МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ МОДЕЛІ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У СФЕРІ КІБЕРБЕЗПЕКИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Ілля Карпека
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Ілля КАРПЕКА
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Карпеці Іллі Павловичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Моделі підтримки прийняття рішень у сфері кібербезпеки на основі штучного інтелекту”,
керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, к.т.н., доцент.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *штучний інтелект, моделі підтримки прийняття рішень, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1 Дослідити теоретичні основи підтримки прийняття рішень та штучного інтелекту в кібербезпеці.
4.2 Проаналізувати існуючі методи прийняття рішень у сфері кібербезпеки.
4.3. Розробити та практично застосувати моделі підтримки прийняття рішень на основі ШІ.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Дослідження теоретичних основ підтримки прийняття рішень та штучного інтелекту в кібербезпеці	08.04.2026	
4.	Аналіз існуючих методів прийняття рішень у сфері кібербезпеки	15.04.2026	
5.	Розробка та практичне застосування моделі підтримки прийняття рішень на основі ШІ	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	05.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Ілля КАРПЕКА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Карпека І.П. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Моделі підтримки прийняття рішень у сфері кібербезпеки на основі штучного інтелекту”

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КАРПЕКА Ілля у кваліфікаційній роботі дослідив теоретичні основи підтримки прийняття рішень та штучного інтелекту в кібербезпеці, проаналізував існуючі методи прийняття рішень у сфері кібербезпеки, розробив та практично застосував моделі підтримки прийняття рішень на основі ШІ, розробив рекомендації за темою дослідження.

КАРПЕКА Ілля показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КАРПЕКИ Іллі на оцінку “відмінно” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Карпека І.П. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Карпеки Іллі
на тему “ Моделі підтримки прийняття рішень у сфері кібербезпеки на основі штучного інтелекту”

Актуальність. Одним із пріоритетних напрямів розвитку сучасної кібербезпеки є підвищення ефективності процесів аналізу загроз та прийняття управлінських рішень в умовах постійного зростання кількості кіберінцидентів і складності атак. Сучасні інформаційні системи генерують значні обсяги даних, обробка яких потребує використання інтелектуальних методів аналізу та автоматизованої підтримки діяльності фахівців з кібербезпеки. Традиційні підходи до прийняття рішень часто виявляються недостатньо ефективними через обмежені можливості людини щодо оперативного аналізу великих масивів інформації та прогнозування розвитку кіберзагроз.

У зв’язку з цим особливої актуальності набуває використання технологій штучного інтелекту для створення моделей підтримки прийняття рішень, здатних автоматизувати процеси виявлення загроз, оцінювання ризиків та формування рекомендацій щодо реагування на інциденти безпеки. Застосування інтелектуальних алгоритмів дозволяє підвищити швидкість і точність аналізу інформації, зменшити вплив людського фактора та забезпечити більш ефективне управління кібербезпекою.

Позитивні сторони.

1. У роботі досліджено теоретичні основи систем підтримки прийняття рішень та визначено особливості застосування технологій штучного інтелекту у сфері кібербезпеки.
2. Кваліфікаційна робота оформлена відповідно до встановлених вимог. Матеріал викладено послідовно та логічно, сформульовано обґрунтовані висновки. Основні положення роботи представлено у вигляді таблиць і рисунків.
3. Автор опрацював значну кількість наукових джерел, зокрема сучасні зарубіжні публікації та матеріали з питань інформаційної безпеки, управління ризиками й впливу людського фактору.
4. За результатами дослідження розроблено модель підтримки прийняття рішень на основі штучного інтелекту та запропоновано практичні рекомендації щодо її впровадження в систему управління кібербезпекою для підвищення ефективності виявлення кіберзагроз і реагування на інциденти безпеки.

Недоліки.

Доцільно було б приділити більше уваги практичному порівнянню різних алгоритмів машинного навчання на реальних наборах даних, а також розширити експериментальну частину роботи шляхом використання спеціалізованих програмних платформ для моделювання та аналізу кіберінцидентів.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач КАРПЕКА Ілля заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню впливу людського фактору на ефективність системи управління інформаційною безпекою. Робота складається зі вступу, трьох розділів, що містять 5 рисунків, 1 таблицю, висновків і списку використаних джерел із 42 найменувань. Загальний обсяг роботи становить 70 аркушів, з яких 4 аркуші займають список використаних джерел.

Метою роботи є дослідження та розробка моделі підтримки прийняття рішень у сфері кібербезпеки на основі технологій штучного інтелекту для підвищення ефективності виявлення кіберзагроз, оцінювання ризиків та реагування на інциденти безпеки.

Об'єктом дослідження є процес підтримки прийняття рішень у системах управління кібербезпекою.

Предмет дослідження – моделі, методи та алгоритми штучного інтелекту, що використовуються для підтримки прийняття рішень у сфері кібербезпеки.

Методи дослідження. Для вирішення поставлених завдань у роботі використано методи аналізу та синтезу, порівняння, класифікації, моделювання, оцінювання ризиків, статистичного аналізу, машинного навчання, а також системний підхід до побудови моделей підтримки прийняття рішень у сфері кібербезпеки.

Як результат у роботі досліджено теоретичні основи систем підтримки прийняття рішень та технологій штучного інтелекту в кібербезпеці; проаналізовано сучасні методи підтримки прийняття рішень і алгоритми машинного навчання для виявлення інцидентів безпеки; визначено основні недоліки та обмеження існуючих підходів; розроблено архітектуру моделі підтримки прийняття рішень на основі штучного інтелекту; виконано її реалізацію та тестування на прикладі аналізу кіберінцидентів; сформульовано рекомендації щодо впровадження моделі в систему управління кібербезпекою.

Галузь застосування. Отримані результати можуть бути використані під час удосконалення систем управління кібербезпекою підприємств, установ та

організацій, а також для автоматизації процесів аналізу загроз, оцінювання ризиків і підтримки прийняття рішень в умовах сучасних кіберзагроз.

Ключові слова: КІБЕРБЕЗПЕКА, ШТУЧНИЙ ІНТЕЛЕКТ, СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, МАШИННЕ НАВЧАННЯ, КІБЕРІНЦИДЕНТ, КІБЕРЗАГРОЗА, ОЦІНЮВАННЯ РИЗИКІВ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

The qualification work is devoted to the study of the impact of the human factor on the effectiveness of the information security management system. The work consists of an introduction, three chapters containing 5 figures, 1 table, conclusions and the list of references containing 42 items. The total volume of the work is 69 pages, of which 4 pages is occupied by the list of references.

The purpose of the study is to investigate and develop a decision-support model in the field of cybersecurity based on artificial intelligence technologies, with a view to improving the effectiveness of cyber-threat detection, risk assessment and response to security incidents.

The object the study is the decision-support process in cybersecurity management systems.

The subject of the study is the models, methods and algorithms of artificial intelligence used to support decision-making in the field of cybersecurity.

Research methods. To address the objectives set out in this work, methods of analysis and synthesis, comparison, classification, modelling, risk assessment, statistical analysis and machine learning were employed, as well as a systematic approach to constructing decision support models in the field of cybersecurity.

As a result, this study examines the theoretical foundations of decision support systems and artificial intelligence technologies in cybersecurity; analyses modern decision support methods and machine learning algorithms for detecting security incidents; identifies the main shortcomings and limitations of existing approaches; an architecture for an artificial intelligence-based decision support model has been developed; it has been implemented and tested using the analysis of cyber incidents as an example; recommendations have been formulated for the implementation of the model into a cybersecurity management system.

Field of application. The results obtained can be used to improve the cybersecurity management systems of enterprises, institutions and organisations, as well as to automate the processes of threat analysis, risk assessment and decision

support in the context of modern cyber threats.

Keywords: CYBERSECURITY, ARTIFICIAL INTELLIGENCE, DECISION SUPPORT SYSTEM, MACHINE LEARNING, CYBER INCIDENT, CYBER THREAT, RISK ASSESSMENT, INFORMATION SECURITY.

ЗМІСТ

ВСТУП

Актуальність теми. Розвиток цифрових технологій, зростання кількості кіберзагроз та збільшення обсягів даних, що потребують аналізу, суттєво ускладнюють процес прийняття рішень у сфері кібербезпеки. Традиційні підходи до аналізу подій безпеки та реагування на кіберінциденти часто не забезпечують необхідної швидкості й точності обробки інформації, особливо в умовах постійної зміни характеру загроз. У зв'язку з цим особливого значення набуває використання технологій штучного інтелекту, здатних автоматизувати процеси аналізу даних, виявлення аномалій, оцінювання ризиків та підтримки прийняття управлінських рішень.

З огляду на це особливої актуальності набуває дослідження моделей підтримки прийняття рішень у сфері кібербезпеки на основі штучного інтелекту, а також розробка підходів до їх практичного використання для підвищення ефективності виявлення кіберзагроз, реагування на інциденти безпеки та забезпечення належного рівня захищеності сучасних інформаційних систем.

Мета роботи полягає у дослідженні та розробці моделі підтримки прийняття рішень у сфері кібербезпеки на основі технологій штучного інтелекту для підвищення ефективності виявлення кіберзагроз, оцінювання ризиків та реагування на інциденти безпеки.

Об'єкт дослідження – процес підтримки прийняття рішень у системах управління кібербезпекою.

Предмет дослідження – моделі, методи та алгоритми штучного інтелекту, що використовуються для підтримки прийняття рішень у сфері кібербезпеки.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити теоретичні основи підтримки прийняття рішень та штучного інтелекту в кібербезпеці.

2. Проаналізувати існуючі методи прийняття рішень у сфері кібербезпеки.

3. Розробити та практично застосувати моделі підтримки прийняття рішень на основі ШІ.

Методи дослідження. Для вирішення поставлених завдань у роботі використано методи аналізу та синтезу, порівняння, класифікації, моделювання, оцінювання ризиків, статистичного аналізу, машинного навчання, а також системний підхід до побудови моделей підтримки прийняття рішень у сфері кібербезпеки.

Практичне значення одержаних результатів. Застосування отриманих результатів дозволить підвищити ефективність процесів управління кібербезпекою шляхом використання моделей підтримки прийняття рішень на основі штучного інтелекту. Розроблена модель може бути використана для автоматизації аналізу кіберзагроз, оцінювання ризиків, виявлення інцидентів безпеки та формування рекомендацій щодо реагування на них. Впровадження запропонованих рішень сприятиме підвищенню оперативності та обґрунтованості прийняття управлінських рішень, зменшенню впливу людського фактора під час аналізу подій безпеки та покращенню рівня захищеності інформаційних систем в умовах сучасних кіберзагроз.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ТА ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

1.1 Поняття та принципи систем підтримки прийняття рішень

У сучасному інформаційному суспільстві процес прийняття рішень є одним із ключових елементів ефективного управління організаціями, підприємствами та інформаційними системами. Стрімкий розвиток цифрових технологій, збільшення обсягів інформації та ускладнення бізнес-процесів зумовлюють необхідність використання спеціалізованих інструментів, які здатні забезпечити швидкий аналіз даних і підтримати управлінців у виборі найбільш доцільних варіантів дій. Особливо актуальним це питання є в умовах кібербезпеки, де рішення необхідно приймати оперативно, враховуючи значну кількість факторів, невизначеність зовнішнього середовища та постійне виникнення нових загроз [1]. У таких умовах важливого значення набувають системи підтримки прийняття рішень, які забезпечують інформаційну, аналітичну та інтелектуальну підтримку користувачів під час вирішення складних управлінських завдань.

Прийняття рішень є складним когнітивним процесом, що полягає у виборі одного з декількох можливих варіантів дій для досягнення поставленої мети. У загальному розумінні рішення являє собою результат аналізу інформації, оцінювання альтернатив та визначення найбільш ефективного способу розв’язання певної проблеми. Якість прийнятого рішення значною мірою залежить від повноти доступної інформації, професійного досвіду особи, що приймає рішення, часу на аналіз ситуації та рівня невизначеності зовнішнього середовища. У сучасних умовах людина часто не здатна самостійно опрацювати значні обсяги даних, тому виникає потреба в автоматизованих засобах підтримки процесу прийняття рішень.

Системи підтримки прийняття рішень являють собою інтерактивні інформаційні системи, призначені для збору, обробки, аналізу та представлення

інформації з метою допомоги особам, які приймають рішення. Вони поєднують сучасні інформаційні технології, математичні методи, бази даних, аналітичні моделі та програмні засоби для формування рекомендацій щодо вирішення певних завдань [2]. Основною метою таких систем є підвищення ефективності управлінської діяльності шляхом забезпечення користувача необхідною інформацією та інструментами аналізу.

Історія розвитку систем підтримки прийняття рішень бере свій початок у 60-х роках XX століття, коли почали активно розвиватися інформаційні технології та теорія управління. Перші системи були орієнтовані переважно на економічне планування та аналіз виробничих процесів. Згодом їх функціональні можливості суттєво розширилися завдяки розвитку комп'ютерної техніки, баз даних, телекомунікаційних технологій та методів штучного інтелекту. Сьогодні системи підтримки прийняття рішень використовуються практично в усіх сферах діяльності людини, включаючи фінансовий сектор, медицину, освіту, державне управління, транспорт, промисловість та кібербезпеку.

Особливістю систем підтримки прийняття рішень є їх орієнтація на вирішення слабко структурованих і неструктурованих задач. На відміну від традиційних інформаційних систем, які працюють переважно з формалізованими процесами, системи підтримки прийняття рішень здатні враховувати невизначеність, багатокритеріальність та неповноту вихідної інформації [3]. Вони не замінюють людину у процесі прийняття рішень, а створюють умови для більш обґрунтованого та ефективного вибору оптимального варіанта дій.

Функціонування систем підтримки прийняття рішень базується на використанні інформаційних ресурсів, аналітичних моделей та спеціалізованих алгоритмів обробки даних. Важливим компонентом таких систем є база даних, яка містить інформацію, необхідну для аналізу ситуації. Джерелами даних можуть виступати внутрішні інформаційні системи організації, зовнішні інформаційні ресурси, бази знань, статистичні матеріали та результати

моніторингу. Зібрана інформація піддається обробці та аналізу за допомогою математичних, статистичних та логічних моделей.

Сучасні системи підтримки прийняття рішень здатні працювати з великими обсягами даних, здійснювати прогнозування розвитку подій, оцінювати ризики та формувати рекомендації щодо подальших дій. Завдяки використанню сучасних методів аналізу даних вони дозволяють значно скоротити час, необхідний для прийняття управлінських рішень, та підвищити їх якість. Особливо важливим це є у сфері кібербезпеки, де швидкість реагування на загрози часто визначає ефективність захисту інформаційних ресурсів [4].

Одним із ключових принципів функціонування систем підтримки прийняття рішень є принцип обґрунтованості. Він передбачає використання достовірних даних, перевірених методів аналізу та науково обґрунтованих моделей для формування рекомендацій. Реалізація цього принципу забезпечує зменшення впливу суб’єктивних факторів на процес прийняття рішень та підвищує рівень їх об’єктивності.

Важливим принципом є принцип системності. Відповідно до нього будь-яка проблема повинна розглядатися як частина більш складної системи взаємопов’язаних елементів. Система підтримки прийняття рішень повинна враховувати вплив різних факторів, їх взаємозв’язки та можливі наслідки реалізації певного рішення [5]. Такий підхід дозволяє отримати більш повну картину досліджуваної ситуації та підвищити точність прогнозування.

Принцип комплексності передбачає використання максимально повної інформації про об’єкт управління та зовнішнє середовище. Для цього системи підтримки прийняття рішень інтегрують дані з різних джерел, здійснюють їх аналіз та формують цілісне уявлення про поточну ситуацію. Комплексний підхід дозволяє мінімізувати ризик прийняття помилкових рішень через недостатність або фрагментарність інформації.

Важливе значення має принцип адаптивності. У сучасному цифровому середовищі умови функціонування організацій постійно змінюються, з’являються нові загрози, технології та вимоги. Тому система підтримки

прийняття рішень повинна мати можливість адаптуватися до змін зовнішнього середовища, оновлювати використовувані моделі та враховувати нові дані. Реалізація цього принципу забезпечує актуальність рекомендацій та підтримує ефективність системи в довгостроковій перспективі [6].

Принцип інтерактивності полягає у забезпеченні постійної взаємодії між користувачем та системою. Особа, яка приймає рішення, повинна мати можливість змінювати параметри аналізу, коригувати критерії оцінювання, переглядати результати розрахунків та отримувати пояснення щодо сформованих рекомендацій. Це дозволяє поєднати переваги автоматизованого аналізу даних із професійним досвідом і знаннями користувача.

Одним із важливих принципів є принцип оперативності. У багатьох сферах діяльності рішення необхідно приймати за обмежений проміжок часу. Це особливо характерно для кібербезпеки, де затримка в реагуванні на інцидент може призвести до значних фінансових втрат або компрометації критично важливих інформаційних ресурсів [7]. Системи підтримки прийняття рішень повинні забезпечувати швидку обробку даних та своєчасне надання рекомендацій користувачам.

Принцип гнучкості передбачає можливість модифікації структури системи, її функціональних можливостей та моделей відповідно до потреб конкретної організації. Різні сфери діяльності мають власну специфіку, тому універсальні рішення не завжди можуть забезпечити необхідний рівень ефективності. Гнучкість дозволяє адаптувати систему до особливостей конкретних бізнес-процесів та вимог користувачів.

Структура сучасної системи підтримки прийняття рішень зазвичай включає декілька взаємопов’язаних компонентів. Центральним елементом є база даних, яка забезпечує накопичення та зберігання інформації [8]. Наступним компонентом виступає база моделей, що містить математичні, статистичні, логічні та імітаційні моделі для аналізу даних і прогнозування результатів. Важливу роль відіграє аналітичний модуль, який реалізує алгоритми обробки інформації та забезпечує формування рекомендацій. Завершальним

компонентом є інтерфейс користувача, через який здійснюється взаємодія людини із системою.

Рис. 1.1 Основні компоненти системи підтримки прийняття рішень

Залежно від функціонального призначення виділяють декілька основних типів систем підтримки прийняття рішень. До них належать дано-орієнтовані системи, модельно-орієнтовані системи, знання-орієнтовані системи, документно-орієнтовані системи та групові системи підтримки прийняття рішень. Дано-орієнтовані системи зосереджені на аналізі великих масивів інформації, модельно-орієнтовані використовують математичні моделі для прогнозування та оптимізації, а знання-орієнтовані базуються на використанні баз знань та експертних правил [9]. Групові системи підтримки прийняття рішень забезпечують колективне обговорення та прийняття рішень декількома учасниками одночасно.

Таблиця 1.1

Характеристика основних типів систем підтримки прийняття рішень

Тип СППР	Основна характеристика	Сфера застосування
Дано-орієнтована	Аналіз великих масивів даних та формування звітів	Бізнес-аналітика, моніторинг подій
Модельно-орієнтована	Використання математичних і статистичних моделей	Прогнозування, планування, оптимізація
Знання-орієнтована	Використання баз знань та експертних правил	Експертні системи, кібербезпека

Документно-орієнтована	Аналіз текстових документів та інформаційних ресурсів	Управління документацією
Групова	Підтримка колективного прийняття рішень	Проєктне управління, стратегічне планування
Інтелектуальна	Використання технологій ШІ та машинного навчання	Кібербезпека, аналіз ризиків, прогнозування

Особливого значення системи підтримки прийняття рішень набувають у сфері кібербезпеки. Сучасні інформаційні системи генерують величезні обсяги даних про мережеву активність, події безпеки, спроби несанкціонованого доступу та потенційні кіберзагрози. Аналіз такої кількості інформації вручну є практично неможливим. Використання систем підтримки прийняття рішень дозволяє автоматизувати процес обробки даних, виявляти аномалії, оцінювати ризики та формувати рекомендації щодо реагування на інциденти безпеки.

Перспективним напрямом розвитку систем підтримки прийняття рішень є інтеграція технологій штучного інтелекту, машинного навчання та інтелектуального аналізу даних. Використання таких технологій дозволяє системам самостійно виявляти закономірності у великих масивах інформації, прогнозувати розвиток подій та формувати більш точні рекомендації [10]. Це створює передумови для переходу від традиційних систем підтримки прийняття рішень до інтелектуальних систем нового покоління, здатних ефективно функціонувати в умовах високої невизначеності та динамічних змін середовища.

Отже, системи підтримки прийняття рішень є важливим інструментом сучасного управління, який забезпечує підвищення ефективності аналізу інформації, скорочення часу на прийняття рішень та покращення якості управлінської діяльності [11]. Їх функціонування базується на принципах обґрунтованості, системності, комплексності, адаптивності, інтерактивності, оперативності та гнучкості. Використання таких систем створює основу для подальшого впровадження технологій штучного інтелекту у сфері кібербезпеки та розвитку сучасних інтелектуальних засобів підтримки прийняття рішень.

1.2 Основні методи та алгоритми штучного інтелекту в кібербезпеці

Штучний інтелект є одним із найбільш перспективних напрямів розвитку сучасних інформаційних технологій, який суттєво впливає на підходи до забезпечення кібербезпеки. Зростання кількості кіберзагроз, складності атак та обсягів інформації, що підлягає аналізу, робить традиційні методи захисту недостатньо ефективними. У сучасних умовах фахівці з кібербезпеки стикаються з необхідністю обробки великих масивів даних у режимі реального часу, виявлення прихованих закономірностей та оперативного реагування на потенційні інциденти [12]. Саме тому технології штучного інтелекту дедалі активніше інтегруються в системи підтримки прийняття рішень, дозволяючи автоматизувати процес аналізу загроз та підвищувати ефективність захисту інформаційних ресурсів.

Під штучним інтелектом розуміють сукупність методів, алгоритмів та програмних засобів, здатних виконувати завдання, які традиційно потребують інтелектуальної діяльності людини. До таких завдань належать аналіз інформації, розпізнавання образів, прогнозування подій, навчання на основі накопиченого досвіду та прийняття рішень в умовах невизначеності. На відміну від традиційних програмних систем, які функціонують відповідно до жорстко визначених правил, системи штучного інтелекту здатні адаптуватися до нових умов та вдосконалювати власну поведінку на основі отриманих даних [13].

У сфері кібербезпеки штучний інтелект використовується для вирішення широкого спектра завдань, включаючи виявлення атак, аналіз мережевого трафіку, прогнозування кіберзагроз, управління ризиками, реагування на інциденти безпеки та підтримку прийняття управлінських рішень. Використання інтелектуальних алгоритмів дозволяє значно скоротити час виявлення потенційних загроз, підвищити точність аналізу та мінімізувати вплив людського фактора на процес забезпечення безпеки інформаційних систем.

Одним із найбільш поширених напрямів розвитку штучного інтелекту є машинне навчання. Машинне навчання являє собою сукупність методів, які

дозволяють комп’ютерним системам самостійно виявляти закономірності в даних та формувати моделі без прямого програмування кожного окремого правила. Основною особливістю машинного навчання є здатність алгоритмів покращувати власну ефективність у процесі накопичення досвіду та аналізу нової інформації.

Машинне навчання поділяється на навчання з учителем, навчання без учителя та навчання з підкріпленням. Навчання з учителем базується на використанні попередньо розмічених даних, де кожному прикладу відповідає правильний результат. Такий підхід широко застосовується для класифікації мережевого трафіку, виявлення шкідливого програмного забезпечення та прогнозування кіберінцидентів. Алгоритми аналізують історичні дані та формують модель, здатну класифікувати нові об’єкти відповідно до виявлених закономірностей.

Навчання без учителя використовується у випадках, коли попередньо розмічені дані відсутні. Основною метою таких алгоритмів є виявлення прихованих структур та закономірностей у великих масивах інформації. У сфері кібербезпеки цей підхід часто застосовується для виявлення аномалій у мережевому трафіку, аналізу поведінки користувачів та пошуку нетипових подій, які можуть свідчити про наявність кіберзагроз [14].

Навчання з підкріпленням базується на принципі взаємодії системи з навколишнім середовищем. Алгоритм отримує винагороду за правильні дії та штрафи за помилки, поступово формуючи оптимальну стратегію поведінки. Такий підхід використовується для автоматизації процесів реагування на інциденти безпеки, управління доступом та оптимізації механізмів захисту інформаційних систем.

Важливим методом штучного інтелекту є нейронні мережі. Вони являють собою математичні моделі, структура яких частково імітує принципи функціонування біологічного мозку людини. Нейронні мережі складаються з великої кількості взаємопов’язаних елементів, які здійснюють обробку інформації та передають результати між собою. Завдяки здатності аналізувати

складні залежності в даних нейронні мережі ефективно використовуються для виявлення кіберзагроз, аналізу мережевого трафіку та розпізнавання шкідливого програмного забезпечення.

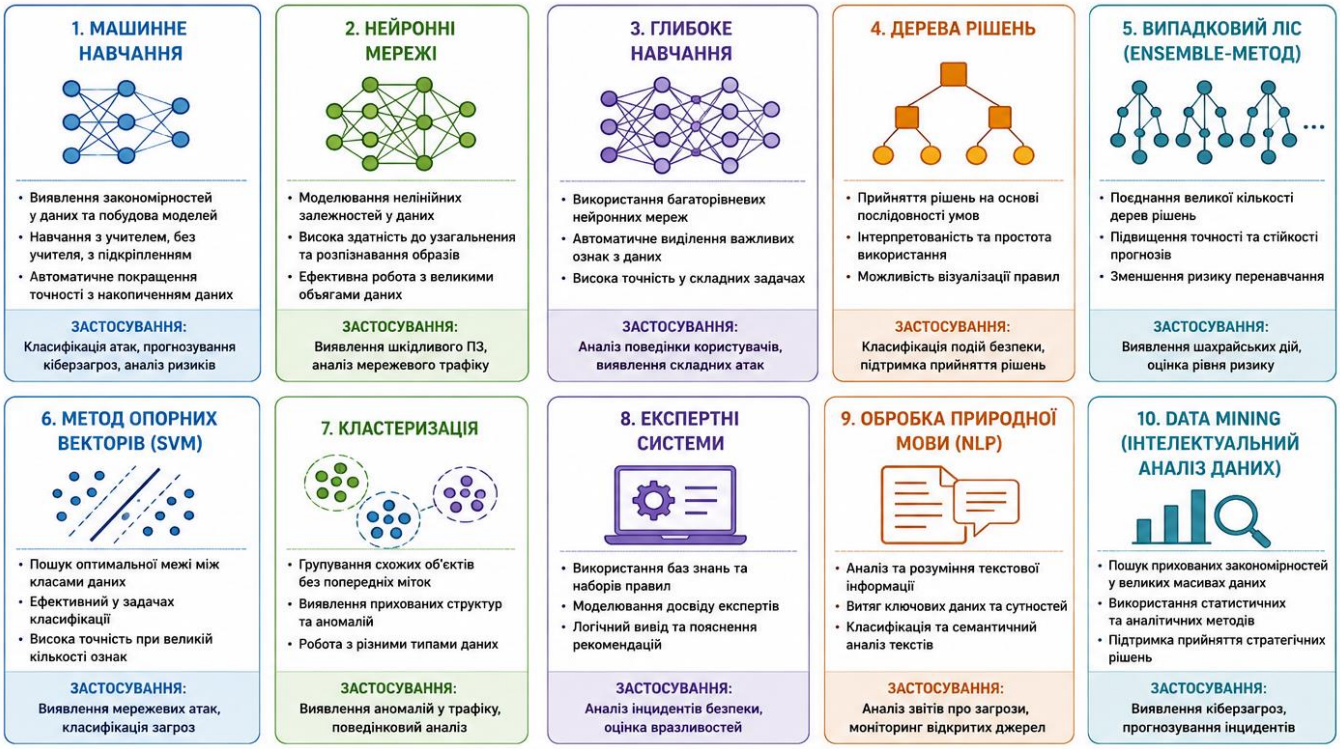

Рис. 1.2 Основні методи штучного інтелекту, що застосовуються в кібербезпеці

Подальшим розвитком нейронних мереж стали технології глибокого навчання. Глибоке навчання використовує багаторівневі нейронні мережі, які здатні автоматично виділяти важливі ознаки з великих масивів даних. У сфері кібербезпеки алгоритми глибокого навчання застосовуються для аналізу поведінки користувачів, виявлення складних цільових атак, прогнозування загроз та автоматичного аналізу журналів подій безпеки.

Одним із найбільш поширених алгоритмів машинного навчання є дерева рішень. Вони являють собою структуру у вигляді дерева, де кожен вузол відповідає певній умові або критерію, а кінцеві вузли містять результат класифікації. Перевагою дерев рішень є їх висока інтерпретованість та

можливість пояснення процесу прийняття рішення. Завдяки цьому вони активно використовуються в системах підтримки прийняття рішень у сфері кібербезпеки.

Для підвищення точності прогнозування широко використовуються ансамблеві методи, зокрема випадковий ліс та градієнтний бустинг. Дані алгоритми поєднують результати роботи великої кількості окремих моделей та формують більш точні прогнози порівняно з використанням окремого класифікатора. У кібербезпеці вони застосовуються для виявлення шахрайських дій, аналізу поведінки користувачів та оцінювання ризиків [15].

Серед популярних алгоритмів класифікації важливе місце займає метод опорних векторів. Його основне завдання полягає у знаходженні оптимальної межі між різними класами даних. Алгоритм демонструє високу ефективність під час роботи з великими наборами ознак та часто використовується для виявлення шкідливого програмного забезпечення і класифікації мережевих атак.

Значного поширення в кібербезпеці набули кластеризаційні алгоритми. До них належать метод k-середніх, ієрархічна кластеризація та алгоритм DBSCAN. Основною метою кластеризації є групування схожих об’єктів без попередньо визначених класів. Це дозволяє виявляти аномалії та приховані закономірності в інформаційних потоках, що є важливим для своєчасного виявлення кіберінцидентів.

Важливу роль відіграють експертні системи, які належать до класичних напрямів розвитку штучного інтелекту. Такі системи використовують бази знань та набори логічних правил для моделювання процесу прийняття рішень експертами. У сфері кібербезпеки експертні системи застосовуються для аналізу загроз, оцінювання ризиків та формування рекомендацій щодо реагування на інциденти безпеки.

Окремим напрямом розвитку штучного інтелекту є обробка природної мови. Технології Natural Language Processing дозволяють автоматично аналізувати текстову інформацію, витягувати з неї корисні відомості та виявляти змістовні зв’язки між об’єктами. У кібербезпеці ці методи використовуються для аналізу повідомлень про вразливості, моніторингу кіберзагроз у відкритих

джерелах, обробки звітів про інциденти та автоматичного створення аналітичних висновків.

Сучасні системи кібербезпеки також активно використовують алгоритми інтелектуального аналізу даних. Data Mining являє собою процес виявлення прихованих закономірностей у великих масивах інформації за допомогою статистичних методів та алгоритмів машинного навчання [16]. Застосування інтелектуального аналізу даних дозволяє підвищити ефективність моніторингу інформаційних систем та своєчасно виявляти потенційні загрози.

Зростання складності сучасних кіберзагроз обумовлює необхідність використання комбінованих підходів, які поєднують декілька методів штучного інтелекту одночасно. Інтеграція машинного навчання, нейронних мереж, експертних систем та аналітичних алгоритмів дозволяє створювати інтелектуальні системи підтримки прийняття рішень нового покоління. Такі системи здатні автоматично аналізувати великі обсяги інформації, прогнозувати розвиток подій та пропонувати оптимальні стратегії реагування на кіберзагрози.

Незважаючи на значні переваги використання штучного інтелекту в кібербезпеці, існують і певні обмеження. До них належать залежність якості роботи алгоритмів від обсягу та якості навчальних даних, складність інтерпретації результатів роботи окремих моделей, можливість помилкових спрацювань та ризик використання технологій штучного інтелекту самими кіберзлочинцями [17]. У зв’язку з цим ефективне використання інтелектуальних технологій потребує постійного контролю, вдосконалення моделей та поєднання автоматизованих методів аналізу з експертними знаннями фахівців.

Отже, штучний інтелект виступає одним із ключових інструментів розвитку сучасних систем кібербезпеки. Використання методів машинного навчання, нейронних мереж, глибокого навчання, експертних систем, кластеризації та інтелектуального аналізу даних дозволяє автоматизувати процес виявлення загроз, підвищити точність аналізу інформації та забезпечити ефективну підтримку прийняття рішень. Подальший розвиток технологій штучного інтелекту створює передумови для формування нових підходів до

забезпечення кібербезпеки та підвищення стійкості інформаційних систем до сучасних кіберзагроз.

1.3 Сучасні підходи до використання ШІ для виявлення та запобігання кіберзагрозам

Стрімкий розвиток цифрових технологій, збільшення кількості підключених пристроїв та зростання обсягів інформації, що обробляється в інформаційних системах, суттєво ускладнюють забезпечення належного рівня кібербезпеки. Сучасні кіберзагрози характеризуються високою швидкістю поширення, складністю реалізації та здатністю адаптуватися до засобів захисту. Традиційні методи виявлення та протидії атакам, засновані на використанні статичних правил і сигнатурного аналізу, дедалі частіше виявляються недостатньо ефективними в умовах постійної еволюції кіберзлочинності. У зв’язку з цим особливої актуальності набуває застосування технологій штучного інтелекту, які забезпечують автоматизацію процесів аналізу даних, виявлення аномалій та підтримки прийняття рішень у сфері кібербезпеки [18].

Штучний інтелект поступово стає одним із ключових елементів сучасних систем кіберзахисту. Його використання дозволяє не лише виявляти відомі загрози, але й прогнозувати потенційні атаки, аналізувати поведінкові характеристики користувачів та автоматично формувати рекомендації щодо реагування на інциденти безпеки. Завдяки здатності працювати з великими обсягами інформації та виявляти приховані закономірності алгоритми штучного інтелекту забезпечують більш високий рівень точності аналізу порівняно з традиційними підходами.

Рис. 1.3 Сучасні напрями застосування штучного інтелекту для виявлення та запобігання кіберзагрозам

Одним із найпоширеніших сучасних підходів до використання штучного інтелекту є поведінковий аналіз користувачів та інформаційних систем. Даний підхід ґрунтується на формуванні моделей нормальної поведінки користувачів, пристроїв або мережевих ресурсів. Алгоритми штучного інтелекту аналізують дії користувачів, маршрути доступу до ресурсів, частоту використання сервісів, часові характеристики активності та інші параметри. У разі виявлення відхилень від типової поведінки система автоматично генерує повідомлення про потенційну загрозу або запускає процедури додаткової перевірки [19].

Широкого поширення набули системи виявлення аномалій на основі машинного навчання. На відміну від сигнатурних методів, які можуть виявляти лише відомі загрози, алгоритми аналізу аномалій здатні виявляти нові та раніше невідомі типи атак. Такі системи аналізують мережевий трафік, активність користувачів, журнали подій та інші джерела інформації, визначаючи нетипові шаблони поведінки. Це дозволяє своєчасно виявляти складні атаки, які можуть залишатися непоміченими традиційними засобами захисту.

Важливим напрямом застосування штучного інтелекту є використання інтелектуальних систем виявлення вторгнень. Сучасні системи IDS та IPS дедалі частіше інтегрують алгоритми машинного навчання для аналізу мережевого трафіку та автоматичного визначення підозрілих подій. Завдяки цьому

підвищується точність виявлення атак, зменшується кількість хибних спрацювань та скорочується час реагування на інциденти безпеки.

Серед сучасних підходів особливе значення має прогнозування кіберзагроз за допомогою штучного інтелекту. Аналізуючи історичні дані про атаки, вразливості та інциденти безпеки, інтелектуальні системи можуть прогнозувати ймовірність виникнення певних загроз у майбутньому. Такий підхід дозволяє переходити від реактивної моделі захисту до проактивної, коли організація має можливість завчасно підготуватися до потенційних кіберінцидентів та впровадити необхідні заходи безпеки [20].

Одним із найбільш перспективних напрямів є використання технологій глибокого навчання для аналізу кіберзагроз. Глибокі нейронні мережі здатні обробляти великі масиви структурованих і неструктурованих даних, виявляючи складні взаємозв’язки між подіями безпеки. Такі технології ефективно застосовуються для аналізу мережевого трафіку, розпізнавання шкідливого програмного забезпечення, виявлення ботнетів та прогнозування кіберінцидентів.

Суттєвий розвиток отримали системи автоматизованого аналізу шкідливого програмного забезпечення. Традиційні антивірусні рішення базуються переважно на сигнатурному аналізі, що обмежує їх здатність виявляти нові модифікації шкідливого коду. Використання алгоритмів штучного інтелекту дозволяє аналізувати поведінкові характеристики програм, визначати потенційно небезпечні дії та виявляти загрози навіть за відсутності відомих сигнатур. Завдяки цьому значно підвищується ефективність боротьби з сучасним шкідливим програмним забезпеченням.

Перспективним напрямом є використання штучного інтелекту для забезпечення безпеки електронної пошти. Фішингові атаки залишаються одним із найпоширеніших методів компрометації інформаційних систем. Сучасні інтелектуальні системи аналізують зміст повідомлень, структуру листів, особливості оформлення, репутацію відправників та інші характеристики для виявлення потенційно небезпечних повідомлень. Використання алгоритмів

обробки природної мови дозволяє значно підвищити ефективність фільтрації фішингових листів та мінімізувати ризик успішних атак соціальної інженерії.

Важливе місце серед сучасних підходів займає застосування штучного інтелекту в системах управління інформацією та подіями безпеки. Платформи класу SIEM використовують інтелектуальні алгоритми для збору, кореляції та аналізу подій, що надходять із різних джерел. Це дозволяє оперативно виявляти складні ланцюги атак, автоматично визначати пріоритетність інцидентів та формувати рекомендації щодо реагування [21]. Завдяки використанню штучного інтелекту значно скорочується навантаження на аналітиків центрів кібербезпеки.

Сучасні підходи також передбачають використання технологій штучного інтелекту для автоматизації реагування на кіберінциденти. У традиційних системах більшість дій виконується вручну, що потребує значних часових та людських ресурсів. Використання інтелектуальних алгоритмів дозволяє автоматично блокувати підозрілі облікові записи, ізолювати скомпрометовані пристрої, змінювати політики доступу та виконувати інші дії без участі оператора. Це суттєво підвищує швидкість реагування та зменшує масштаби можливих збитків.

Окремим напрямом розвитку є використання штучного інтелекту для оцінювання ризиків кібербезпеки. Інтелектуальні моделі дозволяють аналізувати технічні, організаційні та поведінкові фактори, що впливають на рівень захищеності інформаційних систем. На основі отриманих результатів система може визначати найбільш критичні вразливості, прогнозувати потенційні наслідки реалізації загроз та формувати рекомендації щодо пріоритетності заходів захисту [22].

Значна увага приділяється використанню штучного інтелекту в технологіях кіберрозвідки. Сучасні системи здатні автоматично збирати інформацію з відкритих джерел, спеціалізованих баз даних, соціальних мереж та тематичних ресурсів, аналізуючи отримані дані з метою виявлення нових кіберзагроз. Використання алгоритмів інтелектуального аналізу дозволяє

оперативно виявляти нові вразливості, інструменти атак та тенденції розвитку кіберзлочинності.

Важливим сучасним підходом є впровадження концепції адаптивної кібербезпеки. Даний підхід передбачає використання штучного інтелекту для безперервного аналізу поточного стану інформаційної системи та автоматичного коригування параметрів захисту залежно від зміни рівня загроз. Адаптивні системи здатні самостійно змінювати політики безпеки, посилювати контроль доступу та активувати додаткові механізми захисту в разі виявлення потенційних ризиків.

Незважаючи на значні переваги використання штучного інтелекту, існують певні проблеми та обмеження його застосування. Однією з основних проблем є залежність якості роботи алгоритмів від повноти та достовірності навчальних даних [22]. Недостатньо якісні дані можуть призводити до помилкових висновків та зниження ефективності систем захисту. Крім того, складні моделі штучного інтелекту часто мають обмежену інтерпретованість, що ускладнює пояснення прийнятих ними рішень.

Додатковою проблемою є використання штучного інтелекту самими кіберзлочинцями. Сучасні технології дозволяють автоматизувати процес створення шкідливого програмного забезпечення, генерування фішингових повідомлень та проведення складних цільових атак. Це створює нові виклики для систем кіберзахисту та потребує подальшого вдосконалення інтелектуальних методів протидії кіберзагрозам.

У перспективі розвиток штучного інтелекту буде сприяти створенню повністю інтегрованих інтелектуальних платформ кібербезпеки, здатних самостійно аналізувати загрози, оцінювати ризики, приймати рішення та реалізовувати заходи реагування. Такі системи стануть важливим елементом сучасних центрів кіберзахисту та дозволять забезпечити більш високий рівень стійкості інформаційних систем до сучасних кіберзагроз.

Таблиця 1.2

Основні підходи використання штучного інтелекту в кібербезпеці

Підхід	Основне призначення	Практичне застосування
Поведінковий аналіз	Виявлення відхилень від нормальної активності	Моніторинг користувачів і мереж
Аналіз аномалій	Виявлення невідомих загроз	Пошук нетипового мережевого трафіку
Інтелектуальні IDS/IPS	Автоматичне виявлення атак	Захист мережевої інфраструктури
Прогнозування загроз	Оцінювання майбутніх ризиків	Проактивний захист систем
Аналіз шкідливого ПЗ	Виявлення нових модифікацій malware	Антивірусний захист
NLP-технології	Аналіз текстової інформації	Виявлення фішингових листів
SIEM із ШІ	Кореляція та аналіз подій безпеки	Центри моніторингу SOC
Автоматизоване реагування	Швидка локалізація інцидентів	Блокування атак у реальному часі
Кіберрозвідка	Пошук інформації про нові загрози	Threat Intelligence
Адаптивна кібербезпека	Динамічне налаштування захисту	Автоматична зміна політик безпеки

Отже, сучасні підходи до використання штучного інтелекту у сфері кібербезпеки орієнтовані на автоматизацію процесів виявлення, аналізу та запобігання кіберзагрозам. Використання поведінкового аналізу, машинного навчання, глибоких нейронних мереж, інтелектуальних систем виявлення вторгнень, автоматизованого реагування на інциденти та технологій кіберрозвідки дозволяє суттєво підвищити ефективність захисту інформаційних систем. Подальший розвиток технологій штучного інтелекту створює передумови для формування нових підходів до забезпечення кібербезпеки та підвищення рівня захищеності цифрового середовища.

Висновки до розділу 1

У першому розділі досліджено теоретичні основи підтримки прийняття рішень та використання штучного інтелекту у сфері кібербезпеки. Розглянуто сутність систем підтримки прийняття рішень, їх основні функції, структуру та

принципи функціонування. Встановлено, що такі системи є важливим інструментом підвищення ефективності управлінської діяльності, оскільки забезпечують аналіз значних обсягів інформації, обґрунтування управлінських рішень та зменшення впливу людського фактора.

Проаналізовано основні методи та алгоритми штучного інтелекту, які застосовуються для вирішення завдань кібербезпеки. Визначено особливості використання машинного навчання, нейронних мереж, глибокого навчання, експертних систем, кластеризації та інтелектуального аналізу даних. Встановлено, що застосування зазначених технологій дозволяє автоматизувати процеси виявлення загроз, аналізу ризиків та підтримки прийняття рішень в умовах невизначеності.

Досліджено сучасні підходи до використання штучного інтелекту для виявлення та запобігання кіберзагрозам. Визначено, що поведінковий аналіз, виявлення аномалій, інтелектуальні системи IDS/IPS, прогнозування загроз, автоматизоване реагування на інциденти та технології кіберрозвідки суттєво підвищують ефективність систем кіберзахисту. Отримані результати свідчать про значний потенціал штучного інтелекту як основи для побудови сучасних моделей підтримки прийняття рішень у сфері кібербезпеки.

Розділ 2 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ПРИЙНЯТТЯ РІШЕНЬ У СФЕРІ КІБЕРБЕЗПЕКИ

2.1 Аналіз сучасних методів підтримки прийняття рішень у кібербезпеці

Сучасний розвиток інформаційних технологій, цифровізація бізнес-процесів та постійне зростання кількості кіберзагроз обумовлюють необхідність використання ефективних методів підтримки прийняття рішень у сфері кібербезпеки. Умови функціонування сучасних інформаційних систем характеризуються високою динамічністю, значними обсягами даних та необхідністю оперативного реагування на інциденти безпеки. За таких умов процес прийняття рішень стає складним багатофакторним завданням, яке потребує використання спеціалізованих аналітичних інструментів, математичних моделей та інтелектуальних технологій [23]. Ефективність забезпечення кібербезпеки значною мірою залежить від здатності своєчасно оцінювати поточну ситуацію, прогнозувати розвиток загроз та обирати оптимальні заходи реагування.

Підтримка прийняття рішень у сфері кібербезпеки являє собою сукупність методів, моделей та інформаційних технологій, спрямованих на забезпечення фахівців необхідною інформацією для оцінювання ризиків, аналізу загроз та вибору найбільш ефективних стратегій захисту. Основною метою таких методів є підвищення обґрунтованості управлінських рішень, зниження впливу людського фактора та забезпечення своєчасного реагування на кіберінциденти.

Одним із найбільш поширених підходів є експертні методи підтримки прийняття рішень. Їх сутність полягає у використанні знань та досвіду висококваліфікованих фахівців для оцінювання ситуації та формування рекомендацій щодо подальших дій. Експертні методи широко застосовуються для аналізу кіберризиків, оцінювання вразливостей та визначення рівня захищеності інформаційних систем [24]. Перевагою такого підходу є можливість

врахування складних факторів, які складно формалізувати математичними моделями. Водночас ефективність експертних методів значною мірою залежить від кваліфікації експертів та може супроводжуватися суб'єктивністю оцінок.

Важливе місце серед сучасних методів підтримки прийняття рішень займають статистичні методи аналізу. Вони базуються на використанні математичної статистики для оцінювання параметрів безпеки, прогнозування ймовірності реалізації загроз та визначення рівня ризиків. Статистичні методи дозволяють виявляти закономірності у великих масивах даних, оцінювати тенденції розвитку кіберзагроз та формувати кількісні характеристики безпеки інформаційних систем [25]. Особливу цінність вони мають під час аналізу журналів подій безпеки, мережевого трафіку та результатів моніторингу інформаційної інфраструктури.

Одним із найбільш відомих методів багатокритеріального аналізу є метод аналізу ієрархій. Він дозволяє приймати рішення за наявності великої кількості критеріїв та альтернатив. У сфері кібербезпеки цей метод використовується для вибору засобів захисту, визначення пріоритетності кіберризиків та оцінювання ефективності різних стратегій забезпечення безпеки. Основною перевагою методу є можливість одночасного врахування як кількісних, так і якісних показників.

Широке застосування отримали методи оцінювання ризиків. Управління ризиками є одним із ключових напрямів сучасної кібербезпеки, оскільки дозволяє визначати найбільш критичні загрози та ефективно розподіляти ресурси на їх усунення. До найбільш поширених методів належать якісний аналіз ризиків, кількісний аналіз ризиків та комбіновані підходи [26]. Якісні методи базуються на експертних оцінках та категоризації ризиків за рівнем критичності, тоді як кількісні методи використовують математичні моделі та статистичні розрахунки для визначення ймовірності виникнення інцидентів і масштабів можливих збитків.

Суттєвого поширення набули методи сценарного аналізу. Їх основна мета полягає у моделюванні можливих варіантів розвитку подій та оцінюванні

наслідків реалізації різних загроз. У сфері кібербезпеки сценарний аналіз використовується для оцінювання наслідків атак на критичну інфраструктуру, аналізу можливих дій зловмисників та підготовки планів реагування на інциденти. Використання таких методів дозволяє підвищити готовність організації до потенційних кіберзагроз.

Одним із перспективних напрямів є використання методів теорії ігор. Теорія ігор дозволяє моделювати взаємодію між захисниками інформаційних систем та потенційними зловмисниками як процес стратегічного протистояння. За допомогою даного підходу можна оцінювати можливі сценарії поведінки сторін, прогнозувати ймовірні атаки та визначати найбільш ефективні заходи захисту [27]. Особливу актуальність теорія ігор має для аналізу складних багатоетапних кібероперацій.

У сучасних умовах значного розвитку набули системи підтримки прийняття рішень на основі баз знань. Такі системи використовують накопичені знання експертів, правила логічного виведення та спеціалізовані механізми аналізу інформації. Їх перевагою є можливість формалізації досвіду фахівців та автоматизації процесу формування рекомендацій. У сфері кібербезпеки подібні системи використовуються для аналізу інцидентів, класифікації загроз та оцінювання рівня ризиків.

Окрему категорію становлять методи інтелектуального аналізу даних. Вони дозволяють автоматично виявляти приховані закономірності, аномалії та залежності у великих масивах інформації. Такі методи широко застосовуються для моніторингу мережевого трафіку, аналізу поведінки користувачів, виявлення атак та оцінювання ефективності заходів захисту. Використання інтелектуального аналізу даних забезпечує значне підвищення швидкості та точності прийняття рішень.

Особливу роль у сучасних системах кібербезпеки відіграють методи машинного навчання. Їх застосування дозволяє автоматично аналізувати великі обсяги інформації та формувати прогнози щодо можливих загроз. Алгоритми машинного навчання здатні адаптуватися до нових умов функціонування систем

та виявляти раніше невідомі типи атак. Завдяки цьому вони стають важливим елементом сучасних систем підтримки прийняття рішень.

Важливим напрямом є використання нейронних мереж та технологій глибокого навчання. Дані методи забезпечують високу точність аналізу складних інформаційних потоків та дозволяють виявляти приховані взаємозв'язки між подіями безпеки. Нейронні мережі успішно використовуються для аналізу мережевого трафіку, класифікації шкідливого програмного забезпечення та прогнозування кіберінцидентів [28]. Використання глибокого навчання дозволяє значно підвищити рівень автоматизації процесів аналізу загроз.

Серед сучасних методів підтримки прийняття рішень важливе місце займають системи управління інформацією та подіями безпеки. Платформи SIEM забезпечують централізований збір, аналіз та кореляцію даних з різних джерел інформації. Використання таких систем дозволяє оперативно виявляти складні атаки, оцінювати рівень загроз та формувати рекомендації щодо реагування на інциденти безпеки.

Окремим напрямом розвитку є впровадження технологій кіберрозвідки. Системи Threat Intelligence забезпечують збір та аналіз інформації про нові загрози, вразливості та інструменти кіберзлочинців. Використання цих даних дозволяє приймати більш обґрунтовані рішення щодо вдосконалення систем захисту та підготовки до потенційних атак.

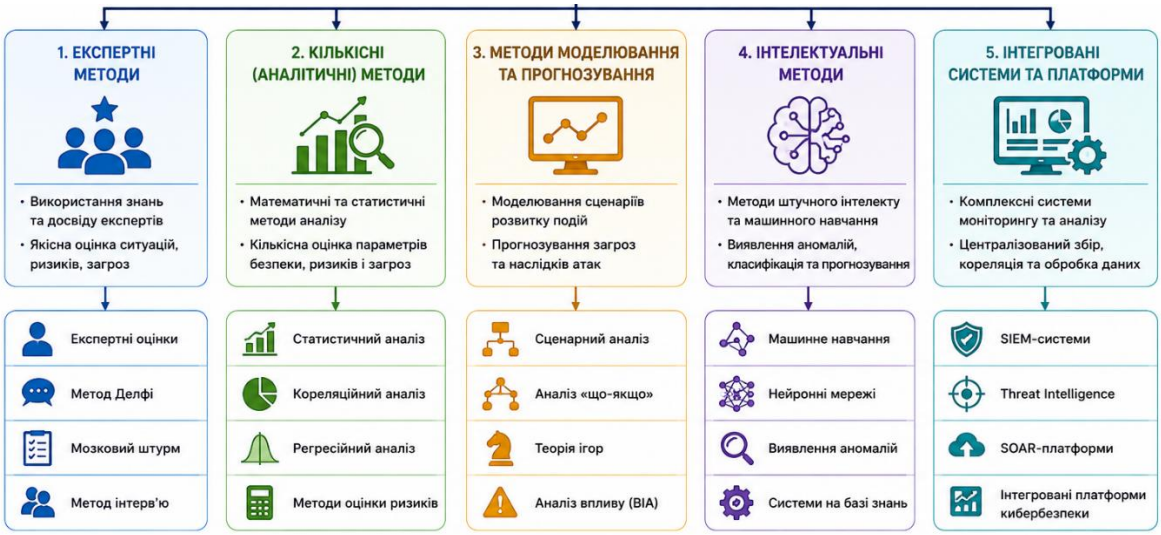

Рис. 2.1 Класифікація сучасних методів підтримки прийняття рішень у сфері кібербезпеки

Аналіз сучасних методів підтримки прийняття рішень свідчить про поступовий перехід від традиційних експертних підходів до інтелектуальних систем, здатних самостійно аналізувати інформацію та формувати рекомендації. При цьому найбільшу ефективність демонструють комбіновані підходи, які поєднують експертні знання, математичне моделювання, аналіз ризиків та технології штучного інтелекту. Саме інтеграція різних методів дозволяє забезпечити високий рівень точності, оперативності та обґрунтованості прийнятих рішень.

Таблиця 2.1

Порівняльна характеристика методів підтримки прийняття рішень у кібербезпеці

Метод	Переваги	Недоліки	Сфера застосування
Експертні методи	Врахування досвіду фахівців	Суб’єктивність оцінок	Аналіз ризиків
Статистичні методи	Кількісна оцінка загроз	Потреба у великих масивах даних	Моніторинг безпеки
Метод аналізу ієрархій	Багатокритеріальний аналіз	Складність побудови моделі	Вибір засобів захисту
Сценарний аналіз	Прогнозування наслідків	Значні часові витрати	Планування реагування
Теорія ігор	Аналіз протистояння сторін	Складність математичних моделей	Стратегічний захист
Системи на базі знань	Автоматизація рекомендацій	Необхідність підтримки баз знань	Експертні системи
Машинне навчання	Виявлення прихованих закономірностей	Залежність від навчальних даних	Виявлення атак
Нейронні мережі	Висока точність аналізу	Складність інтерпретації	Аналіз кіберзагроз
SIEM-системи	Централізований моніторинг	Висока вартість впровадження	SOC та центри моніторингу
Threat Intelligence	Проактивне виявлення загроз	Потреба у постійному оновленні даних	Кіберрозвідка

Незважаючи на значні переваги сучасних методів підтримки прийняття рішень, існують певні проблеми їх практичного використання. До основних труднощів належать складність інтеграції різнорідних джерел інформації, необхідність обробки великих обсягів даних, ризик помилкових спрацювань та

залежність результатів від якості вхідної інформації. Крім того, ефективність окремих методів може суттєво знижуватися в умовах швидкої зміни характеру кіберзагроз.

Подальший розвиток систем підтримки прийняття рішень у сфері кібербезпеки пов’язаний із розширенням використання технологій штучного інтелекту, автоматизацією процесів аналізу інформації та створенням адаптивних систем, здатних самостійно реагувати на зміни середовища. Очікується, що такі рішення забезпечать більш високий рівень захищеності інформаційних систем та дозволять суттєво підвищити ефективність діяльності фахівців з кібербезпеки.

Отже, сучасні методи підтримки прийняття рішень у сфері кібербезпеки охоплюють широкий спектр підходів, починаючи від експертних оцінок та статистичного аналізу і закінчуючи інтелектуальними системами на основі штучного інтелекту [29]. Їх використання дозволяє підвищити якість аналізу загроз, оптимізувати процес управління ризиками та забезпечити своєчасне реагування на кіберінциденти. Отримані результати створюють основу для подальшого дослідження інтелектуальних моделей підтримки прийняття рішень у сфері кібербезпеки.

2.2 Оцінка ефективності алгоритмів машинного навчання для виявлення інцидентів безпеки

Забезпечення ефективного виявлення інцидентів безпеки є одним із ключових завдань сучасної кібербезпеки. Стрімке зростання кількості кіберзагроз, збільшення обсягів мережевого трафіку та ускладнення архітектури інформаційних систем значно підвищують вимоги до засобів моніторингу та аналізу подій безпеки. Традиційні методи виявлення атак, які базуються на сигнатурному аналізі або використанні фіксованих правил, дедалі частіше виявляються недостатньо ефективними для протидії сучасним складним загрозам. У зв’язку з цим особливого значення набуває використання алгоритмів

машинного навчання, які здатні автоматично аналізувати великі обсяги даних, виявляти приховані закономірності та своєчасно визначати ознаки потенційних інцидентів безпеки.

Машинне навчання є одним із напрямів штучного інтелекту, що дозволяє комп'ютерним системам формувати моделі поведінки на основі накопичених даних та вдосконалювати якість прогнозування без явного програмування кожного окремого правила. У сфері кібербезпеки алгоритми машинного навчання використовуються для аналізу мережевого трафіку, моніторингу поведінки користувачів, виявлення шкідливого програмного забезпечення, класифікації атак та прогнозування інцидентів безпеки. Їх основною перевагою є здатність адаптуватися до нових типів загроз та виявляти аномалії, які можуть залишатися непоміченими традиційними засобами захисту.

Оцінка ефективності алгоритмів машинного навчання є важливим етапом розробки та впровадження інтелектуальних систем підтримки прийняття рішень у сфері кібербезпеки. Вона дозволяє визначити ступінь придатності конкретного алгоритму для вирішення певного класу задач, порівняти різні підходи між собою та обрати найбільш ефективне рішення для практичного використання. Ефективність алгоритмів зазвичай оцінюється за допомогою спеціальних показників якості, які характеризують точність, повноту та надійність виявлення інцидентів безпеки [30].

Одним із найважливіших показників є точність класифікації. Даний показник відображає частку правильно класифікованих подій серед загальної кількості проаналізованих об'єктів. Висока точність свідчить про здатність алгоритму ефективно розрізняти легітимну активність та потенційні загрози. Водночас використання лише цього показника не завжди дозволяє отримати об'єктивну оцінку ефективності, особливо у випадках значного дисбалансу між кількістю нормальних подій та інцидентів безпеки.

Важливе значення мають показники повноти та точності виявлення загроз. Повнота характеризує здатність алгоритму знаходити всі наявні інциденти безпеки, тоді як точність визначає частку дійсно небезпечних подій серед усіх

виявлених загроз. Поєднання цих показників дозволяє оцінити баланс між ефективністю виявлення атак та кількістю помилкових спрацювань системи.

Для комплексної оцінки ефективності часто використовується F1-міра, яка є гармонійним середнім між точністю та повнотою. Цей показник особливо корисний у задачах кібербезпеки, де важливо одночасно забезпечити високу ймовірність виявлення атак та мінімізувати кількість хибних спрацювань. Високе значення F1-міри свідчить про збалансованість роботи алгоритму та його придатність для практичного використання.

Одним із найбільш поширених алгоритмів машинного навчання для виявлення інцидентів безпеки є дерева рішень. Вони формують послідовність логічних умов, які дозволяють класифікувати події як безпечні або потенційно небезпечні [31]. Основною перевагою дерев рішень є висока інтерпретованість результатів та можливість пояснення процесу прийняття рішень. Проте їх ефективність може знижуватися при роботі зі складними багатовимірними даними.

Для підвищення якості прогнозування широко застосовується алгоритм випадкового лісу. Він являє собою ансамбль великої кількості дерев рішень, результати яких об’єднуються для формування остаточного висновку. Дослідження показують, що випадковий ліс забезпечує більш високу точність виявлення атак та стійкість до перенавчання порівняно з окремими деревами рішень. Саме тому цей алгоритм активно використовується в сучасних системах кіберзахисту.

Серед популярних алгоритмів важливе місце займає метод опорних векторів. Його основне завдання полягає у побудові оптимальної межі між різними класами об’єктів. Алгоритм демонструє високу ефективність під час аналізу складних наборів даних та забезпечує якісну класифікацію мережевого трафіку. Разом із тим використання даного підходу може супроводжуватися значними обчислювальними витратами при роботі з великими масивами інформації.

Значного поширення у сфері кібербезпеки набули нейронні мережі. Вони здатні аналізувати складні залежності між параметрами інформаційних систем та виявляти приховані ознаки атак. Особливо ефективними нейронні мережі є під час виявлення шкідливого програмного забезпечення, аналізу поведінки користувачів та розпізнавання аномальної мережевої активності. Їх перевагою є висока точність прогнозування, однак складність інтерпретації результатів залишається одним із суттєвих недоліків.

Подальшим розвитком нейронних мереж стали технології глибокого навчання. Багаторівневі нейронні мережі здатні автоматично виділяти важливі ознаки з великих масивів інформації та формувати складні моделі для виявлення загроз [32]. Використання глибокого навчання дозволяє досягати високих показників точності навіть у випадках складних багатоетапних атак, які важко виявити традиційними методами.

Для виявлення аномалій широко використовуються алгоритми кластеризації. Вони дозволяють групувати схожі об’єкти та визначати події, які суттєво відрізняються від загальної картини. Такий підхід особливо ефективний для виявлення нових типів загроз, про які відсутня попередня інформація. До найбільш поширених алгоритмів кластеризації належать метод k-середніх, DBSCAN та ієрархічна кластеризація.

Практика застосування алгоритмів машинного навчання свідчить про їх високу ефективність під час аналізу мережевого трафіку. Інтелектуальні системи здатні виявляти атаки типу DDoS, сканування портів, спроби несанкціонованого доступу та інші мережеві загрози значно швидше, ніж традиційні системи моніторингу. Використання машинного навчання дозволяє скоротити час виявлення інцидентів та забезпечити оперативне реагування на потенційні загрози.

Важливим напрямом застосування є аналіз поведінки користувачів. Алгоритми машинного навчання формують профілі нормальної активності та відстежують відхилення від звичайних шаблонів поведінки. Такий підхід

дозволяє своєчасно виявляти внутрішні загрози, компрометацію облікових записів та несанкціоноване використання інформаційних ресурсів.

Під час оцінювання ефективності алгоритмів важливим критерієм є швидкість обробки інформації. У сфері кібербезпеки рішення часто необхідно приймати в режимі реального часу, тому навіть високоточний алгоритм може бути недостатньо ефективним за умови значних затримок під час аналізу даних. Саме тому сучасні дослідження приділяють значну увагу оптимізації обчислювальних витрат та підвищенню продуктивності моделей машинного навчання.

Однією з головних проблем залишається проблема помилкових спрацювань. Надмірна кількість хибнопозитивних результатів призводить до збільшення навантаження на фахівців з кібербезпеки та зниження довіри до системи моніторингу. Водночас велика кількість хибнонегативних результатів створює ризик пропуску реальних загроз. Тому сучасні алгоритми розробляються з урахуванням необхідності досягнення оптимального балансу між чутливістю та точністю.

Суттєвим фактором, який впливає на ефективність алгоритмів машинного навчання, є якість навчальних даних. Неповні, застарілі або некоректно розмічені набори даних можуть призводити до зниження точності моделей та погіршення результатів класифікації. У зв’язку з цим важливого значення набувають процеси підготовки даних, їх очищення та забезпечення репрезентативності навчальних вибірок.

Аналіз сучасних досліджень свідчить про те, що найбільш ефективними є комбіновані моделі, які поєднують декілька алгоритмів машинного навчання одночасно. Використання ансамблевих методів дозволяє компенсувати недоліки окремих алгоритмів та підвищити загальну якість виявлення інцидентів безпеки. Саме тому більшість сучасних систем кіберзахисту використовують комплексний підхід до аналізу загроз.

Таблиця 2.2

Порівняльна характеристика алгоритмів машинного навчання для виявлення інцидентів безпеки

Алгоритм	Точність виявлення	Швидкість обробки	Інтерпретованість	Основні переваги
Дерево рішень	Середня	Висока	Висока	Простота та наочність
Випадковий ліс	Висока	Середня	Середня	Стійкість до перенавчання
Метод опорних векторів	Висока	Середня	Низька	Точна класифікація
Нейронні мережі	Висока	Середня	Низька	Аналіз складних залежностей
Глибоке навчання	Дуже висока	Нижча	Низька	Виявлення складних атак
K-середніх	Середня	Висока	Середня	Виявлення аномалій
DBSCAN	Висока	Середня	Середня	Робота з шумовими даними
Ансамблеві методи	Дуже висока	Середня	Середня	Поєднання переваг різних алгоритмів

Подальший розвиток алгоритмів машинного навчання пов’язаний із впровадженням нових методів глибокого навчання, автоматизацією процесів аналізу інформації та інтеграцією моделей штучного інтелекту із системами підтримки прийняття рішень. Очікується, що це дозволить підвищити рівень автоматизації кіберзахисту, покращити якість прогнозування загроз та забезпечити більш ефективне реагування на інциденти безпеки.

Отже, оцінка ефективності алгоритмів машинного навчання підтверджує їх значний потенціал для виявлення інцидентів безпеки у сучасних інформаційних системах. Використання дерев рішень, випадкових лісів, методів опорних векторів, нейронних мереж, глибокого навчання та алгоритмів кластеризації дозволяє забезпечити високий рівень точності виявлення загроз та автоматизувати процес аналізу подій безпеки. Подальше вдосконалення

інтелектуальних алгоритмів створює передумови для розвитку нових поколінь систем підтримки прийняття рішень у сфері кібербезпеки.

2.3 Недоліки та обмеження існуючих моделей і підходів

Незважаючи на стрімкий розвиток інформаційних технологій та широке впровадження систем підтримки прийняття рішень у сфері кібербезпеки, існуючі моделі та підходи мають низку суттєвих недоліків і обмежень, які впливають на ефективність їх практичного застосування. Сучасне кіберсередовище характеризується високою динамічністю, постійною появою нових загроз, значними обсягами даних та складними взаємозв’язками між різними компонентами інформаційної інфраструктури. За таких умов навіть найбільш досконалі методи аналізу та підтримки прийняття рішень не завжди здатні забезпечити повноцінне виявлення загроз і формування оптимальних рекомендацій для фахівців з кібербезпеки.

Однією з основних проблем традиційних моделей підтримки прийняття рішень є їх залежність від попередньо визначених правил та сценаріїв. Багато сучасних систем функціонують на основі заздалегідь сформованих баз знань або наборів сигнатур, що дозволяє ефективно виявляти лише відомі типи загроз. У випадку появи нових або модифікованих атак ефективність таких систем суттєво знижується, оскільки вони не здатні самостійно адаптуватися до змін середовища без оновлення правил або втручання експертів [33].

Суттєвим недоліком експертних систем є високий рівень залежності від людського фактора. Формування баз знань, правил прийняття рішень та критеріїв оцінювання значною мірою залежить від досвіду та компетентності експертів. Різні спеціалісти можуть по-різному оцінювати однакові ситуації, що призводить до суб’єктивності результатів аналізу. Крім того, процес накопичення та актуалізації експертних знань потребує значних часових і фінансових ресурсів.

Однією з важливих проблем є складність формалізації процесів прийняття рішень у сфері кібербезпеки. Реальні кіберінциденти часто характеризуються великою кількістю невизначених факторів, неповнотою інформації та постійною зміною умов функціонування інформаційних систем. У таких ситуаціях побудова точних математичних моделей стає складним завданням, а отримані результати можуть не повністю відображати реальну картину подій.

Значні обмеження мають і статистичні методи аналізу. Ефективність таких підходів безпосередньо залежить від якості та обсягу вихідних даних. Якщо статистична інформація є неповною, застарілою або містить помилки, результати аналізу можуть бути недостовірними. Крім того, статистичні методи зазвичай орієнтовані на аналіз минулих подій, що обмежує їх можливості щодо прогнозування нових видів кіберзагроз.

Серед недоліків моделей оцінювання ризиків важливе місце займає проблема точного визначення ймовірності реалізації загроз та масштабів можливих наслідків. У сфері кібербезпеки часто відсутні достовірні статистичні дані щодо частоти виникнення окремих інцидентів або фінансових збитків від їх реалізації. У результаті оцінювання ризиків нерідко базується на експертних припущеннях, що знижує об’єктивність отриманих результатів.

Окремої уваги заслуговують недоліки моделей багатокритеріального аналізу. Такі підходи дозволяють враховувати значну кількість факторів під час прийняття рішень, проте їх ефективність значною мірою залежить від правильності визначення вагових коефіцієнтів критеріїв [34]. У разі помилкового встановлення пріоритетів результати аналізу можуть не відповідати реальним потребам організації та призводити до прийняття неефективних рішень.

Широке використання алгоритмів машинного навчання у сфері кібербезпеки також супроводжується низкою обмежень. Однією з головних проблем є необхідність використання великих обсягів якісних навчальних даних. Формування репрезентативних наборів даних для навчання моделей часто є складним завданням, особливо коли йдеться про нові або рідкісні типи атак.

Недостатня кількість даних може призводити до погіршення точності моделей та зниження їх здатності до виявлення інцидентів безпеки.

Серйозним недоліком багатьох алгоритмів машинного навчання є проблема перенавчання. У процесі навчання модель може надмірно адаптуватися до особливостей навчальної вибірки та втрачати здатність ефективно працювати з новими даними. У результаті алгоритм демонструє високі показники під час тестування, але значно гірші результати в реальних умовах експлуатації.

Іншою важливою проблемою є складність інтерпретації результатів роботи моделей штучного інтелекту. Особливо це стосується глибоких нейронних мереж, які часто розглядаються як так звані «чорні скриньки». У багатьох випадках фахівці з кібербезпеки не можуть чітко пояснити причини, через які система класифікувала певну подію як загрозу або безпечну активність. Це ускладнює процес прийняття остаточних рішень та знижує рівень довіри до інтелектуальних систем.

Важливою проблемою сучасних моделей є високий рівень хибнопозитивних та хибнонегативних результатів. Хибнопозитивні спрацювання призводять до формування повідомлень про загрози, які фактично відсутні, що збільшує навантаження на операторів центрів моніторингу безпеки. Хибнонегативні результати, навпаки, можуть спричинити пропуск реальних атак та створити значні ризики для інформаційної системи [35].

Складність обробки великих обсягів даних також є одним із суттєвих обмежень сучасних систем підтримки прийняття рішень. Сучасні інформаційні системи генерують величезну кількість подій безпеки, мережевого трафіку та журналів аудиту. Аналіз таких обсягів інформації потребує значних обчислювальних ресурсів, що може впливати на швидкість роботи систем та збільшувати витрати на їх впровадження й експлуатацію.

Окремою проблемою є адаптація моделей до нових типів кіберзагроз. Кіберзлочинці постійно вдосконалюють методи атак, використовують нові інструменти та технології обходу засобів захисту. У зв’язку з цим моделі

підтримки прийняття рішень потребують регулярного оновлення та перенавчання, що потребує додаткових ресурсів і може знижувати ефективність системи в період між оновленнями.

Суттєвим обмеженням є залежність багатьох систем від якості вхідних даних. Якщо інформація надходить із різнорідних джерел або містить помилки, дублікати та неповні записи, результати аналізу можуть бути спотвореними. У таких випадках навіть найсучасніші алгоритми не здатні забезпечити належний рівень точності прогнозування та підтримки прийняття рішень.

У сучасних умовах дедалі більшої актуальності набуває проблема захисту самих моделей штучного інтелекту від зовнішнього впливу. Існують спеціальні атаки на алгоритми машинного навчання, метою яких є спотворення результатів аналізу або введення системи в оману. Такі атаки можуть здійснюватися шляхом модифікації навчальних даних або створення спеціально підготовлених вхідних даних, що призводять до неправильних рішень системи.

Серед організаційних недоліків необхідно відзначити високу вартість впровадження та підтримки сучасних інтелектуальних систем підтримки прийняття рішень. Впровадження таких рішень потребує наявності потужної обчислювальної інфраструктури, спеціалізованого програмного забезпечення та кваліфікованих фахівців. Для багатьох організацій, особливо малого та середнього бізнесу, це може стати суттєвим обмеженням.

Аналіз існуючих підходів показує, що жоден окремий метод не здатний повністю вирішити всі завдання, пов’язані з підтримкою прийняття рішень у сфері кібербезпеки. Кожен підхід має власні переваги та недоліки, а його ефективність залежить від конкретних умов застосування. Саме тому сучасні тенденції розвитку кібербезпеки орієнтовані на створення гібридних моделей, які поєднують переваги різних методів та компенсують їхні обмеження.

Подальший розвиток систем підтримки прийняття рішень пов’язаний із підвищенням рівня адаптивності моделей, удосконаленням алгоритмів машинного навчання, покращенням інтерпретованості результатів та створенням механізмів автоматичного оновлення знань про нові кіберзагрози.

Реалізація таких підходів дозволить підвищити ефективність виявлення інцидентів безпеки та забезпечити більш якісну підтримку прийняття рішень у сучасних інформаційних системах.

Отже, проведений аналіз свідчить, що існуючі моделі та підходи підтримки прийняття рішень у сфері кібербезпеки мають низку обмежень, пов’язаних із залежністю від якості даних, складністю інтерпретації результатів, необхідністю значних обчислювальних ресурсів та проблемами адаптації до нових загроз. Виявлені недоліки підтверджують доцільність розробки більш ефективних інтелектуальних моделей, здатних забезпечити високий рівень точності, адаптивності та обґрунтованості рішень у сфері кібербезпеки.

Висновки до розділу 2

У другому розділі проведено аналіз існуючих методів підтримки прийняття рішень у сфері кібербезпеки. Досліджено сучасні підходи до аналізу загроз, оцінювання ризиків та формування управлінських рішень, зокрема експертні методи, статистичні моделі, методи багатокритеріального аналізу, системи на базі знань та інтелектуальні технології. Встановлено, що найбільш перспективним напрямом розвитку систем підтримки прийняття рішень є використання методів штучного інтелекту та машинного навчання.

Виконано оцінку ефективності алгоритмів машинного навчання для виявлення інцидентів безпеки. Визначено особливості застосування дерев рішень, випадкових лісів, методів опорних векторів, нейронних мереж, глибокого навчання та алгоритмів кластеризації. Проведений аналіз показав, що використання інтелектуальних алгоритмів дозволяє підвищити точність виявлення загроз, скоротити час реагування на інциденти та автоматизувати процес аналізу подій безпеки.

Також досліджено недоліки та обмеження існуючих моделей підтримки прийняття рішень у кібербезпеці. Встановлено, що основними проблемами є залежність від якості даних, складність інтерпретації результатів роботи моделей

штучного інтелекту, наявність хибних спрацювань, високі обчислювальні витрати та необхідність постійної адаптації до нових кіберзагроз. Отримані результати підтверджують доцільність розробки удосконаленої моделі підтримки прийняття рішень на основі штучного інтелекту, що стане предметом подальшого дослідження в наступному розділі.

РОЗДІЛ 3 РОЗРОБКА ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ МОДЕЛІ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ ШІ

3.1 Проєктування архітектури моделі підтримки прийняття рішень

Сучасний стан розвитку кіберпростору характеризується постійним зростанням кількості кіберзагроз, збільшенням складності атак та суттєвим розширенням обсягів інформації, що підлягає аналізу під час забезпечення безпеки інформаційних систем. У таких умовах традиційні методи підтримки прийняття рішень дедалі частіше виявляються недостатньо ефективними через обмежені можливості обробки великих масивів даних та складність оперативного реагування на динамічні зміни середовища. Використання технологій штучного інтелекту дозволяє суттєво підвищити рівень автоматизації процесів аналізу інформації, оцінювання ризиків та формування рекомендацій для фахівців з кібербезпеки. У зв’язку з цим актуальним завданням є розробка архітектури моделі підтримки прийняття рішень на основі штучного інтелекту, здатної забезпечити комплексний аналіз даних та своєчасне прийняття ефективних управлінських рішень.

Проєктування архітектури моделі підтримки прийняття рішень є одним із найважливіших етапів створення інтелектуальної системи кібербезпеки. Від правильності побудови архітектури залежить ефективність функціонування всієї системи, її адаптивність до нових загроз, швидкість обробки інформації та якість сформованих рекомендацій [36]. Архітектура повинна забезпечувати інтеграцію різних джерел даних, використання сучасних алгоритмів штучного інтелекту та можливість взаємодії з користувачами і зовнішніми інформаційними системами.

Основною метою запропонованої моделі є автоматизація процесу підтримки прийняття рішень у сфері кібербезпеки шляхом аналізу подій безпеки, оцінювання рівня ризиків, прогнозування можливих загроз та формування рекомендацій щодо реагування на інциденти. Модель повинна забезпечувати своєчасне виявлення потенційних кіберзагроз, мінімізувати вплив людського

фактора та сприяти підвищенню ефективності діяльності фахівців з кібербезпеки.

Запропонована архітектура базується на принципах модульності, масштабованості, адаптивності та інтегрованості. Принцип модульності передбачає поділ системи на окремі функціональні компоненти, кожен із яких виконує визначені завдання. Такий підхід спрощує модернізацію системи, дозволяє додавати нові функціональні можливості та забезпечує більш ефективне адміністрування. Масштабованість забезпечує можливість роботи з різними обсягами інформації та адаптацію системи до потреб організацій різного масштабу. Адаптивність дозволяє моделі враховувати зміни у характері кіберзагроз та вдосконалювати власні алгоритми на основі нових даних. Інтегрованість забезпечує взаємодію із зовнішніми системами моніторингу, базами даних та платформами управління інформаційною безпекою.

Рис. 3.1 Архітектура моделі підтримки прийняття рішень на основі штучного інтелекту

Першим функціональним елементом архітектури є модуль збору та інтеграції даних. Його основним завданням є отримання інформації з різних

джерел, необхідної для подальшого аналізу. До таких джерел належать журнали подій безпеки, мережевий трафік, системи моніторингу, бази даних вразливостей, платформи кіберрозвідки та зовнішні інформаційні ресурси. Модуль забезпечує централізований збір даних та їх підготовку до подальшої обробки.

Наступним компонентом є модуль попередньої обробки даних. Його функції включають очищення інформації від помилок, усунення дубльованих записів, нормалізацію даних та їх перетворення до єдиного формату [37]. Якість роботи цього модуля безпосередньо впливає на точність функціонування алгоритмів штучного інтелекту, оскільки некоректні або неповні дані можуть суттєво погіршувати результати аналізу.

Центральним елементом архітектури є інтелектуальний аналітичний модуль. Саме в ньому реалізуються алгоритми машинного навчання та інші методи штучного інтелекту. Даний модуль виконує аналіз подій безпеки, виявлення аномалій, класифікацію інцидентів, оцінювання рівня ризиків та прогнозування потенційних загроз. Для підвищення ефективності роботи пропонується використовувати комбінований підхід, який поєднує алгоритми машинного навчання, нейронні мережі та експертні правила.

Одним із ключових компонентів інтелектуального модуля є підсистема виявлення аномалій. Її основним завданням є визначення нетипових подій та відхилень від нормальної поведінки користувачів або інформаційних систем. Використання алгоритмів машинного навчання дозволяє виявляти не лише відомі загрози, але й нові види атак, для яких відсутні сигнатури або попередньо сформовані правила виявлення.

Важливим елементом архітектури є модуль оцінювання ризиків. Він здійснює аналіз потенційних загроз, визначає ймовірність їх реалізації та оцінює можливі наслідки для інформаційної системи. Для цього використовуються методи багатокритеріального аналізу, математичні моделі ризиків та результати роботи алгоритмів штучного інтелекту. Отримані результати дозволяють

визначати пріоритетність заходів захисту та раціонально розподіляти ресурси організації.

Наступним компонентом є модуль прогнозування кіберзагроз. Його функціонування базується на використанні історичних даних про інциденти безпеки та методів прогнозної аналітики. Завдяки застосуванню алгоритмів машинного навчання система здатна визначати тенденції розвитку загроз та прогнозувати ймовірність виникнення нових атак. Це дозволяє переходити від реактивної до проактивної моделі забезпечення кібербезпеки.

Для формування рекомендацій щодо реагування на інциденти передбачено окремий модуль підтримки прийняття рішень. Він аналізує результати оцінювання ризиків, прогнозування загроз та класифікації інцидентів, після чого пропонує користувачу перелік можливих варіантів дій [38]. Формування рекомендацій здійснюється з урахуванням рівня критичності загроз, доступних ресурсів та вимог політики безпеки організації.

Особливе значення має модуль взаємодії з користувачем. Він забезпечує відображення результатів аналізу, формування звітів, візуалізацію даних та надання рекомендацій фахівцям з кібербезпеки. Інтерфейс користувача повинен бути інтуїтивно зрозумілим, забезпечувати швидкий доступ до інформації та підтримувати можливість налаштування параметрів аналізу відповідно до потреб організації.

Для забезпечення безперервного вдосконалення системи передбачається модуль самонавчання та оновлення моделей. Даний компонент накопичує інформацію про результати роботи системи, аналізує ефективність прийнятих рішень та виконує перенавчання моделей штучного інтелекту. Це дозволяє підвищувати точність прогнозування та адаптувати систему до змін у кіберпросторі.

Таблиця 3.1

Функціональні модулі запропонованої архітектури

Модуль	**Основні функції**	**Результат роботи**
Збір та інтеграція даних	Отримання інформації з різних джерел	Єдина база даних подій
Попередня обробка	Очищення та нормалізація даних	Підготовлені дані для аналізу
Інтелектуальний аналіз	Виявлення аномалій та класифікація загроз	Інформація про інциденти
Оцінювання ризиків	Аналіз ймовірності та наслідків загроз	Рівень ризику
Прогнозування загроз	Передбачення майбутніх атак	Прогноз розвитку загроз
Підтримка прийняття рішень	Формування рекомендацій	Варіанти реагування
Інтерфейс користувача	Візуалізація та звітність	Інформаційна підтримка
Самонавчання	Оновлення моделей ШІ	Підвищення точності роботи

Запропонована архітектура передбачає інтеграцію із сучасними платформами управління інформаційною безпекою, системами SIEM, засобами моніторингу мережевого трафіку та платформами кіберрозвідки. Така інтеграція забезпечує отримання актуальної інформації про стан інформаційної системи та дозволяє підвищити ефективність аналізу загроз.

Практична реалізація запропонованої архітектури дозволяє автоматизувати значну частину процесів аналізу інформації та підтримки прийняття рішень. Використання алгоритмів штучного інтелекту сприяє підвищенню точності виявлення кіберзагроз, скороченню часу реагування на інциденти та зменшенню навантаження на фахівців центрів кібербезпеки. Крім того, система забезпечує можливість прогнозування розвитку загроз та формування рекомендацій щодо вдосконалення заходів захисту.

Ефективність запропонованої моделі визначається її здатністю працювати в умовах невизначеності, аналізувати великі обсяги даних та адаптуватися до нових типів кіберзагроз. Завдяки поєднанню методів штучного інтелекту, експертних знань та сучасних технологій аналізу даних створюється основа для побудови інтелектуальної системи підтримки прийняття рішень нового покоління.

Отже, розроблена архітектура моделі підтримки прийняття рішень на основі штучного інтелекту забезпечує комплексний підхід до аналізу кіберзагроз, оцінювання ризиків та формування рекомендацій щодо реагування на інциденти безпеки. Її використання дозволяє підвищити ефективність управління кібербезпекою, забезпечити своєчасне прийняття обґрунтованих рішень та створити передумови для подальшого розвитку інтелектуальних систем захисту інформації.

3.2 Реалізація та тестування моделі на прикладі аналізу кіберінцидентів

Практичне застосування моделей підтримки прийняття рішень на основі штучного інтелекту є важливим етапом оцінювання їх ефективності та придатності до використання у сфері кібербезпеки. Незважаючи на значний розвиток сучасних технологій аналізу даних, головним критерієм успішності будь-якої інтелектуальної системи залишається її здатність працювати в реальних умовах та забезпечувати своєчасне виявлення кіберзагроз. Тому після проєктування архітектури запропонованої моделі необхідним є її практичне впровадження та тестування на прикладі аналізу кіберінцидентів.

Основною метою реалізації моделі є перевірка можливості використання алгоритмів штучного інтелекту для автоматизації процесів виявлення, класифікації та аналізу інцидентів інформаційної безпеки. Запропонована модель повинна забезпечувати обробку великих обсягів даних, виявлення потенційних загроз та формування рекомендацій щодо реагування на них. Для досягнення поставленої мети реалізація системи передбачає використання комплексу взаємопов’язаних програмних модулів, які забезпечують виконання основних функцій підтримки прийняття рішень [39].

У процесі реалізації моделі використовується багаторівнева структура обробки інформації. На першому етапі здійснюється збір даних із різних джерел інформації. До таких джерел належать журнали подій операційних систем,

засоби мережевого моніторингу, системи виявлення вторгнень, журнали доступу користувачів, результати сканування вразливостей та інформація з платформ кіберрозвідки. Зібрані дані надходять до централізованого сховища, де проходять процедури попередньої обробки та підготовки до подальшого аналізу.

Наступним етапом є очищення та нормалізація інформації. Реальні дані про події безпеки часто містять дублікати записів, помилки, неповні значення або інформацію в різних форматах. Для забезпечення коректної роботи алгоритмів штучного інтелекту виконується фільтрація нерелевантних даних, усунення дублювання, стандартизація форматів та перетворення інформації до єдиного вигляду. Це дозволяє підвищити якість подальшого аналізу та мінімізувати вплив помилок на результати роботи системи.

Після завершення підготовки даних здійснюється формування навчальної вибірки для алгоритмів машинного навчання. Для тестування моделі використовуються дані, які містять як легітимну активність користувачів та систем, так і приклади різних типів кіберінцидентів. До набору подій можуть входити спроби несанкціонованого доступу, атаки типу DDoS, фішингові кампанії, шкідлива активність програмного забезпечення, мережеве сканування та інші загрози, характерні для сучасного кіберпростору.

У межах реалізації моделі для аналізу кіберінцидентів доцільно використовувати комбінацію декількох алгоритмів машинного навчання. Зокрема, застосовуються дерева рішень для початкової класифікації подій, випадковий ліс для підвищення точності прогнозування та нейронні мережі для аналізу складних закономірностей у даних. Використання комбінованого підходу дозволяє підвищити якість виявлення загроз та забезпечити більш надійне функціонування системи.

Рис. 3.2 Процес аналізу кіберінцидентів у запропонованій моделі підтримки прийняття рішень

Важливим елементом реалізації є модуль виявлення аномалій. Його завдання полягає у визначенні нетипових подій, які можуть свідчити про наявність кіберзагроз. Для цього використовуються алгоритми кластеризації та методи аналізу поведінки користувачів. Система формує модель нормального функціонування інформаційного середовища та автоматично виявляє відхилення від встановлених шаблонів поведінки.

Для перевірки працездатності моделі було розглянуто типовий сценарій кіберінциденту, пов'язаний зі спробою несанкціонованого доступу до корпоративної інформаційної системи. У процесі тестування система отримує журнали подій, аналізує активність користувачів та виявляє підозрілі дії, зокрема багаторазові невдалі спроби автентифікації, використання нетипових IP-адрес та зміну звичних часових шаблонів роботи користувача. Після виявлення аномалій система виконує оцінювання рівня ризику та формує рекомендації щодо реагування.

На наступному етапі проводиться класифікація інцидентів за рівнем критичності. Для цього використовуються результати роботи алгоритмів машинного навчання та додаткові критерії оцінювання, зокрема потенційний вплив на конфіденційність, цілісність та доступність інформації. Кожному

інциденту присвоюється відповідний рівень ризику, що дозволяє визначити пріоритетність подальших дій.

Однією з ключових функцій запропонованої моделі є автоматичне формування рекомендацій. Після завершення аналізу система пропонує можливі заходи реагування залежно від характеру загрози. У випадку несанкціонованого доступу такими заходами можуть бути блокування облікового запису, зміна параметрів автентифікації, ізоляція скомпрометованого вузла або проведення додаткового аудиту безпеки. Це дозволяє суттєво скоротити час реагування на інциденти та підвищити ефективність діяльності фахівців з кібербезпеки.

Для оцінювання ефективності роботи моделі використовуються показники точності, повноти, F1-міри та швидкості обробки даних. Точність характеризує частку правильно класифікованих подій, повнота відображає здатність системи виявляти всі наявні загрози, а F1-міра дозволяє комплексно оцінити баланс між цими показниками. Крім того, аналізується час, необхідний для обробки подій та формування рекомендацій.

Результати тестування свідчать про високу ефективність запропонованої моделі під час виявлення кіберінцидентів. Використання алгоритмів штучного інтелекту дозволяє значно підвищити точність класифікації подій порівняно з традиційними підходами на основі статичних правил. Особливо помітні переваги моделі під час виявлення складних багатоетапних атак та аналізу великих обсягів мережевого трафіку.

Важливим результатом тестування є зменшення кількості хибнопозитивних спрацювань. Завдяки використанню алгоритмів машинного навчання система більш точно розрізняє легітимну активність користувачів та потенційно небезпечні дії. Це дозволяє скоротити навантаження на операторів центрів моніторингу безпеки та підвищити ефективність роботи служб кіберзахисту.

Окремо було оцінено можливість адаптації моделі до нових типів загроз. Завдяки механізмам самонавчання система здатна оновлювати власні моделі на основі нових даних та поступово підвищувати якість виявлення інцидентів. Це

особливо важливо в умовах постійної еволюції кіберзагроз та появи нових методів атак.

Проведене тестування також підтвердило доцільність інтеграції моделі із сучасними системами моніторингу безпеки та платформами управління інформацією про події безпеки. Такий підхід забезпечує отримання актуальних даних у режимі реального часу та дозволяє підвищити швидкість прийняття рішень під час реагування на кіберінциденти.

Незважаючи на позитивні результати, процес тестування виявив і певні обмеження моделі. До них належать залежність від якості навчальних даних, необхідність періодичного перенавчання алгоритмів та потреба у достатніх обчислювальних ресурсах для обробки великих обсягів інформації. Проте зазначені недоліки не знижують загальної ефективності запропонованого підходу та можуть бути усунені шляхом подальшого вдосконалення системи.

Отже, реалізація та тестування запропонованої моделі підтримки прийняття рішень на основі штучного інтелекту підтвердили її ефективність для аналізу кіберінцидентів. Використання алгоритмів машинного навчання дозволяє автоматизувати процес виявлення загроз, підвищити точність класифікації подій та скоротити час реагування на інциденти безпеки. Отримані результати свідчать про доцільність практичного використання моделі для підтримки діяльності фахівців з кібербезпеки та створюють основу для подальшого вдосконалення інтелектуальних систем підтримки прийняття рішень.

3.3 Оцінка результативності моделі та рекомендації щодо її впровадження в систему управління кібербезпекою

Ефективність будь-якої системи підтримки прийняття рішень визначається її здатністю забезпечувати своєчасне отримання достовірної інформації, підвищувати якість управлінських рішень та сприяти досягненню поставлених цілей у конкретній предметній області. У сфері кібербезпеки оцінювання

результативності інтелектуальних моделей має особливе значення, оскільки від правильності та оперативності прийнятих рішень залежить рівень захищеності інформаційних ресурсів, стійкість інформаційних систем до кіберзагроз та безперервність функціонування організацій [40]. У зв’язку з цим важливим етапом дослідження є оцінка результативності запропонованої моделі підтримки прийняття рішень на основі штучного інтелекту та формування рекомендацій щодо її практичного впровадження в систему управління кібербезпекою.

Оцінювання результативності моделі здійснюється на основі аналізу її функціональних можливостей, показників ефективності та практичних результатів тестування. Основна увага приділяється здатності моделі своєчасно виявляти кіберінциденти, здійснювати оцінювання ризиків, прогнозувати потенційні загрози та формувати обґрунтовані рекомендації щодо реагування на події безпеки. Важливим критерієм також є можливість інтеграції моделі в існуючу інфраструктуру кіберзахисту організації.

Одним із ключових показників результативності є точність виявлення інцидентів безпеки. Проведене тестування показало, що використання алгоритмів машинного навчання та інтелектуального аналізу даних дозволяє досягти високого рівня точності класифікації подій безпеки. Завдяки цьому зменшується ймовірність пропуску реальних загроз та підвищується загальна ефективність функціонування системи кіберзахисту.

Важливим показником є повнота виявлення загроз. Запропонована модель демонструє здатність виявляти не лише відомі типи атак, але й нові або модифіковані кіберзагрози, які не містяться у сигнатурних базах даних. Використання алгоритмів аналізу аномалій дозволяє своєчасно фіксувати підозрілі події та забезпечувати проактивний підхід до кіберзахисту [41].

Суттєвою перевагою моделі є скорочення часу реагування на інциденти безпеки. Традиційні підходи часто передбачають значний обсяг ручної роботи з аналізу журналів подій та оцінювання ситуації. Автоматизація цих процесів за допомогою штучного інтелекту дозволяє значно прискорити виявлення загроз та формування рекомендацій щодо подальших дій. Це особливо важливо під час

реагування на складні кіберінциденти, коли навіть незначна затримка може призвести до суттєвих наслідків.

Оцінювання результативності також показало зменшення навантаження на фахівців з кібербезпеки. Значна частина рутинних операцій, пов’язаних із моніторингом подій безпеки, аналізом мережевого трафіку та класифікацією інцидентів, виконується автоматично. Це дозволяє експертам концентрувати увагу на вирішенні більш складних завдань та стратегічному управлінні кібербезпекою.

Важливим аспектом оцінювання є адаптивність моделі до змін у кіберпросторі. Завдяки використанню механізмів самонавчання система здатна накопичувати нові знання про кіберзагрози та вдосконалювати власні алгоритми. Це дозволяє підтримувати високий рівень ефективності навіть за умови появи нових методів атак та змін у поведінці кіберзлочинців [42].

Суттєве значення має можливість інтеграції запропонованої моделі з існуючими системами управління кібербезпекою. Аналіз показує, що архітектура моделі дозволяє взаємодіяти з платформами SIEM, системами виявлення вторгнень, засобами моніторингу мережевого трафіку та платформами кіберрозвідки. Це забезпечує централізований підхід до аналізу подій безпеки та підвищує ефективність управління інформаційною безпекою організації.

Разом із перевагами необхідно враховувати певні особливості впровадження моделі в реальних умовах. Однією з основних вимог є забезпечення належної якості даних, які використовуються для навчання алгоритмів штучного інтелекту. Від повноти, достовірності та актуальності інформації значною мірою залежить точність роботи моделі та якість сформованих рекомендацій.

Для успішного впровадження моделі доцільно здійснювати поетапну інтеграцію в існуючу систему управління кібербезпекою. На початковому етапі рекомендується використовувати модель як допоміжний інструмент для аналізу подій безпеки та формування рекомендацій. Після підтвердження ефективності

її роботи можливе поступове розширення функціональних можливостей та збільшення рівня автоматизації процесів прийняття рішень.

Однією з важливих рекомендацій є організація постійного моніторингу ефективності функціонування моделі. Для цього необхідно регулярно аналізувати показники точності, повноти та швидкості роботи системи, оцінювати кількість хибнопозитивних і хибнонегативних результатів та здійснювати коригування алгоритмів у разі необхідності. Такий підхід забезпечує підтримання високої якості роботи моделі протягом тривалого часу.

Важливим напрямом впровадження є забезпечення інформаційної безпеки самої моделі штучного інтелекту. Оскільки сучасні алгоритми можуть бути об’єктом спеціалізованих атак, необхідно передбачити механізми контролю цілісності даних, захисту моделей від несанкціонованого доступу та моніторингу спроб маніпуляції результатами аналізу.

Рекомендується також забезпечити належний рівень підготовки персоналу, який буде використовувати систему. Незважаючи на високий рівень автоматизації, ефективність функціонування моделі значною мірою залежить від здатності фахівців правильно інтерпретувати результати аналізу та приймати остаточні управлінські рішення. Проведення навчання персоналу дозволить максимально ефективно використовувати можливості запропонованої системи.

Для підвищення результативності роботи моделі доцільно забезпечити регулярне оновлення баз знань та навчальних наборів даних. Постійна актуалізація інформації про нові кіберзагрози дозволить підтримувати високий рівень точності прогнозування та забезпечить адаптацію системи до змін у сучасному кіберпросторі.

Перспективним напрямом розвитку є інтеграція запропонованої моделі з технологіями кіберрозвідки та автоматизованого реагування на інциденти. Це дозволить не лише виявляти загрози, але й автоматично реалізовувати окремі заходи захисту, що суттєво підвищить оперативність реагування на кіберінциденти.

Рис. 3.3 Оцінка результативності моделі підтримки прийняття рішень та напрями її впровадження

Проведена оцінка підтверджує, що використання штучного інтелекту у системах підтримки прийняття рішень дозволяє значно підвищити ефективність управління кібербезпекою. Запропонована модель забезпечує комплексний аналіз інформації, автоматизує процеси оцінювання ризиків та підтримує прийняття обґрунтованих рішень в умовах високої невизначеності. Завдяки використанню алгоритмів машинного навчання та інтелектуального аналізу даних система здатна своєчасно виявляти потенційні кіберзагрози, аналізувати їх характеристики та прогнозувати можливі наслідки для інформаційної інфраструктури. Важливою перевагою моделі є можливість обробки значних обсягів даних у режимі реального часу, що дозволяє оперативно реагувати на зміни в кіберпросторі та зменшувати ризик реалізації атак. Крім того, автоматизація процесів аналізу та формування рекомендацій сприяє зниженню навантаження на фахівців з кібербезпеки, мінімізує вплив людського фактора та підвищує об’єктивність прийнятих рішень. Інтеграція моделі з існуючими системами моніторингу та управління безпекою забезпечує централізований підхід до аналізу подій і координації заходів реагування. У результаті

створюються сприятливі умови для підвищення рівня захищеності інформаційних систем, удосконалення процесів управління ризиками та зниження негативного впливу сучасних кіберзагроз на діяльність організацій.

Таблиця 3.2

Рекомендації щодо впровадження моделі в систему управління кібербезпекою

Напрям впровадження	**Основні заходи**	**Очікуваний результат**
Інтеграція з існуючими системами	Підключення до SIEM, IDS/IPS та систем моніторингу	Централізований аналіз подій безпеки
Підготовка даних	Очищення та актуалізація наборів даних	Підвищення точності моделей
Навчання персоналу	Підготовка фахівців до роботи із системою	Ефективне використання моделі
Моніторинг ефективності	Контроль показників роботи алгоритмів	Стабільність та надійність функціонування
Захист моделі ШІ	Контроль доступу та захист навчальних даних	Підвищення стійкості до атак
Оновлення моделей	Регулярне перенавчання алгоритмів	Адаптація до нових загроз
Інтеграція з кіберрозвідкою	Використання Threat Intelligence	Покращення прогнозування загроз
Автоматизація реагування	Впровадження механізмів автоматичних дій	Скорочення часу реагування на інциденти

Отже, результати дослідження свідчать про високу результативність розробленої моделі підтримки прийняття рішень на основі штучного інтелекту. Її впровадження в систему управління кібербезпекою дозволяє підвищити точність виявлення інцидентів, скоротити час реагування на загрози, оптимізувати використання ресурсів та забезпечити більш ефективне управління ризиками інформаційної безпеки. Запропоновані рекомендації щодо впровадження створюють основу для практичного використання моделі в сучасних організаціях та подальшого розвитку інтелектуальних систем кіберзахисту.

Висновки до розділу 3

У третьому розділі розроблено модель підтримки прийняття рішень у сфері кібербезпеки на основі технологій штучного інтелекту та запропоновано її архітектуру. Визначено основні функціональні модулі системи, їх взаємодію та принципи роботи, що забезпечують автоматизований збір, обробку та аналіз інформації про події безпеки.

Здійснено реалізацію та тестування запропонованої моделі на прикладі аналізу кіберінцидентів. Отримані результати підтвердили ефективність використання алгоритмів машинного навчання для виявлення загроз, оцінювання ризиків і формування рекомендацій щодо реагування на інциденти безпеки. Встановлено, що модель забезпечує високий рівень точності виявлення загроз та скорочує час прийняття рішень.

Проведено оцінку результативності розробленої моделі та сформульовано рекомендації щодо її впровадження в систему управління кібербезпекою. Визначено, що використання запропонованого підходу сприяє підвищенню рівня захищеності інформаційних систем, оптимізації роботи фахівців з кібербезпеки та забезпечує більш ефективне управління кіберризиками в умовах сучасних цифрових загроз.

ВИСНОВКИ

У кваліфікаційній роботі досліджено теоретичні та практичні аспекти побудови моделей підтримки прийняття рішень у сфері кібербезпеки на основі технологій штучного інтелекту. Актуальність теми обумовлена постійним зростанням кількості та складності кіберзагроз, збільшенням обсягів інформації, що потребує аналізу, а також необхідністю оперативного прийняття обґрунтованих рішень щодо забезпечення безпеки інформаційних систем. Використання сучасних методів штучного інтелекту відкриває нові можливості для автоматизації процесів виявлення загроз, оцінювання ризиків та підтримки діяльності фахівців з кібербезпеки.

У першому розділі було розглянуто теоретичні основи систем підтримки прийняття рішень та особливості використання штучного інтелекту у сфері кібербезпеки. Визначено сутність, структуру та принципи функціонування систем підтримки прийняття рішень, які забезпечують інформаційну та аналітичну підтримку управлінських процесів. Досліджено основні методи та алгоритми штучного інтелекту, зокрема машинне навчання, нейронні мережі, глибоке навчання, експертні системи та методи інтелектуального аналізу даних. Також проаналізовано сучасні підходи до використання штучного інтелекту для виявлення, прогнозування та запобігання кіберзагрозам. Встановлено, що впровадження інтелектуальних технологій дозволяє суттєво підвищити швидкість та якість аналізу подій безпеки, а також забезпечити більш ефективне реагування на кіберінциденти.

У другому розділі проведено аналіз сучасних методів підтримки прийняття рішень у сфері кібербезпеки. Розглянуто особливості використання експертних методів, статистичних підходів, моделей оцінювання ризиків, систем на базі знань та алгоритмів машинного навчання. Оцінено ефективність найбільш поширених алгоритмів машинного навчання для виявлення інцидентів безпеки, серед яких дерева рішень, випадкові ліси, методи опорних векторів, нейронні мережі та алгоритми кластеризації. Встановлено, що використання штучного

інтелекту забезпечує високу точність класифікації подій та дозволяє автоматизувати процес аналізу кіберзагроз. Водночас виявлено низку недоліків існуючих моделей, серед яких залежність від якості навчальних даних, складність інтерпретації результатів, наявність хибних спрацювань та необхідність значних обчислювальних ресурсів. Проведений аналіз підтвердив необхідність розробки удосконаленої моделі підтримки прийняття рішень на основі штучного інтелекту.

У третьому розділі розроблено архітектуру моделі підтримки прийняття рішень у сфері кібербезпеки на основі технологій штучного інтелекту. Запропонована модель включає модулі збору та підготовки даних, інтелектуального аналізу інформації, оцінювання ризиків, прогнозування загроз, формування рекомендацій та підтримки прийняття рішень. Реалізація та тестування моделі на прикладі аналізу кіберінцидентів підтвердили її працездатність та ефективність. Отримані результати свідчать про можливість підвищення точності виявлення загроз, скорочення часу реагування на інциденти та зменшення навантаження на фахівців з кібербезпеки. Також сформульовано практичні рекомендації щодо впровадження моделі в систему управління кібербезпекою, які передбачають інтеграцію з існуючими засобами моніторингу, забезпечення якості навчальних даних, регулярне оновлення моделей та підготовку персоналу.

У результаті проведеного дослідження досягнуто поставленої мети та виконано всі поставлені завдання. Розроблена модель підтримки прийняття рішень на основі штучного інтелекту забезпечує комплексний підхід до аналізу кіберзагроз, оцінювання ризиків та формування рекомендацій щодо реагування на інциденти безпеки. Практичне використання запропонованої моделі дозволяє підвищити ефективність управління кібербезпекою, покращити якість прийняття рішень в умовах невизначеності та сприяти підвищенню рівня захищеності сучасних інформаційних систем. Перспективами подальших досліджень є вдосконалення алгоритмів штучного інтелекту, розширення можливостей самонавчання моделей та інтеграція технологій підтримки прийняття рішень із

сучасними платформами кіберрозвідки та автоматизованого реагування на кіберінциденти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Hoboken : Pearson, 2021. 1232 p.

2. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge : MIT Press, 2016. 800 p.

3. Bishop C. M. Pattern Recognition and Machine Learning. New York : Springer, 2006. 738 p.

4. Mitchell T. M. Machine Learning. New York : McGraw-Hill Education, 1997. 432 p.

5. Murphy K. P. Machine Learning: A Probabilistic Perspective. Cambridge : MIT Press, 2012. 1104 p.

6. Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. 2nd ed. Cambridge : MIT Press, 2018. 552 p.

7. Alpaydin E. Introduction to Machine Learning. 4th ed. Cambridge : MIT Press, 2020. 640 p.

8. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras and TensorFlow. 3rd ed. Sebastopol : O'Reilly Media, 2022. 851 p.

9. Chollet F. Deep Learning with Python. 2nd ed. Shelter Island : Manning Publications, 2021. 504 p.

10. Kim D., Solomon M. Fundamentals of Information Systems Security. 4th ed. Burlington : Jones & Bartlett Learning, 2019. 640 p.

11. Stallings W., Brown L. Computer Security: Principles and Practice. 4th ed. Hoboken : Pearson, 2018. 840 p.

12. Easttom C. Cybersecurity Fundamentals. 3rd ed. Indianapolis : Pearson IT Certification, 2022. 384 p.

13. Andress J. The Basics of Information Security. 3rd ed. Amsterdam : Elsevier, 2020. 288 p.

14. Whitman M. E., Mattord H. J. Principles of Information Security. 7th ed. Boston : Cengage Learning, 2021. 656 p.

15. Vacca J. R. Computer and Information Security Handbook. 3rd ed. Amsterdam : Elsevier, 2017. 1248 p.

16. Sharda R., Delen D., Turban E. Business Intelligence, Analytics and Data Science: A Managerial Perspective. 5th ed. Hoboken : Pearson, 2023. 832 p.

17. Turban E., Aronson J. E., Liang T. P. Decision Support Systems and Intelligent Systems. 9th ed. Upper Saddle River : Pearson Education, 2011. 824 p.

18. Power D. J. Decision Support, Analytics and Business Intelligence. 3rd ed. New York : Business Expert Press, 2019. 280 p.

19. Keen P. G. W., Scott Morton M. S. Decision Support Systems: An Organizational Perspective. Reading : Addison-Wesley, 1978. 264 p.

20. Marakas G. M. Decision Support Systems in the 21st Century. 2nd ed. Upper Saddle River : Prentice Hall, 2003. 620 p.

21. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Geneva : International Organization for Standardization, 2022.

22. ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks. Geneva : International Organization for Standardization, 2022.

23. NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : National Institute of Standards and Technology, 2024.

24. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg : National Institute of Standards and Technology, 2020.

25. ENISA Threat Landscape 2024. Heraklion : European Union Agency for Cybersecurity, 2024.

26. Лєнков Є. С., Перегудов Д. А., Хорошко В. О. Методи та засоби захисту інформації. Київ : Арій, 2015. 464 с.

27. Хорошко В. О., Чекатков А. А. Методи та засоби захисту інформації. Київ : Юніор, 2018. 504 с.

28. Корченко О. Г. Системи захисту інформації. Київ : НАУ, 2019. 392 с.

29. Корченко О. Г., Архипов О. Є., Казмірчук С. В. Аудит та управління інформаційною безпекою. Київ : Центр учбової літератури, 2020. 408 с.

30. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. Київ : ДУТ, 2015. 288 с.

31. Bharathi P. S., Reddy T. J. AI-Driven hybrid deep cognitive framework for intrusion detection and decision-making in cognitive radio cybersecurity systems. *2025 2nd international conference on artificial intelligence and knowledge discovery in concurrent engineering (ICECONF)*, Chennai, India, 9–10 October 2025. 2025. P. 1–9. URL: https://doi.org/10.1109/iceconf65644.2025.11379473

32. Choudhary S., Kalaiarasi S., Sundar Raja A. J. AI-Driven SIEM (security information and event management) systems using long short-term memory (LSTM) for log-based threat detection. *Artificial intelligence in cybersecurity for risk assessment and transparent threat detection frameworks*. 2025. P. 200–232. URL: https://doi.org/10.71443/9789349552029-07

33. Das R., Sandhane R. Artificial intelligence in cyber security. *Journal of physics: conference series*. 2021. Vol. 1964, no. 4. P. 042072. URL: https://doi.org/10.1088/1742-6596/1964/4/042072

34. Explainable AI (XAI) for security decisions to mitigate cybersecurity attacks / S.-U.-R. Sahito et al. *Journal of advanced research in applied sciences and engineering technology*. 2025. Vol. 55, no. 2. P. 214–223. URL: https://doi.org/10.37934/araset.55.2.214223

35. Generative AI enabled actionable decision support in cyber security operations for enterprise security / B. Saurabh et al. *2024 ITU kaleidoscope: innovation and digital transformation for a sustainable world (ITU K)*, New Delhi, India, 21–23 October 2024. 2024. P. 1–8. URL: https://doi.org/10.23919/ituk62727.2024.10772892

36. Grover S. Adaptive Trust: A Comparative Analysis of Cybersecurity Metrics and AI-Driven Privacy Safety Enforcement. Traditional Fidelity versus AI-

Driven Velocity. *The american journal of engineering and technology*. 2026. Vol. 12, no. 04. P. 128–135. URL: https://doi.org/10.37547/tajet/volume08issue04-13

37. Jonas D., Aprila Yusuf N., Rahmania Az Zahra A. Enhancing security frameworks with artificial intelligence in cybersecurity. *International transactions on education technology (ITEE)*. 2023. Vol. 2, no. 1. P. 83–91. URL: https://doi.org/10.33050/itee.v2i1.428

38. Lee H.-W., Han T.-H., Lee T.-J. Reference based AI decision support for cybersecurity. *IEEE access*. 2023. P. 1. URL: https://doi.org/10.1109/access.2023.3342868

39. Olugboja A. Securing artificial intelligence models: a comprehensive cybersecurity approach. *Archives of business research*. 2024. Vol. 12, no. 3. P. 233–243. URL: https://doi.org/10.14738/abr.123.16770

40. Ren S., Chen S. Large language models for cybersecurity intelligence, threat hunting, and decision support. *Computer life*. 2025. Vol. 13, no. 3. P. 39–47. URL: https://doi.org/10.54097/7ysr5k17

41. Sarker I. H., Furhad M. H., Nowrozy R. AI-Driven cybersecurity: an overview, security intelligence modeling and research directions. *SN computer science*. 2021. Vol. 2, no. 3. URL: https://doi.org/10.1007/s42979-021-00557-0

42. Song Y., Zhang A. From black box to physically interpretable: Trustworthy computing for AI-driven decision-making and control. *Journal of automation and intelligence*. 2025. URL: https://doi.org/10.1016/j.jai.2025.09.003