017 з використанням технологій штучного інтелекту та здійснити її навчання;

2.1 Порівняльний аналіз популярних моделей зрілості ІБ

У попередньому підрозділі було визначено найбільш актуальні зрілості кібербезпеки, а саме: SSE-CMM[27], C2M2[28], CCSMM[29] та NICE[30]. Методологія для порівняльного вивчення згаданих моделей базується на таксономії, запропонованій Халворсеном та Конраді [55].

Таксономія, описана Халворсеном та Конраді , містить перелік двадцяти п’яти релевантних функцій для порівняння систем вдосконалення інформаційних систем. Функції об’єднані у п’ять категорій:

- Загальні характеристики: ця категорія включає ознаки, що описують загальні атрибути середовища вдосконалення.
- Задіяні процеси: ця категорія включає функції, що описують використання середовища.

- Організаційні характеристики: ця категорія включає ознаки, що описують взаємозв'язок між ознаками, пов'язаними з атрибутами організації та середовищем, в якому вона використовується.
- Якісні характеристики: ця категорія включає ознаки, пов'язані з виміром якості. Наприклад, аспекти вимірювання якості та що означає якість з точки зору показників якості.
- Результативні показники: ця категорія включає ознаки, що описують результати використання середовища, витрати на досягнення результатів та методи, що використовуються для його перевірки.

На рисунку 2.1 показані категорії та особливості оригінальної систематики Халворсена та Конраді, призначені для порівняння середовищ удосконалення процесів.

Ця таксономія була пристосована для порівняння моделей зрілості можливостей кібербезпеки. Для адаптованої систематики категорії якості та результату були відхилені, оскільки вони не дозволяли порівняти моделі зрілості можливостей кібербезпеки. Більше того, усі моделі мають спільне:

- Оброблення процесів оцінки та вдосконалення, фокус на постійному вдосконаленні та забезпечуванні результатів, що дозволяють приймати рішення,
- Мають подібні риси як за якістю, так і за типом отриманих результатів.
- Мають подібні процеси.

Особливості категорій «Загальний», «Процес» та «Організація» були переглянуті.

У категорії загальних характеристик були визначені такі ознаки:

- Рік останньої редакції: цей пункт може надати інформацію про поточний розвиток моделі завдяки постійним змінам, що існують у кібербезпеці.
- Організаційне середовище: якщо модель зрілості можливостей кібербезпеки орієнтована на всю організацію чи ні. Цей пункт надає

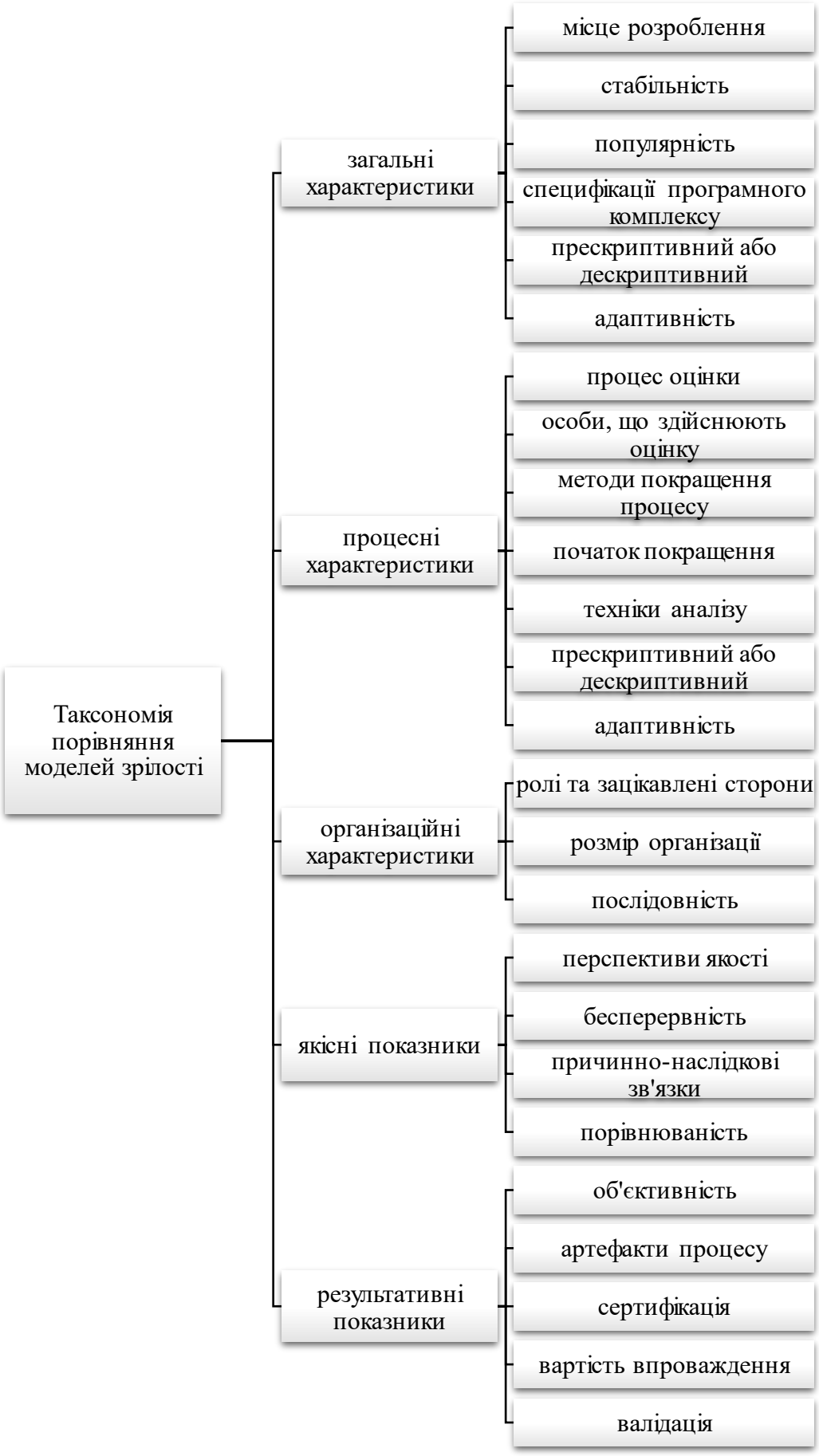


Рисунок 2.1 - Таксономія Хольраді

інформацію про те, чи модель була створена для конкретної потреби в кібербезпеці або для всіх організаційних середовищ.

- Вимірює управління ризиками (загрози та вразливості): якщо модель зрілості вимірює управління ризиками конкретним або загальним чином.

Що стосується категорії процесів, були враховані такі особливості:

- Прикладний сектор: область впровадження моделі, яка корисна для розуміння цілей моделі.
- Глибина: це залежить від складності використовуваної перевірки. Цей пункт допомагає нам розрізнити моделі, що мають більшу деталізацію у відповідних рівнях зрілості, та прості в цьому аспекті.

Що стосується категорії організаційних характеристик, були враховані такі особливості:

- Визначення ролей та відповідальності: якщо модель зрілості можливостей кібербезпеки має чітко визначені ролі та функції. Це допомагає нам знати, яка модель має кращу структуру, хто що повинен робити.
- Рівень документації для впровадження: якщо є якась документація для підтримки та допомоги у впровадженні моделі. Таким чином, ми можемо знати, на якому рівні деталізації є інформація для реалізації моделі.

Кожну ознаку оцінювали наступним чином:

- Орієнтованість на кібербезпеку. Ця функція оцінюється "ТАК", якщо це модель, орієнтована на кібербезпеку, а "НІ" - інакше.
- Рік останньої редакції. За цією функцією оцінюється останній рік огляду, чим нещодавніший, тим кращий.
- Організаційне середовище. Якщо модель орієнтована на всю організацію, вона оцінюється як "ТАК". У випадку, якщо він орієнтований на конкретну сферу організації, він оцінюється як “НІ”.

- Сфера застосування. Ця особливість представлена назвою області (ів), на яку була спрямована модель з моменту її створення.
- Глибина. Ця функція оцінюється як “ЗАГАЛЬНА”, якщо існує лише перший рівень оцінки в межах рівня зрілості. Він вважається «ДЕТАЛЬНИМ», якщо модель має другий рівень оцінки за рівнями зрілості.
- Вимірює управління ризиками (загрози та вразливості). Ця характеристика розглядається як “ЗАГАЛЬНА”, якщо не проводиться безпосередня оцінка ризику. У разі прямої оцінки ризик оцінюється як “ДЕТАЛЬНИЙ”.
- Визначення ролей та відповідальності. Якщо в моделі є чітко визначені ролі та профілі, вона оцінюється "ТАК", інакше - "НІ".
- Рівень документації для впровадження. Рівень документа вважається «ВИСОКИМ», якщо є технічний документ, Посібник із впровадження та відповідні документи. Рівень документації вважається «СРЕДНИМ», якщо він має технічний документ та відповідні документи. Рівень документації вважається “НИЗЬКИМ”, якщо він має лише вступні документи.

2.1.1 Cybersecurity Capability Maturity Model

Міністерство енергетики США у співпраці з Університетом Карнегі Меллона опублікувало модель зрілості та можливостей у галузі кібербезпеки. Остання версія (1.1) моделі була опублікована в лютому 2014 року [28].

Модель організована у десять доменів, і кожен домен є логічною групою практик кібербезпеки. Практики в кожному домені об’єднані в цілі, які представляють досягнення в домені. Домени та цілі перераховані в таблиці 1.

Модель визначає чотири рівні зрілості, від рівня 0 до рівня 3, які застосовуються незалежно до кожного домену моделі. Опис кожного рівня наведено в таблиці 2.

Модель C2M2 має описовий характер. Зміст моделі представлений на високому рівні абстракції, так що її можуть інтерпретувати організації різних типів, структур та розмірів.

Таблиця 2.1

Домени та заходи моделі C2M2

Домени	Заходи
Управління ризиками	• Сформувати стратегію управління ризиками кібербезпеки • Управління ризиком кібербезпеки
Управління активами, змінами та конфігурацією	• Управління інвентаризацією активів • Керування конфігурацією активів • Керування змінами активів
Управління доступом	• Встановлення та підтримка контролю доступу осіб
Управління загрозами та вразливостями	• Виявлення та реагування на загрози зменшують вразливі місця в кібербезпеці
Ситуаційна обізнаність	• Виконувати журналювання • Виконувати моніторинг • Створення та підтримка загальної операційної картини
Обмін інформацією та комунікації	• Поділитися діяльністю з управління інформацією в галузі кібербезпеки
Реагування на події та інциденти, безперервність операцій	• Виявлення подій кібербезпеки • Реагуйте на інциденти та ескалаційні події кібербезпеки • План безперервності та управлінська діяльність

Таблиця 2.1

Домени та заходи моделі C2M2 (Продовження)

Домени	Заходи
Управління ланцюгами поставок та зовнішніми залежностями	• Визначення залежностей • Управління діяльністю з управління ризиками залежностей
Управління робочою силою	• Призначення відповідальності за кібербезпеку • Контроль життєвого циклу робочої сили • Розвиток робочої сили кібербезпеки • Збільшення обізнаності про кібербезпеку • Управлінська діяльність
Управління програмою кібербезпеки	• Створити програму кібербезпеки • Створення та підтримка архітектури кібербезпеки • Виконуйте безпечну розробку програмного забезпечення • Управлінська діяльність

Таблиця 2.2

Рівні зрілості за моделлю C2M2

Рівень показника зрілості	Опис рівня
0	Модель не містить цілей для досягнення рівня 0. Ефективність на рівні 0 просто означає, що рівня 1 у даному домені не досягнуто
1	У кожному домені рівня 1 міститься набір початкових заходів. Для досягнення рівня 1 ці початкові заходи можуть виконуватися спеціально, але вони повинні виконуватися

Таблиця 2.3

Рівні зрілості за моделлю C2M2 (Продовження)

Рівень показника зрілості	Опис рівня
2	Виконання організацією заходів є стабільнішим. На рівні 2 організація може бути впевненішою в тому, що ефективність доменних практик буде підтримуватися з часом
3	На рівні 3 практика у домені стабілізується і керується організаційними директивами високого рівня, такими як політика безпеки

2.1.2 Модель Systems Security Engineering Capability Maturity Model (SSE-CMM)

Спочатку його фінансувало Агентство національної безпеки США (АНБ). Перша версія моделі була опублікована в жовтні 1996 року, а остання версія (3.0) моделі - у червні 2003 року [28].

SSE-CMM має два виміри, "домен" і "можливість". Доменний вимір складається з усіх практик, які спільно визначають інженерію безпеки, і ці практики називаються “базовими практиками”. Виміри спроможності представляють практики, які вказують на здатність управління та інституціоналізацію процесу, і ці практики називаються "загальними практиками". Загальні практики представляють заходи, які слід проводити як частину виконання базових практик.

SSE-CMM містить 129 базових практик, організованих у 22 технологічних областях. З них 61 базова практика, організована в 11 технологічних областях, охоплює всі основні галузі інженерної безпеки. Інші 68 базових практик (організованих в інших 11 технологічних областях), пов’язаних з Проектом та Організацією, показані в Таблиці 3. Базові практики організовані в технологічних областях, і кожна технологічна область має набір цілей, що відображають очікуваний стан організація, яка

успішно виконує область процесу. Організація, яка застосовує базову практику процесу, повинна також досягти своїх цілей.

Загальні практики згруповані в логічні області, що називаються “Загальними ознаками”, які об’єднані у п’ять “Рівнів зрілості”, що представляють посилення можливостей організації.

Загальні ознаки призначені для опису основних змін у типовому способі організації для виконання робочих процесів, а кожна спільна ознака має одну або кілька загальних практик.

SSE-CMM має п'ять рівнів зрілості, як показано в таблиці 4. Описана модель вважається моделлю, не зосередженою на кібербезпеці, але це модель, яка була адаптована для цієї мети через відсутність моделей, характерних для кібербезпеки.

Таблиця 2.4

Сфери інженерної, проектної та організаційної безпеки

Сфери інженерної безпеки	Проектна та організаційна безпека
PA01 Адміністрування контролів безпеки	PA12 Забезпечення якості
PA02 Оцінювання впливу	PA13 Управління конфігураціями
PA03 Оцінювання ризиків ІБ	PA14 Управління проектними ризиками
PA04 Оцінювання загроз	PA15 Моніторинг та контроль технічних зусиль
PA05 Оцінювання вразливостей	PA16 Планування технічних зусиль
PA06 Гарантування безпеки	PA17 Визначення процесу системної інженерії організації

Таблиця 2.5

Сфери інженерної, проектної та організаційної безпеки (продовження)

Сфери інженерної безпеки	Проектна та організаційна безпека
PA07 Координація безпеки	PA18 Покращення процесу системної інженерії організації
PA08 Моніторинг стану безпеки	PA19 Керування розвитком продуктової лінійки
PA09 Забезпечення безпеки	PA20 Управління середовищем підтримки інженерної системи
PA10 Визначення вимог безпеки	PA21 Проведення постійного навчання
PA11 Верифікація та валідація безпеки	PA22 Координація з поставниками

Таблиця 2.6

Рівні зрілості за моделлю SSE-CMM

Рівень зрілості	Опис рівня
Рівень 1, "Виконується неофіційно"	Як правило, виконуються базові заходи процесу. Виконання цих базових практик може не ретельно плануватися та відстежуватися
Рівень 2, "Заплановано та відстежувано"	Виконання базових заходів процесу планується та відстежується. Продуктивність відповідно до визначених процедур перевіряється
Рівень 3, “Добре визначено”	Базові практики виконуються за чітко визначеним процесом із використанням затверджених, адаптованих версій стандартних, документованих процесів
Рівень 4, “Кількісно контрольований”	Детальні показники ефективності збираються та аналізуються.

Таблиця 2.7

Рівні зрілості за моделлю SSE-CMM (продовження)

Рівень зрілості	Опис рівня
Рівень 4, “Кількісно контрольований”	Це призводить до кількісного розуміння можливостей процесу та покращення здатності прогнозувати продуктивність
Рівень 5, “Постійне вдосконалення”	Кількісні цілі ефективності (цілі) для ефективності та ефективності процесу встановлюються, виходячи з бізнес-цілей організації

2.1.3 Модель Community Cyber Security Maturity Model (CCSMM)

Розроблена Центром забезпечення та забезпечення безпеки інфраструктури (CIAS) Університету Сан-Антоніо, штат Техас, модель зрілості кібербезпеки спільноти (CCSMM) призначена для задоволення потреб держав та громад щодо розробки життєздатної та стійкої програми кібербезпеки. Єдина версія (1.0) моделі була опублікована в 2006 році [53].

Модель визначає особливості громад та держав у міру дозрівання їх програм кібербезпеки. Він використовує такі аспекти, як знання з кібербезпеки, політики та процедур безпеки, обмін інформацією всередині та між організаціями, а також навчання та освіта з кібербезпеки.

Держави складаються з громад, а громади - з організацій, і модель відповідає зв’язкам, що існують між державою, громадою та організаціями. Модель представлена тривимірно. У моделі CCSMM існує п’ять рівнів зрілості для організацій, громад та держав, які прогресують по кожному з них у порядку, наведеному в таблиці 5. Ця модель проводить оцінку високого рівня, оскільки вона орієнтована на держави, громади та організації.

Таблиця 2.5

Рівні зрілості за моделлю CCSMM

Рівень зрілості	Опис рівня
Рівень 1, "Початковий"	Організації, громади та держави на цьому рівні мають незначну інформацію про кібербезпеку, її аналіз та оцінку або зовсім відсутні
Рівень 2, “Створено”	Керівництво організацій, громад та держав цього рівня усвідомлює кіберзагрози, проблеми та необхідність прийняття кібербезпеки. Вони також визнають необхідність спільного навчання та освіта в галузі кібербезпеки
Рівень 3, “самооцінювання”	На цьому рівні керівники організацій, громад та держав активно пропагують обізнаність щодо кібербезпеки та співпрацюють з іншими у створенні навчальних та освітніх програм
Рівень 4, “Інтегрований”	Коли кібербезпека інтегрована, вона включається в кожен процес, коли організація, громада чи держава мають чітко визначені програми
Рівень 4, “Постійне покращення”	Для організацій, громад та держав на цьому рівні кібербезпека є імперативом бізнесу. Суб’єкти на цьому рівні здатні навчати інших

2.1.4 Модель National Initiative for Cybersecurity Education – Capability Maturity Model (NICE)

Національна ініціатива з питань кібербезпеки (NICE) виникла з інтегральної ініціативи з кібербезпеки (CNCI), ініціативи 8 - Розширити освіту в галузі кібернетики, яка була заснована президентом США Джорджем

Бушем в Президентській директиві про національну безпеку в січні 2008 року, розвивати персонал з технологічним профілем у галузі кібербезпеки, що має відповідні знання та навички. Для досягнення цих цілей NICE-компонент 3 зосереджує увагу на структурі кібербезпеки персоналу, зокрема в управлінні талантами та ролі планування персоналу. Єдина версія (1.0) моделі була опублікована в серпні 2014 року [31].

Модель зрілості NICE виділяє ключові види діяльності за трьома основними напрямками:

- Процес та аналітика: процес представляє ті дії, які пов’язані з фактичними кроками, які організація робить для виконання планування робочої сили, та те, як ці етапи інтегруються з іншими важливими бізнес-процесами в організації. Аналітика представляє діяльність, пов’язану з даними попиту та пропозиції та використанням інструментів, моделей та методів для проведення аналізу планування робочої сили.
- Інтегроване управління: представляє діяльність, пов'язану зі створенням структур управління, розробкою та наданням керівних вказівок та керуванням прийняттям рішень. Це складова частина загальної стратегії та бачення планування робочої сили організації, а також розподілу відповідальності, сприяння інтеграції та видачі вказівок щодо планування.
- Підготовлені професіонали та спроможні технології: представляє діяльність, пов’язану із створенням професійних кадрів з планування робочої сили в організації. Технологія Enabling Technology представляє діяльність, пов'язану з доступністю та використанням систем даних.

Модель зрілості NICE має три рівні зрілості. Ці рівні наведені в таблиці 6.

Щоб використовувати цю модель, організації повинні чітко розуміти свої поточні кадрові можливості, оскільки вони стосуються трьох областей

сегменту та здатності демонструвати конкретні докази діяльності, описаної в моделі.

Таблиця 2.6

Рівні зрілості за моделлю NICE

Рівень зрілості	Опис рівня
Обмежений рівень	Обмежений - це найосновніший рівень, який зображає організацію, яка має сфери її планування робочої сили з кібербезпеки ще в зародковому стані. Ця ключова сфера організації знаходиться на початку її розвитку, наприклад, обмежена установка процесів, без чітких вказівок, без структуровані дані та методи аналізу
Прогресуючий рівень	Рівень розвитку описує деякі аспекти робочої сили з кібербезпеки планування в організації, яка розпочала свою діяльність, та створення певної інфраструктури для підтримки зусиль
Оптимізований рівень	Відображає ключові сфери можливостей планування робочої сили в організації, які повністю розроблені, інтегровані з іншими бізнес-процесами та можуть підтримувати різні рівні аналізу робочої сили та навантаження, результати яких сприяють короткостроковому та довгостроковому прийняттю рішень щодо кібербезпеки робочої сили

2.1.5 Результати порівняльного аналізу

Особливості, визначені для оцінки моделей, були визначені раніше в кінці розділу. 3. Проаналізувавши моделі зрілості можливостей кібербезпеки, отримані в результаті систематичного огляду, була складена таблиця, що підсумовує порівняння між ними. У таблиці 7 наведено значення функцій для кожної з моделей (C2M2 [28], NICE [31], CCSMM [53] та SSE-CMM [27]), описаних у попередньому розділі.

Таблиця 2.7

Порівняння моделей зрілості можливостей кібербезпеки

Моделі	C2M2	NICE	CCSMM	SSE-CMM
Загальні характеристики				
Орієнтованість на кібербезпеку	+	+	+	-
Рік останньої редакції	2014	2014	2006	2008
Організаційне середовище	+	-	-	+
Відповідність стандартам безпеки	NIST	-	NIST	-
Управління ризиками (загрози та уразливості)	Детальний рівень	Загальний рівень	Загальний рівень	Детальний рівень
Процесні характеристики				
Сектор застосування	Енергетика	Виробництво	Громадські об’єднання	Інженерія безпеки
Глибина	Детальний рівень	Загальний рівень	Загальний рівень	Детальний рівень
Організаційні характеристики				
Визначення ролей та відповідальності	+	+	-	+
Рівень документації для впровадження	середній	середній	низький	високий

Результати дослідження свідчать про те, що моделі зрілості можливостей кібербезпеки мають суттєву подібність. Основна відмінність визначається у сфері, на яку вони орієнтовані, та в рівні глибини найкращих практик, які слід застосувати. Основні результати, виявлені в порівнянні, наступні:

- Було визначено сфери, на яких орієнтовані моделі, чи були вони задумані для кібербезпеки чи в іншій галузі, а також в додаткових роботах, чи були вони пристосовані для використання в кібербезпеці [27-32, 53-63].
- Моделі, які є більш загальними (SSE-CMM та C2M2) та охоплюють усі сфери діяльності організації, охоплюють усі атрибути безпеки (конфіденційність, цілісність та доступність).
- Серед аналізованих моделей [27-32, 53-63] є моделі, особливості оцінки яких є дуже загальними (NICE, CCSMM) порівняно з іншими (C2M2, SSE-CMM). Більш конкретні моделі надають більше інформації для належної класифікації та оцінки їхньої практики, а також надають більш детальні вказівки для покращення рівня показників зрілості.

На додаток до порівнянь, описаних у цій роботі, використовуючи рядок пошуку "модель зрілості кібербезпеки" в двигуні "google academical". Було отримано 990 документів у вільному доступі, і було встановлено, що найбільш згадані моделі - це ті, що порівнюються в цьому документі. Було знайдено також додаткові моделі, які не використовувались у систематичному огляді, такі як:

- Open Information Security Management Maturity Model (O-ISM3) [56];
- ISF Maturity Model Accelerator (ISF MM) [57];
- Control Objectives for Information and Related Technologies - Version 5 (COBIT 5) [58];
- Building Security in Maturity Model (BSIMM) [59].
- Resilia [60],
- CERT-RMM [61]
- SUNY ISI [62].

Усі моделі можуть бути адаптовані до різних типів організацій; однак їм потрібен певний рівень налаштування. Існують такі моделі, як C2M2 та CCSMM, які розроблені для реалізації разом із структурою NIST.

Не було виявлено оновлень моделей за останні 3 роки.

Єдиною зрілою моделлю можливостей кібербезпеки, яка орієнтована на кібербезпеку, оновлюється і орієнтована на всю організацію, є C2M2.

Модель SSE-CMM - це модель, яка вже кілька років працює на ринку, але не орієнтована безпосередньо на кібербезпеку, хоча вона застосовується в цій галузі.

Більше того, було встановлено, що всі моделі зрілості можливостей кібербезпеки потребують рівня персоналізації, який буде впроваджений в організації.

Усі моделі зрілості можливостей кібербезпеки базуються на управлінні ризиками кібербезпеки, але лише SSE-CMM та C2M2 вимірюють управління ризиками більш конкретним чином.

2.2. Розробка моделі оцінювання захищеності ІС на основі стандарту ISO/IEC 27001:2017

Міжнародний стандарт ISO/IEC 27001:2017 базується на британських стандартах BS7799 та ISO/ IEC 17799. Він містить вимоги щодо встановлення, впровадження, експлуатації, моніторингу, критичного аналізу, підтримки та вдосконалення СУІБ [64]. СУІБ, як визначено цим стандартом, є "тією частиною загальної системи управління, яка базується на підході до ділового ризику для встановлення, впровадження, експлуатації, моніторингу, перегляду, підтримання та вдосконалення інформаційної безпеки". Цей стандарт використовується у всьому світі усіма типами організацій як основа для управління політикою організації та впровадження інформаційної безпеки. Він використовується малими, середніми та великими організаціями.

Стандарт ISO 27001:2017 містить перелік вимог до СУІБ організації. В результаті виникає питання, як же виконати ці вимоги, в якому обсязі і на якому рівні деталізації для різних за величиною компаній. Дуже часто менеджери з інформаційної безпеки звертають увагу саме на розмір організації і майже ніколи на рівень її організаційного та технологічного розвитку. Відповідь на це питання допоможе дати модель зрілості, на основі оцінки рівня зрілості процесів інформаційної безпеки підприємства.

Підкреслимо, що ISO/IEC 27001 містить вказівки щодо створення системи управління інформаційною безпекою в компанії, однак вона не враховувалась у результатах систематичного огляду, оскільки вона не пропонує власне модель зрілості.

В основі даного стандарту лежить процесний підхід та модель Plan-Do-Check-Act (PDCA), як показано на Рис 2.2, яка застосовується для структурування всіх процесів СУІБ.

Рисунок 2.2 - Модель PDCA

Відповідно до ISO / IEC 27001, діяльність щодо процесів СУІБ може бути узагальнена наступним чином [64]:

- A1: Створення СУІБ - “Встановлення політики, цілей, процесів та процедур СУІБ, що мають відношення до управління ризиками та підвищення інформаційної безпеки для досягнення результатів відповідно до загальної політики та цілей організації”.
- A2: Впровадження та експлуатація СУІБ - “Впровадження та експлуатація політики, засобів управління, процесів та процедур СУІБ”.
- A3: Моніторинг та перегляд СУІБ - „Оцініть та, де це можливо, виміряйте ефективність процесу відповідно до політики СУІБ, цілей та практичного досвіду та повідомте результати керівництву для огляду”.
- A4: Підтримка та вдосконалення СУІБ - «Вживання коригувальних та профілактичних заходів, заснованих на результатах внутрішнього аудиту та перегляду СУІБ або іншої відповідної інформації, для постійного вдосконалення СУІБ».

Це ті дії, які повинненні виконуватися у СУІБ у відповідності до стандарту ISO/IEC 27001.

На основі результатів огляду літератури [27-32, 53-63], було виявлено кілька робіт, які можуть бути використані для визначення відповідності даному стандарту. Було відібрано перелік моделей зрілості, які використовували різні методологічні підходи. Потім кожна модель зрілості була проаналізована відповідно до ступеня, в якому вони охоплюють та відповідають раніше визначеному базовому рівню.

Кожну модель зрілості було класифікувано за вимогами стандарту, використовуючи шкалу Лікерта, яка ранжується від 1 (дуже низька) до 5 (дуже висока). Після цього аналізу було визначено, що лише шість моделей зрілості набрали в сукупності щонайменше 10 балів:

- Open Information Security Management Maturity Model (O-ISM3) [56];
- Systems Security Engineering – Capability Maturity Model (SSE-CMM) [28];
- ISF Maturity Model Accelerator (ISF MM) [57];
- Control Objectives for Information and Related Technologies - Version 2019 (COBIT 2019) [58];
- Cyber Security Capability Maturity Model (C2M2) [29],
- Building Security in Maturity Model (BSIMM) [59].

В таблиці 2.8 продемонстровано результати оцінки. В ході оцінювання було досягнуто середнього загального балу 12, максимальний бал 20.

Таблиця 2.8

Оцінка охоплення контролів безпеки за стандартом ISO / IEC 27001:2017

Модель зрілості	A1	A2	A3	A4	Сума
O-ISM3	2	3	4	4	13
SSE-CMM	2	4	4	2	12
ISF MM	2	2	3	3	10
COBIT 2019	4	2	4	2	12
ONG C2M2	3	2	2	3	10
BSIMM	3	4	4	4	15
Загальна оцінка	2,6	2,8	3,5	3	12

Отже, виходячи з результатів аналізу, не існує моделі зрілості, яка б задовільно відповідала враховувала вимоги ISO / IEC 27001.

Відповідно, якщо жодна існуюча модель не здатна вирішити виявлену проблему, повинна бути розроблена нова модель зрілості. Розроблена модель зрілості, представлена в Таблиці 9, приймає встановлені структурні елементи, сфери та функції кращих практик, наявних в ISO / IEC 27001. Як

детально описано раніше в методології дослідження, було застосувано ітераційний процес для розвитку моделі зрілості.

Загалом було використано дві ітерації. Детально процес синтезу моделі описано нижче:

Таблиця 2.9

Модель зрілості СУІБ

Рівень зрілості	Контролі
Рівень 1: Планування	2.1 - Визначити сферу застосування та межі СУІБ.
	2.2 - Розробити політику СУІБ.
	2.3 - Визначити підхід до оцінки ризиків.
	2.4 - Виконати ідентифікацію ризиків.
	2.5 - Проведення аналізу та оцінки ризиків.
	2.6 - Визначення варіантів оброблення ризиків.
	2.7 - Визначення цілей та контролів критеріїв для оброблення ризиків.
	2.8 - Отримати дозвіл на затвердження залишкових ризиків.
	2.9 - Отримати дозвіл на впровадження та функціонування СУІБ.
	2.10 - Підготовка положення про застосовності.
Рівень 2: Впровадження	3.1 - Сформулювати план оброблення ризиків.
	3.2 - Впровадити план оброблення ризиків.
	3.3 – Впровадженння обраних контролів.
	3.4 – Визначити як вимірювати ефективність впроваджений контролів.
	3.5 - Впровадити програми з навчання та поінформованості.
	3.6 - Управляти функціонуванням СУІБ.
	3.7 - Управляти ресурсами СУІБ.
	3.8 - Впровадити процедури та інші контролі для уможливлення термінового виявлення подій безпеки та реагування на інциденти безпеки.

Таблиця 2.9

Модель зрілості СУІБ (Продовження)

Рівень 3: Моніторинг	4.1 - Виконувати процедури моніторингу та перегляду, а також інші контролі.
	4.2 - Проводити регулярні перегляди ефективності СУІБ.
	4.3 - Вимірювати ефективність контролів.
	4.4 – Переглядати оцінку ризиків.
	4.5 – Переглядати залишкові ризики.
	4.6 – Переглядати ідентифіковані прийнятні рівні ризиків.
	4.7 – Проводити регулярно внутрішні аудити.
	4.8 – Переглядати СУІБ.
	4.9 - Оновлювати плани безпеки.
	4.10 - Реєструвати дії та події.
Рівень 4: Вдосконалення	5.1 - Впроваджувати в СУІБ ідентифіковані вдосконалення.
	5.2 - Здійснювати відповідні коригувальні та запобіжні дії.
	5.3 - Доводити до відома всіх зацікавлених сторін інформацію щодо дій та вдосконалень СУІБ.
	5.4 - Забезпечувати, що вдосконалення досягають намічених цілей.

Перша ітерація: На першому кроці визначего визначили характеристики та структуру моделі зрілості. Було запропоновано п’ять рівнів зрілості: початковий, керований, визначений, кількісно керований та оптимізований. Подібні рівні зрілості можна знайти в різних усталених моделях зрілості, таких як [39-44]. У першій ітерації було зосереджено увагу лише на частині процесу СУІБ ISO/IEC 27001, а саме на етапі планування. Для кожного критерію моделі зрілості було змодельовано те, чим проявлявся цей критерій на різних рівнях зрілості.

Друга ітерація: У другій ітерації було повністю переглянуто визначення рівнів зрілості, запропонувавши п'ять нових рівнів зрілості: початковий, планування, впровадження, моніторинг та вдосконалення. Ці рівні зрілості базуються на циклі PDCA, що використовується в ISO / IEC 27001, як показано на малюнку 7. У таблиці 8 детально викладено контролі, на яких базується пропонована модель зрілості, що полегшить користувачеві, який звик до ISO/IEC 27001, зрозуміти модель зрілості та встановити зв’язок між тим, що вимагається в кожному критерії оцінки, та вимогами, зазначеними в ISO / IEC 27001.

Як результат було визначено наступні рівні зрілості:

- (Рівень 1) Виконується неофіційно;
- (Рівень 2) Заплановано;
- (Рівень 3) Добре визначено;
- (Рівень 4) Кількісно контрольовано;
- (Рівень 5) Постійне вдосконалення.

Для підвищення від рівня X до рівня X + 1 організація повинна відповідати всім критеріям від рівня X, що робить цю модель зрілості послідовною «підхідною». Організація може очікувати від підвищення рівня зрілості, що їх процес СУІБ буде дедалі більше керованою, визначеною та легше оптимізованою.

2.2.1. Визначення базової парадигми моделі оцінювання

ШІ все більше впливає на повсякденне життя людей і відіграє ключову роль у цифровій трансформації завдяки своїм автоматизованим можливостям прийняття рішень. Використання ШІ для автоматизованого прийняття рішень особливо важливе у таких критично важливих сферах безпеки як автономні транспортні засоби, інтелектуальне виробництво, електронні медичні

системи та ін. Однак дана технологія має як переваги, так і викликає стурбованість.

Розглядаючи питання безпеки в контексті ШІ, варто зауважити, що методи та системи ШІ, що використовують ШІ, можуть призвести до несподіваних результатів і можуть бути підроблені для маніпулювання очікуваними результатами [65]. Це особливо стосується розробки програмного забезпечення на основі штучного інтелекту, яке часто базується на повністю чорних моделях, або воно може навіть використовуватися зі зловмисними намірами, наприклад ШІ як засіб для посилення кіберзлочинності та сприяння атакам зловмисних супротивників. Тому так важливо забезпечити безпеку власне у ШІ. Зокрема, важливо:

- розуміти, що саме підлягає захисту (активи, яким загрожують специфічні загрози ШІ),
- розуміти відповідні моделі управління даними (включаючи розробку, оцінку та захист даних та процес навчання систем ШІ),
- комплексно керувати загрозами в багатопартійній екосистемі, використовуючи спільні моделі та таксономії,
- розробити спеціальні засоби контролю, щоб забезпечити безпеку самого ШІ.

Для правильного формування інтелектуальної системи важливо дотримуватися структурованого та методичного підходу, щоб зрозуміти його різні аспекти. З цієї причини варто здійснити функціональний огляд життєвого циклу типових систем ШІ.

Життєвий цикл системи ШІ включає кілька взаємозалежних фаз, починаючи від її проектування та розробки (включаючи такі підфази, як аналіз вимог, збір даних, навчання, тестування, інтеграція), встановлення, розгортання, експлуатацію, обслуговування та утилізацію. Враховуючи складність систем штучного інтелекту (і загалом інформаційних), було визначено декілька моделей та методологій для управління цією складністю,

особливо на етапах проектування та розробки, такі як водоспад, спіраль, гнучка розробка програмного забезпечення, швидке створення прототипів та інкрементальні [66].

Життєвий цикл ШІ визначає етапи, яким повинна слідувати організація, щоб скористатися перевагами методів ШІ, зокрема моделей машинного навчання, щоб отримати практичну цінність. Моделялі машинного навчання здійснюють математичне перетворення вхідних даних у новий результат, наприклад розпізнавання облич. І навпаки, алгоритми використовуються для оновлення параметрів моделі (навчання) або для виявлення закономірностей та відносин у нещодавно наданих даних та виведення результату [67]. Узагальнена модель життєвого циклу інтелектуальних систем зображена на Рисунку 2.3 [65-72]. Метою створення еталонної моделі є створення концептуальної бази, що забезпечує спільне розуміння активів, що складають систему ШІ, та їх значущих взаємозв'язків. Це полегшує розподіл власників за різними активами, з одного боку, а з іншого боку, забезпечує систематизований, структурований спосіб аналізу відповідних загроз безпеці.

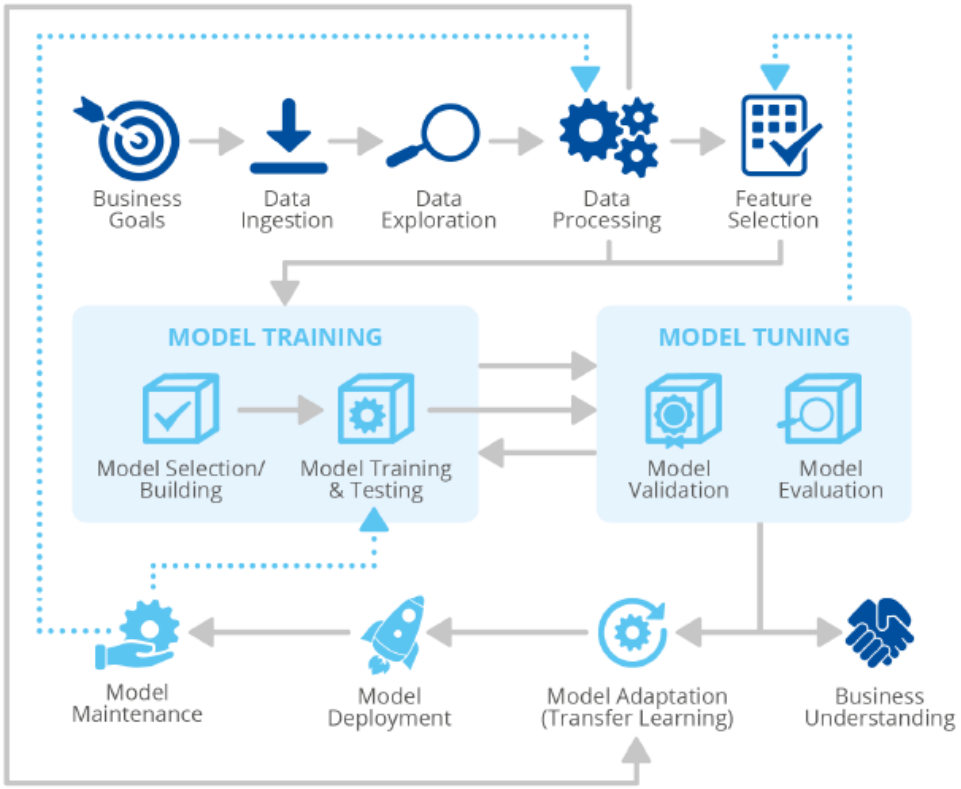


Рисунок 2.3 - Узагальнений життєвий цикл інтелектуальної моделі

Дані є одним з найцінніших активів штучного інтелекту. Рисунок 2.4 ілюструє трансформацію даних на різних етапах життєвого циклу: передача даних, дослідження даних, попередня обробка даних, важливість функцій, навчання, тестування та оцінка. Трансформація даних протягом життєвого циклу ШІ включає кілька інших типів активів, таких як залучені актори, обчислювальні ресурси, програмне забезпечення тощо, і навіть деякі нематеріальні активи, такі як процеси, культура та те, як досвід та знання акторів можуть принести потенційні ненавмисні загрози (наприклад, ненавмисне упередження).

Рисунок 2.4 Процес підготовки даних для моделювання

Перед проведенням розробки моделі важлив повністю визначити бізнес-контекст застосування системи штучного ШІ та зібрати дані для аналізу, а також визначити контролі, які будуть використані для оцінки ступеня досягнення цих цілей.

Штучний інтелект (ШІ), який іноді називають машинним інтелектом, - це інтелект, який демонструється машинами, на відміну від природного інтелекту, який демонструє людина. Тобто, ШШ – це здатність системи правильно інтерпретувати зовнішні дані, вчитися на таких даних та використовувати ці знання для досягнення конкретних цілей та завдань за допомогою гнучкої адаптації [67].

Штучні нейронні мережі (artificial neural network, ANN): це обчислювальні системи, натхненні, але не ідентичні біологічним нейронним мережам, що складають мозок тварин. ANN базується на колекції зв’язаних

одиниць або вузлів, званих штучними нейронами (AN), які вільно моделюють нейрони в біологічному мозку. Кожне з'єднання, як синапси в біологічному мозку, може передавати сигнал іншим нейронам. Коли штучний нейрон отримує один або кілька сигналів, він обробляє їх і вирішує, подавати сигнал будь-яким нейронам, підключеним до нього [76].

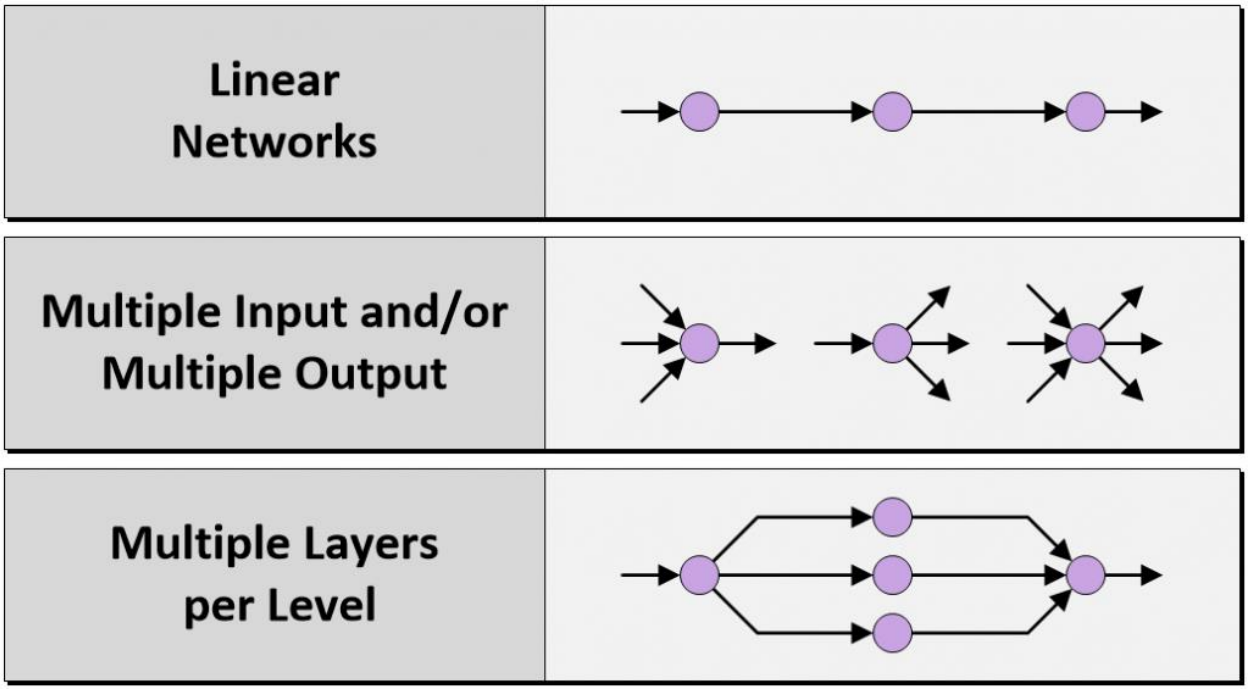


Рисунок 2.5 - Види зв’язків вузліу у ANN

Звичайна форма ANN формується із шарів, виходи з кожного шару подають входи на наступний шар. Ранні ANN були обмежені лише декількома шарами, кожен з яких містив лише кілька вузлів, але сьогоднішні ANN можуть мати сотні або тисячі шарів, кожен з яких складається з тисяч вузлів. Більше того, ранні системи підтримували лише лінійні мережі з одним шаром на рівень, тоді як сучасні мережі можуть підтримувати кілька входів та / або декілька виходів разом з декількома шарами на рівень.

Такі системи «вчаться» виконувати завдання, розглядаючи приклади, як правило, без програмування певних правил для конкретних завдань. Наприклад, у разі розпізнавання зображень вони можуть навчитися ідентифікувати зображення, що містять квіти, аналізуючи приклади

зображень, які люди позначили як "квітка" (доповнена типом квітки) або "без квітки", після чого вони може використовувати результати для ідентифікації квітів на інших зображеннях [78].

Глибока нейронна мережа (deep neural network, DNN): це штучна нейронна мережа з великою кількістю шарів штучних нейронів між вхідним та вихідним шарами. Згорткова нейронна мережа (convolutional neural network, CNN) є однією з форм реалізації, і в даний час CNN є методом вибору для обробки візуальних та інших двовимірних даних.

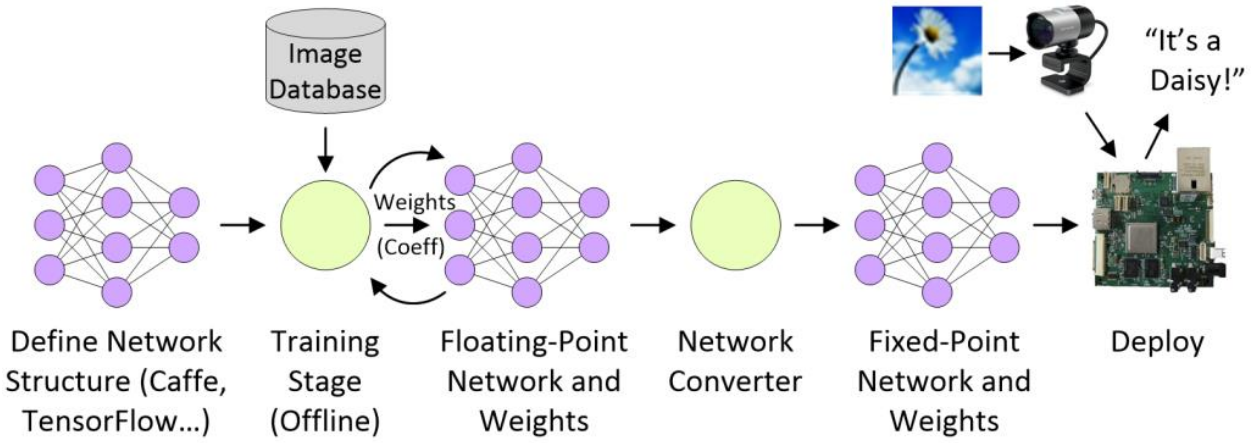


Рисунок 2.6 - Алгоритм використання ANN для розпізнавання зображень

Глибока нейронна мережа (deep neural network, DNN): це штучна нейронна мережа з великою кількістю шарів штучних нейронів між вхідним та вихідним шарами. Згорткова нейронна мережа (convolutional neural network, CNN) є однією з форм реалізації, і в даний час CNN є методом вибору для обробки візуальних та інших двовимірних даних.

DNN - це, як правило, мережі прямої передачі даних, в яких дані надходять із вхідного рівня на вихідний рівень, не циклічно повертаючись назад. Для порівняння, рекурентні нейронні мережі (recurrent neural networks , RNN), в яких дані можуть надходити в будь-якому напрямку, краще підходять для таких програм, як мовне моделювання [79].

Машинне навчання (Machine Learning, ML) - це наукове вивчення алгоритмів та статистичних моделей, які комп'ютерні системи використовують для виконання конкретного завдання без використання чітких інструкцій, спираючись натомість на закономірності та умовиводи. Машинне навчання розглядається як підмножина штучного інтелекту. Алгоритми машинного навчання будують математичну модель на основі зразкових даних, відомих як "навчальні дані", для того, щоб робити прогнози або приймати рішення, не будучи явно запрограмованими на виконання завдання. [80]

Подібно до того, як машинне навчання розглядається як підмножина штучного інтелекту, глибоке навчання (Deep Learning, DL) розглядається як підмножина машинного навчання. Глибоке навчання може бути під наглядом, частково контрольоване або без нагляду. Архітектури глибокого навчання, такі як DNN, CNN та RNN, були застосовані до таких областей, як комп'ютерний зір, розпізнавання мови, обробка природних мов, розпізнавання аудіо, фільтрація соціальних мереж, машинний переклад, біоінформатика, дизайн ліків, аналіз медичних зображень, перевірка матеріалів та програми настільних ігор, де вони дали результати, порівнянні з - у деяких випадках перевершуючими - експертами-людьми [76-82].

Для підвищення швидкості та коректності рішень, щодо управління роботою кібернетичної системи доволі часто використовуються методи машинного навчання [76-82]. З кожними новими набутими знаннями якість та швидкість майбутнього аналізу постійно зростає. До методів машинного навчання можна віднести наступні наведені на Рисунку 13.

Навчання з учителем (supervised learning): один із видів машинного навчання, в ході якого системі надається множина прикладів «стимул-реакція» для визначення конкретної «реакції» для певного набору «стимулів», які не належать наявній множини прикладів. Машина використовує минулі дані, які люди вже позначили як хороші чи погані, реальні атаки чи помилкові спрацювання захисних систем, шахрайські чи

звичайні дії). Навчання з учителем включає класифікацію (classification), регрес (regression) та глибоке вивчення (deep learning) [83-89].

Навчання без учителя (unsupervised learning) – один із видів машинного навчання, в ході якого системі не надаються жодні дані про минулі події. Таким чином система навчається виконувати поставлене завдання самостійно. Даний вид навчання підходить для вирішення задач виявлення внутрішніх взаємозв'язків, залежності, закономірності, що існують між об’єктами наявної навчальної вибірки, тобто вирішує задачі кластеризації, генерації асоціативних правил та відповідності шаблону [84].

Навчання з підкріпленням (reinforcement learning): це метод машинного навчання, при якому відбувається навчання моделі, яка не має відомостей про систему, але має можливість здійснювати будь-які дії в ній [85]. Дії переводять систему в новий стан і модель отримує від системи певну відповідь (feedback).

Напівавтоматичне навчання – ще один вид машинного навчання, що використовує велику : спосіб машинного навчання, різновидність навчання з учителем, яке потребує великий набір помаркованих даних та менший набір немаркованих даних. Даний спосіб являє собою середнє між видом навчання без учителя та з учителем. На думку авторів [85-87], саме напівавтоматичне навчання дозволяє досягнути більшої точності моделей [85-87].

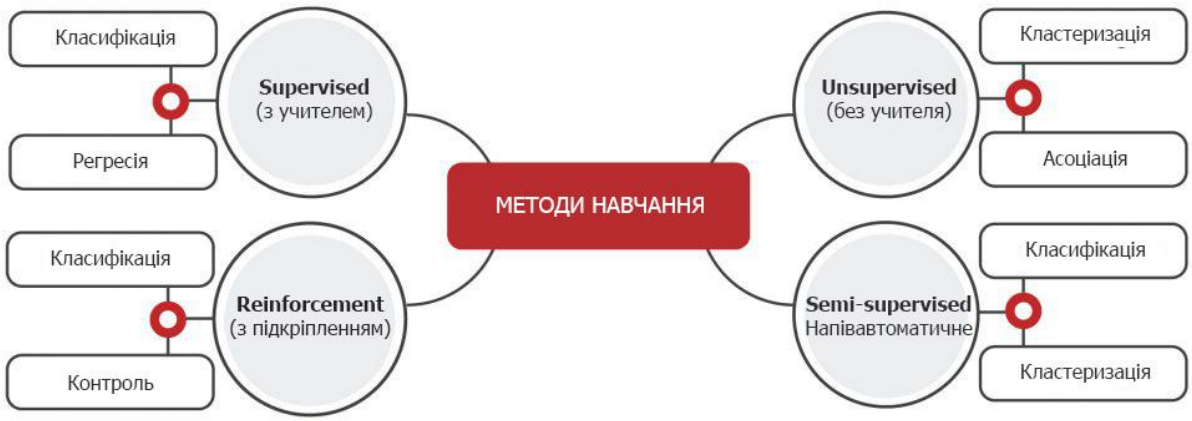


Рисунок 2.7 - Існуючі методи машинного навчання

Вибір моделі також включає вибір її стратегії навчання. Цей результат навчання використовується для модифікації моделі з метою покращення її ефективності. Існують багато навчальних алгоритмів для мінімізації помилок, більшість з яких базуються на градієнтному спуску. Навчальні алгоритми мають власні гіперпараметри, включаючи функцію, яка використовується для обчислення помилки моделі (наприклад, середня квадратична помилка), і розмір партії, тобто кількість мічених зразків, які подаються до моделі для накопичення значення помилки до використовувати для адаптації самої моделі.

Метод зворотного поширення помилки (англ. Backpropagation) – ітеративний метод, в основі якого лежить алгоритм оновлення ваг багатошарового перцептрону за допомогою обчислення стохастичного градієнтного спуску [90-94] для мінімізації помилок роботи нейронної мережі. Під час ітерації даного методу відбувається поширення сигналів помилки від виходів до входів мережі. Однак, даний метод вимагає використання диференційованої передавальної функції.

1974 року був одночасно описаний А. Галушкіним [90] і Полом Дж. Вербосом [91]. Популярності набув після розвитку Девідом І. Румельхартом, Дж. Е. Хінтон і Рональдом Дж. Вільямсом [92].

Зрізаний лінійний вузол[95] або випрямлений лінійний вузол[96] (англ. rectified linear unit, ReLU), є диференційованою передавальною функцією (функцією активації), яка математично визначена таким чином:

$$f(x) = x^+ = \max(0, x)\,,$$

де *x* - вхідне значення нейрона.

Вона є аналогом напівперіодичного випрямляча у схемотехніці. Ця передавальна функція була запроваджена для динамічних мереж Ганлозером (англ. Hahnloser) та іншими у 2000 році[97] з біологічним підґрунтям та математичним обґрунтуванням.

ReLU часто використовується в задачах комп'ютерного зору та розпізнавання мови.

2.2.2. Розробка алгоритму попередньої підготовки даних

На етапі збору даних дані отримуються з безлічі джерел. Необроблені дані можуть мати будь-яку структуру або не мати її взагалі, щоб скласти багатовимірні набори даних (вектори), для подальшого використання та зберігання. Дані можна отримувати безпосередньо з джерел у режимі реального часу, також відомим як потокове передавання, або шляхом імпорту пакетів даних, коли дані періодично імпортуються великими макропакетами або невеликими мікропакетами.

Набори даних - це, як правило, сукупність записів даних з різноманітними властивостями та супутніми деталями, що походить від моделі даних. Однак відкритих наборів даних, що стосуються оцінки зрілості інформаційних систем, немає. Причиною цього є конфіденційність та етика корпоративних даних.

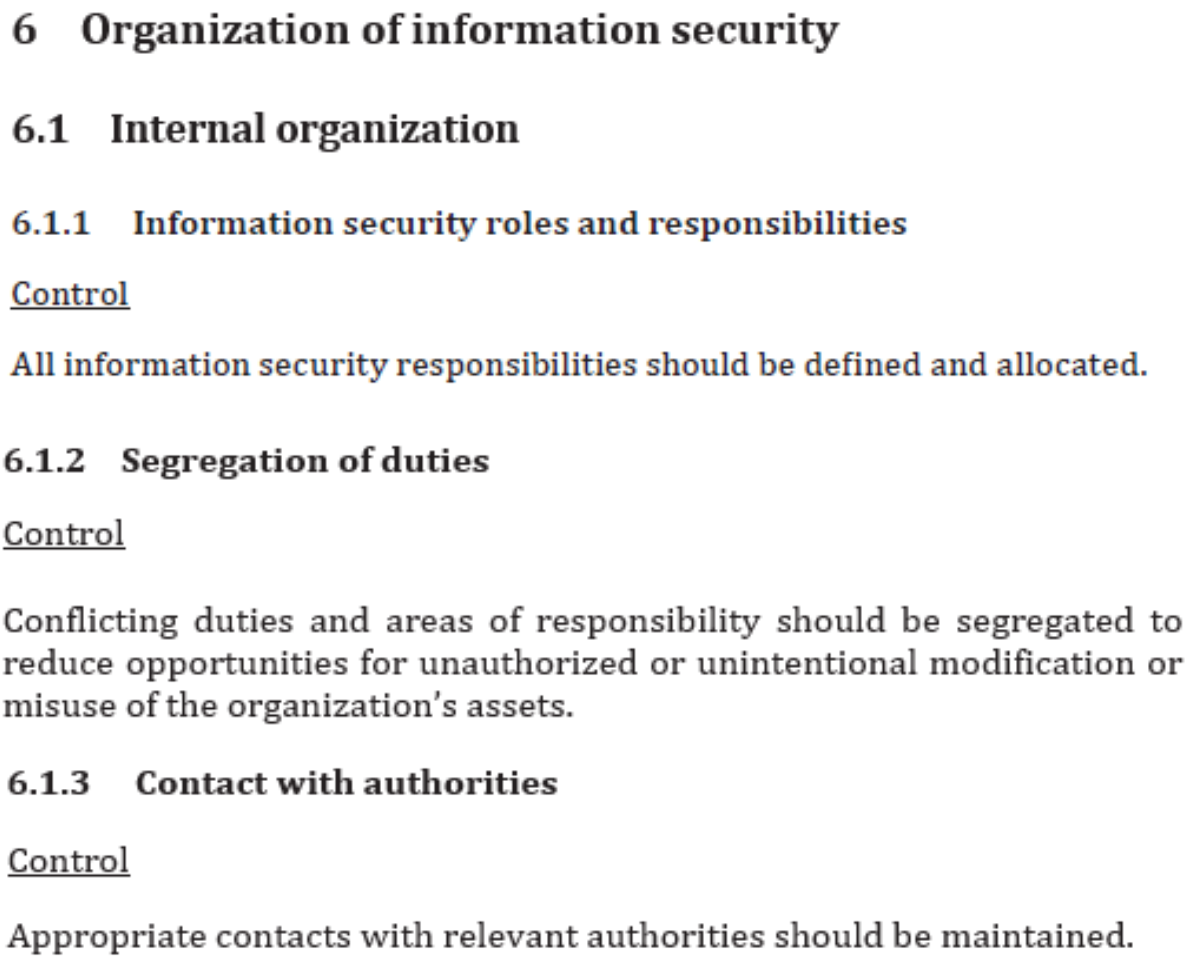
Внаслідок данох обставини, вхідні дані генерувались випадковим чином відповідно до опитувальника, заснованого на порівнянні стандартів ISO 27X та стандартах ISO 21827: 2008 для оцінки зрілості для конкретних цілей цього дослідження.

Міжнародний стандарт ISO / IEC 27002:2017 [73] дає рекомендації для розробки і впровадження організаціями системи менеджменту інформаційної безпеки, в контексті вибору, впровадження та управління коштами управління з урахуванням наявних ризиків. Він містить понад повний опис і рекомендації по впровадженню засобів управління інформаційною безпекою в порівнянні з міжнародним стандартом ISO / IEC 27001 до: 2013.

Даний міжнародний стандарт містить 14 розділів, що містять 35 основних категорій інформаційної безпеки і 114 засобів управління, перелік яких подано в стандарті ISO / IEC 27001 (Додаток А). Відзначимо, що

порядок розділів абсолютно не відображує порядок їх важливості для конкретної організації.

Анкета підготовлена з урахуванням усіх доменів та засобів управління ISO / IEC 27002:2017. Приклад структури контролів ISO / IEC 27002:2017 навенедно на рис. 2.8. Зразок анкети наведено в таблиці 10:



6 Organization of information security

6.1 Internal organization

6.1.1 Information security roles and responsibilities

Control

All information security responsibilities should be defined and allocated.

6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

Рисунок 2.8 - Зразок структури розділів та контролів у ISO 27002

Нехай A1 є атрибутом, який представляє оцінку контролю безпеки. Атрибут набуває значень в діапазоні від 0 до 5. Математично його можна визначити наступним чином:

$$A1 \in I = \{0, \dots, 5\}.$$

Набір даних складається з 10831 екземплярів. Екземпляр даних складається з двох частин, набору оцінок контролю безпеки та пов'язаного з ним класу. Приклад набору даних продемонстровано на Рис. 2.9.

Таблиця 2 10

Зразок опитувальника

Питання	Опис	Розділ ISO/IEC 27002:2013	Оцінка
Чи підтримує організація стандарти конфігурації безпеки інформаційних систем і застосунків?	Наскільки зрілими є стандарти «зміцнення» для різних платформ, щоб забезпечити більш сильні налаштування безпеки, ніж передбачено за замовчанням?	12.1.2 Управління змінами	[0..5]
Чи перевіряються, авторизуються та повідомляються зміни в інформаційних системах?	Чи існує процес контролю змін для виробничих систем, таких як те, що зміни просто не вносяться «на льоту» програмістами, системними адміністраторами, адміністраторами баз даних або іншими?	12.1.2 Управління змінами	[0..5]
Чи достатньо відокремлені обов'язки для забезпечення ненавмисної або несанкціонованої зміни інформації?	Наскільки добре виконано розподіл обов'язків? Чи мають розробники доступ до виробництва? Чи має адміністратор баз даних прихований доступ до баз даних?	6.1.2 Розподіл обов'язків	[0..5]

3	5	0	2	1	Planned
5	2	2	1	3	WellDefined
4	4	5	3	0	Planned
2	2	2	4	5	WellDefined
3	4	5	3	3	Planned
5	1	5	4	0	Planned
4	1	2	0	5	Planned
5	3	1	1	0	Planned

Рисунок 2.9 - Приклад набору даних

2.2.3. Підготовка даних до навчання

Дослідження даних - дуже трудомістка фаза життєвого циклу. На цьому етапі важливо розуміти тип даних, які були зібрані. Числові та категоріальні є найбільш відомими категоріями разом із мультимедійними даними (наприклад, зображеннями, аудіо, відео тощо) [75].

Числові дані піддаються побудові графіків і дозволяють обчислювати описову статистику та перевіряти, чи відповідають дані простим параметричним розподілам, наприклад, розподілу Гаусса. Значення відсутніх даних також можна виявити та обробити на етапі дослідження. Категоричні змінні - це ті, які мають дві або більше категорії, але без внутрішнього порядку. Якщо змінна має чітке впорядкування, то вона розглядається як порядкова змінна.

Графічне представлення частотного розподілу екземплярів даних у наборі навчальних матеріалів за відповідним класом показано на Рис. 12.

На етапі попередньої обробки даних використовуються методи очищення, інтеграції та трансформації даних. Цей процес спрямований на покращення якості даних, що покращить продуктивність та ефективність загальної моделі, заощадивши час на етапі навчання аналітичних моделей та сприяючи покращенню якості результатів. Зокрема, термін очищення даних

позначає методи виправлення невідповідностей, усунення шуму та анонімізації / псевдонімізації даних.

Інтеграція даних об'єднує дані, що надходять з декількох джерел, тоді як перетворення даних готує дані для подачі аналітичної моделі, як правило, шляхом кодування в числовому форматі. Типовим кодуванням є одноразове кодування, яке використовується для представлення категоріальних змінних як двійкових векторів. Це кодування спочатку вимагає, щоб категоріальні значення були зіставлені з цілими значеннями. Потім кожне ціле значення представляється у вигляді двійкового вектора, що є всіма нульовими значеннями, крім положення цілого числа, яке позначене 1.

Після перетворення в числа дані можуть піддаватися подальшим типам трансформації: повторному масштабуванню, стандартизації, нормалізації та маркуванню. В кінці цього процесу отримується числовий набір даних, який буде основою для навчання, тестування та оцінки моделі.

Як показано на Рис.2.10, вхідний набір даних має однаки нормального розподілу.

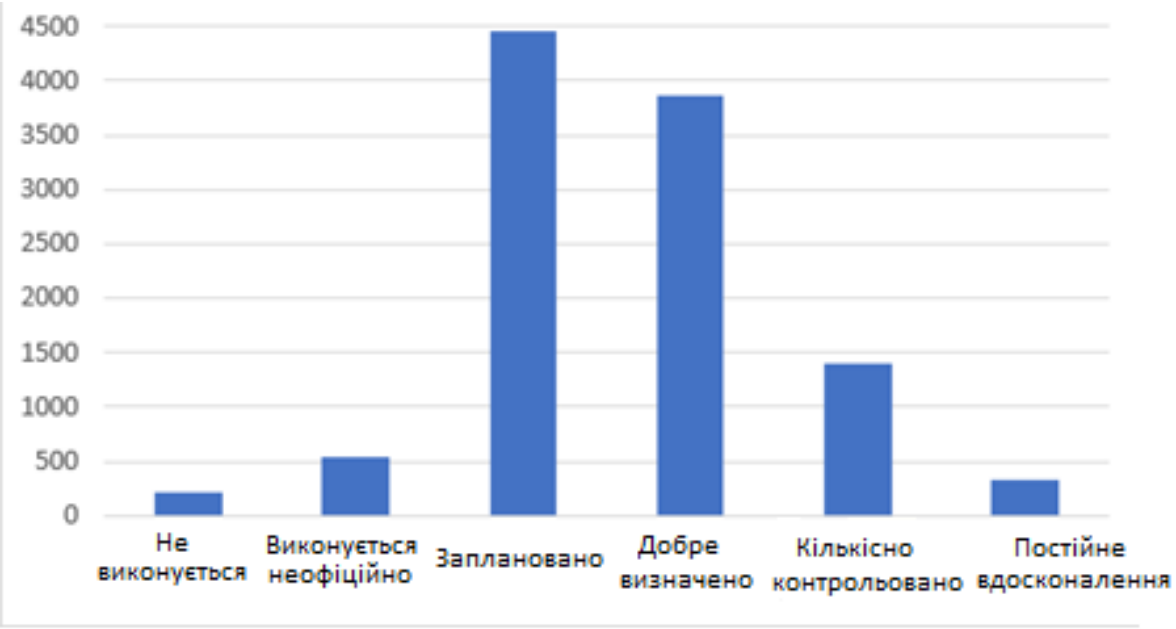


Рисунок 2.10 Розподіл екземплярів даних у навчальній вибірці

2.2.4. Синтез та навчання моделі з використанням штучних нейронних мереж

З вищезазначених причин було визначено будувати модель оцінки зрілості на основі ANN, штучної нейронної мережі прямого поширення сигналу із зворотним розповсюдженням похибки, зокрема багатошаровий перцептрон.

Багатошаровий персептрон - це вид організації нейронної мережі прямого поширення сигналу [83]. Типовим перцептроном є повністю насичена мережа, що означає, що кожен вузол в одному рівні з'єднується з певною вагою до кожного вузла в наступному шарі. Як правило, він складається з вхідного шару, прихованих шарів та вихідного шару, як показано на рис. 2.11.

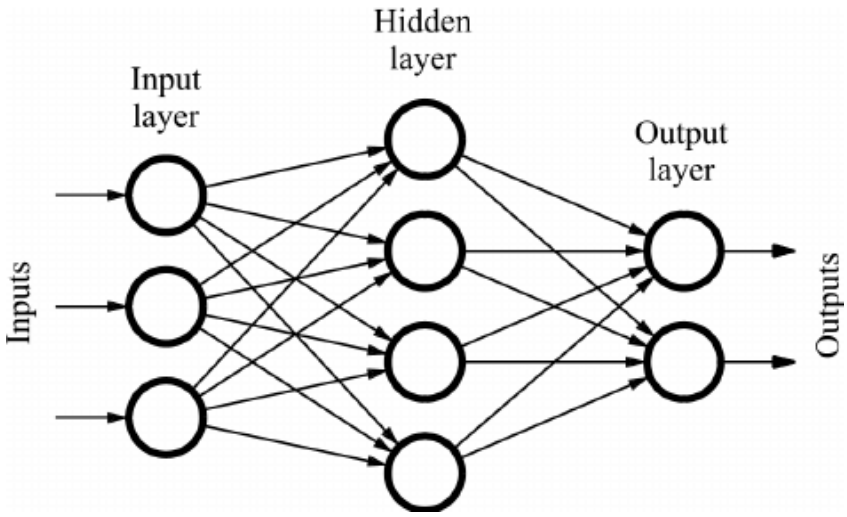


Рисунок 2.11 - Багатошаровий перцептрон з одним прихованим шаром

Запропонована модель складається з трьох шарів вузлів: вхідного шару, прихованого шару та вихідного шару. Початкові ваги визначаються випадковим чином.

Вхідний рівень представлений вхідними змінними. Приховані шари виконують певні перетворення над вхідними даними. Вузол у прихованому шарі використовує зважене лінійне підсумовування та, зокрема, функцію

активації. Тоді вихідний рівень отримує значення з останнього прихованого шару. Вихідний рівень виробляє вихідні значення, тобто вердикт або прогноз з урахуванням вхідних даних.

Для визначення виходу мережі використовується функція активації ReLU.

Модель зрілості можна вважати структурованою сукупністю елементів, що деталізують особливості ефективних процесів СУІБ, тоді кількість вузлів на вхідному рівні дорівнює кількості елементів керування ISO: 27002: 2013, а вхідними даними для кожного вузла є розрахункове значення для конкретного контролю безпеки відповідно. Деталі збору наборів даних описані в попередньому розділі. Таким чином, вхідний вектор можна визначити, як у (1), де x_1, x_2, ..., x_n позначають оцінку для конкретного $i^{го}$ контролю безпеки, а n – це кількість вузлів у вхідному шарі.

$$X^T = [x_1\ x_2 \cdots x_n],\ x_i \in I = \{0, \ldots, 5\} \quad (2.1)$$

Вихідний рівень моделі складається з 6 вузлів, які представляють рівень зрілості, як описано раніше. Правило відображення рівня зрілості описане в Таблиці 2.11.

Таблиця 2.11

Правило відображення рівня зрілості

Назва рівня	**Числове значення**
Не виконується	0
Виконується неофіційно	1
Заплановано	2
Добре визначено	3
Кількісно контрольовано	4
Постійне вдосконалення	5

Кількість нейронів прихованого шару визначено у відповідності з кращими практиками, зокрема, як середнє арифметичне між кількістю вузлів у вхідному та вихідному шарах і дорівнює 60.

Алгоритм обраної моделі нейронної мережі реалізований в програмному забезпеченні Weka [74]. Середовище Waikato для аналізу знань (Weka) - це безкоштовна бібліотека класів Java, розроблена для дослідницьких цілей в університеті Ваїкато (Нова Зеландія). Він пропонує широкий спектр алгоритмів та інструментів машинного навчання: попередня обробка даних, класифікація, регресія, кластеризація, правила вилучення асоціацій, візуалізація тощо.

Weka також містить Інтерфейс прикладного програмування, написаний на Java, який реалізує існуючі алгоритми навчання з мінімальними налаштуваннями.

Дане ПЗ підтримує імпорт даних у форматі ARFF (Attribute-Relation File Format). Це текстовий файл ASCII, який описує модель даних через атрибути та екземпляри даних. Файли ARFF впорядковані в такому порядку: назва відношення, список використаних атрибутів та екземпляри даних, що подаються рядок за рядком [74].

Приклад згенерованих даних у форматі ARFF відобрадено на Рис. 2.12.

```
@relation MaturityLevels

@attribute A1 {0,1,2,3,4,5}
```

Рисунок 2.12 - Приклад згенерованих даних у форматі ARFF

Після попередньої підготовки, обрана модель повинна пройти фазу навчання. Під час навчання моделі подаються пакети вхідних векторів і, використовуючи обрану функцію активації для адаптації внутрішніх параметрів моделі, зіставляє розраховані дані з вхідного набору з позначеною міткою. Це дозволяє моделі зрозуміти дані, краще їх аналізувати,

і таким чином поступово призводить до більш точних, очікуваних результатів.

Алгоритм зворотного розповсюдження обрано для навчання моделі. Ідея полягає в тому, щоб розрахувати похибку між передбачуваним та фактичним значенням і зменшити частоту помилок після неї, змінивши всі ваги через шари. Цільове значення відоме за атрибутом class навчального набору даних.

Для підвищення надійності результатів наявний набір даних розділяється на навчальний набір, що використовується для встановлення параметрів моделі, і тестовий тестів, де критерії оцінки (наприклад, частота помилок) реєструються лише для того, щоб оцінити ефективність моделі поза навчальним набором.

Схеми перехресної перевірки випадковим чином розділяють кілька разів набір даних на тренування та тестову частину фіксованих розмірів (наприклад, 80% та 20% доступних даних), а потім повторюють етапи навчання та перевірки на кожному розділі.

Налаштування моделі зазвичай накладається на етап навчання моделей. Деякі параметри визначають роботу моделі на високому рівні, такі як їх функція навчання чи модальність, і їх неможливо дізнатись із вхідних даних. Ці спеціальні параметри, які часто називають гіперпараметрами [98], потрібно налаштовувати вручну, хоча за певних обставин вони можуть бути налаштовані автоматично шляхом пошуку простору параметрів моделі. Цей пошук, який називається оптимізацією гіперпараметрів [98], часто виконується за допомогою класичних методів оптимізації, таких як Grid Search, але можна використовувати випадковий пошук та байєсівську оптимізацію.

Важливо зауважити, що на етапі налаштування моделі використовується спеціальний набір даних, який часто називають набором для перевірки, відмінний від навчальних та тестових наборів, що використовувались на попередніх етапах. Також може бути розглянута фаза

оцінки для оцінки меж результатів та оцінки поведінки моделі в екстремальних умовах, наприклад, із використанням неправильних / небезпечних наборів даних. Важливо зазначити, що, залежно від кількості гіперпараметрів, що підлягають регулюванню, спробувати всі можливі комбінації може бути просто недоцільним.

Для навчання моделі використовувались такі гіперпараметри: швидкість навчання 0.3 швидкість оновлення ваги 0.2, час навчання 50. Набір даних навчання складається з 10831 прикладів оцінки зрілості.

Швидкість навчання являє собою розмір кроку на кожній ітерації та визначає, наскільки швидко модель адаптується до проблеми. Імпульс – це значення швидкісті оновлення ваги. А час навчання - це кількість епох, які потрібно пройти моделі. [98]

Висновки за розділом 2

В даному розілі виконано наступні задачі:

1. Виконати порівняльний аналіз моделей зрілості у сфері ІБ;
2. Визначення базової парадигми моделі оцінювання;
3. Розробка алгоритму попередньої підготовки даних;
4. Підготовка даних для моделювання;
5. Синтезувати модель зрілості СУІБ з визначенням відповідності досліджуваної ІС на відповідність вимогам стандарту ISO/IEC 27001:2017 з використанням технологій штучного інтелекту та здійснити її навчання;

Проаналізувавши моделі зрілості можливостей кібербезпеки, отримані в результаті систематичного огляду, була складена таблиця, що підсумовує порівняння між ними. Результати дослідження свідчать про те, що моделі зрілості можливостей кібербезпеки мають суттєву подібність. Основна відмінність визначається у сфері, на яку вони орієнтовані, та в рівні глибини найкращих практик, які слід застосувати.

Усі моделі можуть бути адаптовані до різних типів організацій; однак їм потрібен певний рівень налаштування. Єдиною зрілою моделлю можливостей кібербезпеки, яка орієнтована на кібербезпеку, оновлюється і орієнтована на всю організацію, є C2M2. Усі моделі зрілості можливостей кібербезпеки базуються на управлінні ризиками кібербезпеки, але лише SSE-CMM та C2M2 вимірюють управління ризиками більш конкретним чином.

На основі результатів огляду літератури [27-32, 53-63], було виявлено кілька робіт, які можуть бути використані для визначення відповідності стандарту ISO/IEC 27001:2017. Однак, не існує моделі зрілості, яка б задовільно враховувала вимоги ISO / IEC 27001. Відповідно, якщо жодна існуюча модель не здатна вирішити виявлену проблему, повинна бути розроблена нова модель зрілості.

Для цього, по-перше, було розроблено базову парадигму моделі зрілості, внаслідок чого для синтезу моделі було обрано аппарат нейронних мереж прямого поширення сигналу та зворотнього поширення похибки. Також підготовлено перелік вимог для кожного рівня зрілості у відповідності з вимогами стандарту ISO/IEC 27001 та ISO/IEC 27002. Для подальшого тренування та вирішення задачі класифікації було обрано алгоритм навчання з учителем, зворотнє поширення похибки для корекції внутрішніх параметрів моделі та функцію активації ReLU.

Наступним етапом була розробка алгоритму попередньої підготовки даних до навчання та власне підготовка даних. Для цього було сформовано та продемонстровано анкету з урахуванням усіх доменів та засобів управління ISO / IEC 27002:2017 і згенеровано дані.

Останнім етапом був синтез та навчання моделі з використанням аппарату нейронних мереж. Окрім раніше зазначеного, модель має наступну конфігурацію:

- Кількість нейронів у шарі входу: 114.
- Кількість нейронів у прихованому шарі: 60.

- Кількість нейронів у шарі виходу: 6.
- Швидкість навчання 0.3.
- Швидкість оновлення ваги 0.2.
- Час навчання 50.
- Набір даних навчання складається з 10831 прикладів оцінки зрілості.

РОЗДІЛ 3
ПЕРЕВІРКА АДЕКВАТНОСТІ МОДЕЛІ ТА ПРОПОЗИЦІЇ ЩОДО ЇЇ ВДОСКОНАЛЕННЯ

В даному розділі буде проведений аналіз адекватності моделей та висунуті пропозиції щодо її вдосконалення. Аналіз адекватності дозволяє перевірити ступінь відповідності моделі реальній системі з набором певних властивостей [100].

Адекватність моделі визначається багатьма факторами, які відносяться до двох груп. Перша група включає фактори, зумовлені невизначеністю постановки задачі, неповнотою вихідної інформації та зневажанням деякими параметрами. Друга група включає виключення апроксимацію, інтерполяцію, припущення, заміну нелінійних елементів лінійними, ідеалізація функціонування системи і т.д. Тобто, включає в себе припущення та обмеження розробки моделі і призводить до систематичних похибок.

Перевірка адекватності моделі виконувалася у декілька етапів:

1. Оцінка охоплення контролів за допомогою онтологічних дефіцитів Ванда та Вебера [99]. Див. Рис.;
2. оцінка охоплення контролів та вимог стандарту ISO / IEC 27001 моделлю зрілості СУІБ, за методологією, використаною у попередньому розділі під час порівнянь інших моделей.

3.1 Аналіз адекватності моделі за методом Ванда та Вебера

Щоб оцінити повноту охоплення вимог стандарту ISO/IEC 27001 розробленою моделлю зрілості, було проведено аналіз за методом Ванда та Вебера. Ванд і Вебер визначають онтологічну оцінку методу граматики, де порівнюються два набори концепцій для виявлення чотирьох онтологічних недоліків, як показано на Рис. 3.1:

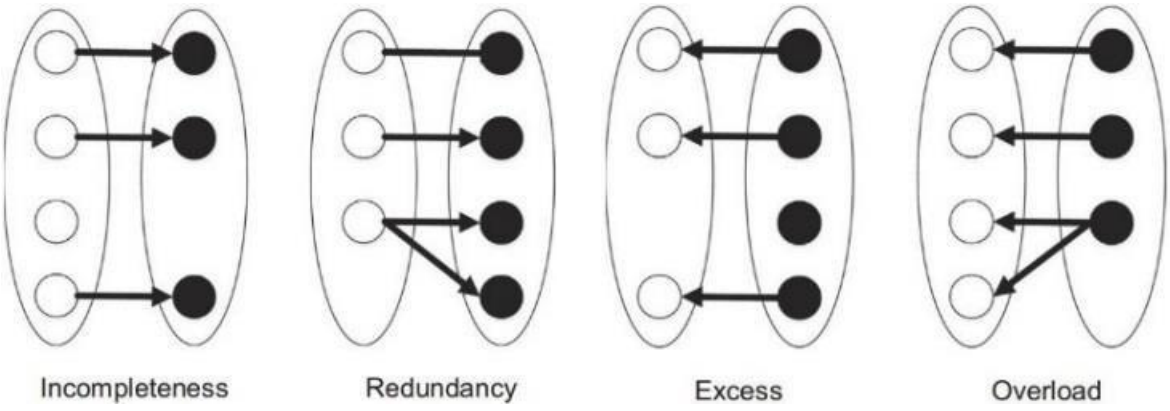


Рисунок 3.1 - Онтологічні дефіцити Ванда та Вебера [99]

- Незавершеність - чи можна кожен елемент першого набору зіставити з елементом другого набору? Якщо немає тотального відображення, воно вважається неповним;
- Надлишковість - чи є елементи у першому наборі, що відображаються більше ніж одному елементу у другому наборі? Якщо так, відображення вважається Надлишковість;
- Надмірність - чи кожен елемент з другого набору зіставляється з елементом у другому наборі? Отображення вважається надмірним, якщо є елементи з другого набору без зв'язку;
- Перевантаженість - чи кожен елемент другого набору зіставляється лише з одним елементом першого набору? Охоплення вважається перевантаженим, якщо будь-який елемент у другому наборі має більше одного зв'язку з будь-яким елементом першого набору.

Онтологічна оцінка охоплення вимог стандарту ISO/IEC 27001 пропонованої моделі зрілості СУІБ детально викладена в таблиці 12.

Виходячи з результатів аналізу, модель є завершеною, адже має повне покриття контролів IEC 27001. Надмірність та надлишок відсутні. Однак, вимога ISO / IEC 27001 “4.2.3- d)” була перевантажена, оскільки, на наш погляд, вона описує вимоги до трьох різних видів діяльності. В результаті, було створено три різні критерії оцінки для цієї вимоги. Нарешті, модель

зрілості СУІБ охоплює всі вимоги, деталізовані в розділі 4 ISO/IEC 27001, що означає, що загальний бал за тією ж шкалою становить 20.

Таблиця 3.1

Охоплення вимог стандарту ISO/IEC 27001 пропонованої моделі зрілості СУІБ за методом оцінки Ванда та Вебера

Етап циклу Демінга	Контролі пропонованої моделі зрілості	Вимога ISO/IEC 27001	Оцінка за методом Ванда та Вебера
Планування	**Рівень зрілості: заплановано**		
	Визначити сферу застосування та межі СУІБ.	4.2.1 - a)	Повний
	Розробити політику СУІБ.	4.2.1 – b)	Повний
	Визначити підхід до оцінки ризиків.	4.2.1 – c)	Повний
	Виконати ідентифікацію ризиків.	4.2.1 – d)	Повний
	Проведення аналізу та оцінки ризиків.	4.2.1 – e)	Повний
	Визначення варіантів оброблення ризиків.	4.2.1 – f)	Повний
	Визначення цілей та контролів критеріїв для оброблення ризиків.	4.2.1 – g)	Повний
	Отримати дозвіл на затвердження залишкових ризиків.	4.2.1 – h)	Повний
	Отримати дозвіл на впровадження та функціонування СУІБ.	4.2.1 – i)	Повний
	Підготовка положення про застосовності.	4.2.1 – j)	Повний

Таблиця 3.2

Охоплення вимог стандарту ISO/IEC 27001 пропонованої моделі зрілості СУІБ за методом оцінки Ванда та Вебера (продовження)

Виконання	**Рівень зрілості: Добре визначено**		
	Сформулювати план оброблення ризиків.	4.2.2 - a)	Повний
	Впровадити план оброблення ризиків.	4.2.2 - b)	Повний
	Впровадженння обраних контролів.	4.2.2 - c)	Повний
	Визначити як вимірювати ефективність впроваджений контролів.	4.2.2 - d)	Повний
	Впровадити програми з навчання та поінформованості.	4.2.2 - e)	Повний
	Управляти функціонуванням СУІБ.	4.2.2 - f)	Повний
	Управляти ресурсами СУІБ.	4.2.2 - g)	Повний
	Впровадити процедури та інші контролі для уможливлення термінового виявлення подій безпеки та реагування на інциденти безпеки.	4.2.2 - h)	Повний
Перевірка	**Рівень зрілості: кількісно контрольовано**		
	Виконувати процедури моніторингу та перегляду, а також інші контролі.	4.2.3 – a)	Повний
	Проводити регулярні перегляди ефективності СУІБ.	4.2.3 – b)	Повний
	Вимірювати ефективність контролів.	4.2.3 – c)	Повний
	Переглядати оцінку ризиків.	4.2.3 – d)	Перевантажений
	Переглядати залишкові ризики.	4.2.3 – d)	Перевантажений

Таблиця 3.3 – Охоплення вимог стандарту ISO/IEC 27001 пропонованої моделі зрілості СУІБ за методом оцінки Ванда та Вебера (продовження)

Перевірка	**Добре визначено: постійне вдосконалення**		
	Впроваджувати в СУІБ ідентифіковані вдосконалення.	4.2.4 – a)	Повний
	Здійснювати відповідні коригувальні та запобіжні дії.	4.2.4 – b)	Повний
	Доводити до відома всіх зацікавлених сторін інформацію щодо дій та вдосконалень СУІБ.	4.2.4 – c)	Повний
	Забезпечувати, що вдосконалення досягають намічених цілей.	4.2.4 – d)	Повний
Дія	**Добре визначено: постійне вдосконалення**		
	Впроваджувати в СУІБ ідентифіковані вдосконалення.	4.2.4 – a)	Повний
	Здійснювати відповідні коригувальні та запобіжні дії.	4.2.4 – b)	Повний
	Доводити до відома всіх зацікавлених сторін інформацію щодо дій та вдосконалень СУІБ.	4.2.4 – c)	Повний
	Забезпечувати, що вдосконалення досягають намічених цілей.	4.2.4 – d)	Повний

Після перших двох етапів оцінки ми оцінили п’ять реальних організацій. Дані були анонімізовані для забезпечення конфіденційностію

Організація "1" - державний інститут, відповідальний за сприяння та розвиток адміністративної модернізації у своїй країні. Його функціонування відбувається за трьома напрямами: обслуговування споживачів, цифрове перетворення та спрощення.

Організація “2” – є частиною ділового сектору уряду країни, який виробляє та постачає товари та послуги, що вимагають високих стандартів безпеки, а саме: монети, банкноти та документи, такі як картки громадянина та паспорти.

Організація "3" - це державний вищий навчальний заклад, в якому навчається приблизно 13 700 студентів.

Організація "4" - це державна установа науково-технічних досліджень та розробок, метою якої є сприяння створенню, розвитку та розповсюдженню досліджень у галузях, пов'язаних з цивільним будівництвом.

Організація "5" - це приватна організація, яка займається розробкою та обслуговуванням програмного забезпечення, надаючи послуги по всьому світу з різними офісами в Європі. Для кожної з цих п’яти організацій була виконана оцінка зрілості СУІБ. Результат оцінювання відображений у Таблиці 3.4. У цій таблиці «+» означає задовільну оцінку, порожня клітинка означає незадовільну оцінку. В останніх стовпцях показано кінцевий рівень зрілості для кожної організації.

Таблиця 3.4

Результат оцінки зрілості підприємств з використанням пропонованої моделі зрілості СУІБ

Контроль	**Організація**				
	1	**2**	**3**	**4**	**5**
2.1	+	+	+	+	+
2.2	+	+	+	+	+
2.3	+	+	+	+	+
2.4	+	+	+	+	+
2.5	+	+	+	+	+
2.6	+	+	+	+	+
2.7	+	+	+	+	+
2.8	+	+	+	+	+
2.9	+	+	+	+	+
2.1	+	+	+	+	+
3.1	+	+		+	+
3.2	+	+		+	+

3.3	+	+		+	+
3.4	+	+		+	+
3.5	+	+	+	+	+
3.6	+	+	+	+	+
3.7	+	+	+	+	+
3.8	+	+		+	+
4.1	+			+	+
4.2	+			+	+
4.3	+		+	+	+
4.4	+			+	
4.5	+			+	+
4.6	+	+		+	
4.7	+	+		+	
4.8	+	+	+	+	
4.9	+			+	+
4.1	+			+	
5.1	+				+
5.2	+				+
5.3	+				
5.4	+				
Рівень зрілості	**5**	**3**	**2**	**4**	**3**

Для досягнення певного рівня зрілості організація повинна відповідати всім критеріям для цього конкретного рівня та всім рівням нижче, що означає, що організація на рівні зрілості 3 відповідає всім критеріям рівня зрілості 1, 2 і 3.

Як можна зрозуміти з таблиці 3.4, ми змогли оцінити виконання кожного з контролів оцінки, що, у свою чергу, дозволило нам визначити рівень зрілості СУІБ для кожної з п’яти організацій. Результати оцінки показали, що модель зрілості правильно визначала рівні зрілості, і вони насправді відповідають сприйняттю зрілості СУІБ, впровадженій в організації. Потім ці результати використовувались організаціями для створення планів вдосконалення, спеціально адаптованих до їх організаційного контексту.

3.2 Перевірка точності моделі за допомогою статистичних методів

Для перевірки точності моделі вихідний набір було розділено на менші частини: 70% для навчання, 15% для контрольної вибірки та 15% для тестової вибірки. Після цього модель була оцінена двома різними методами: спочатку проводився метод перехресної перевірки для ідентифікації статистичних даних про ефективність моделі, потім модель знову тренували, але використовуючи 100% набору даних, щоб дати найбільш точну модель для отримання найнадійнішої класифікаційної моделі.

Результати навчання моделі представлені далі. Час, необхідний для тестування моделі на навчальних даних, становить 12.24 секунди. Підсумок результатів наведено в таблиці 3.5. Матрицю плутанини можна знайти в таблиці 15. Отримана точність за класами зображена в таблиці 3.5.

Таблиця 3.5

Підсумок аналізу точності моделі

Класифіковано правильно (у відсотках)	99.6492%
Класифіковано неправильно (у відсотках)	0.3508 %
Каппа-коефіцієнт	0.9949
Середня абсолютна похибка	0.002
Середньоквадратична похибка	0.0329
Відносна похибка	0.8814%
Середньоквадратична відносна похибка	9.7481%

Статистика Каппи описує точність класифікатора[101]. Якщо значення менше або дорівнює нулю, це означає, що не існує відповідності (узгодженості) між еталонним значенням та вхідним вектором даних. В іншому випадку, якщо значення знаходиться в діапазоні від 0.01 до 0.20, це означає, що узгодженості немає або існує незначна. Діапазон 0.21–0.40 можна інтерпретувати як незначний рівень точності. 0,41–0,60 – середній

рівень точності. 0.61–0.80 великий рівень точності, а 0.81–1.00 – дуже високий рівень точності.

Помилковою класифікацією вважатимемо таку класифікацію, під час якої було зараховано вхідний вектор даних до класу, якому він не належить. Матриця невідповідностей використовується для оцінки ефективності класифікаційної моделі [101]. Вона надає інформацію про невідповідність класифікацій, яка також може бути використана для визначення ймовірної тенденції наявних помилок.

Таблиця 3.6

Матриця невідповідностей

Рівень 0	Рівень 1	Рівень 2	Рівень 3	Рівень 4	Рівень 5	Класифіковано як
208	10	0	0	0	0	Рівень 0
6	526	7	5	0	0	Рівень 1
0	0	4462	0	0	0	Рівень 2
0	0	10	3847	0	0	Рівень 3
0	0	0	0	1410	0	Рівень 4
0	0	0	0	0	340	Рівень 5

Матриця невідповідностей демонструє, що для перших трьох класів існують помилкові класифікації, що може бути викликано недостатньо збалансованим набором даних. Це означає, що даний набір даних слід скоригувати для досягнення кращих результатів у майбутніх дослідженнях

Істинно позитивні і справжні негативні класифікації вказують, коли класифікатор виконав задачу правильно. Хибні позитивні та помилкові класифікації вказують, коли класифікатор помилився.

Точність - міра правильності; він показує відсоток правильно позначених позитивних екземплярів даних, так що його також називають

прогнозним позитивним значенням. Низьке значення точності, як правило, пов’язане з більшою кількістю помилкових спрацьовувань.

Таблиця 3.7

Матриця невідповідностей

Клас	0	1	2	3	4	5	Зважене середнє
Істинно позитивні результати	0.954	0.967	1	0.997	1	1	0.996
Істинно негативні результати	0.001	0.001	0.003	0.001	0	0	0.001
Влучність	0.972	0.981	0.996	0.999	1	1	0.996
Повнота	0.954	0.967	1	0.997	1	1	0.996
F-міра	0.963	0.974	0.998	0.998	1	1	0.996
MCC	0.962	0.973	0.997	0.997	1	1	0.995
Площа ROC-кривої	1	0.991	0.998	0.998	1	1	0.998
Площа PRC-кривої	0.987	0.979	0.994	0.997	1	1	0.995

Влучність - це статистична метрика, що виявляє відсоток правильно класифікованих позитивних результатів. Дану метрику також називають значущістю. Низьке значення влучності, як правило, пов’язане з високою кількістю хибних позитивних класифікацій [101].

Повнота - це статистична метрика, що виявляє відсоток даних, які позначені як позитивний результат. Дану метрику також називають чутливістю. Низьке значення чутливості, як правило, пов’язана з великою кількістю помилкових негативних класифікацій[101].

F-Міра - це міра точності моделі на наданому наборі даних [101], являє собою середнє гармонійне між влучністю та повнотою. Набуває значень від 0 до 1, де 1 – найвищі значення повноти та влучності.

Коєфіцієнт кореляції Метью (MCC) або коефіцієнт фі використовується в машинному навчанні як показник якості бінарних класифікацій [101].

Крива робочої характеристики приймача (receiver operating characteristic, ROC) використовується для опису залежності використовуваних параметрів, щоб в одному випадку модель могла правильно виконувати класифікацію позитивних випадків, а в іншому випадку вона неправильно трактує негативні випадки як позитивні. Площа, обмежена даної кривою, використовується як показник точності класифікатору. Чим ближче значення до 1, тим вище точність [101].

Крива «повнота-влучність» (precision-recall curve, PRC) показує відношення значення точності для відповідних значень чутливості. Площа під кривою може бути використана як підсумок продуктивності роботи моделі. [101] Дана метрика виявляється зазвичай більш інформативною, коли вибірка вхідних даних сильно нерівномірна; це альтернатива ROC-кривих для даних з нерівномірним розподілом.

Отже, навчена модель успішно класифікувала 99,649% набору даних, надійність класифікатора становить 0.9949, що можна трактувати як майже ідеальне узгодження даниз, а середньоквадратична відносна похибка становить 9.748%. Серед інших результатів тренованої моделі: коефіцієнт істинних спрацьовувань – 0.996, коефіцієнт помилкових спрацьовувань – 0.001, влучність – 0.996, повнота- 0.996, f-міра – 0.996, коєфіцієнт кореляції Метью – 0.995, площа ROC - 0,998, площа PRC – 0.995.

Наведені значення вказують на те, що навчена модель описує реальний неавтоматизований процес оцінки зрілості ІС на прийнятному рівні, і її можна рекомендувати використовувати в процесі реального аудиту СУІБ.

Висновки за розділом 3

В даному розділі було вирішено задачу проведення аналізу адекватності розробленої моделі.

В результаті виконання задачі було виявлено, що пропонована модель є завершеною, адже має повне покриття контролів IEC 27001. Надмірність та надлишок відсутні. Навчена модель описує реальний неавтоматизований процес оцінки зрілості ІС на прийнятному рівні, і її можна рекомендувати використовувати в процесі реального аудиту СУІБ.

Модель, розроблена в результаті цього дослідження, може бути використана як частина системи підтримки прийняття рішень, щоб дати особам, що приймають рішення в галузі кібербезпеки, (а) приймати обґрунтовані рішення, вибираючи найкращий варіант для пом'якшення визначених вразливостей / загроз та підтримання безперервності бізнесу у ворожому кіберсередовищі; (б) аналізувати сильні та слабки сторони процесів СУІБ; (в) для вироблення стратегії еволюційного вдосконалення можливостей, ефективності і результативності СУІБ. Як результат, це також сприятиме скороченню часу та фінансових ресурсів на оцінку безпеки підприємствами.

Розробка моделі моделі оцінки зрілості защищеності ІС була виконана на основі контролів та вимог ISO 27001 та ISO 27002 та аппарату нейронних мереж прямого поширення сигналу та зворотнього поширення похибки. Методологію, описану в цьому документі, можна розширити, щоб синтезувати модель для різних наборів контролю безпеки та визначення відповідності іншим стандартам безпеки або політиці безпеки підприємства.

Однак, щоб детальніше проаналізувати корисність моделі зрілості та вдосконалити дану модель, пропонується оцінити використання моделі зрілості СУІБ у різних галузях промисловості, це призведе до більш загальної а об’єктивної оцінки моделі і дозволить провести міжгалузевий бенчмаркінг.

ВИСНОВКИ

Кібербезпека стає одним з головних пріоритетів для більшості підприємств. Для досягнення прийнятного рівня кібербезпеки оцінка безпеки є одним із найважливіших завдань, яке потрібно виконати. Однак у сучасних інструментів є недоліки, коли мова йде про визначення відповідного рівня безпеки для кожної компанії або коли дані різноманітні або погано структуровані. Метою даної роботи було розробити модель оцінки захищеності ІС з урахуванням вимог стандарту ISO 27001:2017 та ISO27002:2017, яка могла б використовуватися на реальному підприємстві як частина системи підтримки прийняття рішень, щоб дати особам, що приймають рішення в галузі кібербезпеки:

а) приймати обґрунтовані рішення, вибираючи найкращий варіант для пом'якшення визначених вразливостей / загроз та підтримання безперервності бізнесу у ворожому кіберсередовищі;
б) можливість аналізувати сильні та слабки сторони процесів СУІБ;
в) можливість вироблення стратегії еволюційного вдосконалення можливостей, ефективності і результативності СУІБ.

Як результат, це сприятиме скороченню часу та фінансових ресурсів на оцінку безпеки підприємствами.

У вступі обґрунтовано актуальність обраної теми, визначено мету і сформульовані задачі для досягнення поставленої мети. Перераховані основні наукові результати досліджень, показана практична значимість та подано відомості по апробації роботи.

У першому розділі було проведено аналіз літературних джерел та постановка проблеми дослідження. В рамках даного аналізу було визначено сучасні підходи до забезпечення ІБ, теоретичні засади для створення систем підтрики прийняття рішень про захищеність ІС, особливості використання моделей зрілості в сфері ІБ та особливості використання засобів штучного

інтелекту в задачах ІБ. Заключний параграф включає в себе постановку завдань дослідження.

Суть пропонованого методу прийняття рішення полягає в формалізації оцінюваних характеристик безпеки, їх обробці та прийнятті рішення про безпеку ІС. Основними етапами методу є:

1. Визначення оцінюваних характеристик безпеки.

2. Розрахунок класифікаційних ознак (прийняття рішення).

3. Логічна обробка (інтерпретація рішення).

Таким чином, з експерта знімається навантаження з вирішення завдань визначення оцінюваних характеристик безпеки і прийняття рішення. Основним його завданням стає контроль роботи ІС і підтримка критеріїв оцінювання безпеки в актуальному стані.

Дослідження існуючих моделей зрілості інформаційнох безпеки дозволило встановити найбільш поширені моделі та визначити набір характеристик безпеки, оцінюваних експертом при прийнятті рішення про його безпеку. Однак, не існує моделі зрілості, яка б задовільно враховувала вимоги ISO / IEC 27001. Відповідно, було вирішено розробити нову модель зрілості.

Другий розділ присвячено розробці моделі оцінювання захищеності ІС.

Для цього, по-перше, було розроблено базову парадигму моделі зрілості, внаслідок чого для синтезу моделі було обрано аппарат нейронних мереж прямого поширення сигналу та зворотнього поширення похибки. Також підготовлено перелік вимог для кожного рівня зрілості у відповідності з вимогами стандарту ISO/IEC 27001 та ISO/IEC 27002.

Для подальшого тренування та вирішення задачі класифікації було обрано алгоритм навчання з учителем, зворотнє поширення похибки для корекції внутрішніх параметрів моделі та функцію активації ReLU.

Наступним етапом була розробка алгоритму попередньої підготовки даних до навчання та власне підготовка даних. Для цього було сформовано та

продемонстровано анкету з урахуванням усіх доменів та засобів управління ISO / IEC 27002:2017 і згенеровано дані.

Останнім етапом був синтез та навчання моделі з використанням аппарату нейронних мереж.

У третьому розділі особливу увагу приділено обґрунтуванню ефективності застосування даної моделі з використаннням апарату штучних нейронних мереж для вирішення поставленого завдання. Модель зрілості СУІБ була оцінена багатоперспективним методом та статистичними засобами.

В результаті виконання задачі було виявлено, що пропонована модель є завершеною, адже має повне покриття контролів IEC 27001. Надмірність та надлишок відсутні. Навчена модель описує реальний неавтоматизований процес оцінки зрілості ІС на прийнятному рівні, і її можна рекомендувати використовувати в процесі реального аудиту СУІБ.

Модель, розроблена в результаті цього дослідження, може бути використана як частина системи підтримки прийняття рішень, щоб дати особам, що приймають рішення в галузі кібербезпеки, (а) приймати обґрунтовані рішення, вибираючи найкращий варіант для пом'якшення визначених вразливостей / загроз та підтримання безперервності бізнесу у ворожому кіберсередовищі; (б) аналізувати сильні та слабки сторони процесів СУІБ; (в) для вироблення стратегії еволюційного вдосконалення можливостей, ефективності і результативності СУІБ. Як результат, це також сприятиме скороченню часу та фінансових ресурсів на оцінку безпеки підприємствами.

Рішення завдань дозволило зробити висновок, що мета, поставлена в роботі, повністю досягнута.

На підставі отриманих результатів необхідно зауважити, що методологію, описану в даній роботі, можна розширити для можливості синтезу моделі, яка б підтримувала різні набори контролю безпеки та

визначення відповідності іншим стандартам безпеки або політиці безпеки підприємства.

Для більш глибокого аналізу корисності моделі зрілості та її вдосконалення, пропонується оцінити використання моделі зрілості СУІБ у різних галузях промисловості, це призведе до більш загальної а об’єктивної оцінки моделі і дозволить провести міжгалузевий бенчмаркінг.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27000 Information security management systems. Overview and vocabulary - Системы менеджмента информационной безопасности. Обзор и терминология.

2. M. Z. Zgurovskyi (2016). Technology foresight of Ukrainian economy in the medium (up to 2020) and long term (until 2030) horizons (According to the materials of the scientific report at the meeting of the Presidium of NAS of Ukraine November 4, 2015), Visn. Nac. Akad. NaukUkr., Vol. 1, 2016, pp. 57–68. Available at: https://doi.org/10.15407/visn2016.01.057.

3. Panaousis, E. Cybersecurity Games and Investments: A Decision Support Approach [Text] / E. Panaousis, A. Fielder, P. Malacaria, C. Hankin, F. Smeraldi // Lecture Notes in Computer Science. – 2014. – P. 266–286. doi: 10.1007/978-3-319-12601-2_15

4. Fielder, A. Decision support approaches for cyber security investment [Text] / A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi // Decision Support Systems. – 2016. – Vol. 86. – P. 13–23. doi: 10.1016/j.СППР.2016.02.012

5. Chang, L.-Y. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system [Text] / L.-Y. Chang, Z.-J. Lee // 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY). – 2013. doi: 10.1109/ifuzzy.2013.6825462

6. Atymtayeva, L. Building a Knowledge Base for Expert System in Information Security [Text] / L. Atymtayeva, K. Kozhakhmet, G. Bortsova // Advances in Intelligent Systems and Computing. – 2014. – P. 57–76. doi: 10.1007/978-3-319-05515-2_7

7. Decision support for Cybersecurity risk planning Loren Paul Rees a, Jason K. Deane a,∗, Terry R. Rakes a, Wade H. Baker b a Department of Business Information Tech-logy, Pamplin College of Business, Virginia Tech., Blacksburg, VA 24061, United States b Verizon Business Security Solutions, Ashburn, VA 20147, United States

8. В.Л. Токарев, А.А. Сычугов МЕТОД АУДИТА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ Моделирование, оптимизация и информационные технологии. Научный журнал, Том 7, № 1 http://moit.vivt.ru/ doi: 10.26102/2310-6018/2019.24.1.036

9. Y. Cheng, J. Deng, J. Li, S. DeLoach, A. Singhal and X. Ou, "Metrics of Security," 2014. [Online]. Available: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=917850.

10. Ben-Asher, N. Effects of cyber security knowledge on attack detection [Text] / N. Ben-Asher, C. Gonzalez // Computers in Human Behavior. – 2015. – Vol. 48. – P. 51–61. doi: 10.1016/j.chb.2015.01.039

11. Ou Yang, Y.-P. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment [Text] / Y.-P. Ou Yang, H.-M. Shieh, G.-H. Tzeng // Information Sciences. – 2013. – Vol. 232. – P. 482–500. doi: 10.1016/ j.ins.2011.09.012

12. Linda, O. Fuzzy logic based anomaly detection for embedded network security cyber sensor [Text] / O. Linda, M. Manic, T. Vollmer, J. Wright // 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS). – 2011. doi: 10.1109/ cicybs.2011.5949392

13. Mashkina, I. V. Issues of information security control in virtualization segment of company information system [Text] / I. V. Mashkina, M. B. Guzairov, V. I. Vasilyev, L. R. Tuliga-va, A. S. Ko-valov // 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM). – 2016. doi: 10.1109/scm.2016.7519715

14. Kanatov, M. Expert systems for information security management and audit. Implementation phase issues [Text] / M. Kanatov, L. Atymtayeva, B. Yagaliyeva // 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS). – 2014. doi: 10.1109/scis-isis.2014.7044702

15. Korzhyk, D. Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness [Text] / D.

Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, M. Tambe // Journal of Artificial Intelligence Research. – 2011. – Vol. 41. – P. 297–327.

16. Rees, L. P. Decision support for Cybersecurity risk planning [Text] / L. P. Rees, J. K. Deane, T. R. Rakes, W. H. Baker // Decision Support Systems. – 2011. – Vol. 51, Issue 3. – P. 493–505. doi: 10.1016/j.СППР.2011.02.013

17. Akhmetov, B. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity [Text] / B. Akhmetov, V. Lakh-, Y. Boiko, A. Mishchenko // Eastern-European Journal of Enterprise Tech-logies. – 2017. – Vol. 1, Issue 2 (85). – P. 4–15. doi: 10.15587/1729-4061.2017.90506

18. Goztepe, K. Designing Fuzzy Rule Based Expert System for Cyber Security [Text] / K. Goztepe // International Journal of Information Security Science. – 2012. – Vol. 1, Issue 1. – P. 13–19.

19. Oglaza, A. Authorization Policies: Using Decision Support System for Context-Aware Protection of User's Private Data [Text] / A. Oglaza, R. Laborde, P. Zarate // 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. – 2013. doi: 10.1109/trustcom.2013.202

20. Ларичев, О. И. Системы поддержки принятия решений. Современное состояние и перспективы их развития [Электронный ресурс] / О. И. Ларичев, А. Б. Петровский // Итоги науки и техники. Сер. Техническая кибернетика. — Москва : ВИНИТИ, 1987. — Т.21. — С. 131–164. — Режим доступа : http://www.raai.org/library/papers/Larichev/Larichev _Petrovsky_1987.pdf (дата обращения : 23.04.2019).

21. Терелянский, П. В. Системы поддержки принятия решений. Опыт проектирования : монография / П. В. Терелянский. —Волгоград :ВолгГТУ. 2009.—127 с.

22. Power D. J. «What is a DSS?» // The On-Line Executive Journal for Data-Intensive Decision Support, 1997.—v. 1.—N3.

23. Lakhno, V. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features

[Text] / V. Lakh-, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko, T. Zhmurko // Eastern-European Journal of Enterprise Tech-logies. – 2016. – Vol. 3, Issue 9 (81). – P. 30–38. doi: 10.15587/1729-4061.2016.71769

24. Gamal, M. M. A Security Analysis Framework Powered by an Expert System [Text] / M. M. Gamal, B. Hasan, A. F. Hegazy // International Journal of Computer Science and Security (IJCSS). – 2011. – Vol. 4, Issue 6. – P. 505–527.

25. Gutzwiller, R. S. A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts [Text] / R. S. Gutzwiller, S. M. Hunt, D. S. Lange // 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). – 2016. doi: 10.1109/cogsima.2016.7497780

26. E. Dubois, P. Heymans, N. Mayer, R. Matulevicius, “A Systematic Approach to Define the Domain of Information System Security Risk Management,” Intentional Perspectives on Information Systems Engineering, 2010.

27. SSE Project Team: System Security Engineering Capability Maturity Model (SSE-CMM): Model Description Document Version 3.0. Technical report, SSE-CMM (2003)

28. Department of Energy.: Cybersecurity Capability Maturity Model (C2M2): Version 1.1. Technical report, Department of Homeland Security (2014)

29. White, G.B.: The community cyber security maturity model. In: IEEE International Conference on Techlogies for Homeland Security, pp. 173–178. IEEE Press, Wakefield (2011)

30. US Department of Homeland Security.: Cybersecurity Capability Maturity Model: Version 1.0. White paper, Department of Homeland Security (2014)

31. The Open Group.: Open Information Security Management Maturity Model (O-ISM3). Technical report, Open Group (2011)

32. Jorrigala, Vyshnavi. “Business Continuity and Disaster Recovery Plan for Information Security.” (2017).

33. Intelligent System for Information Security Management: Architecture and Design Issues Mariana Hentea Excelsior College, Albany, USA Issues in Informing Science and Information Technology Volume 4, 2007

34. AI TOOLS IN DECISION MAKING SUPPORT SYSTEMS: A REVIEW GLORIA PHILLIPS-WREN International Journal on Artificial Intelligence Tools Vol. 21, No. 2 (2012) 1240005 (13 pages)

35. Artificial Intelligence in Cybersecurity Nadine Wirkuttis and Hadas Klein Cyber, Intelligence, and Security | Volume 1 | No. 1 | January 2017

36. AI CYBERSECURITY CHALLENGES Threat Landscape for Artificial Intelligence ISBN 978-92-9204-462-6 - DOI 10.2824/238222 © European Union Agency for Cybersecurity (ENISA), 2020

37. Leslie F. Sikos AI in Cybersecurity ISSN 1868-4394 ISSN 1868-4408 (electronic) https://doi.org/10.1007/978-3-319-98842-9 Kim-Kwang Raymond Choo, Ph.D.

38. O`Reilly Machine Learning & Security

39. 1,2Chenmeng Sui, 1Yanzhao Liu, 2Yun Liu, A Software Security Assessment System Based On Analysis of Vulnerabilities Journal of Convergence Information Technology(JCIT) Volume7, Number6, April 2012 doi:10.4156/jcit.vol7.issue6.26

40. Thaler, S. (2019). Automation for information security using machine learning.

41. Sarker IH. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. 2021.

42. Hubskyi, Oleksandr, et al. "Detection of SQL Injection Attack Using Neural Networks." International scientific-practical conference. Springer, Cham, 2020.

43. Babenko Tetiana, Hnatiienko Grygorii, Vialkova Vira /Modeling of information security system and automated expert assessment of integral quality of system functional stability// in the X Inter-University Conference “Engineer of the

21st Century". 11 December 2020 at the University of Bielsko-Biała (ATH) in Bielsko-Biała, Poland

44. Hrechko Viktoriia, Tetiana Babenko “Defining the meaningful attributes of network traffic” THEORETICAL AND APPLIED SCIENCE JOURNAL ENGINEERING ACADEMY OF UKRAINE (2017)

45. Dmitry Palko, Tetiana Babenko, Larysa Myrutenko and Andrii Bigdan Model of information security critical incident risk assessment. IEEE International Conference on Problems of Infocommunications Science and Technology, (PIC S&T 2020) for October, 6-9 in Kharkiv, Ukraine.

46. Т.В. Бабенко, Г.М. Гнатієнко, В.І. Вялкова / Моделювання системи інформаційної безпеки та автоматизована оцінка інтегральної якості впливу контролів на функціональну стійкість організаційної системи// в XX Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2020). Інститут проблем реєстрації інформації НАН України, 10 грудня 2020 року, Київ

47. Sarker, Iqbal H. "Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective." SN Computer Science 2.3 (2021): 1-16.

48. Jiawei H, Jian P, Micheline K. Data mining: concepts and techniques. Amsterdam: Elsevier; 2011

49. ISACA (COBIT 5). http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

50. International Organization for Standarization. https://www.iso.org/obp/ui/#iso:std:iso-iec: 27001:ed-2:v1

51. SSE Project Team: System Security Engineering Capability Maturity Model (SSE-CMM): Model Description Document Version 3.0. Technical report, SSE-CMM (2003)

52. Department of Energy.: Cybersecurity Capability Maturity Model (C2M2): Version 1.1.Technical report, Department of Homeland Security (2014)

53. White, G.B.: The community cyber security maturity model. In: IEEE International Conference on Technologies for Homeland Security, pp. 173–178. IEEE Press, Wakefield (2011)

54. US Department of Homeland Security.: Cybersecurity Capability Maturity Model: Version 1.0. White paper, Department of Homeland Security (2014)

55. Halvorsen, C.P., Conradi, R.: A taxonomy to compare SPI frameworks. In: Ambriola, V. (ed.) EWSPT 2001. LNCS, vol. 2077, pp. 217–235. Springer, Heidelberg (2001). doi:10. 1007/3-540-45752-6_17

56. The Open Group, “Open Information Security Management Maturity Model (O-ISM3),” 2011.

57. ISF, “Time to grow using maturity models to create and protect value," in Information Security Forum ISF,.2014.

58. IT Governance Institute, COBIT 5 – A business Framework for the Governance and Management of Enterprise IT, 2012.

59. CMMI Product Team, “CMMI for Development, Version 1.3,” Carnegie Mellon Univ., -. -vember, p. 482, 2010.

60. Axelos Global Best Practices. https://www.axelos.com/Corporate/media/Files/Syllabi/RESILIA-Practitioner-2015-Exam-Syllabus-v1.pdf. RESILIA Practitioner Examination Syllabus

61. Matthew, J.B.: Advancing Cybersecurity Capability Measurement Using the CERT ® - RMM Maturity Indicator Level Scale: Version 1.1. Technical report, Carnegie Mellon University (2013)

62. MM Lessing: Best practices show the way to Information Security Maturity. http://researchspace.csir.co.za/dspace/bitstream/handle/10204/3156/Lessing6_2008.pdf? sequence=1&isAllowed=y

63. Rea-Guaman, A.M., Sánchez-García, I.D., San Feliu, T., Calvo-Manzano, J.A.: Maturity models in cybersecurity: a systematic review. In: 12a

Conferencia Ibérica de Sistemas y Tecnologías de Información (CISTI 2017), Lisbon (2017)

64. ISO 27001:2017, International Standard ISO/IEC Information technology — Security techniques — Information security management systems — Requirements, vol. 2017, 2017.

65. AI CYBERSECURITY CHALLENGES Threat Landscape for Artificial Intelligence DECEMBER 2020 ENISA, ISBN 978-92-9204-462-6 - DOI 10.2824/238222

66. Grechko V., Babenko T., Myrutenko L. Secure Software Developing Recommendations //2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). – IEEE, 2019. – С. 45-50.

67. Sarker I. H. Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective //SN Computer Science. – 2021. – Т. 2. – №. 3. – С. 1-16

68. Jüngling, S. et al. “Towards AI-based Solutions in the System Development Lifecycle.” AAAI Spring Symposium: Combining Machine Learning with Knowledge Engineering (2020).

69. Arnold, M., Boston, J., Desmond, M., Duesterwald, E., Elder, B., Murthi, A., Navrátil, J., & Reimer, D. (2020). Towards Automating the AI Operations Lifecycle. ArXiv, abs/2003.12808.

70. Yin, Jianxiong. “Scalable AI Computing Lifecycle.” VLSI-DAT (2019).

71. Álvarez-Rodríguez, J. et al. “Challenges and opportunities in the integration of the Systems Engineering process and the AI/ML model lifecycle.” (2019).

72. Kloeckner, K., Davis, J., Fuller, N.C., Lanfranchi, G., Pappe, S., Paradkar, A., Shwartz, L., Surendra, M., & Wiesmann, D. (2018). Transforming the IT Services Lifecycle with AI Technologies. SpringerBriefs in Computer Science.

73. International Standard ISO/IEC 27002. 2017 — Information technology — Security techniques — Code of practice for information security controls.

74. Bouckaert, Remco R., et al. "WEKA manual for version 3-9-1." University of Waikato, Hamilton, New Zealand (2016).

75. Jebb A. T., Parrigon S., Woo S. E. Exploratory data analysis as a foundation of inductive research //Human Resource Management Review. – 2017. – Т. 27. – №. 2. – С. 265-276.

76. Xin Y. et al. Machine learning and deep learning methods for cybersecurity //Ieee access. – 2018. – Т. 6. – С. 35365-35381.

77. Liu H., Lang B. Machine learning and deep learning methods for intrusion detection systems: A survey //applied sciences. – 2019. – Т. 9. – №. 20. – С. 4396.

78. Rathore H. et al. Malware detection using machine learning and deep learning //International Conference on Big Data Analytics. – Springer, Cham, 2018. – С. 402-411.

79. Theofilatos A., Chen C., Antoniou C. Comparing machine learning and deep learning methods for real-time crash prediction //Transportation research record. – 2019. – Т. 2673. – №. 8. – С. 169-178.

80. Shinde P. P., Shah S. A review of machine learning and deep learning applications //2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). – IEEE, 2018. – С. 1-6.

81. Wang P., Fan E., Wang P. Comparative analysis of image classification algorithms based on traditional machine learning and deep learning //Pattern Recognition Letters. – 2021. – Т. 141. – С. 61-67.

82. Campesato O. Artificial Intelligence, Machine Learning, and Deep Learning. – Stylus Publishing, LLC, 2020.

83. Dixit M. et al. An overview of deep learning architectures, libraries and its applications areas //2018 International Conference on Advances in

Computing, Communication Control and Networking (ICACCCN). – IEEE, 2018. – С. 293-297.

84. Mahdavifar S., Ghorbani A. A. Application of deep learning to cybersecurity: A survey //Neurocomputing. – 2019. – Т. 347. – С. 149-176.

85. Dixit P., Silakari S. Deep learning algorithms for cybersecurity applications: A technological and status review //Computer Science Review. – 2021. – Т. 39. – С. 100317.

86. Xin Y. et al. Machine learning and deep learning methods for cybersecurity //Ieee access. – 2018. – Т. 6. – С. 35365-35381.

87. Handa A., Sharma A., Shukla S. K. Machine learning in cybersecurity: A review //Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. – 2019. – Т. 9. – №. 4. – С. e1306.

88. Sarker I. H. et al. Cybersecurity data science: an overview from machine learning perspective //Journal of Big Data. – 2020. – Т. 7. – №. 1. – С. 1-29.

89. Dua S., Du X. Data mining and machine learning in cybersecurity. – CRC press, 2016.

90. Галушкин А. И. Синтез многослойных систем распознавания образов. — М.: «Энергия», 1974.

91. Werbos P. J., Beyond regression: New tools for prediction and analysis in the behavioral sciences. Ph.D. thesis, Harvard University, Cambridge, MA, 1974.

92. Rumelhart D.E., Hinton G.E., Williams R.J., Learning Internal Representations by Error Propagation. In: Parallel Distributed Processing, vol. 1, pp. 318—362. Cambridge, MA, MIT Press. 1986.

93. Барцев С. И., Охонин В. А. Адаптивные сети обработки информации. Красноярск : Ин-т физики СО АН СССР, 1986. Препринт N 59Б. — 20 с.

94. Барцев С. И., Гилев С. Е., Охонин В. А., Принцип двойственности в организации адаптивных сетей обработки информации, В кн.: Динамика

химических и биологических систем. — Новосибирск: Наука, 1989. — С. 6-55.

95. LeCun, Yann; Bengio, Yoshua; Hinton, Geoffrey. Deep learning (англ.) // Nature. — 2015. — Vol. 521. — P. 436—444. — doi:10.1038/nature14539.

96. Goodfellow I, Bengio Y, Courville A. Deep learning. MIT press; 2016 Nov 10.

97. R Hahnloser, R. Sarpeshkar, M A Mahowald, R. J. Douglas, H.S. Seung (2000). Digital selection and analogue amplification coexist in a cortex-inspired silicon circuit. Nature 405: 947–951.

98. Yang L., Shami A. On hyperparameter optimization of machine learning algorithms: Theory and practice //Neurocomputing. – 2020. – Т. 415. – С. 295-316.

99. Y. Wand, R. Weber, “On the ontological expressiveness of information systems analysis and design grammars,” Inf. Syst. J. vol. 3 no. 4, pp. 217–237, 1993.

100. A. Hevner, S. Chatterjee, “Design Research in Information Systems: Theory and Practice,” Springer, Heidelberg, 2010.

101. Portugal I., Alencar P., Cowan D. The use of machine learning algorithms in recommender systems: A systematic review //Expert Systems with Applications. – 2018. – Т. 97. – С. 205-227.