Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В. о. завідувача кафедри кібербезпеки
та захисту інформації
_____Іван ПАРХОМЕНКО
«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступінь *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Метод оцінювання захищеності інформаційно-комунікаційних систем на базі штучного інтелекту»

Виконавець: студент ІІ курсу, групи КБ-22м

_____ **Богдан ТЕМЧУР**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Олександр ЛАПТЄВ	
Нормоконтроль	Юрій БАБЕНКО	

Київ 2024

Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В. о. завідувача кафедри кібербезпеки
та захисту інформації
_____Іван ПАРХОМЕНКО
«17» листопада 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-22 Темчура Богдана Володимировича
(група) (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Метод оцінювання захищеності інформаційно-комунікаційних систем на базі штучного інтелекту

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	процес аналізу ефективних методів, які використовують штучний інтелект для оцінки рівня безпеки інформаційно-комунікаційних систем
Предмет досліджень	метод оцінювання захищеності інформаційно-комунікаційних систем на базі штучного інтелекту
Мета	проаналізувати штучний інтелект як метод оцінювання захищеності інформаційно-комунікаційних мереж; запропонувати власні практичні рекомендації щодо технології оцінки захищеності інформаційно-комунікаційних систем на базі штучного інтелекту
Вихідні дані для проведення роботи	методи оцінювання захищеності мереж на основі штучного інтелекту

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалення оцінювання захищеності інформаційно-комунікаційних систем за рахунок власних практичних рекомендацій

Практична цінність дослідження та розкриття питань пов'язаних із оціненням захищеності інформаційно-комунікаційних систем на базі штучного інтелекту, а також їх практичним застосуванням у подальших наукових дослідженнях у контексті практичного використання штучного інтелекту в питанні оцінювання захисту комунікаційних систем

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана в повному обсязі відповідно до теми

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Уточнення постановки задачі	17.11.2023 – 29.01.2024
Аналіз літературних джерел	30.01.2024 – 12.02.2024
Ознайомлення з основами безпеки інформаційно-комунікаційних систем	13.02.2024 – 21.02.2024
Дослідження актуальних підходів до застосування технології оцінювання захищеності мереж	22.02.2024 – 26.02.2024
Аналіз стандартів у сфері оцінювання захищеності інформаційних систем	27.02.2024 – 04.03.2024
Дослідження штучного інтелекту як явища та його застосування	05.03.2024 – 10.03.2024
Дослідження методів використання штучного інтелекту в інформаційній безпеці України	11.03.2024 – 17.03.2024
Аналіз використання методу штучного інтелекту для оцінки рівня безпеки систем	18.03.2024 – 19.03.2024
Розробка власних практичних рекомендації щодо технології оцінки захищеності інформаційно-комунікаційних мереж на базі штучного інтелекту	20.03.2024 – 25.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	26.04.2024 – 12.05.2024
Подача пакету документів на розгляд ЕК	13.05.2024 – 18.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків через втручання в роботу систем

Соціальний ефект Покращення технологій оцінювання захищеності інформації

7. ДОДАТКОВІ ВИМОГИ

Завдання видав	_____	Олександр ЛАПТЄВ
	(підпис)	(ім'я, ПРІЗВИЩЕ)
Завдання прийняв до виконання	_____	Богдан ТЕМЧУР
	(підпис)	(ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.

Термін подання дипломної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків та списку використаних джерел. Основний текст займає 80 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. У пояснювальній записці кваліфікаційної роботи міститься 13 рисунків та 67 літературних джерел.

Методи дослідження: для написання даної дипломної роботи нами було використано метод наукового аналізу, метод інтерпретації результатів та системний метод. Також нами було використано метод науково-методичного дослідження. За допомогою представлених та використаних нами методів, нами було проведено комплексне дослідження та сформовано основні елементи даного наукового дослідження.

У першому розділі даної роботи нами було використано метод науково-методичного дослідження, за допомогою якого нами було опрацьовано теоретичну базу дослідження, матеріал провідних науковців та сформовано в представлений нами перший розділ. Також у даному розділі ми використовували системний метод, за допомогою якого нами було систематизовано опрацьований матеріал та викладено в послідовності нашого дослідження.

У другому та третьому розділах даної наукової праці нами було використано метод аналізу та метод інтерпретації результатів, за допомогою яких нами було проведено порівняльний аналіз досліджуваних нами питань, сформовано власні висновки та інтерпретовано отримані результати аналізу з нашого дослідження. На основі використаних методів нами було сформовано власні висновки та практичні рекомендації з предмету дослідження та сформовано основні поняття інформаційної безпеки комунікаційних систем на основі штучного інтелекту.

Об’єктом дослідження є процес аналізу ефективного методу, який використовує штучний інтелект для оцінки рівня безпеки інформаційно-комунікаційних систем.

Предметом дослідження є метод оцінювання захищеності інформаційно-комунікаційних систем на базі штучного інтелекту.

У роботі проаналізовані базові поняття та підходи по інформаційній безпеці комунікаційних мереж; досліджені сучасні методи використання штучного інтелекту в інформаційній безпеці та інформаційно-комунікаційних системах; запропоновані власні практичні рекомендації щодо технології оцінки захищеності інформаційно-комунікаційних систем на базі штучного інтелекту.

Ключові слова : інформаційно-комунікаційні системи, оцінювання захищеності, захист даних, штучний інтелект, загрози інформаційній безпеці.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІКС	-	Інформаційно-комунікаційна система
ВВС	-	Взаємодії відкритих систем
АІС	-	Автоматизована інформаційна система
НСД	-	Несанкціонований доступ
ІБ	-	Інформаційна безпека
OSSTMM	-	Open-Source Security Testing Methodology Manual
МЕ	-	Мережевий екран
МЗСП	-	Мережа зв’язку спеціального призначення
СЗСП	-	Система зв’язку спеціального призначення
ОТС	-	Організаційно-технічна система
ІКМ	-	Інформаційно-комунікаційна мережа
ШІ	-	Штучний інтелект
КІІ	-	Критична інформаційна інфраструктура
ІТВ	-	Інформаційний технічний вплив
СЗЗК	-	Система зв’язку загального користування

ЗМІСТ

ВСТУП

Актуальність теми : Тема "Метод оцінювання захищеності інформаційно-комунікаційних систем на базі штучного інтелекту" є вкрай актуальною в сучасному світі цифрової безпеки. Захищеність інформаційних систем стає все більш важливою у зв'язку з поширенням кіберзлочинності та зростанням обсягів конфіденційної інформації, що обробляється та передається через ці системи.

Захищена інформаційно-комунікаційна мережа має бути захищена від зловмисних і випадкових атак, бути надійною, стабільною, давати гарантію на конкретний час реагування, вільну доступність послуг та інформації, цілісність інформації та всього обладнання, точність усіх цих розрахунків.

Використання штучного інтелекту для оцінювання захищеності ІКС може забезпечити більш ефективний та автоматизований підхід до виявлення потенційних загроз інформаційній безпеці. Методи машинного навчання та аналізу великих обсягів даних можуть допомогти в ідентифікації аномальних паттернів у мережевому трафіку, виявленні вразливостей програмного забезпечення та інших потенційних загроз безпеці.

Разом із цим, за умови впровадження інформаційно-комунікаційних технологій на повну потужність реалізується наскрізна безпека передачі інформації для абсолютно різних видів мережевих і комунікаційних послуг, кількість та якість яких постійно зростають.

Загальний розвиток технологій штучного інтелекту, а також поширення ІКС у всіх сферах життя роблять дану тему дипломної роботи вкрай актуальною й важливою для подальшого розвитку цифрового світу.

Науковою новизною даної роботи є удосконалення оцінювання захищеності інформаційно-комунікаційних систем за рахунок власних практичних рекомендацій.

Аналіз останніх досліджень та публікацій: в області оцінювання захищеності інформаційно-комунікаційних систем на базі штучного інтелекту було проведено чимало досліджень і опубліковано доробок наукових робіт. Найважливіші напрямки:

використання машинного навчання для виявлення загроз безпеці, розробка систем виявлення вразливостей, створення імітаційних моделей для аналізу ризиків, розробка систем прогнозування злочинності, автоматизоване управління вразливостями.

Мета роботи : проаналізувати штучний інтелект як метод оцінювання захищеності інформаційно-комунікаційних мереж; запропонувати власні практичні рекомендації щодо технології оцінки захищеності інформаційно-комунікаційних систем на базі штучного інтелекту.

Для досягнення даної мети необхідно вирішити такі завдання :

- проаналізувати базові поняття та підходи по інформаційній безпеці інформаційно-комунікаційних систем;
- дослідити сучасні методи використання штучного інтелекту в інформаційній безпеці та інформаційно-комунікаційних системах;
- запропонувати власні практичні рекомендації щодо технології оцінки захищеності інформаційно-комунікаційних систем на базі штучного інтелекту.

Об’єктом дослідження є процес аналізу ефективних методів, які використовують штучний інтелект для оцінки рівня безпеки інформаційно-комунікаційних систем.

Предметом дослідження є метод оцінювання захищеності інформаційно-комунікаційних систем на базі штучного інтелекту.

Методи дослідження дипломної роботи :

- метод наукового аналізу;
- метод інтерпретації результатів;
- системний метод;
- метод науково-методичного дослідження.

РОЗДІЛ 1
АНАЛІЗ БАЗОВИХ ПОНЯТЬ ТА ПІДХОДІВ ПО ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

1.1. Основи безпеки інформаційно-комунікаційних систем

Інформаційна безпека грунтується на багаторівневих принципах безпеки. Це означає, що безпека забезпечується на кожному з рівнів моделі ВВС, а послуги, що відповідають функціональним потребам, стають розподеними між даними рівнями. Модель ВВС нараховує сім рівнів обробки інформації [1]:

1) фізичний;
2) канальний;
3) мережний;
4) транспортний;
5) сеансовий;
6) представний;
7) прикладний.

Модель OSI

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі , сигналами і двійковими даними

Рисунок 1.1 - Модель OSI

Кожен без виключення рівень працює з конкретними завданнями та функціями, забезпечуючи діяльності на конкретному рівні. У режимі Air Force усі рівні мають свої засоби та служби. Об’єкти співпрацюють між собою через інтерфейси та протоколи. Функції, що надає BBC Model Organization. ITI-T стандартизує телевізійні послуги, функції передачі та послуги безпеки [2].

Служби безпеки мають задачу гарантувати безпеку для системи. Термін «безпека системи» має відношення до такого стану системи, який мінімізує вразливість ресурсів, що є доступними в системі. Уразливість – це недолік, який потенційно може бути використаним для незаконного доступу до системи чи інформаційного середовища. Загрози можна вважати потенційними порушеннями інформаційної безпеки. ITI-T X.800, що класифікує загрози на свідомі та випадкові, визначає такі загрози інформаційним ресурсам в інформаційно-комунікаційних мережах:

- ♦ знищення та руйнування інформаційних джерел;
- ♦ викривлення або модифікація інформації;
- ♦ пограбування, втрата інформаційних ресурсів;
- ♦ витік закритої інформації;
- ♦ переривання послуг.

Після виявлення потенційної загрози відразу розроблюється ряд завдань для забезпечення безпеки. Зі сторони забезпечення інформаційної безпеки список засобів захисту можна інтерпретувати як деяку сукупність функціональних сервісів, що разом утворюють потрібний функціональний профіль захисту. Кожен із сервісів – це набір конкретних можливостей, що дають можливість убезпечити себе від набору загроз. Служби безпеки системи побудовані за принципом ієрархічної багатошарової модульності: служби безпеки – служби безпеки – функціональні служби безпеки - механізми захисту [1].

Безпекові служби класифікуються на фазу зв'язку та рівень ВПС. У використанні тих самих послуг на різних рівнях існують розбіжності. За запитом певні послуги безпеки не є необхідними. Деякі послуги можуть надаватися на декількох рівнях.

Безпекова політика для кожної зі служби може реалізовуватися за допомогою відмінних між собою механізмів безпеки (окремо або в комбінації) залежно від обраного об’єкта політики. Сервіси фізичного рівня є основою. Метою захисту фізичного рівня є потрібний захист фізичного потоку бітів даних (служба класифікації з’єднань) та забезпечення конфіденційності та безпечного перебігу трафіку (служба класифікації потоків даних). Захист фізичного рівня гарантується за допомогою обладнання для шифрування [2].

Послуги, які надає фізична безпека, можуть бути застосовані окремо або в комплексі. До прикладу, при дуплексній одночасній двоточковій передачі можна надати повну конфіденційність з’єднання. Для інших типів передач, наприклад асинхронні передачі, можна отримати лише невеликий рівень конфіденційності підключення. Важливість служби безпеки на рівні мережі важко переоцінити.

Протокол служб мережі ВВС для доступу, підключення та маршрутизації мережі користується безпековими механізмами. В інформаційній безпеці інформаційно-комунікаційних систем можна виокремити такі механізми безпеки [2]:

♦ Конфіденційність (методики криптографії та шифрування), яка повинна давати гарантію, що технічна інформація мережі та дані користувачів будуть не розкритими та не доступними для суб’єктів, що не мають необхідних дозволів. Орім цього, навіть якщо використовуються доступні засоби захисту, необхідно гарантувати захист недоторканості системної інформації з дати встановлення;

♦ цифровий підпис;

♦ контроль доступу, що має на меті визначати дозволений перелік операцій для кожного з об'єктів та контролювати дотримання всіх специфікацій;

♦ механізми (сервіси) цілісності даних, що повинні задовольнити цілісність, точність і надійність інформації, яка передається по системі, та даних користувачів, що зберігаються в базі даних;

♦ перевірка ідентичності – встановлення правдивості ідентичності користувача за наданою ним особистою інформацією;

♦ заповнення трафіку;

♦ контроль маршрутизації;

♦ послуга ідентифікації об'єктів першого рівня – гарантується шляхом обмінювання засобами безпечної аутентифікації (захищеного пароля) та цифрового підпису;

♦ служби аутентифікації виникнення даних – механізми шифрування або підпису;

♦ послуга прихованості з’єднання – механізми забезпечення шифрування й/або контроль маршрутизації;

♦ послуги конфіденційності поза з'єднанням – засоби керування шифруванням і маршрутизацією;

♦ механізм прихованості трафіка – механізм для наповнення трафіку конкретною інформацією на рівні системи або каналу та керування навігацією разом із Службою конфіденційності;

♦ використовувати засоби недоторканості даних для надання послуг цілісності з'єднання, іноді в поєднанні з механізмами криптографії;

♦ гарантування послуги забезпечення цілісності без механізмів недоторканості даних, іноді в поєднанні з механізмами криптографії [2].

Структура інформаційної безпеки комунікаційної системи має в собі комплексну (зверху, вниз та наскрізь) мережеву безпеку всіх об’єктів, послуг і застосунків, виявляючи, прогнозуючи та нівелюючи порушення безпеки [1].

Захищеними мають бути всі складові інформаційно-комунікаційної системи : лінії, канали, системи обміну, обладнання, ПЗ, інформація та люди. Є також необхідність у правильній побудові підходів до безпеки інформації для всіх компонентів комунікаційних систем, особливо інформаційних додатків, комунікаційних протоколів і ресурсів. Фінішною метою є вибір найбільш ефективного способу подолання загроз при використанні систем інформаційної безпеки, витрати на який не будуть перевищувати очікувану вартість збитків при реалізації потенційної загрози. Структура інформаційної безпеки чітко розділяє складну мережу між її зварешальними точками на окремі компоненти.

Відділ дотримується чітокого, інтегрованого, наскрізного підходу до забезпечення інформаційної безпеки для планування безпеки та оцінювання кібербезпеки.

Є думка, що архітектура безпеки інформації тісно пов’язана з трьома архітектурними компонентами: механізмами безпеки, рівнями та площинами, які вони забезпечують. Механізм інформаційної безпеки — це набір деяких заходів безпеки, що захищає від усіх потенційних загроз безпеці, підтримує політики безпеки, визначені для конкретної мережі, та конктролює дотримання набору правил керування безпекою [2].

Ці заходи, що не обмежуються конкретною мережею, а також використовуються до програм і заключних користувачів, вживаються постачальниками послуг або компаніями, що мають необхідну ліцензію на роботу у сфері надання послуг безпеки. Механізмами захисту інформації системи є: контроль доступу, автентифікація, недоторканність участі в обмінах, конфіденційність даних, безпека зв'язку. У порівнянні з ITC-T Rec. X.800, новий механізм захисту мережевої інформації забезпечує доступність і конфіденційність. Забезпечення доступності має на увазі, що події, які мають деякий вплив на систему, не спричиняють відмови у наданні доступу до послуг мережі, інформаційних ресурсів, служб і різних програм. Гарантування конфіденційності направлене на захист ресурсів інформації, що теоретично можна отримати шляхом слідкування за операціями в мережі[1].

Прикладами такої інформації є сторінки в інтернеті, що відвідує юзер, місце розташування користувача, IP-адреса або назва пристрою BH8 у інформаційно-комунікаційній системі постачальника послуг. Необхідно також зазначити, що державні документи у фері захисту інформаційних ресурсів не маюуть у собі визначення механізмів гарантування власності, що, цілком імовірно, є наслідком відсутності в нашій країні звичаю незайманості приватної власності. Проте Конституція України, Закон України “Про телекомунікації» (стаття 9), положення про ліцензії та інші нормативно-правові акти окреслюють норми захисту таємності зв'язку “для забезпечення недоторканості інформації щодо споживачів, договорів,

наданих комунікаційних послуг, тривалість послуги, зміст, спосіб оплати, шлях передачі тощо”.

Навіть у випадку, коли в договорі не було обговорено надання послуг із забезпечення таємності інформації про користувача, повинні існувати способи для забезпечення конфіденційності такого роду інформації. Механізми інформаційної безпеки застосовуються для боротьби з різними типами загроз. З метою гарантування повної безпеки інформаційно-комунікаційних систем, механізми для забезпечення безпеки об’єднуються в рівні безпеки. Далі, на кожному з цих рівнів є декілька видів механізмів безпеки інформації - площина інформаційної безпеки [1].

Існують такі системні рівні мережево-орієнтованих засобів забезпечення безпеки інформації: рівень гарантування безпеки інфраструктури, рівень гарантування безпеки послуг інформації, рівень гарантування інформаційної безпеки застосувань. У Рекомендації ITRG-T X.805 зазначено, що всі три перелічені рівні інформаційної безпеки можуть бути щастосованими на всіх семи рівнях моделі ВВС, тому що вона має свою власну інфраструктуру, яка гарантує ясно визначені послуги та програми [2].

Рівень безпеки інформації програми концентрується на безпеці системинх програм, що надаються клієнтам постачальника послуг. Ці програми дають можливість мережевим службам і центрам обробки даних виконувати передачу ресурсів додатків, функції керування довідкою, голосом та електронною поштою, а також більш розширені функції, як, до прикладу, управління телекомунікаціями користувчів, навчання на відстані, відеозустрічі та багато чого іншого. На рівні існують потенційні цілі атаки на безпеку: програми користувачів, програми постачальників і постачальники послуг.

Площина інформаційної безпеки – система інформаційної безпеки, що працює в захищеній системі. Окреслено три рівні інформаційно-комунікаційної безпеки, що відповідають трьом операціям мережевої безпеки: рівень управління над безпекою, рівень контролю безпеки та сигналізації та рівень безпеки кінцевого користувача. Ці площини вказують на особливі потреби інформаційної безпеки та мають відношення до реалізації управління системою, організації управління мережею та сигналізації

заключних користувачів. Мережі повинні бути розроблені таким чином, щоб процеси в одній площині безпеки не були залежними від таких процесів у інших площинах безпеки [29].

До прикладу, хвиля запитів заключних користувачів до служб доменних імен (ВМ8) не повинна заважати інтерфейсу керування, адміністрування, обслуговування та підтримки (OAM&R), щоб адміністратори мали можливість приймати правильні та обгрунтовані рішення.

Кожен із типів функцій системи, що були представлені, має свої власні потреби забезпечення безпеки. Структура площин безпеки інформації дає можливість диференціювати деякі особливості безпеки стосовно різних дій, що пов’язані з цими самими площинами, здійснюючи їх оцінку самостійно, окремо одну від одної [1].

Площина керування гарантує функції надійності, працездатності та безпеки (РСАР8). Підмережі, які виконують функції передачі трафіку для зручності управління, можна застосовувати за межами трафіку користувачів.

Методологічний підступ до забезпечення безпеки інформаційно-омунікаційних систем полягає в аналізі кожного окремого захисного механізму на всіх трьох рівнях інформаційної безпеки та також трьох площинах безпеки інформації. Отже, маємо дев’ять модулів безпеки, кожен із яких має вісім механізмів безпеки, які можуть бути використаними на окремих рівнях і в окремих площинах.

Також необхідно усвідомлювати, що залежно від потреб конкретної мережі може стати в нагоді повний або частково неповний набір засобів інформаційно-комунікаційної безпеки, рівнів і площин безпеки інформації. Архітектура інформаційної безпеки має право використовуватися відносно кожної мережі на будь-якому рівні протоколів [2].

Прикладний рівень характеризує безпеку користувацьких програм, доступ до яких забезпечується через мережу e-Thai IP. Аналогічно, для мереж асинхронної передачі (ATM), які розміщені на двох рівнях стеку протоколів, рівень інфраструктури характеризує окремі комутатори та канали зв'язку «точка-точка» між цими комутаторами. Рівень обслуговування описує абсолютно різні класи методів передачі (постійна швидкість передачі, змінна швидкість передачі в реальному часі,

доступна швидкість передачі та невизначена швидкість передачі), що рекомендуються [2].

Наостанок, рівень програми має відношення до кінцевого користувача, що використовує мережу банкоматів, щоб отримати доступ до програми для відеоконференцій [1].

Загрози безпеці інформації – це різноманітні дії, які в підсумку можуть призвести до послаблення інформаційної безпеки. Якщо сказати по-іншому, це потенційні події, процеси чи дії, що можуть зіпсувати інформацію та комп'ютерні системи. Загрози інформаційної безпеки можна розділити на дві групи: природні загрози та техногенні загрози. До природних загрзі відносяться такі, що не залежать від людей, наприклад, урагани, повені, пожежі тощо [3].

Штучні загрози конкретно залежать від людини й можуть бути навмисними або випадковими. Ненавмисні загрози походять від необережної поведінки, недбалості та незнання тих чи інших нюансів. Прикладом такої загрози є встановлення непотрібних для роботи програмних забезпечень і подальше пошкодження системи, що може привести до втрати інформації. На відміну від випадкових загроз, навмисні - генеруються спеціально. Сюди можна віднести атаки хакерів як "з вулиці", так і з середині фірми або компанії [4].

Проблеми безпеки інформації хвилюють фахівців із комп'ютерної безпеки та багатьох звичайних користувачів комп'ютерів ще з кінця 1980тих і початку 1990тих років. Це може бути пов'язано з великими змінами, які інформаційні технології приносять у життя суспільства.

Новітні автоматизовані інформаційні системи (АІС) – це доволі таки важкі механізми, що формуються з великого числа складових із різним рівнем автономності, взаємозв'язку, обміну інформацією. Майже кожен не застрахований від невдачі або впливу посторонніх факторів.

Незважаючи на те, що цей метод доволі дорогий, можливості комп'ютерних автоматизованих інформаційних систем дали змогу показати слабкі місця в безпеці інформації. Неминучим наслідком є зростаючі витрати та сили, що направлені на покращення захисту інформації.

Проте для ефективності застосваних заходів необхідно виявити загрози інформаційній безпеці, можливі канали витоку інформаційних ресурсів та способи незаконного доступу до даних, що знаходяться під захиистом [3].

1.2. Актуальні підходи до застосування оцінювання захищеності інформаційно-комунікаційних мереж

Мережа зв'язку спеціального призначення (МЗ СП) є інфраструктурою комунікацій, спрямованою на задоволення потреб органів державної влади, оборонних структур, забезпечення безпеки та збереження правопорядку в країні. Якщо говорити технічно, МЗ СП може бути описана як система зв'язку спеціального призначення (СЗ СП). Ця система складається з взаємопов'язаних між собою технічних засобів та персоналу, які розташовані у просторі та призначені для обміну конкретною інформацією у мережах військового та державного управління, а також в системах забезпечення безпеки та правопорядку. [7].

Дослідження структури та принципів функціонування спеціальної системи зв'язку (СЗ СП), яке представлено в різних роботах, підтверджує, що вона є складною організаційно-технічною системою (ОТС). Ця система складається з різноманітних інформаційно-комунікаційних комплексів спеціального призначення (ІКС СП). [8].

Інформаційно-комунікаційна мережа (ІКМ) складається з ряду мережевих вузлів, які пов'язані між собою лініями зв'язку та працюють на основі єдиної транспортної технології. Вона діє згідно з єдиною системою маршрутизації, адресації та управління. В мережі присутні граничні вузли, які керують доступом до мережі та маршрутизують інформацію до інших суміжних інформаційно-телекомунікаційних систем, а також вузли, що відповідають за обробку, передачу, зберігання та обробку інформації. Загальний висновок стосовно цього полягає в тому, що даний розділ розглядає абстрактну ІКМ СП як прототип об'єкта КІІ, який є частиною спеціальної системи зв'язку та входить до складу Єдиних систем екстреної служби України. [7].

Аналіз структури та принципів функціонування спеціальної системи зв'язку (СЗ СП), проведений на основі наукових досліджень, показав, що в сучасних умовах

розвитку цієї системи відбувається низка значних змін. До основних таких змін можна віднести:

- перехід від розподілених спеціальних систем зв'язку (СЗ СП), що функціонують в різних органах державного та військового управління, до єдиної СЗ СП, побудованої на багатошаровому принципі (зазвичай, включає космічний, повітряний, наземний та морський ешелони).

- широка інтеграція сегментів систем зв'язку оперативних підрозділів та комерційних інформаційно-телекомунікаційних мереж до складу СЗ СП.

- активне впровадження технологій комутації пакетів замість традиційних технологій комутації каналів в СЗ СП.

- широке застосування комерційних протоколів та технологій у складі СЗ СП, зокрема, протоколів IP (Internet Protocol) та MPLS (Multiprotocol Label Switching).

- конвергенція окремих мереж і систем зв'язку в єдиний інформаційний простір з урахуванням концепції NGN (Next Generation Networks).

- широке використання супутникових систем зв'язку (ССЗ) для забезпечення глобальної зв'язності та керування в СЗ СП, включаючи цивільні супутникові системи операторів зв'язку.

- використання тактичних мереж адаптивних мобільних радіомереж Mesh/MANET в мережах СЗ СП.

- використання методів обробки великих обсягів даних, а також хмарних та Grid-технологій для організації розподіленого зберігання та обробки великих масивів даних. [8].

При цьому для інформаційно-телекомунікаційної мережі (ІТКМ) спеціального призначення (СП), що є базовим елементом спеціальної системи зв'язку (СЗ СП), ці тенденції призводять до наступної фундаментальної вразливості ІТКМ СП, що значно знижує рівень її інформаційної безпеки (ІБ). Побудова ІТКМ СП на основі комерційних протоколів та технологій зв'язку, а також їх інтеграція з комерційними інформаційно-телекомунікаційними системами (ІТКС) зі складу спеціальних систем зв'язку, створює можливість для реалізації інформаційно-технічних впливів (ІТВ) через спеціальні системи зв'язку.

До обов'язків безпеки, необхідних для протидії інформаційно-технологічним загрозам на інформаційних системах суб'єктів критичної інфраструктури, входять:

- виявлення та аналіз уразливостей, що впливають на інформаційні системи, координація дій для їх виправлення;
- аналіз зареєстрованих подій у складі обслуговуваних інформаційних систем та їх захисту для виявлення ознак інформаційно-технічних загроз, спрямованих на ці системи;
- організація реагування на виявлені інформаційно-технічні загрози, а у випадку інциденту - ліквідація наслідків такого інциденту;
- проведення розслідувань інцидентів та аналіз інформаційно-технічних загроз, які не було можливо запобігти;
- навчання персоналу з інформаційно-технічних загроз та проведення кібернавчань.

Відповідно до вимог (Наказ від 25.12.2017 «Про затвердження Вимог щодо забезпечення безпеки значущих об'єктів критичної інформаційної інфраструктури України») у системі захисту повинні бути впровадженні основні заходи, багато з яких безпосередньо направлені на протидію ІТБ зловмисників [8]:

- інвентаризація компонентів ІТКС та дослідження їх вразливостей;
- контроль та аналіз потоку мережевого трафіку;
- перевірка безпеки;
- захист від вірусів;
- запобігання вторгненням;
- реагування на інциденти тощо.

У цьому контексті власник має повне право самостійно визначати, яким чином будуть впроваджені заходи захисту. Важливо зазначити, що ці заходи є лише базовими, тобто необхідними, але не достатніми для забезпечення повної безпеки об'єкту критичної інфраструктури. Згідно з встановленими процедурами, власник об'єкту критичної інфраструктури має провести самостійний аналіз потенційних загроз, що актуальні для об'єкта, і самостійно визначити, як слід впровадити базові

заходи захисту. У разі, якщо виявиться, що цих заходів недостатньо для захисту від потенційних загроз, власник має самостійно посилити базові заходи захисту або розробити додаткові. В такому контексті аудит інформаційної безпеки є ключовим інструментом, який дозволяє оцінити рівень потенційних загроз для об'єкта критичної інфраструктури та ступінь його захищеності[11].

Аналіз досліджень демонструє, що найбільш перспективними напрямками вдосконалення SEIM-систем аудиту об'єктів критичної інфраструктури є:

• підвищення повноти та своєчасності збирання даних про події у складові та підсистеми інформаційно-телекомунікаційних систем;

• підвищення рівня інтелектуалізації обробки даних про події в компонентах та підсистемах інформаційно-телекомунікаційних систем, включаючи використання технологій багатовимірного кореляційного аналізу та штучного інтелекту;

• створення позитивного зворотного зв'язку у системі шляхом оперативного виявлення інформаційно-технологічних загроз та негайного розроблення заходів захисту від них;

• моделювання дій зловмисників з автоматичною генерацією на основі результатів моделювання як високовірогідних сценаріїв зловмисницьких дій, так і адекватних та ефективних сценаріїв захисту;

• підвищення рівня інтелектуалізації інтерфейсу між людиною та машиною системи, щодо адаптації візуалізації подання інформації про події у систему, що відповідає системі зорового сприйняття людини-оператора, з метою покращення інформаційної наповненості та ергономіки системи[8].

У сучасній теорії аудиту інформаційної безпеки спостерігається ситуація, в якій більшість досліджень у цій сфері зосереджена на експертному аудиті та оцінці відповідності, переважно на базі моделей аналізу ризиків або стандартів інформаційної безпеки. Проте, тестування, зокрема тестування спеціалізованими засобами безпеки, залишається маловивченою областю аудиту. Існують окремі дослідження, що присвячені цьому типу тестування, наприклад, тестування на проникнення, але ці роботи мають більш практичний спрямований, ніж теоретичний.

Рисунок 1.2 – Основні етапи процесу тестування

Тестування представляє собою процес перевірки виконання вимог до системи шляхом спостереження за її роботою у визначеному наборі спеціально обраних ситуацій. Кожен окремий захід, спрямований на дослідження системи або вивчення її функціонування, називається тестом. Тестовий інформаційно-технічний вплив – це вплив на інформаційний ресурс, інформаційну систему, інформаційну інфраструктуру, на технічні засоби або програми, основні завдання яких полягають у отриманні, передачі, обробці, зберіганні та відтворенні інформації з метою виявлення вразливостей об'єкта, на який здійснюється вплив[14].

На рисунку 1.2 представлена загальна класифікація заходів, методів та засобів тестування, що використовуються в аудиті інформаційної безпеки. На сьогоднішній день існує підхід до тестування, коли більшість процесів оцінки безпеки систем базується на аналізі відповідності формальним вимогам з інформаційної безпеки або шляхом тестування за моделями. Проте вимоги до інформаційної безпеки, як правило, формулюються на основі аналізу інцидентів, що часто призводить до їх відставання від сучасних можливостей та практик зловмисників.

Дослідження, що фокусуються на експериментальному тестуванні реальних інформаційних систем, розглядають такі методи та сценарії переважно як "тестування на проникнення" або як "інструментальний аудит". Однак в українській практиці відсутній чіткий системний або загальнотеоретичний підхід до проведення подібного типу аудиту.

Деякі вітчизняні дослідження з тестування на проникнення підкреслюють важливість виявлення найбільш "виразних" уразливостей або тих, виправлення яких приносить найбільші економічні вигоди компанії, яка проводить аудит. Одночасно спостерігається зростання кількості тестів, які проводяться у формі експериментальних досліджень реального об'єкту або його прототипу. Ця тенденція особливо виражена у випадку тестування програмного забезпечення[14].

Зазвичай для цього використовуються віртуальні машини, через які проводиться контрольоване виконання тестованого програмного забезпечення. Далі розвиток цього методу тестування привів до створення так званих кіберполігонів, які віртуалізують як апаратну, так і програмну частину розподіленої інформаційної системи і дозволяють випробувати захист від різних відомих інцидентів та загроз інформаційної безпеки. В даний момент цей напрямок активно розвивається, і йому присвячено дослідження [15].

Маршрутизація пакетів повідомлень в ІТКС та їх передача по лініях зв'язку для забезпечення обміну інформацією між кореспондентами здійснюється через транзитні вузли СЗЗК. Визначення маршруту руху пакетів до СЗЗК є складним завданням через великий вибір альтернативних маршрутів між кожною парою кореспондентів. Вузли СЗЗК (тобто маршрутизатори операторів зв'язку) здійснюють вибір маршруту [19].

При виборі маршруту серед доступних альтернатив враховуються критерії, такі як потенційна пропускна здатність та завантаженість ліній (каналів) зв'язку, затримки, що виникають у каналах, та їх надійність, а також кількість транзитних вузлів СЗЗК та їхня надійність. З метою забезпечення безпеки інформаційної взаємодії кореспондентів необхідно проводити порівняльну оцінку різних структур ІТКС, що враховує їхню здатність забезпечити інформаційну взаємодію в умовах

навмисних або випадкових програмних перешкод, що можуть призвести до погіршення якості ІТКС та спричинити надмірне навантаження на процеси пристрою, що здійснює інформаційну взаємодію.

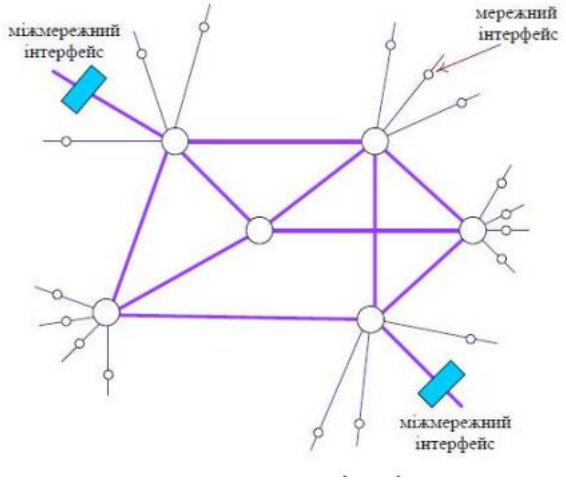

Рисунок 1.3 – Інформаційно-комунікаційна мережа

Ця постановка задачі викликає наступні протиріччя. Протиріччя між потребою забезпечити високу достовірність результатів оцінки та зростанням ресурсів, необхідних для її вирішення, що викликане змінами кількості ліній та вузлів зв'язку інформаційно-комунікаційної системи, які вразливі до впливу перешкод. Також існує протиріччя між необхідністю оцінити адаптаційні можливості ІКС та необхідністю отримати цю оцінку для перспективних значень показників безпеки вузлів та ліній зв'язку, що враховують деструктивний вплив середовища [20].

Методологія спрямована на вирішення вищезгаданих протиріч. Як інтегральний показник життєздатності ІКС, обрана ймовірність РНС порушення зв'язку між кореспондентами (абонентами), а для вузла ІКС - коефіцієнт доступності КД i, де i = 1, 2, 3, ..., n, що відображає його можливості забезпечення абонентів послугами зв'язку з необхідною якістю. У тексті нижче наведено порядок отримання значень показників, конкретні критерії та їх внесок у підсумкову оцінку.

Методика ґрунтується на теоріях перколяції, математичній статистиці та ймовірності. Вплив навмисних та випадкових програмних перешкод на комунікаційній системі, що викликають послідовні відмови, аналогічно процесу

протікання (перколяції), можна описати в рамках цих теорій, що дозволяє узагальнено, але просто відтворити процеси епідемій на деградованій структурі ІКС. У контексті теорії перколяції такі завдання розв'язуються для вузлів та зв'язків [22].

Під час розв'язання перколяційного завдання за вузлами у моделі деградації ІТКС виконують такі послідовні дії для досягнення поставленої мети. Спочатку встановлюють вихідні дані, такі як схема зв'язку між органами управління, вимоги до показників якості ІТКС та мінімальне допустиме значення комплексного показника безпеки ПКmin, а також ідентифікатори вузлів та наявність між ними ліній зв'язку. Структура та параметри розподіленої інформаційно-комунікаційної системи (типологія її елементів) визначаються зазначеними вихідними даними.

У процесі, схема комунікації та вимоги до характеристик якості ІТКС встановлюються системою вищого рівня у ієрархії, такою як управління відомства, в якій організовано зв'язок. Якщо інформація про структуру ССЗП не доступна як вихідні дані від оператора зв'язку, її зазвичай знаходять за допомогою моніторингу мережі СЗЗК з використанням спеціалізованого програмного забезпечення. Повнота та достовірність результатів моніторингу залежить від кількості та просторового розташування засобів моніторингу [22].

У цьому випадку достовірність визначається співставленням результатів моніторингу з реальною структурою СЗЗК. Має сенс мати пункти моніторингу у кожному захищеному сегменті ІКС, який з'єднаний з СЗЗК. Таке розподілене програмне забезпечення дозволить вирішити завдання підсистеми моніторингу. Топології та типології комунікаційної мережі використовуються для виявлення всього різноманіття альтернативних структур ІКС для обміну інформацією між органами управління.

Коефіцієнт доступності і-го вузла ІТКС, який відображає його ефективність, розраховується за формулою: КД і = ((Ті -ТП і) / Ті) · 100%, де ТП і – час, протягом якого абонентам недоступні послуги від вузла зв'язку з потрібною якістю (час «простою»), а Ті - загальний час роботи вузла комунікаційної системи. Вплив навмисних або випадкових перешкод на вузол ІКС призводить до додаткового навантаження на зв'язок та пристрої, що використовуються.

У результаті цього збільшується період часу, протягом якого послуги від вузла зв'язку стають недоступними для абонентів з необхідною якістю (відомий як час "простою"), і показник доступності вузла інформаційно-комунікаційної системи зменшується. Використання ІКС та експерименти на її частинах показують, що мінімальне допустиме значення показника доступності має перебувати в діапазоні 0,6 < КДmin < 1 [13].

Потім необхідно встановити значення комплексного показника безпеки для кожного вузла мережі. Під комплексним показником ПК і-го вузла ІКС розуміється об'єднання (його нормоване числове значення) показників безпеки, які визначають здатність цього вузла комунікаційної системи протистояти потенційним загрозам безпеки. Розрахунок ПК і може бути проведений різними методами: шляхом сумування, множення або обчисленням середнього арифметичного значень показників безпеки вузла [23].

Крім того, вихідні дані, які визначають параметри системи, включають мінімальне допустиме значення комплексного показника безпеки ПКmin для вузлів ІКС та різні варіанти підключення абонентів до ІКС. Значення ПКmin встановлюють як обов'язковий критерій (точніше, як директиву), враховуючи реалізацію функцій безпеки, що забезпечують мінімальний рівень довіри до виробника та експлуатанта обладнання (встановлено нормативно).

1.3. Розгляд стандартів у сфері оцінювання захищеності інформаційних систем

Уряди впроваджують інформаційні системи з метою ефективного надання різноманітних послуг громадянам. Цифрові товари, такі як електронні книги, відеопродукти та програмне забезпечення, а також онлайн-послуги, наприклад ігри та соціальні мережі, інтегруються у ці інформаційні системи.

Часто інформаційні системи стикаються з різними загрозами, які можуть викликати різноманітні види шкідливих наслідків, що може призвести до серйозних

фінансових втрат. В різних дослідженнях зазначаються системні проблеми безпеки інформаційних систем.

- маніпулювання правом доступу в обмежений інформаційний простір;
- викрадення інформацих ресурсів із корпоративних систем і баз даних;
- деформація інформації, підробка документів в електронному вигляді;
- промислове стеження;
- викрадення коштів із банківських рахунків;
- вірусні загрози.

Центральним елементом вирішення проблем безпеки в інформаційних технологіях є розробка системи вимог, критеріїв і показників рівня безпеки інформаційних технологій.

На сьогоднішній день проблема тестування та оцінки засобів забезпечення інформаційної безпеки (ІБ) та оцінки захищеності автоматизованих систем (АС) залишається актуальною, що підтверджується аналізом як вітчизняних, так і зарубіжних стандартів у цій галузі. Важливим елементом оцінки безпеки є проведення тестування, яке служить підтвердженням того, що засоби захисту відповідають стандартам та працюють належним чином [23].

Стандартизація полягає у створенні та установленні обов'язкових або рекомендованих вимог, норм, правил та характеристик.

Самі стандарти представляють собою нормативні документи, що формуються на основі узгодження, підтвердженого визнаним органом, з метою забезпечення оптимальної організації у певній галузі. Вони встановлюють загальні принципи, правила та характеристики, призначені для широкого та повторного використання, що стосуються змісту різних видів діяльності або їх результатів.

Стандарти у сфері інформаційної безпеки мають за мету розробити чіткий набір критеріїв, які дозволять мінімізувати можливі загрози для системи. Ці критерії визначають вимоги до якості. Така система градації дозволяє охарактеризувати будь-яку систему інформаційної безпеки та порівняти розроблену модель з поточним станом справ [24].

Стандарти інформаційної безпеки є основним інструментом критеріального орієнтира, який використовується для вирішення конкретних завдань щодо забезпечення безпеки автоматизованих систем. У якості ключових стандартів у сфері визначення вимог до засобів захисту, їх оцінки та тестування можна виділити наступні документи:

1. Керівні документи, зокрема: «Керівний документ. Кошти обчислювальної техніки. Міжмережеві екрани. Захист від несанкціонованого доступу до інформації. Показники безпеки від несанкціонованого доступу до інформації».

2. Загальні критерії безпеки інформаційних технологій і автентичний йому ДСТУ ISO 15408-2002;

3. Open-Source Security Testing Methodology Manual (OSSTMM), ISECOM-методологія тестування безпеки;

4. Guideline on Network Security Testing, NIST Special Publication 800-42 – практичний посібник для тестування безпеки мережі. Надалі ці стандарти та положення будуть розглядатися зі сторони їх застосування до процесу тестування міжмережевих екранів [25, 26].

В документі установлено п'ять рівнів захисту конфіденційної інформації, класифікованих залежно від ступеня захищеності від несанкціонованого доступу (НСД), що враховує перелік показників захищеності.

Кожен клас має свою власну мінімальну набір вимог щодо захисту інформації. Залежно від важливості оброблюваної інформації, для систем класу 3А та 2А повинні використовуватися заходи захисту відповідних класів захищеності.

- при обробці інформації з грфом секретно – не нижче 3 класу;
- при обробці інформації з грфом “цілком секретно” – не нижче 2 класу;
- при обробці інформації з грфом “особливої важливості” – не нижче 1 класу.

До показників захищеності віднесено:

– Управління доступом;

– Адміністрування: ідентифікація та аутентифікація;

– Реєстрація;

– Цілісність;

– Відновленість;

– Тестування;

– Управління адміністратора захисту;

– Документація для тестування;

– Конструкторська (проектна) документація. До явних мінусів керівництва можна покласти жорсткість і статичність критеріїв захищеності, відсутність необхідної гнучкості в підході оцінки (головний акцент для формування вимог робиться на гарантуванні таємності й цілісності інформації) [26].

Якщо клас екрана вищий за третій і третій, необхідно перевірити, чи він операційний для всіх програм, що використовуються для зовнішнього обміну інформацією. Класифікація АС та СВТ була розроблена без врахування розподіленої архітектури сучасних систем, і майже всі комерційні засоби захисту, які доступні на ринку, відповідають вимогам вищого, ніж перший, класу захищеності (за винятком криптографічних алгоритмів, які мають бути сертифіковані) [28].

«Загальні критерії»

Даний стандарт пропонує методи, підходи та засоби для забезпечення захисту інформації. Також, подібно до "Загальних критеріїв", які визначені в РД Держтехкомісії, використовується для проведення сертифікаційних випробувань. "Загальні критерії" слугують методологією для формулювання вимог оцінки безпеки. Оцінка інформаційної безпеки базується на моделях (профілях) безпеки, які включають в себе перераховані у стандарті функції. Ці функції системи інформаційної безпеки гарантують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації.

У стандарті відображено всі функції у вигляді чотирьохрівневої ієрархічної структури, що включає клас, сімейство, компонент та елемент. Аналогічно до цього представлені вимоги щодо якості. Стандарт виділяє 11 класів функцій, які включають аудит, ідентифікацію та аутентифікацію, криптографічний захист, конфіденційність, передачу даних, захист даних, управління безпекою системи, ефективне використання ресурсів, доступ до системи та надійність засобів. В стандарті ISO

15408 визначено низку профілів, які описують стандартні модулі системи безпеки, наприклад, міжмережевий екран [33].

Кожен функціональний клас має свою особисту назву. Категоріальна інформація представлена у вигляді скороченої назви, яка складається з трьох символів. Ця коротка назва класу використовується для специфікації коротких імен сімейств даного класу.

Назва сім'ї надає важливу категоріальну та описову інформацію, яка необхідна для ідентифікації та категоризації функціональних сім'ї. Кожна функціональна сім'я має свою унікальну назву. Інформація про категорію складається з короткої назви, що містить сім символів. Перші три символи ідентичні короткій назві класу, за якими слідує символ підкреслення та коротка назва сімейства (XXX_YYY). Унікальна коротка форма назви є основним посиланням для компонентів. [34].

Функціональні сімейства мають у собі один або більше одного компонентів, із яких можна вибрати будь-який. Метою даного розділу є наділення користувачів інформацією для обрання відповідного функціонального компонента після того, як сімейство визначено як необхідну або корисну частину їхніх вимог до безпеки. У цьому розділі описується доступні компоненти функціонального сімейства та обґрунтування їх. Докладні відомості про компоненти містяться в кожному з них. Взаємозв'язки між компонентами всередині функціонального сімейства можуть бути ієрархічними, але можуть і не бути. Компонент вважається ієрархічним відносно іншого, якщо він забезпечує більш високий рівень безпеки. [37].

Кожному компоненту призначено набір елементів. Кожен елемент має окреме визначення і є автономним. Функціональний елемент представляє собою вимогу безпеки, подальший розподіл якої не призводить до значної користі при оцінці. Це найменший фрагмент функціональних вимог безпеки, який визнаний та узагальнений в стандарті ISO/IEC 15408.

Взаємозв'язки між функціональними компонентами виникають у випадку, коли компонент не може функціонувати самостійно і ґрунтується на функціональності або взаємодії з іншим компонентом для свого належного функціонування.

Перелік залежностей визначає найменші функціональні або впевнені компоненти, які необхідні для виконання вимоги безпеки, пов'язані з ідентифікованим компонентом. Крім того, компоненти, які перебувають у ієрархічній залежності від визначеного компонента, також можуть використовуватися для задоволення цієї залежності. Зазначені в ISO/IEC 15408-2 залежності є обов'язковими з точки зору стандарту [37].

Таким чином, «Загальні критерії»:

– дозволяє визначити повноцінний перелік вимог до механізмів безпеки, а також критерії їх оцінювання (показники захисту інформації);

– дозволяє здійснити оцінювання відноснг того, наскільки сильно наповнена система інформаційної безпеки з технічної точки зору, але при оцінюванні незважаючи на повний комплекс заходів відносно забезпечення захисту інформації.

Методологія тестування безпеки (OSSTMM)

Рисунок 1.4 – Емблема OSSTMM

Цей документ містить загальну стратегію та пропонує конкретні поради стосовно організації процесу тестування на безпеку. Він визначає основні терміни, вказує об'єкти тестування та рекомендує шаблони документів для проведення тестів. У OSSTMM ідентифіковано категорії безпеки, які взаємодіють між собою :

– безпека інформації (information security)

– безпека процесу (process security)

– безпека технологій Інтернету (internet technology security)

– комунікаційна безпека (communications security)

– бездротова безпека (wireless security)

– фізична безпека (physical security)

Перелічені нами категорії розділені на модулі [37].

Процес тестування визначається як безперервний і простежується через всі модулі та категорії. При проведенні тестування кожного модуля розподіляється на стадії збору даних "data" (що ґрунтується на певних припущеннях щодо системи) та перевірки цих припущень "verification". Інформація, зібрана в результаті тестування окремого модуля, може бути використана як остаточний результат або вхідні дані для тестування наступного модуля. Тестування міжмережевих екранів відноситься до категорії безпеки Інтернет-технологій.

Крім цього, у межах модуля з безпеки Інтернет-технологій можна визначити моделі, результати тестування яких будуть застосовані для здійснення тестування міжмережевих екранів :

– сканування портів;

– виявлення систем і сервісів;

– моніторинг уразливостей;

– тестування маршрутизації;

– злом паролів;

– дослідження стійкості до атак (у тому числі атак по типу «відмови в обслуговуванні»).

Однією з очевидних недоліків цієї методології є відсутність рекомендацій стосовно формування системи вимог до засобів захисту інформації, а також відсутність рекомендацій щодо вибору та застосування інструментів для тестування. Крім того, перерахованих вище підходів недостатньо для оцінки ефективності функціонування захисних засобів та оцінки захищеності автоматизованих систем.

Посібник із тестування мережевої безпеки (NIST) [38].

Рисунок 1.5 - NIST 800-42

Даний стандарт містить практичні рекомендації щодо організації процесу тестування мережевої безпеки, визначає ролі, інструменти та етапи життєвого циклу, на яких необхідно проводити тестування. Згідно з документом, об'єктами мережевої безпеки є міжмережеві екрани, маршрутизатори та комутатори, а також сервери різних типів (веб, електронної пошти, DNS, FTP та інші) [38].

Ці об'єкти проходять через класичний життєвий цикл, який включає формування вимог, розробку (або придбання), використання, експлуатацію та вилучення з експлуатації. Тестування їх безпекових властивостей слід проводити на етапах впровадження (під час вибору пристрою) та експлуатації (для оцінки рівня захищеності та правильності функціонування). У документі розглядаються різні підходи до оцінки мережевої безпеки, включаючи:

– мережеве сканування (network mapping)

– сканування вразливостей (vulnerability scanning)

– злом пароля (password cracking)

– аналіз лог-журналів (log review)

– перевірка файлів на цілісність (file integrity checkers)

– тестування на проникнення (penetration testing)

Ці методи можна використовувати для тестування міжмережевих екранів як індивідуально, так і в комплексі. Наприклад, процес сканування вразливостей завжди включає в себе аналіз мережі (визначення відкритих портів та ідентифікацію систем),

а перед початком тестування на проникнення зазвичай виконується пошук (сканування) вразливостей. [38].

Стандарт "Guideline on Network Security Testing" представляє собою корисний практичний довідник з організації процесу оцінки стану мережевої безпеки. Проте він не містить вимог щодо конкретних засобів мережевої безпеки, на відповідність яким потрібно проводити тестування.

Стандарти з оцінки безпеки майже не містять конкретних методик, що призводить до значного розриву між загальними принципами та практичними інструментами для їх впровадження та контролю. Аналіз зарубіжних і вітчизняних стандартів у сфері інформаційної безпеки підтверджує, що для успішного застосування цих стандартів потрібно розробляти додаткові спеціальні методики, алгоритми та засоби оцінки захищеності та проведення тестування [38].

Висновки за розділом 1

Отже, з проведеного нами дослідження в першому розділі, можемо зробити такий висновок, що рівень інформаційної безпеки інфраструктури комунікаційної мережі складається із засобів мережі передачі інформації та різних елементів мережі та захищається механізмом захисту інформації. Рівень інфраструктури складається з основних блоків систем, сервісів і додатків. Прикладами компонентів на рівні інфраструктури є окремі маршрутизатори, комутатори та служби, крім цього сюди можна додати канали зв’язку, що поєднують конкретні маршрутизатори, комутатори та сервери.

Послуги, що надаються клієнтам, надаються в якості транспортних функцій та функцій включення до служб, що гарантують доступ до інформаційно-комунікаційної мережі, інших служб, наприклад телефонної служби, служби перевірки якості сервісу, віртуальних приватних мереж, послуг швидкого пересилання повідомлень тощо. Оскільки постачальник послуг, а також його клієнти є потенційними суб’єктами загроз безпеки, то для їх захисту використовується рівень інформаційної безпеки послуги. Наприклад, зловмисники можуть спробувати

заблокувати функції постачальника послуг або втрутитися в обслуговування окремих клієнтів.

РОЗДІЛ 2
МЕТОДИ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

2.1. Дослідження штучного інтелекту як явища, його етапи та застосування

На перехресті 2022-2023 років в Україні основною темою обговорень став Chat GPT, який фактично став синонімом штучного інтелекту (ШІ). Він раптово увірвався в наше повсякдення, породив нову хвилю страху перед штучним інтелектом. Зовсім недавно головним обуренням було те, що ШІ захопить світ, встановить свої правила та контролюватиме все або стане загрозою, спрямованою на знищення людства. Але сьогодні цей перелік поповнився новим страхом - втрати роботи. Ці страхи, здавалося б, протистоять безліччю переваг, які штучний інтелект може принести в наше життя. Четверта промислова революція, 4IR, або Індустрія 4.0, обіцяє бути більш ефективною, безпечною та точною [39].

Засновник терміна "ШІ" вважається Джон Маккарті (John McCarthy). Його часто називають "батьком" штучного інтелекту, і вважають одним із головних учених у цій сфері. Вже у 1956 році він разом з іншими учасниками, що готували виступ на конференцію в Дартмуті, окреслив штучний інтелект як "науку й техніку, налаштовані на генерування розумних машин".

Згодом сталося чимало подій і проривів, але термін "ШІ" завжди пояснювався в контексті визначення Маккарті або, принаймні, з урахуванням його.

У сучасному розумінні, ми визначаємо штучний інтелект як галузь інформатики, що спеціалізується на розробці та створенні комп'ютерних систем, здатних виконувати завдання, які зазвичай вимагають рівня інтелекту, схожого на людський [39].

На перший погляд, це визначення здається досить адекватним і зрозумілим для інтуїтивного сприйняття. Однак, при ретельному аналізі може виникнути непорозуміння щодо того, що розуміється під "інтелектом, що зазвичай асоціюється

з людським інтелектом". Поняття інтелекту часто асоціюється з усіма аспектами людської поведінки, хоча не кожна з них може вважатися такою. Наприклад, багато рутинних дій, які характеризують людську активність, можуть бути визнані завданнями, "пов'язаними з людським інтелектом". Але через їх рутинність вони стали стандартними і повторюються без змін. Це означає, що вони можуть бути передбачені наперед, і, відповідно, не розглядаються як прояв інтелекту.

Рисунок 2.1 – Сучасний світ : людина та штучний інтелект за її спиною

Штучний інтелект має мати кілька впорядкованих характеристик, схожих на ті, які притаманні людині, що створює цей інтелект. Це означає, що можна сформулювати більш точне визначення ШІ. Штучний інтелект — це наукова галузь та технологія, що дозволяє комп'ютерам вирішувати проблеми, подібно до людей, які вміють адаптуватися до обставин, навчатися, обробляти інформацію, робити висновки та приймати рішення самостійно [39].

Досягнення такого рівня не є простим завданням, і одним із способів досягнення цього є поступове ускладнення технології, яку вже названо ШІ, але насправді вона представляє собою лише вузький штучний інтелект. Для кращого розуміння цієї теми, слід ознайомитися з чотирма видами штучного інтелекту.

Класифікація штучного інтелекту найкраще проводиться відповідно до досліджень професора Аренда Гінця, який вважається одним із найуспішніших у цій

сфері. Він запропонував чотири категорії для більшої ясності та даліїшого розвитку ШІ [39].

Реактивні машини. Цей тип штучного інтелекту не має можливості запам’ятовувати події, не пам’ятає минулого та не може аналізувати майбутні ситуації на основі передбачень. Все, що вона робить, це вибирає найкраще рішення у даному контексті в даний момент. Ідеальним прикладом є Deep Blue від IBM, суперкомп’ютер, який у 1990 році переміг шахового гросмейстера Гаррі Каспарова. Deep Blue є типовим представником реактивної машинної інтелектуальної системи, яка володіє знаннями лише про рухи фігур на шаховій дошці і обмежена правилом не допускати повторення однакового ходу тричі, і це все. Таким чином, при повторенні ситуацій вона завжди виконує одну і ту ж дію. Це нагадує поведінку Sphex ichneumoneus, про яку ми говорили раніше. Реактивна машинна інтелектуальна система буде вести себе аналогічно при кожному зіткненні з однаковою ситуацією. Це може бути корисним у вузькоспеціалізованих умовах, наприклад, якщо потрібно автоматично керувати автомобілем за заданою траєкторією. Однак відсутність здатності до адаптації може створювати проблеми. Наприклад, якщо на дорозі, по якій йде траєкторія, розпочинаються будівельні роботи, змінюється напрямок руху або щось інше. У таких випадках транспортний засіб з реактивною машиною не зможе приймати вірні рішення або адекватно реагувати на небезпеку на дорозі. Це підкреслює важливість розробки штучного інтелекту, здатного адаптуватися до змінних умов і вчитися на новому досвіді для більш безпечної та ефективної роботи у реальному світі [40].

Системи з обмеженою пам'яттю. Ці системи можуть дивитися у минуле і спостерігати зміни з часом, але не обмежуються виключно негайною інформацією. Таким чином, продовжуючи аналогію з автомобілем, керованим штучним інтелектом, можна уявити собі саморухомі автомобілі, які відстежують швидкість і напрямок інших транспортних засобів і враховують цю інформацію в процесі прийняття рішень. Однак, хоча такий штучний інтелект має доступ до пам'яті, він зберігає її лише на короткий час. Таким чином, він не може навчатися та здобувати досвід у подальших ситуаціях. Все, що він може зробити, це використовувати інформацію для

негайних дій або прийняття рішень. Побудова систем штучного інтелекту, які можуть розвивати повне уявлення про щось, запам’ятовувати досвід і вчитися на ньому, стає складним завданням. Один з підходів полягає в розв'язанні цієї проблеми за допомогою методів, що базуються на дарвінівській еволюції. Ці методи дозволяють системам штучного інтелекту створювати власні представлення та адаптуватися до нових ситуацій. Крім того, використовуючи еволюційні алгоритми, системи ШІ можуть повторювати та покращувати свою продуктивність з часом, аналогічно до того, як живі організми еволюціонують та адаптуються в природі [41].

Теорія розуму. Наразі невідомо, як саме створити штучний інтелект такого рівня, але людство працює в цьому напрямку. Визначення такого штучного інтелекту тісно пов'язане з тим, що в психології називається "теорією розуму" - самосвідомістю інших людей. Наприклад, розуміння того, що вони мають цілі, наміри, емоції і т.д., які впливають на їхні рішення. Штучний інтелект із теорією розуму - це комп'ютерна програма, яка може розуміти, як люди думають і відчувають. Вона може передбачати, що люди зроблять і чому вони це зроблять. Така програма може визначати, коли люди щасливі, сумні, злі або відчувають інші емоції. Вона може використовувати цю інформацію, щоб краще спілкуватися з людьми та бути уважнішою до їхніх потреб і бажань. Штучний інтелект, який використовує теорію розуму, допомагає комп'ютерам бути розумнішими та соціальнішими, щоб бути корисними для людей [41].

Самосвідомий штучний інтелект. Як випливає з назви, повинен мати свідомість, як і люди. Це наступний етап його розвитку після теорії розуму. Зазвичай з цим пов'язані нові, більш етичні проблеми.

Якщо штучний інтелект починає усвідомлювати себе, то в якійсь мірі він стає особистістю. Цей тип штучного інтелекту розуміє людей, знає про їхні емоції та думки, а також розуміє відсутність цього в собі і матиме щось інше, щось штучне. Але тут виникає проблема, адже невідомо, як саме на це відреагує штучний інтелект. Це може призвести до безлічі міркувань, гіпотез, антиутопій та інших теорій. Але незалежно від усього, слід розуміти, що людство ще не наблизилось до цього етапу. Більше того, навіть неясно, чи буде можливо створити такий рівень штучного

інтелекту. Тому що це настільки складно, що навіть незрозуміло, чи можливо це взагалі. З огляду на ці чотири типи/етапи штучного інтелекту, перше визначення, яке ми навели, свідчить про те, що на даний момент штучний інтелект не існує. Однак чому всі говорять про нього, ніби він існує? Просто через те, що його зазвичай поділяють на вузький і загальний штучний інтелект, відомий також як слабкий і сильний ШІ. Вузький штучний інтелект може виконувати лише певний діапазон завдань, і чим він розвиненіший, тим більше можливостей він надає. Загальний штучний інтелект може виконувати всі завдання як людина, можливо навіть краще, бути самосвідомим і т.д. Цей поділ можна розглядати як еволюційний процес, в якому ми заздалегідь знаємо про всі наступні ланки. І якщо ми продовжимо аналогію, то зараз ми перебуваємо приблизно на фазі "австралопітеків" і рухаємося до Homo sapiens. Щоб пройти такий шлях, штучний інтелект повинен потужно вдосконалюватися. Його постійно треба навчати, і навчати. Наразі для цього існують декілька методів навчання [41].

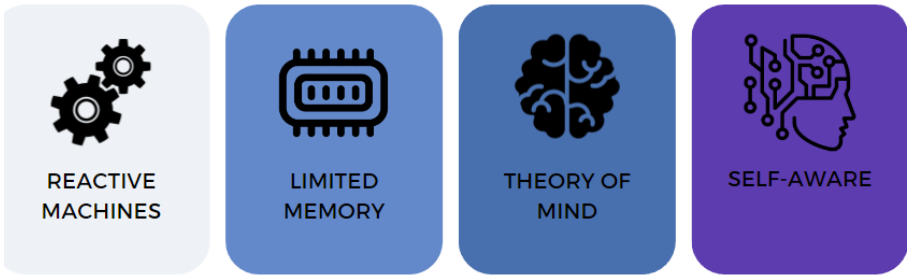

Рисунок 2.2 – Чотири етапи щтучного інтелекту

Щоб уникнути реактивного підходу, штучний інтелект має мати здатність запам'ятовувати інформацію, порівнювати її з попередньо засвоєною та вносити корективи для вдосконалення. Цей процес відомий як машинне навчання, яке має чотири основні типи навчання, що використовуються в даний час [42].

Контрольоване навчання. У машинному навчанні воно означає навчання системи коректній класифікації даних та їхньому упорядкуванню. Цей процес передбачає попереднє маркування категорій даних людьми. Наприклад, для навчання

ШІ розпізнавати котів можуть використовуватися тисячі зображень котів з різних кутів та ракурсів, позначених як коти. В результаті система зможе ідентифікувати сутність кота.

Навчання без контролю. Воно дозволяє штучному інтелекту самостійно визначати індивідуальні характеристики та риси для формування категорій. У відміну від контрольованого навчання, тут немає заздалегідь відомого кінцевого результату. ШІ самостійно визначає, які критерії використовувати та як розподіляти дані, і цей процес не контролюється людьми [42].

Напівконтрольоване навчання. Це поєднання двох попередніх методів, де ШІ отримує обмежену кількість данних, які мають певне позначення, і використовує їх для подальшого самонавчання. У цьому випадку ми також заздалегідь знаємо, який результат має бути в кінці.

Навчання з підкріпленням. Штучний інтелект працює з метою досягнення певного результату. Це досягається за допомогою позитивного підкріплення у випадку успіху і негативного підкріплення у випадку невдачі. Винагорода може змінюватися в залежності від того, наскільки точно завдання виконано: збільшуватися, якщо виконано правильніше, або, навпаки, зменшуватися, якщо ШІ обрала неправильний шлях. Цей підхід можна порівняти з грою "гаряче-холодно". Машинне навчання використовує різноманітні методи, підходи і спеціальні моделі, такі як алгоритми, які аналізують дані та приймають рішення на їх основі. Одним із таких типів моделей є нейронні мережі, які будуть розглянуті докладніше [42].

Нейронні мережі. Нейронні мережі є одним із найбільш розповсюджених методів навчання штучного інтелекту, що базується на імітації роботи нейронів у людському мозку. Це система штучних нейронів, відомих як перцептрони, які виступають як обчислювальні вузли, призначені для класифікації або аналізу інформації. На кожному рівні перцептрони виконують певні операції та передають інформацію наступним вузлам на наступному рівні. Якщо мережа має більше трьох рівнів, її називають глибокою нейронною мережею або просто глибоким навчанням. Нейронні мережі мають різні типи, існують декілька основних, які ми розглянемо далі.

Нейронні мережі прямого зв'язку. Ми розпочинаємо з найстарішого типу - нейронної мережі прямого зв'язку (FFNN). У цій моделі дані передаються безпосередньо від одного шару персептронів до наступного, аж до отримання кінцевого результату. FFNN відомі своєю потужністю та використанням спеціального алгоритму зворотного поширення помилок, який коригує результат, спочатку переміщуючись від кінцевого шару до початкового. Цей алгоритм, відомий як алгоритм зворотного поширення помилок, сприяє підвищенню точності результатів [43].

Конкурентні нейронні мережі. Recurrent neural networks (RNN) - це нейронні мережі з рекурентними зв'язками, що відрізняються від прямих мереж тим, що вони можуть зберігати послідовності у часі в своїй пам'яті. Наприклад, вони можуть зберігати слова з попередніх шарів і використовувати їх у поточних. Рекурентні нейронні мережі часто застосовуються для розпізнавання мови, аналізу зображень та інших завдань, де важлива послідовність даних.

Довго/короткочасна пам'ять. Одним із типів нейронних мереж є Long Short-Term Memory (LSTM), яка є розширеною версією рекурентної нейронної мережі (RNN). Вона здатна не лише зберігати слова, але й запам'ятовувати цілі шари інформації з попередніх рівнів за допомогою спеціальних блоків пам'яті. Часто використовується для завдань, що пов'язані з розпізнаванням мови, так само як і RNN.

Згорткові нейронні мережі. Convolutional neural networks (CNN) - це мережі, які застосовуються переважно до обробки зображень. Вони працюють шар за шаром, аналізуючи деталі, такі як кольори, риси та краї, і об'єднуючи їх в один загальний шар. Це найбільш універсальна модель серед усіх типів нейронних мереж [43].

Рисунок 2.3 – Складові штучного інтелекту у вигляді сегментів

Тепер розглянемо кілька успішних застосувань штучного інтелекту в різних сферах.

OPENAI I CHATGPT. OpenAI спеціалізується на розробці штучного інтелекту, а Chat GPT можна вважати одним з їх найбільш вдалих проектів. Ця комп'ютерна програма використовує штучний інтелект для взаємодії з користувачами у форматі чату. Крім того, вони надають свій API, який викликав значний інтерес серед стартапів у сфері штучного інтелекту на початку 2023 року.

INSILICO MEDICINE. Insilico Medicine використовує штучний інтелект для створення нових препаратів та вивчення можливих цілей терапії. Вони застосовують методи глибокого навчання, генетичні алгоритми та інші техніки машинного навчання для аналізу молекулярних структур, моделювання біологічних процесів і прогнозування ефективності та токсичності можливих медикаментів [43].

SIEMENS. Завдяки штучному інтелекту Siemens оптимізує та автоматизує виробничі процеси у різних галузях своєї діяльності, включаючи автомобільну, енергетику, машинобудування та інші. Системи штучного інтелекту відстежують стан обладнання, передбачають можливі несправності та пропонують оптимальні заходи з обслуговування та заміни. Це допомагає уникнути нещасних випадків та скоротити час простою окремих машин, що, в свою чергу, підвищує ефективність виробництва та загальну продуктивність.

NETFLIX. Netflix збирає велику кількість даних про вподобання та поведінку своїх користувачів, включаючи переглянуті фільми, виставлені рейтинги, жанри та інші фактори. Шляхом використання алгоритмів машинного навчання, штучний інтелект аналізує ці дані та формує індивідуальні профілі вподобань для кожного користувача-глядача. Після цього ШІ використовує ці профілі для рекомендацій фільмів та телепередач, які, ймовірно, сподобаються даному користувачеві [44].

2.2. Методи використання штучного інтелекту в інформаційній безпеці України

У сучасних умовах глобалізації, інформаційна безпека стає визначним фактором для реалізації національних інтересів та здатності країни подолати кризові ситуації в умовах зовнішньої агресії. Ефективне управління інформаційною безпекою з боку держави, яка є основним суб'єктом її забезпечення, може протистояти загрозам, які впливають на соціально-економічне та політичне життя країни. Сфера оборони та безпеки в сучасному світі є відразу головною, і вона переживає значні зміни завдяки впровадженню технологій штучного інтелекту, що перебудовують баланс сил між державами [45].

Штучний інтелект є продуктом людської творчості, який володіє здатністю до логічного мислення, керування своєю діяльністю та обґрунтування прийнятих рішень, проте не може адаптуватися до зміни умов.

Штучний інтелект – це, перш за все, технології. Саме технології, які застосовуються для виготовлення систем і продуктів. До таких механізмів відносяться :

- машинне навчання;
- комп'ютерний зір;
- когнітивістика;
- NLP (Natural Language Processing);
- глибоке навчання тощо.

Технології штучного інтелекту в нинішньому світі впроваджуються за наступними напрямами:

- розпізнавання та синтез мови;
- інтелектуальні системи підтримки прийняття рішень;
- перспективні методи штучного інтелекту.

У галузі інформаційної безпеки застосування штучного інтелекту виникло зі спрощених завдань (на початку 2000-х років), які полягали у створенні систем, що полегшують роботу фахівців різних профілів, зокрема, вірусних аналітиків. З плином часу обсяг шкідливих файлів став настільки великим, що вже не вистачало ручного або простого автоматизованого аналізу. Ці системи виявляли патерни у шкідливому коді й дозволяли здійснити хоча б мінімальну атрибуцію. Іншими словами, вони забезпечували певну інформацію реверс-інженерам та вірусним аналітикам, яка допомагала класифікувати програмне забезпечення за певними критеріями.

Застосування штучного інтелекту в безпеці інформації обумовлено перш за все двома причинами :

- необхідністю оперативного реагування під час настання кіберінциденту;
- нестачею кваліфікованих спеціалістів з кіберзахисту [45].

На сьогоднішній день застосування штучного інтелекту в сфері інформаційної безпеки значно розширилося. Існують глобальні компанії, які аналізують великі обсяги даних в мережі, що можуть вказувати на нові загрози або, наприклад, передбачати атаки "нульового дня". У цих компаніях наявні системи, які збирають об'ємні набори даних, аналізують їх за допомогою передових технологій штучного інтелекту, виявляють закономірності, здійснюють кластеризацію даних та прогнозують загрози. Без використання таких технологій опрацювати подібний обсяг інформації практично неможливо. Тут широко використовуються нейронні мережі та методи кластеризації.

Штучний інтелект активно використовується для відслідковування загроз, де на основі інформації, зібраної з різних джерел, включаючи відкриті та закриті, прогнозуються потенційні загрози для інформаційної безпеки. Це призвело до значного збільшення масштабів завдань та обсягу застосування штучного інтелекту в

галузі інформаційної безпеки за останні двадцять років. Штучний інтелект виявляється ефективним помічником у боротьбі з кіберзагрозами [45].

Останнім часом спостерігається зростання ризиків інформаційної безпеки для державних органів у всіх країнах світу, що спричинене трьома основними факторами. По-перше, це розширення поверхні атаки, що частково пов'язане зі збільшенням кількості підключених до Інтернету пристроїв, яке у 2020 році оцінювалося на рівні 30,73 мільярда доларів США. По-друге, кіберзлочинці навчилися обходити брандмауери та програмне забезпечення безпеки, яке раніше було ефективним. По-третє, фрагментація рішень у галузі кібербезпеки створює прогалини, через які дані стають вразливими [46].

Найбільш перспективною стратегією інформаційної безпеки є випереджальний загальний підхід, який тримає в собі чотири найголовніші галузі:

- виявлення та дослідження загроз;
- безпека даних і застосунків;
- управління ідентифікацією;
- безпека мереж і систем.

В Україні важливим етапом реформування оборонно-промислового комплексу є застосування інноваційних технологій штучного інтелекту. Оскільки провідні країни світу доволі активно вивчають та застосовують можливості штучного інтелекту в галузі оборони. Наприклад, міжнародна компанія Thales Group, що спеціалізується на цифровій ідентифікації безпеки, розробляє та виробляє інформаційні системи для авіаційної та військової сфер, що створює міцну основу для швидкого та ефективного захисту різних секторів критичної інфраструктури, таких як енергетика, хімічна промисловість, транспорт, екологія та інші. Ця компанія сприяє забезпеченню інформаційної безпеки державних органів, приватних компаній та [46].

У 2019 році Швейцарія уклала угоду з Thales Group, що передбачає поставку елементів центру обробки зображень IMINT. Ця система дозволить збирати та аналізувати різноманітні цифрові зображення, використовуючи передові технології штучного інтелекту. Це надасть можливість Збройним Силам Швейцарії виявляти

загрози та застосовувати відповідні моделі захисту.власників об'єктів критичної інфраструктури [46].

Сенсорні інструменти Thales, які базуються на штучному інтелекті Cybels, пропонують новаторський захист від кібератак у сферах критичної інфраструктури. Система Cybels Sensor постійно моніторить різні джерела потенційних атак, використовуючи технології штучного інтелекту. Фахівці з лабораторії Thales виявили нові види шкідливих програм. При виявленні загроз система Cybels Sensor приховує відповідну сигнатуру, щоб кіберзлочинці не могли її виявити та обійти захист. Крім того, ця технологія може аналізувати кожен файл, що проходить через мережу, виявляючи можливі загрози, шкідливі програми та інші аномалії [46].

2 грудня 2020 року в Україні було затверджено Концепцію розвитку штучного інтелекту за Розпорядженням Кабінету Міністрів України №1556-р. Ця концепція має на меті визначення основних напрямів та пріоритетних завдань для розвитку технологій штучного інтелекту з метою підвищення конкурентоспроможності національної економіки та захисту інформаційно-комунікаційних систем. Вона передбачає застосування технологій штучного інтелекту для моніторингу соціальних мереж та інтернет-ресурсів з метою аналізу аудиторії та виявлення певних проблем. Однією з основних мет Концепції є забезпечення інформаційної безпеки, для чого були визначені основні напрями її забезпечення (рис. 2.4) [46].

Рисунок 2.4 – Основні напрями забезпечення інформаційної безпеки

Спочатку впровадження штучного інтелекту може здатися складним та витратним рішенням, доступним лише для інноваційних компаній з великими бюджетами. Однак використання його у сфері управління інформаційною безпекою стає критично необхідним для всіх підприємств, незалежно від їх розмірів або галузі.

У сучасний період кількість атак постійно зростає, а ландшафт загроз швидко змінюється. Наприклад, продукти компанії Kaspersky за кожен квартал забезпечують захист від більш ніж 700 мільйонів онлайн-атак у всьому світі, тоді як Cisco блокує 20 мільярдів мережевих атак щодня. При такому об'ємі злочинної діяльності зловмисники активно використовують автоматизовані засоби для кібератак, у тому числі застосовують технології штучного інтелекту для їх оптимізації та модернізації, а також для обхіду відомих засобів захисту.

Наприклад, відомий троян Emotet є ефективним прототипом, який поширюється головним чином через спам-фішинг. Група, що стоїть за створенням Emotet, може легко використовувати штучний інтелект для посилення своїх атак.

Іншою можливою сферою, де може бути шкідливе застосування штучного інтелекту, є удосконалення процесу підбору паролів або обхід двофакторної аутентифікації. У 2017 році дослідники створили бота, який зміг обходити CAPTCHA

з ефективністю 90%, використовуючи технології штучного інтелекту. За допомогою різноманітних джерел даних, доступних у даркнеті, зловмисники можуть створювати атаки. Тому виробники систем захисту активно впроваджують технології штучного інтелекту та машинного навчання для виявлення та прогнозування кіберзагроз і реагування на них у реальному часі. Згідно з даними Webroot, приблизно 85% професіоналів з інформаційної безпеки вважають, що зловмисники використовують технології штучного інтелекту для своїх цілей [47].

У 2019 році експерти (MarketsandMarkets, Zion Market Research) оцінили світовий ринок технологій штучного інтелекту в галузі інформаційної безпеки на рівні 8,8 мільярдів доларів США. Прогнозується, що ця цифра зросте до 38,2 мільярдів доларів США до 2026 року з річним темпом зростання на 23% (рис.2.5) [47].

Головними причинами зростання даного ринку є:

- підростаюча кількість юзерів мережі Інтернет та значне збільшення кількості пристроїв, що підключені;
- збільшення інцидентів кіберзагроз;
- зростання уразливості мережі Wi-fi до загроз безпеці.

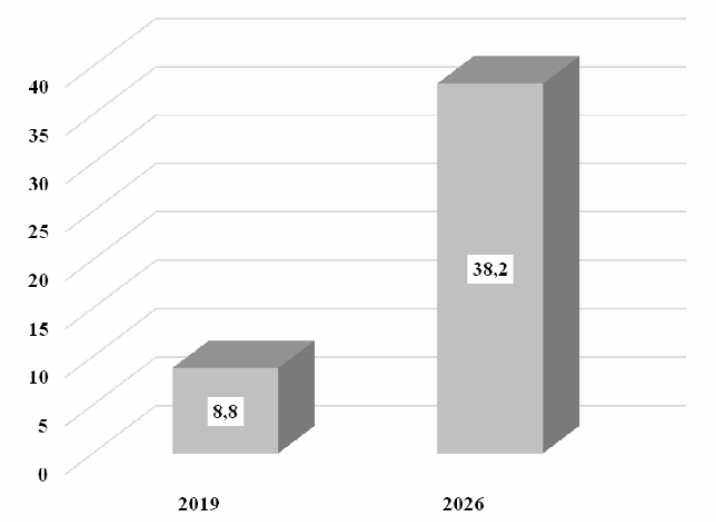

Рисунок 2.5 – Прогноз об’єму світового ринку штучного інтелекту в інформаційній безпеці на 2019-2026 роки, млрд дол США

Поза тим, ключові можливості штучного інтелекту на ринку інформаційної безпеки включають рост попиту на хмарні рішення з безпеки серед малих та середніх підприємств, а також зростання використання соціальних мереж для виконання бізнес-функцій.

Підприємства, що використовують технології штучного інтелекту для аналізу поведінки та продуктивної аналітики, отримують значні результати, такі як підвищення ефективності виявлення атак, зменшення часу реакції та витрат на організацію безпеки. Згідно з дослідженням Capgemini Research Institute, 64% підприємств з річною виручкою понад 1 млрд доларів США заявляють, що застосування технологій штучного інтелекту дозволяє їм скоротити витрати на виявлення та реагування на загрози безпеки, а близько 75% стверджують про скорочення часу реакції (на 12%) [48].

Продукти компаній, які використовують технології поведінкового аналізу та передбачувальної аналітики, можна класифікувати двома способами: за їх функціональним і технологічним типом, а також за сценаріями їх використання.

Рисунок 2.6 – Розподіл продуктів із застосуванням технологій штучного інтелекту за сценаріями використання

Технології штучного інтелекту розкривають нові горизонти для розвитку сучасних засобів захисту інформації. У зв'язку з останніми тенденціями у цифровій аналітиці інформаційної безпеки помітно зростає як обсяг, так і складність даних, що генеруються в цифровому просторі. Крім того, кіберзлочинці значно трансформували свої підходи та техніки атак. Багато з сучасних DDoS-атак будуються на основі "розумних" ботнетів, які, не маючи централізованого керівництва, можуть самостійно організовуватися та вирішувати складні завдання. Підходи до соціальної інженерії також значно вдосконалилися: зловмисники вивчили, як автоматизувати розсилку через різні канали, надсилаючи інформацію, яка виглядає дуже автентично для користувачів. Це призвело до того, що більшість компаній стикаються з ситуацією, коли традиційні методи забезпечення інформаційної безпеки стають малоефективними або абсолютно неефективними та збитковими.Основними видами технологій штучного інтелекту в мережі інформаційної безпеки є [49]:

1. EDR (Endpoint Detection and Response) – платформи для виявлення атак на робочих станціях, серверах та інших комп’ютерних пристроях (кінцевих точках) і швидка реакція на них - це невід’ємна частина захисту. Завдяки застосуванню технологій штучного інтелекту, продукти цієї категорії можуть виявляти невідомі шкідливі програми, автоматично класифікувати загрози та самостійно реагувати на них, передаючи дані у центр управління. Штучний інтелект приймає рішення на основі загальної бази знань, накопиченої завдяки збору даних з безлічі пристроїв. Окрім цього, деякі продукти цього типу використовують технології штучного інтелекту для розмітки даних на кінцевих точках і подальшого контролю за їх переміщенням, з метою виявлення внутрішніх загроз. [49].

2. NDR (Network Detection and Response) – прилади і аналітичні платформи, які виявляють мережеві атаки та надають можливість швидко на них реагувати, є важливою складовою інфраструктури. Використовуючи накопичену статистику та базу знань про загрози, продукти цього типу здатні виявляти шляхом технологій штучного інтелекту загрози у мережевому трафіку і автоматично реагувати на них, змінюючи конфігурацію мережевих пристроїв та шлюзів. Частину цих продуктів спеціалізується на захисті інфраструктури хмарних провайдерів. Ще один сценарій

використання штучного інтелекту в мережевому захисті - це аналіз поштового трафіку для виявлення фішингу.

3. UEBA (User and Entity Behavior Analytics) – системи аналізу поведінки користувачів та інформаційних сутностей мають на меті виявлення незвичайних ситуацій і використовують їх для виявлення загроз, як внутрішніх, так і зовнішніх. Одним з основних застосувань технологій штучного інтелекту в продуктах типу UEBA є автоматичне виявлення аномалій у поведінкових моделях користувачів та різних інформаційних систем. Знайдені аномалії класифікуються за допомогою штучного інтелекту як різні загрози та ризики для організації. Метою виявлення аномальної поведінки може бути моніторинг та управління доступом, виявлення шахрайства, захист конфіденційної інформації, а також перевірка дотримання різних нормативних вимог.

4. TIP (Threat Intelligence Platform) – платформи передбачення загроз та реагування на них використовують велику кількість різноманітних даних, які зберігаються у великому наборі даних (Data Lake), а також індикатори компрометації (IoC). Використання штучного інтелекту допомагає підвищити ефективність виявлення невідомих загроз на ранніх етапах; цей сценарій схожий на роботу SIEM-систем, але зорієнтований на зовнішні джерела даних та зовнішні загрози [49].

5. SIEM (Security Information and Event Management) – рішення, які здійснюють моніторинг інформаційних систем у реальному часі, аналізують події безпеки, що надходять від мережевих пристроїв, засобів захисту інформації, IT-сервісів, інфраструктури систем та додатків, та допомагають виявити інциденти інформаційної безпеки. У таких системах накопичується велика кількість даних з різних джерел, а використання технологій штучного інтелекту дозволяє виявити аномалії за допомогою евристичних методів та зменшити помилкові спрацьовування під час зміни моделей даних.

2.3. Оцінювання ризиків безпеки інформаційної системи із застосуванням штучного інтелекту

"Стандарти оцінки ризиків" містять поради щодо використання технологій та методів для кожного з перерахованих аспектів управління ризиками. Рекомендовані методи в основному базуються на експертній оцінці, тому потребують значних зусиль для впровадження і залежать від людського фактору, що у свою чергу призводить до виникнення додаткових ризиків, пов'язаних із можливими систематичними дефектами у механізмах управління ризиками, викликаними помилковими або необ'єктивними думками експертів, які беруть участь у процесі. Також варто відзначити, що успішне використання запропонованих класичних технологій значною мірою залежить від процесів збору інформації з різних джерел, її обробки, структурування та передачі великих обсягів даних, а також систематизації знань, отриманих в результаті управління ризиками [52].

Розглядаючи зазначені вище результати стандартів оцінки ризиків, виходять деякі важливі пропозиції для удосконалення процесів управління ризиками. По-перше, варто розглянути можливість використання математичних моделей штучного інтелекту для ключових завдань оцінки ризиків, таких як ідентифікація та виявлення нових видів ризиків, а також оцінка ймовірності настання ризиків та потенційних наслідків в разі їх настання. По-друге, майже всі процеси управління ризиками можуть бути інтегровані в інтелектуальні інформаційні системи, що базуються на онтології предметної області. Впровадження таких систем створює можливості для підвищення ефективності та якості формалізації знань у сфері управління ризиками [52].

Оцінка ймовірності виникнення ризику може бути розглянута як окрема задача класифікації і вирішуватися за допомогою моделей штучного інтелекту, які визначають ймовірність того, що об'єкт належить до певного класу. Ця класифікація є складовою завдань навчання з учителем, де навчальний набір складається з множини X, що містить ознаки об'єктів, і відповідної множини Y, яка містить мітки класів, до яких належать ці об'єкти.

У статичному вигляді завдання класифікації являє собою конструювання алгоритму відображення множини X у множину У, що здатне зіставити будь-який об'єкт із відповідними мітками.

Отже, оцінка ймовірності виникнення ризику сводиться до бінарної класифікації. В якості навчальних даних для класифікаційної моделі використовуються накопичені історичні записи про події ризику, що сталися у минулому, а також про характеристики суб'єктів та об'єктів, пов'язаних з цими ризиками [53].

Класифікаційна модель, навчена на цих даних, прогнозує ймовірність виникнення певного типу ризику у майбутньому, враховуючи характеристики суб'єктів та об'єктів, що стосуються ситуації, яку аналізують. У цьому контексті ймовірність виникнення ризику фактично визначає ймовірність приналежності об'єкта до класу А, де клас А відповідає наявності ризику, а клас В - його відсутності.

Якщо треба визначати вірогідність настання якихось типів ризиків, можна використовувати два способи:

- використання способу мультикласової класифікації (коли будь-який об'єкт із множини X може взаємодіяти одночасно з кількома класами);
- використання декількох бінарних класифікаторів, кожен із яких дуже гарно пристосований для найбільш точної оцінки якогось певного типу ризику.

Важливою особливістю, яку треба ураховувати, є можливість виникнення випадкових або умисних помилок під час документування фактів про настання ризиків у минулому у історичних даних. Найбільш серйозною проблемою є ситуація, коли з метою приховання настання ризику (інциденту) об'єкт помилково відмічається оператором як безрізиковий. Це призводить до утворення прихованих, не виявлених ризиків. В результаті в історичному наборі даних з'являється спотворена та ненадійна інформація, що суттєво погіршує якість моделей, які навчаються на цьому наборі даних для оцінки ймовірності настання ризиків [53].

Один із ефективних методів протидії цьому фактору - використання автоматизованого підходу до ідентифікації нових типів ризиків за допомогою виявлення аномалій. Аномальні об'єкти можуть бути виключені з навчального набору

даних для класифікаторів, які працюють з відомими (відомими) типами ризиків, або можуть бути розглянуті окремою групою (кластером) виявлених аномалій як потенційно нові типи ризиків, які можуть бути використані для навчання окремих класифікаторів (у другому випадку результати ідентифікації нових типів ризиків, по суті, становлять додаткові мітки для набору даних, що використовуються для навчання класифікаційних моделей) [55].

Виявлення ризиків - це ітеративний процес знаходження нових видів ризиків і визначення їх основних характеристик для майбутньої сенсової інтерпретації, дослідження та обробки.

З погляду штучного інтелекту, завдання ідентифікації ризиків може розглядатися як пошук аномалій у історичних наборах даних, пов'язаних із галуззю застосування ризик-менеджменту. Аномальність у таких даних може бути пояснена наявністю взаємозв'язків і взаємодій між об'єктами та суб'єктами діяльності, що вже призводить до розгортання прихованих (ще не виявлених) ризикових ситуацій та їх наслідків, або може вказувати на потенційні джерела виникнення таких ситуацій у майбутньому.

Для визначення вірогідності виникнення ризику можна використовувати як "стандартні методи" машинного навчання, так і глибокі нейронні мережі. Оптимальна конфігурація нейронної мережі вибирається залежно від характеру даних з навчального набору: для оцінки ймовірності виникнення ризику можна застосовувати як взаємопов'язані нейронні мережі, такі, наприклад, як згорткові або рекурентні.

Перлічимо найбільш поширені та використовані типи класифікаторів, які дають можливість визначити не тільки приналежність об'єкта, що оцінюється, до класу ризику, а й вірогідність належності до цього самого класу:

- логістична регресія;
- найближчі сусіди;
- вирішальні дерева;
- випадковий ліс:
- градієнтний бустнг [55].

Практика свідчить, що ефективність зазначених моделей класифікації залежить від конкретної природи завдання та властивостей даних. Тому в більшості випадків рекомендується навчати кілька різних моделей з різними налаштуваннями, а вибір найоптимальнішої моделі та її параметрів проводити на основі метрик якості, здобутих на тестовому наборі даних.

Методи штучного інтелекту можуть бути застосовані для оцінки ймовірності ризиків і мають потенціал для більш ефективного та якісного вирішення цих завдань порівняно з традиційними методами. Це досягається шляхом зменшення навантаження на експертів та зниження впливу людського чинника на процес та результати оцінки ризиків [55].

Зазвичай можливі наслідки при виникненні ризику можуть бути числово виражені, що залежить від багатьох факторів, які описують сам ризик, а також стан пов'язаних з ним процесів, об'єктів та суб'єктів у момент виникнення ризику. Тому оцінка величини ймовірних наслідків при виникненні ризику може бути розглянута як окреме завдання регресії і може бути вирішена за допомогою відповідних моделей штучного інтелекту. Регресія, подібно до класифікації, відноситься до завдань навчання з учителем, де навчальний набір даних складається з множини X, що містить ознаки об'єктів, та відповідної множини, що містить числові значення. Узагальнено, завдання регресії полягає у побудові алгоритму, який відображає множину X на множину У, здатного призначити будь-якому об'єкту числове значення.

У навчальній вибірці, що складається з множини X, для створення регресійної моделі містяться дані про минулі випадки ризиків, а також значення ознак, що описують ці ризики. Множина У включає числові значення, які кількісно відображають наслідки виникнення ризику (наприклад, суму збитків та витрат організації, суму нарахованих штрафів).

Також регресію можна розглядати як завдання кількісного визначення ризику у менш конкретному відношенні, коли потрібно не лише розрахувати можливі матеріальні витрати, але й прогнозувати значення, яке відображає рівень будь-якої величини або ступінь ризику. У таких випадках часто необхідно проводити додаткову інтерпретацію результатів моделі, порівнюючи прогнозні значення з певними

критеріями класифікації ризику, що визначені для конкретної сфери діяльності організації. Зазвичай такі критерії розробляються на основі експертних оцінок і закріплюються у відповідних галузевих документах, таких як нормативні акти, стандарти або рекомендації [55].

Регресійні моделі можуть комбінуватися з раніше викладеними класифікаційними моделями для оцінки ймовірності настання ризиків. Система штучного інтелекту, яка використовує як класифікацію, так і регресію, може створювати інтегральну оцінку ризику. Ця оцінка складається з ймовірності виникнення ризику та кількісної оцінки можливих наслідків.

Аналогічно до методів оцінки ймовірності виникнення ризику з використанням класифікаторів, для оцінки вірогідних наслідків ризику можуть бути застосовані як “типові методи” машинного навчання (до прикладу, лінійна регресія, метод найближчих сусідів, дерева рішень, випадковий ліс, градієнтний бустінг), так і глибокі нейронні мережі.

Автоматизована оцінка вразливостей - це систематичний процес перевірки слабких місць безпеки в системі, використовуючи автоматизовані інструменти для ідентифікації, класифікації, аналізу та визначення пріоритетів вразливостей. Ці інструменти використовуються для доступу до сховищ вразливостей, отримання інформації від постачальників про вразливості, керування активами та каналів аналізу загроз з метою виявлення, класифікації та оцінки серйозності вразливостей, а також для надання рекомендацій щодо їх усунення [56].

Дослідники використовують фаззинг, який базується на штучному інтелекті, для виявлення уразливостей у програмних і апаратних інтерфейсах та програмах. Цей процес полягає у введенні помилкових, неочікуваних або випадково згенерованих даних у програму чи інтерфейс, а потім в моніторингу подій, таких як збої, невдалі твердження коду, незадокументовані переходи або процедури налагодження, а також можливих витоків пам’яті. Використання методів штучного інтелекту дозволяє розробити автоматизовану систему для виявлення потенційних атак, генерації вхідних даних, створення ймовірних тестів та аналізу збоїв, як продемонстровано на рисунку 2.7. Дослідники також використовують міркування та обробку природної

мови для генерації вихідного коду, щоб збільшити охоплення коду за допомогою більш унікальних шляхів виконання, що є одним з ключових аспектів системи розумного фаззингу. Генерація тестів стала однією з найбільш досліджуваних областей фаззингу на основі штучного інтелекту для веб-браузерів, компіляторів, кіберфізичних систем, бібліотек програмного забезпечення та простих комп'ютерних програм [56].

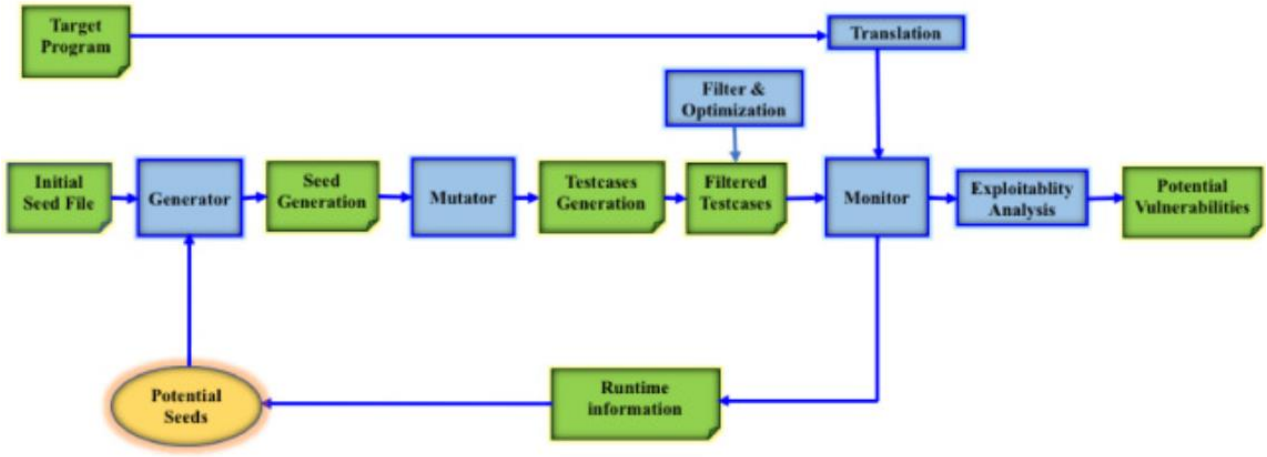

Рисунок 2.7 – Розумний процес фазингу для виявлення вразливостей

Автоматизоване тестування на проникнення — це методика, спрямована на проникнення в область потенційних атак, використовуючи відомі вразливості або вразливості "нульового дня", щоб встановити, який доступ може отримати зловмисник у даному середовищі. Дослідники активно працюють над розробкою автономного тестування на проникнення, використовуючи методи навчання з підкріпленням, спрямовані на великі мережі і алгоритми керування мережею.

Оцінка вразливостей та визначення пріоритетів є ключовим етапом, метою якого є встановлення важливості кожної вразливості та надання звіту на основі її серйозності та впливу на систему. Методи штучного інтелекту використовуються для оцінки серйозності кожної вразливості, враховуючи контекст системи, бізнес-даних та рівень загрози, а також легкість і ступінь потенційних шкідливих наслідків. Дослідники працювали над автоматизованою оцінкою та узгодженням серйозності вразливостей, використовуючи конвеєр машинного навчання на основі показників

серйозності вразливостей та профілю загроз. Наприклад, Самтані провів оцінку вразливостей пристроїв SCADA, використовуючи дані Shodan, і класифікував їх за чотирма рівнями ризику: критичний, високий, середній і низький. Браун використав граф атак для обчислення оцінки вразливостей та ризику використання для кожного пристрою Інтернету речей на основі топології мережі, яку визначив адміністратор мережі [56].

Моделювання маршруту атаки — це стратегічний метод зменшення ризику, що допомагає командам забезпечення безпеки шляхом відображення потенційно вразливих шляхів у мережі для оцінки ризику, виявлення вразливостей та впровадження заходів для захисту ключових активів. Вчені використовують методи штучного інтелекту для створення моделей маршрутів атак, використовуючи повідомлення про вторгнення або описи вразливостей. Деякі дослідники використовують повні дані кібербезпеки, такі як повідомлення про вторгнення, вразливості, журнали та мережевий трафік, щоб моделювати дії як зловмисника, так і захисника, та приймати запобіжні заходи в реальному часі.

Висновки за розділом 2

На даний момент штучний інтелект можна точно описати як корисний інструмент, який все ще знаходиться на етапі конкурентної переваги. Ті, у кого вона є, більш успішні в цій гонці. Але також потрібно враховувати, що темпи і тенденції розвитку також свідчать про те, що незабаром ШІ стане звичною справою, і тоді ті, у кого його немає, просто не зможуть взагалі брати участь у цій гонці.

У контексті інформаційної безпеки штучний інтелект – програмне забезпечення, яке здатне інтерпретувати стан середовища, розпізнати певні події та самостійно прийняти необхідні заходи. Технології штучного інтелекту ефективно справляються з розшифруванням закономірностей та аномалій, тому можуть бути інструментом моніторингу загроз. Надійна стратегія інформаційної безпеки також допомагає захистити персональні дані населення та державні дані та алгоритми, що стає важливішим у міру розгортання нових моделей штучного інтелекту.

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

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

РОЗДІЛ 3
ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДУ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ

3.1. Використання методу штучного інтелекту для оцінки рівня безпеки інформаційних та комунікаційних систем

Використання методів штучного інтелекту для оцінки рівня безпеки інформаційних та комунікаційних систем стає все більш поширеним і значущим у сучасному світі. Такий підхід дозволяє автоматизувати процеси аналізу, виявлення вразливостей та вирішення проблем безпеки в реальному часі, забезпечуючи більш ефективний та оперативний контроль за захистом інформації. Також застосування методів штучного інтелекту дозволяє підвищити ефективність та точність процесів аналізу та виявлення потенційних загроз. Поговоримо про деякі з основних способів, які використовуються в даній галузі [57].

Аналіз аномалій. Штучний інтелект може бути використаний для виявлення аномальних паттернів у активах, мережевому трафіку чи користувацькій поведінці. Методи машинного навчання дозволяють створювати моделі, які визначають зміни відносно звичайної поведінки інформаційної системи, що може свідчити про можливі загрози безпеці. Для початку проходить збір даних, які необхідно проаналізувати. Ці дані можуть бути структурованими (наприклад, таблиці з бази даних) або неструктурованими (текст, зображення, аудіо тощо). Перш ніж розпочати аналіз, дані часто піддаються попередній обробці, щоб усунути шум, виправити помилки або нормалізувати дані. Далі відбувається вибір моделі аналізу. Є багато різних методів та моделей для виявлення аномалій, включаючи статистичні методи, машинне навчання та нейронні мережі. Вибір конкретної моделі залежить від типу даних та специфіки проблеми. Якщо використовується метод машинного навчання або нейронні мережі, модель потребує навчання на вхідних даних для виявлення

нормальної поведінки системи. Після того, як модель навчена, вона застосовується до нових даних для виявлення аномалій. Це може бути виявлення відхилень від очікуваних статистичних закономірностей або виявлення відхилень від нормальної поведінки системи. Наостанок знайдені аномалії потребують подальшого аналізу для встановлення їх природи та потенційних наслідків. Загалом, аналіз аномалій з використанням штучного інтелекту є потужним інструментом для виявлення проблем та викликів у різних сферах діяльності, що дозволяє оперативно реагувати на них та приймати відповідні заходи [57].

Прогнозування ризиків. Штучний інтелект може використовуватися для аналізу потенційних загроз та вразливостей системи на основі історичних даних. Моделі машинного навчання можуть оцінювати ризики та розробляти стратегії захисту в залежності від імовірності та важкості атак. Системи ШІ для прогнозування ризиків навчаються на великих обсягах даних, які містять інформацію про минулі події. Ці дані можуть включати інформацію про кібератаки, фінансові кризи, страхові випадки, проблеми зі здоров'ям та виробничі аварії. Штучний інтелект використовує ці дані для виявлення закономірностей та факторів, які призводять до цих подій. Потім ШІ може використовувати цю інформацію для прогнозування ймовірності того, що подібні події відбудуться в майбутньому.

Ідентифікація шкідливих програм і вразливостей. Системи ШІ можуть автоматично сканувати програмне забезпечення на виявлення вразливостей та шкідливих програм. Вони можуть використовувати методи аналізу коду або статистичних методів для ідентифікації потенційно небезпечних ділянок програмного забезпечення. Машинне навчання може використовуватися для розробки моделей, які виявляють аномальні патерни в програмному коді або мережевому трафіку, які можуть свідчити про наявність шкідливих програм. Ці моделі можуть навчатися на основі великої кількості даних про відомі віруси та інші загрози, щоб вони могли ефективно виявляти нові загрози. Штучний інтелект може аналізувати статистику та знання про вразливості програмного забезпечення для ідентифікації потенційних вразливостей, які можуть бути використані зловмисниками для атак. Це може включати аналіз інформації про попередні атаки,

відомі програмні дірки безпеки та інші джерела. Штучний інтелект може також використовуватися для аналізу текстових джерел, таких як форуми, блоги та соціальні медіа, для виявлення ознак або попереджень про нові загрози або вразливості [57].

Автоматизована оцінка відповідності стандартам безпеки. Штучний інтелект може бути використаний для автоматизованої перевірки відповідності системи встановленим стандартам безпеки, таким як ISO 27001, NIST, або GDPR. Він може аналізувати конфігурації системи, політики доступу та інші параметри для виявлення відхилень від вимог безпеки. Штучний інтелект може бути використаний для сканування систем і мереж з метою ідентифікації вразливостей та невідповідностей стандартам безпеки. Це може включати сканування веб-додатків, мережевих портів, конфігурацій серверів. На основі результатів аналізу штучний інтелект може генерувати звіти про відповідність і рекомендації щодо усунення виявлених проблем. Це допомагає організаціям швидко знайти та виправити потенційні вразливості та невідповідності. Штучний інтелект може постійно вдосконалювати свої алгоритми на основі нової інформації та досвіду. Він може використовувати методи машинного навчання для адаптації до нових загроз та змін у вимогах стандартів безпеки.

Прогнозування інцидентів безпеки. Системи ШІ можуть використовувати дані про попередні інциденти безпеки для прогнозування майбутніх загроз та розробки стратегій захисту. Вони можуть використовувати методи аналізу даних для виявлення зв'язків між різними видами інцидентів та прогнозування ймовірності їх виникнення. Штучний інтелект може використовуватися для моделювання кібератак та оцінки їх потенційного впливу на системи. Це може допомогти IT-адміністраторам розробити більш ефективні плани реагування на інциденти. ШІ може використовуватися для автоматизації багатьох завдань, пов'язаних з безпекою систем, таких як сканування вразливостей, патч-менеджмент та реагування на інциденти. Це може звільнити час IT-адміністраторів для інших важливих завдань [57].

Одним із основних напрямків використання штучного інтелекту в сфері кібербезпеки є машинне навчання. Моделі машинного навчання можуть бути натреновані на великій кількості даних про типові загрози, атаки, аномальну

поведінку користувачів та систем, щоб вони могли автоматично розпізнавати підозрілі або шкідливі дії. Наведемо список із деяких конкретних застосувань.

Виявлення загроз інтелектуальної безпеки. Моделі машинного навчання можуть аналізувати великі обсяги даних для виявлення несправедливих доступів, незвичайної активності користувачів або зловмисних програм.

Автоматизоване виявлення та відповідь на загрози. Системи штучного інтелекту можуть автоматично виявляти шкідливі дії та реагувати на них у реальному часі, наприклад, блокуючи атакуючий трафік або ізолюючи компрометовані системи [57].

Автоматичне управління доступом. Системи ШІ можуть використовуватися для автоматизованого контролю доступу, виявлення недопущених спроб вторгнення та застосування політик безпеки.

3.2 Порівняльні оцінки ефективності оцінювання захищеності інформаційних та комунікаційних систем

Порівняльні оцінки ефективності оцінювання захищеності інформаційних та комунікаційних систем дуже важливі для забезпечення безпеки в сучасному цифровому світі. Оцінка захищеності систем дозволяє виявляти слабкі місця та потенційні загрози для інформації та засобів комунікації, що можуть бути використані зловмисниками [60].

Одним із ключових аспектів порівняльної оцінки ефективності є визначення критеріїв і метрик, за якими буде проводитися оцінка. Для інформаційних систем це може включати в себе такі параметри, як рівень шифрування, наявність та якість механізмів аутентифікації та авторизації, здатність до виявлення та реагування на кібератаки тощо. У комунікаційних системах важливими можуть бути параметри, пов'язані з захистом від перехоплення чи модифікації передаваних даних, безпека протоколів зв'язку, захист від атак на рівні мережі тощо.

Порівняльні оцінки також можуть враховувати фактори, пов'язані з ефективністю виявлення та реагування на загрози. Наприклад, час, необхідний для

виявлення та ліквідації інциденту безпеки, може бути важливим показником ефективності [60].

Крім того, важливо враховувати контекст використання системи при порівняльних оцінках. Наприклад, системи, які використовуються у фінансовій сфері або в урядових органах, можуть вимагати більш високого рівня захисту порівняно з системами, які використовуються в менш критичних областях.

Ще однією важливою складовою порівняльних оцінок є аналіз витрат на заходи забезпечення безпеки та їх відповідність отриманим результатам. Оцінка ефективності повинна бути здійснена у контексті витрат, щоб забезпечити оптимальне співвідношення між заходами безпеки та витратами на них.

Загалом, порівняльні оцінки ефективності оцінювання захищеності інформаційних та комунікаційних систем є складним завданням, яке вимагає аналізу різноманітних аспектів безпеки та врахування контексту їх використання [61].

Нормативний документ “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу” (далі в тексті - Критерії) встановлює критерії оцінювання захисту інформації, що оброблюється в комп'ютерних мережах, від незаконного доступу. Цей документ є методологічною базою для фіксування вимог із захисту інформації в комп'ютерних мережах від незаконного доступу; створення гарно захищених комп'ютерних мереж і засобів захисту від незаконного доступу; оцінювання захищеності даних у комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, яка вимагає захисту).

Критерії надають стандартизовану шкалу для оцінки ефективності захисних механізмів інформації від несанкціонованого доступу, які впроваджені в комп'ютерних системах. Вони є основою для розробки комп'ютерних систем, в яких передбачається реалізація захисних функцій інформації.

Критерії можуть бути використані для оцінки широкого спектру комп'ютерних систем, таких як однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені мережі, мережі, об'єктно-орієнтовані системи та інші.

Під час оцінки, якість захисту оброблюваної інформації від несанкціонованого доступу в комп'ютерній системі аналізується на основі двох видів вимог: вимог до функцій захисту, або послуг безпеки, та вимог до гарантій [61].

У рамках Критеріїв, комп'ютерна система розглядається як асортимент функціональних послуг. Кожна послуга складається з набору функцій, спрямованих на протидію певному набору загроз. Кожна послуга може включати кілька рівнів. За рівнем послуги можна оцінити ступінь захисту від певних загроз. Ці рівні утворюють ієрархію за ступенем повноти захисту, хоча не завжди є строгою підмножиною один одного.

Загрози, пов'язані з несанкціонованим доступом до інформації, представляють загрози конфіденційності. Якщо потрібно обмежити доступ до інформації, то відповідні заходи слід шукати в розділі "Критерії конфіденційності". У цьому розділі описані такі заходи (у дужках наведено позначення для кожного): довірча конфіденційність, адміністративна конфіденційність, використання об'єктів, виявлення прихованих каналів, конфіденційність обміну (експорт/імпорт).

Загрози, пов'язані з несанкціонованою зміною інформації, представляють загрози цілісності. Якщо потрібно обмежити можливість модифікації інформації, то відповідні заходи слід шукати в розділі "Критерії цілісності". У цьому розділі описані такі заходи: довірча цілісність, адміністративна цілісність, відновлення й цілісність при обміні [61].

Загрози, які можуть призвести до обмеження доступу до комп'ютерних систем або оброблюваної інформації, вважаються загрозами доступності. Якщо потрібно захиститися від відмови в доступі або забезпечити стійкість до збоїв, слід звертатися до розділу "Критерії доступності". У цьому розділі розглядаються такі заходи: ефективне використання ресурсів, стійкість до відмов, можливість гарячої заміни, відновлення після виникнення збоїв.

Розпізнавання та контроль за активностями користувачів, а також управління комп'ютерною системою становлять об'єкт послуг зі спостереження та управління. Якщо виникає необхідність в контролі за активностями користувачів або законному доступі, а також у перевірці здатності захисних засобів до виконання їх функцій,

відповідні заходи варто шукати у розділі "Критерії спостереження". У цьому розділі описуються наступні послуги: реєстрація, ідентифікація та аутентифікація, безпечний канал, розподіл обов'язків, цілісність захисних засобів, самотестування, аутентифікація під час обміну, аутентифікація відправника (гарантія авторства), аутентифікація отримувача (гарантія отримання) [62].

За винятком функціональних критеріїв, які дають змогу оцінити прсутність послуг безпеки в комп'ютерній мережі, цей документ має критерії певних гарантій, які дають можливість оцінити правильність реалізації послуг. Критерії гарантій включають у себе вимоги до архітектури комплексу механізмів захисту, середовища розробки, послідовності розробки, випробування комплексу мехінізмів захисту, середовища функціонування й документації для експлуатації. У цих Критеріях застосовується сім рівнів гарантій (Г-1,..., Г-7), що є структурними. Ієрархія ступенів гарантій відбиває потроху наростаючу міру певності в тому, що надані в комп'ютерній системі послуги дають змогу протистояти деяким загрозам, що механізми, які їх приводять у дію, у свою чергу правильно впроваджені й можуть гарантувати очікуваний користувачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Структуру Критеріїв показано на рисунку 3.1.

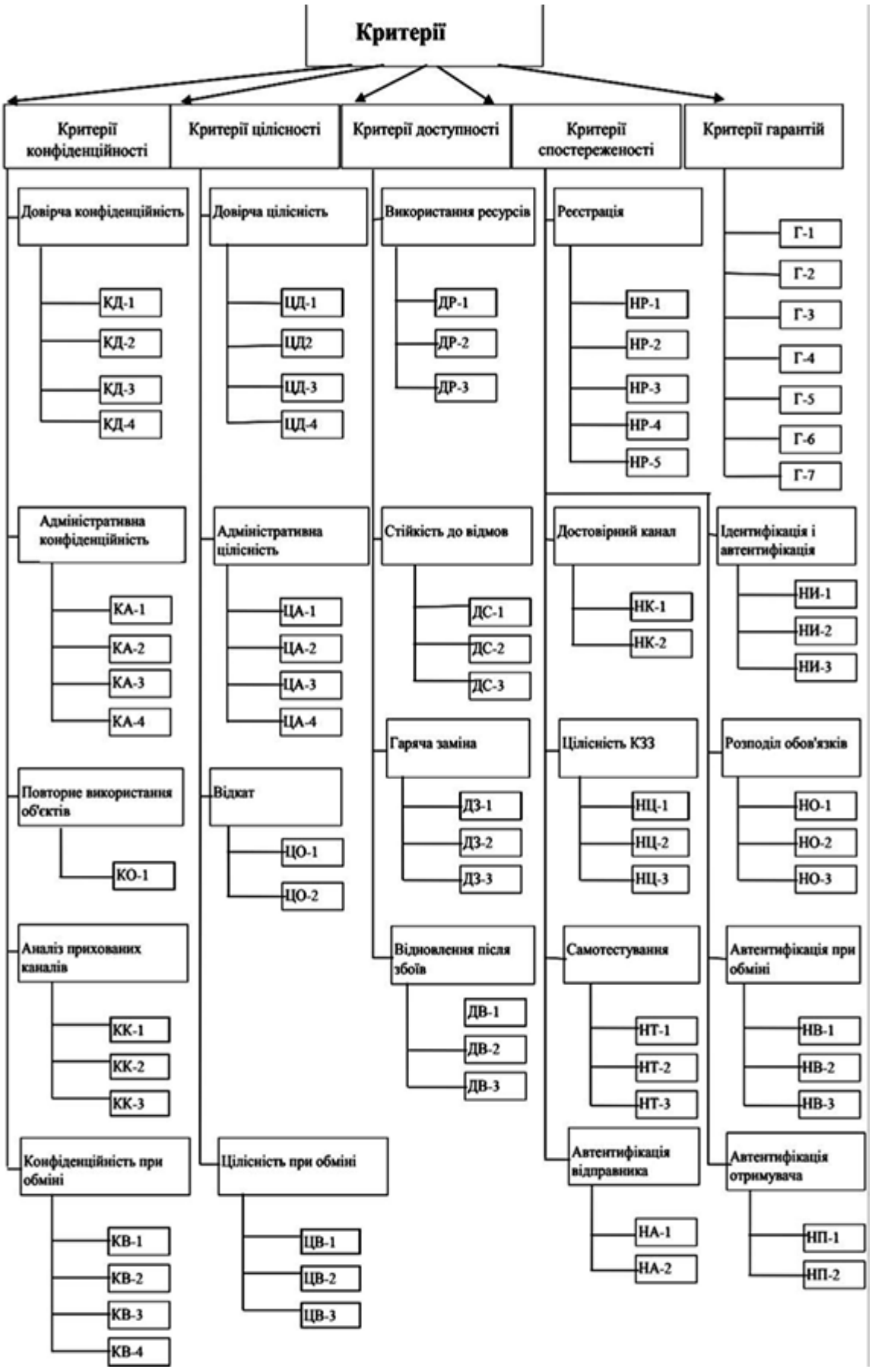

Рисунок 3.1 – Структура нормативного документу Критерії

3.3 Практичні рекомендації щодо технології оцінки захищеності інформаційно-комунфкаційних систем на базі штучного інтелекту

Перш ніж впроваджувати технологію оцінки захищеності на базі штучного інтелекту, необхідно чітко визначити свої цілі. Чого саме ми хочемо досягти за допомогою цієї технології? Які ризики ми визначили найважливішими для себе? Також потрібно визначити, які типи даних хочемо аналізувати. Це можуть бути журнали систем, трафік мережі, файли журналів, код програмного забезпечення та інше. Необхідно вибрати, які конкретно типи загроз ми хочемо виявляти? Це можуть бути шкідливі програми, вразливості, атаки типу "людина в середині" тощо.

Відповідно до наших цілей, треба вибрати правильну технологію. Існує безліч різних технологій оцінки захищеності на базі штучного інтелекту, кожна з яких має свої сильні та слабкі сторони. Важливо вибрати технологію, яка відповідає нашим потребам та ресурсам. При виборі технології слід враховувати деякі фактори. Необхідно розуміти, наскільки точно технологія може виявляти загрози, наскільки швидко вона може аналізувати дані. Також треба знати, чи може технологія масштабуватися для обробки великих обсягів даних та наскільки легко взагалі використовувати дану технологію? Також не можна оминати питання ресурсів, що необхідно буде вкласти в дану технологію.

Для того, щоб технологія оцінки захищеності на базі штучного інтелекту працювала ефективно, їй потрібні високоякісні дані. Важливо очистити та нормалізувати свої дані, щоб видалити будь-які помилки або невідповідності. Нам також може знадобитися позначити свої дані, щоб ШІ міг навчитися розпізнавати різні типи загроз.

Після того, як ми вже вибрали технологію та підготували свої дані, необхідно розгорнути технологію оцінки захищеності на базі штучного інтелекту. Це може включати встановлення програмного забезпечення, налаштування параметрів та навчання ШІ на наших даних.

Дуже доречним може виявитися використання аналітики даних та машинного навчання для створення прогностичних моделей, що може допомогти передбачити можливі кібератаки та реагувати на них заздалегідь.

Дуже важливо постійно відстежувати та обслуговувати свою технологію оцінки захищеності на базі штучного інтелекту. Нам потрібно буде оновлювати свої дані, щоб включити нові загрози, а також налаштовувати технологію, щоб вона відповідала нашим мінливим потребам.

Потрібно використовувати моніторинг та аналіз поведінки користувачів, це дозволяє виявляти аномальні дії, які можуть свідчити про можливі загрози безпеці.

Також технологію оцінки захищеності на базі ШІ можна інтегрувати з іншими інструментами безпеки, такими як системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS). Це може допомогти нам отримати більш повне уявлення про стан інформаційної безпеки.

Потрібно регулярно удосконалювати знання своїх співробітників у сфері технологій оцінки захищеності на базі штучного інтелекту, як більш ефективно її використовувати. Це допоможе їм краще зрозуміти ризики, з якими стикається організація, та те, як вони можуть допомогти захистити наші системи.

Дуже важливо переконатися, що використання нами технології оцінки захищеності на базі ШІ відповідає всім відповідним законам та нормативним актам.

Висновки за розділом 3

Значимість та перспективи використання штучного інтелекту в сфері кібербезпеки переоцінити доволі важко. Використання штучного інтелекту в оцінці захищеності інформаційно-комунікаційних систем має значний потенціал для підвищення рівня безпеки та виявлення загроз. Методи штучного інтелекту, такі як машинне навчання та аналітика даних, дозволяють автоматизувати та поліпшити процеси виявлення вразливостей та аномалій в ІКС. Практичне застосування методів штучного інтелекту вже спостерігається в реальних умовах, де вони допомагають виявляти та усувати загрози кібербезпеці. Необхідно продовжувати розвивати методи штучного інтелекту для кібербезпеки, зокрема, шляхом вдосконалення алгоритмів, збільшення обсягу доступних даних та розробки нових технологій. Однаково важливо враховувати виклики та обмеження використання штучного інтелекту в цілях

кібербезпеки, такі як конфіденційність даних, етичні аспекти та можливість використання атаками штучного інтелекту. Штучний інтелект повинен інтегруватися з загальною стратегією кібербезпеки організації, доповнюючи традиційні методи та інструменти.

У цілому, практичне застосування методів штучного інтелекту для підвищення ефективності оцінювання захищеності інформаційно-комунікаційних систем є перспективним напрямком розвитку, який може значно покращити кібербезпеку та захист інформації в сучасному цифровому середовищі.

ВИСНОВКИ

Область оцінювання захищеності інформаційно-комунікаційних систем на базі штучного інтелекту є ключовою для забезпечення кібербезпеки в сучасному цифровому світі. Дана дипломна робота дозволила зрозуміти, як штучний інтелект може бути застосований для виявлення вразливостей, аномалій та загроз в інформаційно-комунікаційних системах, що дозволяє забезпечити їхню ефективну захищеність. Також у роботі були запропоновані власні практичні рекомендації щодо оцінювання захищеності ІКС на основі штучного інтелекту.

Дослідження та аналіз існуючих методів показали широкий спектр можливостей, які відкриває штучний інтелект у цій області. Використання методів машинного навчання, аналізу даних та нейронних мереж може значно підвищити ефективність виявлення та реагування на потенційні загрози кібербезпеки.

Використання штучного інтелекту в оцінці захищеності інформаційно-комунікаційних систем має значний потенціал для підвищення рівня безпеки та виявлення загроз. Необхідно продовжувати розвивати методи штучного інтелекту для кібербезпеки, зокрема, шляхом вдосконалення алгоритмів, збільшення обсягу доступних даних та розробки нових технологій.

Однак, важливо враховувати, що штучний інтелект не є універсальним рішенням і має свої обмеження. Для успішного застосування методів штучного інтелекту в області кібербезпеки, необхідна якісна підготовка та аналіз даних, а також постійне оновлення та вдосконалення алгоритмів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ємельянов С.Л. Основи інформаційної безпеки. Одеса: Фенікс, 2014. 357 с.

2. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. К.: ВД “Гельветика”, 2017. 168 с.

3. Остапов С. Е. Технології захисту інформації: навч. посіб. Харків, 2013. 476 с. 8 Електронне урядування: опорний конспект лекцій. К., 2012. 264 с.

4. Громико І. О. Загальна парадигма захисту інформації: визначення термінів від носіїв до каналів витоку інформації / І. О. Громико // Системи обробки інформації. Х.: ХУПС, 2016. Вип. 9 (58). С. 3-9.

5. Кобозева А.А. Аналіз захищеності інформаційних систем: підручник / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. К.: ДУІКТ, 2010. 316 с.

6. Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є., Політика інформаційної безпеки: підручник. – Луганськ: вид-во СНУ ім.. В.Даля, 2019, 300 с.

7. Новицький А. Правове регулювання інституціоналізації інформаційного суспільства в Україні : [монографія] / А. Новицький. – Ірпінь : НУ ДПС України, 2011. 444 с.

8. Гуцалюк М.В., Гайсенюк Н.А. Організація захисту інформації. – К.: Альтерпрес, 2015. 541 с.

9. Марущак А.І. Технологічні основи захисту інформації з обмеженим доступом: курс лекцій. – К.: КНТ, 2017. 208 с.

10. Василюк В. Об’єкти захисту інформації. Методи та засоби захисту інформації / В. Василюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 2 (13). – С. 88–102.

11. Клімушин П.С. Електронне урядування в інформаційному суспільстві: монографія / П.С. Клімушин, А.О. Серенок. – Х.: Вид-во ХарРІ НАДУ «Магістр», 2010. 312 с.

12. Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. – К.: ДУІКТ, 2016. 126 с.

13. Головань С. Про термінологію в області безпеки інформації / С. Головань, А. Давиденко, Л. Щербак // Збірник наукових праць Інституту проблем моделювання в енергетиці імені Г.Є. Пухова. – 2013. Вип. 66. С. 31–35.

14. Шепета О. Адміністративно-правові засади технічного захисту інформації : дис. … канд. юрид. наук : спец. 12.00.07 «Теорія управління; адміністративне право і процес; фінансове право; інформаційне право» / О. Шепета ; Нац. академія Служби безпеки України. – К., 2011. 215 с.

15. Андрєєв В.І. Основи інформаційної безпеки: підручник / В.І. Андрєєв, В.О. Хорошко, В.С. Чередніченко [та ін.] – К.: ДУІКТ, 2019. 292 с.

16. Задорожня Л. М., Коваль М. І., Брижко В. М. Питання вдосконалення законодавства України у сфері інформації та інформатизації: додаток до наукового журналу “Правова інформатика”. / За ред. чл.-кор. АПрН України М. Я. Швеця. – К.: НДЦПІ, 2015. 31 с.

17. Закон України «Про захист інформації в автоматизованих системах» // *Відомості Верховної Ради України*, 1994. № 31. С. 286.

18. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики. – К.: АДПС України, 2018. 187 с.

19. Казакова Н.Ф. Задачі захисту інформаційних ресурсів від впливу зовнішніх загроз // Матер. II молод. наук. конф. «Сучасні інформаційні технології в повсякденній діяльності та підготовці фахівців», 31 березня 2016 р., Одеса : ОНЮА, 2016. 69 с.

20. Козакова Н.Ф. Інформаційне забезпечення системи управління якістю продукції в сфері телекомунікацій

21. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть [Текст] / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. 2019. № 14 : Міжнародні відносини. С. 46-48.

22. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. 288 с.

23. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. / Б.А. Кормич. К., Принт. 2014. 169 с.

24. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. К.: "Кондор", 2014. 384.

25. Кочарян А. Б. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навч.-метод. посіб. / А. Б. Кочарян, Н. І. Гущина. К., 2019. 100 с.

26. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. Х.: Вид. ХНЕУ, 2018. 510 с.

27. Ляшенко І. О. Європейські критерії безпеки інформаційних технологій. Сучасні інформаційні технології у сфері безпеки та оборони. 2012. № 1 (13). С. 84–86.

28. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак; під ред. В.О. Хорошко. – Луганськ: Ноулідж, 2012. 480 с.

29. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти. Х.: УВС, 2020. 368 с.

30. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22; 22. НД ТЗІ 2.5-008-2002.

31. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 2019. С. 22.

32. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

33. Бабаєв В.М. Електронне урядування: текст лекцій / В.М. Бабаєв, М.М. Новікова, С.О. Гайдученко. Х.: ХНУМГ, 2014. 127 с.

34. Постанова Кабінету Міністрів України “Про створення Національного автоматизованого інформаційного фонду стандартів” від 01.02.1995 р. № 84 із змінами, внесеними Постановою КМУ від 16.03.2000 р. № 501.

35. Правова інформатика: системна інформатизація законотворчої, правозастосовної, правоохоронної, судочинної та правоосвітньої діяльності в Україні. – Ужгород: ІВА, 2020. 611 с.

36. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2017. 365 с.

37. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – К. : Держстандарт України, 2017. 15 с.

38. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – К. : Держстандарт України, 2017. 16 с.

39. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.

40. Цимбалюк В. С. Окремі питання щодо визначення категорії “інформаційна безпека” у нормативно-правовому аспекті. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2014. № 8.С. 30-33.

41. Цимбалюк В. С. Сутність і зміст правової інформатики (методологічний аспект). // Правова інформатика. – 2005. – № 4(8). – С. 18-30.

42. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє. В. М. Фурашев, Д. В. Ланде, О. М. Григор’єв, О. В. Фурашев. – К.: Інжиніринг, 2015. 164 с.

43. Якубівська Ю. Є. Колізії норм права та компетенції органів управління у сфері інтелектуальної власності як загроза інформаційній безпеці / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. Серія : Юридичні науки. - К. : УДУФМТ, 2015. № 4 (81). С. 37-42.

44. www.zfort.com.ua/blog/sho-take-shtuchnii-intelekt

45. Duchi J. Adaptive subgradient methods for online learning and stochastic optimization / J. Duchi, E. Hazan, Y. Singer // Journal of Machine Learning Research. — 2011. — P. 2121–2159.

46. Liu P. SVM or deep learning? A comparative study on remote sensing image classification / P. Liu, K.K.R. Choo, L. Wang, F. Huang // Soft Computing. — Vol. 21, N 23. — 2017.

47. Pirotti F. Benchmark of machine learning methods for classification of a Sentinel-2 image / F. Pirotti, F. Sunar, M. Piragnolo // International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences. — Vol. 41. — 2016.

48. Mnih, V. Playing Atari with deep reinforcement learning. Technical Report / Kavukcuoglu, K., Silver, D., Graves, A., Antonoglou, I., Wierstra, D., Riedmiller M. – DeepMind Technologies, 2013 – C. 7

49. Zhang F. Scene classification via a gradient boosting random convolutional network framework / F. Zhang, B. Du, L. Zhang // IEEE Transactions on Geoscience and Remote Sensing. — Vol. 54, N 3. — 2016.

50. Zhao W. Learning multiscale and deep representations for classifying remotely sensed imagery / W. Zhao, S. Du // ISPRS Journal of Photogrammetry and Remote Sensing. — Vol. 113. — 2016.

51. Vilovatyh, A.V. (2020), “Towards a theory of global security in the emerging digital age”, Svobodnaya mysl, vol. 4

52. The Verkhovna Rada of Ukraine (2020), The Order of Ukraine “The concept of artificial intelligence development in Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (Accessed 7 December 2021).

53. Nishimenko, O. A. (2016), “Information security of Ukraine at the present stage of development of the state and society”, Nashe pravo, vol. 1

54. Markets and Market (2019), “Artificial Intelligence in Cybersecurity Market by Offering”, available at: https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html (Accessed 7 December 2021).

55. Thales (2019), “Leveraging artificial intelligence to maximize critical infrastructure cybersecurity”, available at: https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximizecritical-infrastructure (Accessed 7 December 2021).

56. Гладка Ю. А. Аналіз застосування технологій штучного інтелекту в кібербезпеці / Ю.А. Гладка, Є. О. Назаренко //Наукові праці Третьої міжнар. наук.-практ. конф.«Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій»,).–К.: НУХТ, 25–26 січня 2021 р.(Київ, Україна

57. Гончар С. Ф. Метод оцінювання ризиків кібербезпеки інформаційних систем SMART GRID / С.Ф.Гончар //Вчені записки ТНУ імені ВІ Вернадського. Серія: Технічні науки 31.70. – 2020

58. Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій (Guide for Conducting Risk Assessments. National Institute of Standards and Technology) [Текст]. – Gaithersburg: National Institute of Standards and Technology, 2000

59. Методи штучного інтелекту в кібербезпеці [Електронний ресурс] : навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: І.В. Стьопочкіна, О.М. Новіков.

60. J.W. Mikhail, J.M. Fossaceca, R. Iammartino. A semi-boosted nested model with sensitivity-based weighted binarization for multi-domain network intrusion detection

61. Z. Li, A.L. Rios, L. Trajković. Machine learning for detecting anomalies and intrusions in communication networks

62. M. Rhode, P. Burnap, K. Jones. Early-stage malware prediction using recurrent neural networks

63. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://e-tk.lntu.edu.ua/pluginfile.php/25377/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2018.pdf

64. T. Al-Shehari, R.A. Alsowail. An insider data leakage detection using one-hot encoding, synthetic minority oversampling and machine learning techniques

65. H.I. Kure, S. Islam, M. Ghazanfar, A. Raza, M. Pasha. Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system

66. A. Binbusayyis, T. Vaiyapuri. Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM

67. P. Singh, A. Pankaj, R. Mitra. Edge-detect: edge-centric network intrusion detection using deep neural network