НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ОЦІНКА ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВИЯВЛЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕКИ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Новосельський Дмитро Олексійович

Керівник: к.ф-м.н., доцент
Чепурна Олена Євгенівна

Рецензент: к.т.н., доцент
Кухаренко Сергій Вікторович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Новосельському Дмитру Олексійовичу

1. Тема роботи: «Оцінка інтелектуальних систем виявлення загроз кібербезпеки»
Керівник роботи: доцент, к.ф.-м.н, Чепурна Олена Євгенівна
затверджені наказом НУ ОЮА від 02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 року
3. Дата видачі завдання«15» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Оцінка інтелектуальних систем виявлення загроз кібербезпеки» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека.

Містить 3 рисунків, 6 таблиці, 20 літературних джерел за переліком посилань. Робота виконана на 60 сторінках загального тексту і 48 сторінках основного тексту.

Метою роботи є розробка та оцінка інтелектуальних систем для виявлення та аналізу загроз кібербезпеки з використанням методів машинного навчання.

Об’єктом розробки є системи кібербезпеки, предметом розробки є інтелектуальні алгоритми для виявлення загроз. Шляхи досягнення мети включають аналіз сучасних методів кібербезпеки, розробку та тестування моделей машинного навчання, а також їх інтеграцію в існуючі системи захисту.

Робота має високий ступінь реалізації, оскільки розроблені методи були успішно впроваджені у вигляді програмного забезпечення, що дозволяє автоматизовано виявляти кіберзагрози.

Результати роботи можуть бути використані при розробці нових та покращенні існуючих систем кібербезпеки для виявлення та запобігання кіберзагрозам у різних сферах, включаючи фінансовий сектор, державні установи та комерційні організації.

Можливими напрямками подальших досліджень є покращення алгоритмів машинного навчання для виявлення нових типів загроз, розширення функціональних можливостей систем виявлення загроз, а також інтеграція розроблених систем з іншими засобами кібербезпеки для комплексного захисту інформаційних систем.

КІБЕРБЕЗПЕКА, ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ, ВИЯВЛЕННЯ ЗАГРОЗ, МАШИННЕ НАВЧАННЯ, АНАЛІЗ ДАНИХ, АВТОМАТИЗАЦІЯ, ЗАХИСТ ІНФОРМАЦІЇ.

ABSTRACT

Qualification work on the topic "Evaluation of Intelligent Cybersecurity Threat Detection Systems" for the first (bachelor's) level of higher education in specialty 125 "Cybersecurity", educational program: Cybersecurity. Contains 3 figures, 6 tables, 4 appendices, and 20 references according to the list of references. The work is executed on 60 pages of general text and 48 pages of main text.

The purpose of this work is to develop and evaluate intelligent systems for detecting and analyzing cybersecurity threats using machine learning methods.

The object of the development is cybersecurity systems, and the subject of the development is intelligent algorithms for threat detection. The ways to achieve the goal include analyzing current cybersecurity methods, developing and testing machine learning models, and integrating them into existing protection systems.

The work has a high degree of implementation, as the developed methods have been successfully implemented in software that allows for the automated detection of cyber threats.

The results of the work can be used in the development of new and improvement of existing cybersecurity systems for detecting and preventing cyber threats in various fields, including the financial sector, government institutions, and commercial organizations.

Possible directions for further research include improving machine learning algorithms for detecting new types of threats, expanding the functional capabilities of threat detection systems, and integrating the developed systems with other cybersecurity tools for comprehensive protection of information systems.

CYBERSECURITY, INTELLIGENT SYSTEMS, THREAT DETECTION, MACHINE LEARNING, DATA ANALYSIS, AUTOMATION, INFORMATION PROTECTION.

ЗМІСТ

ВСТУП

Актуальність теми. Актуальність обраної теми надзвичайно висока у контексті стрімкого розвитку сучасного кіберпростору та появи нових, більш виразних загроз для інформаційної безпеки. Свідчиться про значний приріст як кількісний, так і якісний кіберзагроз, що настає за постійним удосконаленням технологій кіберзахисту. Інтелектуальні системи виявлення загроз вирішують стратегічно важливе завдання у забезпеченні цілісності та безпеки інформаційних ресурсів. Сучасне суспільство стоїть перед викликами, пов'язаними не лише зі збільшенням обсягу кіберзагроз, а й з їхньою різноманітністю, що вимагає глибокого аналізу та розробки нових стратегій для ефективного протистояння цим викликам. Дослідження теми аналізу інтелектуальних систем виявлення загроз у сфері кібербезпеки є кроком у напрямку створення ефективних та інноваційних рішень для забезпечення кібербезпеки в умовах постійно зростаючого рівня кількісних та якісних кіберзагроз.

З кожним роком технології стають більш складними та розширюють свої можливості. Це відкриває нові можливості для кіберзлочинців і створює потребу у вдосконаленні інтелектуальних систем виявлення загроз. Кількість та складність кіберзагроз постійно зростає. Від традиційних вірусів до складних атак на інфраструктуру, необхідно розробляти інтелектуальні системи, які можуть ефективно реагувати на різноманітні загрози.

Сучасне суспільство є високопідключеним, що створює додаткові шляхи для кіберзлочинців. Інтелектуальні системи повинні бути готові до аналізу великого обсягу даних та виявлення загроз в реальному часі. Кіберзлочинці постійно адаптують свої методи, використовуючи нові технології та тактики. Інтелектуальні системи повинні бути гнучкими та готовими до реагування на постійні зміни у сфері кібербезпеки.

Інтелектуальні системи виявлення загроз грають ключову роль у забезпеченні безпеки та цілісності інтелектуальної власності. Зростання значення інтелектуальної власності створює необхідність у високоефективних засобах

захисту. Взаємодія кібербезпеки та інтелектуальної власності вимагає дослідження та розробки комплексних стратегій, щоб забезпечити ефективний захист інформаційних ресурсів та прав власності.

Дослідження зазначених факторів стає основою для розробки і вдосконалення інтелектуальних систем виявлення загроз у сфері кібербезпеки, що робить тему надзвичайно актуальною та важливою у сучасному інформаційному суспільстві.

Мета дослідження полягає у вивченні та оцінці ефективності використання інтелектуальних систем для виявлення загроз кібербезпеці. Зокрема, метою є аналіз можливостей інтелектуальних систем у виявленні кіберзагроз, визначення їхнього впливу на ефективність національної кібероборони та розробка рекомендацій щодо оптимізації використання цих систем у сфері кібербезпеки.

Завдання дослідження:

- аналіз загальних концепцій кібербезпеки та визначення ролі інтелектуальних систем у цій сфері.
- вивчення можливостей інтелектуальних систем у виявленні та аналізі кіберзагроз.
- оцінка ефективності інтелектуальних систем у реагуванні на кібератаки та забезпеченні кіберстійкості.
- аналіз тенденцій розвитку технологій інтелектуальних систем у контексті кібербезпеки.
- формулювання рекомендацій щодо використання інтелектуальних систем для виявлення кіберзагроз.

Об’єкт дослідження – процес виявлення та аналізу кіберзагроз з використанням інтелектуальних систем у сфері кібербезпеки.

Предмет дослідження є застосування інтелектуальних систем у виявленні та аналізі кіберзагроз, їхня роль у реагуванні на кібератаки та забезпеченні кіберстійкості, а також перспективи розвитку цих систем у майбутньому.

Методи дослідження: Для отримання фундаментального розуміння методів та технологій, що використовуються в інтелектуальних системах для виявлення

кіберзагроз, проводитиметься аналіз наукових джерел, статей, публікацій та інших джерел інформації. Це дозволить охопити історичний розвиток цих систем, сучасні тенденції та теоретичні основи їхньої роботи.

В рамках дослідження будуть розглянуті та проаналізовані інтелектуальні системи з точки зору системного підходу. Це дозволить оцінити взаємозв'язки між різними компонентами системи та їх вплив на загальну ефективність у виявленні кіберзагроз.

Для аналізу даних та виявлення закономірностей і тенденцій у використанні інтелектуальних систем у кібербезпеці будуть використані статистичні методи. Це дозволить отримати об'єктивні дані про ефективність цих систем та їхній вплив на стійкість до кіберзагроз.

Практичне значення отриманих результатів. Розроблені методи та моделі машинного навчання можуть бути використані для покращення систем виявлення кіберзагроз, що дозволить підвищити рівень захищеності інформаційних систем та мереж.

Застосування нових підходів до виявлення та аналізу кіберзагроз дозволить оперативно реагувати на потенційні атаки та мінімізувати їхні негативні наслідки для організацій.

Використання передових технологій у сфері кібербезпеки допоможе зменшити ризики втрати даних, фінансових втрат та порушень законодавства, що може значно підвищити стійкість бізнесу.

Застосування результатів дослідження дозволить оптимізувати процеси управління кіберзагрозами, що призведе до підвищення ефективності роботи та забезпечить більш швидке виявлення та реагування на потенційні загрози.

Публікації та апробація кваліфікаційної роботи. Результати дослідження було апробовано на Всеукраїнській науково-практичній конференції здобувачів вищої освіти «СУСПІЛЬСТВО ТА ДЕРЖАВА В УМОВАХ ВОЄННОГО СТАНУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ»

1 ВВЕДЕННЯ В КІБЕРБЕЗПЕКУ ТА ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ

1.1 Загальні концепції кібербезпеки

У сучасному інформаційному суспільстві, де кіберпростір стає не від'ємною складовою повсякденного життя, концепції кібербезпеки визначають ключові принципи та стратегії, спрямовані на забезпечення безпеки, конфіденційності та доступності інформації. Розгляд загальних концепцій кібербезпеки є важливим етапом для розуміння основних аспектів цієї області.

Протягом останніх 30-40 років широке використання комп'ютерних та телекомунікаційних технологій у різних сферах життєдіяльності призвело до збільшення кількості загроз. Ці загрози можуть спричинити значні шкоди як окремим особам, так і державам, а також на міжнародному рівні. Це підкреслило необхідність нейтралізації або мінімізації цих загроз. У цьому контексті був введений термін "кібербезпека", який вперше набув поширення в середині 1990-х років, коли уряд Сполучених Штатів Америки розпочав активне дослідження цієї проблеми.[1]

Під час виявлення та аналізу кіберінцидентів і кібератак суб’єкти забезпечення кібербезпеки визначають їхню критичність для визначення подальших заходів. Кіберінциденти оцінюються за п'ятьма рівнями, починаючи від некритичного (рівень 0) до надзвичайного (рівень 5). Кожен рівень визначає ступінь загрози для функціонування інформаційних систем та можливі наслідки для національної безпеки.[2]

Згідно Закону України «Про основні засади забезпечення кібербезпеки України» Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;[3]

Перш за все, кібербезпека охоплює комплекс заходів, спрямованих на захист інформації в кіберпросторі від різноманітних загроз. Ці загрози можуть включати

кібератаки, витоки даних, використання вразливостей програмного забезпечення та інші форми кіберзлочинів. Концепції кібербезпеки передбачають розробку та впровадження технічних, організаційних та правових заходів для запобігання, виявлення та відновлення від таких загроз.

Ключовим аспектом загальних концепцій кібербезпеки є також забезпечення доступності інформації. Це означає, що інформація повинна бути доступною для тих, хто має на це право, і відновлюватися швидко після можливих випадків кібератак чи інших інцидентів.

Загальні концепції кібербезпеки визначають основні принципи, які визначають стратегії та заходи для забезпечення безпеки в кіберпросторі. Розгляд цих концепцій є важливим для розуміння складності та різноманітності завдань, пов'язаних із забезпеченням цілісності, конфіденційності та доступності інформації.

Принцип цілісності інформації передбачає необхідність забезпечення незмінності та цілісності інформації, щоб вона не піддавалася незаконним модифікаціям чи порушенням.

Забезпечення конфіденційності полягає в тому, щоб гарантувати, що інформація доступна та використовується тільки тим, хто має на це право, мінімізуючи ризики несанкціонованого доступу.

Принцип доступності визначає необхідність забезпечення того, щоб інформація була доступною для тих, хто має право на її використання, у всі часи, навіть під час можливих кібератак чи інших небажаних інцидентів.

Згідно з принципом відповідальності, сторони, що управляють інформацією, несуть відповідальність за забезпечення її безпеки та виконання необхідних заходів для запобігання інцидентам.

Принцип невідмовності передбачає використання заходів для забезпечення безперебійного функціонування систем та відновлення після можливих випадків втрати доступності.

Кібербезпека стикається з різноманітністю кіберзагроз, які включають в себе атаки на конфіденційність, цілісність та доступність інформаційних ресурсів.

Розуміння різних видів кіберзагроз є ключовим для розробки ефективних заходів з кіберзахисту та виявлення загроз у реальному часі.

У контексті загальних концепцій кібербезпеки важливо визначити способи виявлення загроз. Це може включати в себе використання сучасних технологій аналізу журналів, інтелектуальних систем виявлення аномалій та аналітичних інструментів для відстеження незвичайної активності.

Однією з ключових аспектів концепції кібербезпеки є можливість ефективної інтеграції із сховищами даних. Це означає, що інтелектуальні системи виявлення загроз повинні мати здатність аналізувати великі обсяги даних, що може бути використано для вчасного виявлення аномальної активності.

Концепція кібербезпеки передбачає адаптивність до нових загроз, що розвиваються.. Це включає в себе вдосконалення систем та стратегій відповіді на атаки на основі отриманих знань і досвіду попередніх інцидентів.

Ці аспекти доповнюють загальні концепції кібербезпеки та створюють основу для подальшого розгляду ролі інтелектуальних систем виявлення загроз у контексті цих аспектів. Розуміння різноманітності кіберзагроз, методів їх виявлення та інтеграції з даними є ключовим для розробки ефективних та адаптивних стратегій кібербезпеки.

1.2 Важливість та роль інтелектуальних систем у сфері кібербезпеки

Підвищення ефективності виявлення загроз: Інтелектуальні системи виявлення загроз грають визначальну роль у підвищенні ефективності виявлення та реагування на потенційні кіберзагрози. Завдяки використанню алгоритмів машинного навчання та аналізу великих обсягів даних, ці системи можуть швидко і точно виявляти аномальну активність та невідповідності стандартному зразку.

Важливість інтелектуальних систем полягає в їх здатності до аналізу і реагування в реальному часі на кіберзагрози. Це надає можливість вчасно виявляти та усувати загрози до того, як вони спричинять значні збитки або втрати.

Інтелектуальні системи можуть використовувати складні аналітичні методи для розуміння структури та характеру кіберзагроз. Це дозволяє здійснювати глибокий аналіз, враховуючи різноманітні аспекти загроз, і допомагає у формуванні цілісної стратегії кібербезпеки.

Інтелектуальні системи дозволяють мінімізувати вплив кібератак, оскільки вони здатні виявляти та реагувати на загрози швидше, ніж традиційні методи. Це сприяє скороченню часу реакції та обмеженню збитків, пов'язаних з атаками.

Інтелектуальні системи можуть використовувати дані для прогнозування потенційних загроз та навіть попереджати про можливі атаки. Це дозволяє приймати запобіжні заходи та підготовленість до можливих кіберзагроз.

Важливість інтелектуальних систем у сфері кібербезпеки визначається їхньою здатністю забезпечувати швидке та ефективне виявлення, аналіз та реагування на кіберзагрози, сприяючи загальній стійкості та безпеці інформаційного середовища.

В сучасному цифровому середовищі важливість інтелектуальних систем у сфері кібербезпеки надзвичайно висока. Ці системи виконують ключову роль у забезпеченні ефективного виявлення, аналізу та захисту від кіберзагроз. Одним із основних аспектів важливості інтелектуальних систем є їхня здатність негайно реагувати на кіберзагрози та адаптувати свої алгоритми для виявлення нових атак.

Аналіз великої кількості даних, який здійснюють інтелектуальні системи, дозволяє ідентифікувати потенційні загрози та вживати заходів для їх попередження навіть до початку конкретної атаки. Це сприяє зменшенню ризику та впливу кіберзагроз на інформаційні ресурси.

Використання інтелектуальних систем у кібербезпеці також призводить до ефективної оптимізації процесів захисту інформаційних ресурсів, що дозволяє зменшити витрати на управління кібербезпекою та відновлення після атак. У кіберпросторі, насиченому різноманітними загрозами, це стає надзвичайно важливим для підтримки стійкості та безпеки.

Інтелектуальні системи забезпечують комплексний аналіз ситуації, враховуючи не лише окремі атаки, а й взаємодію з іншими складовими

інфраструктури. Це сприяє створенню повноцінних стратегій управління ризиками та вчасному реагуванню на загрози.

Застосування інтелектуальних систем також сприяє розробці прогностичних моделей, які дозволяють передбачати можливі майбутні загрози та визначати ефективні стратегії кіберзахисту. Такий підхід є важливим для побудови стійких та інноваційних рішень у сфері кібербезпеки.

Їхня здатність реагувати в реальному часі на кіберзагрози визначається їх аналітичними здібностями та здатністю до адаптації. Миттєва реакція на аномальну активність та невідповідності стандартним зразкам дозволяє ефективно виявляти та усувати загрози до виникнення значних збитків чи втрат.

Складна аналітика інтелектуальних систем допомагає розуміти структуру та характер кіберзагроз, що важливо для комплексного аналізу ситуації та формування цілісних стратегій кібербезпеки. Використання таких систем дозволяє мінімізувати вплив кібератак, оскільки вони оперативно виявляють та реагують на загрози, сприяючи обмеженню збитків.

Важливим фактором виступає також їхня здатність до створення прогностичних моделей, що дозволяють передбачати можливі майбутні загрози та визначати стратегії кіберзахисту. Такий підхід виявляється критичним для розробки стійких та інноваційних рішень у сфері кібербезпеки.

Важливість інтелектуальних систем у сфері кібербезпеки необхідно розглядати у контексті їхньої багатосторонньої взаємодії з іншими компонентами інфраструктури. Ця взаємодія охоплює співпрацю з мережевими елементами, антивірусними програмами, моніторинговими системами та іншими складовими кібербезпеки для створення комплексного захисту. Зазначається, що взаємодія цих систем визначає їхню ефективність та важливість для сфери кібербезпеки в цілому.

Паралельно із цим, важливо розглянути етичні аспекти використання інтелектуальних систем у кібербезпеці. Це включає питання прозорості, конфіденційності та можливості зловживання такими технологіями. Наголошується на необхідності етичного застосування цих технологій для забезпечення довіри та безпеки.

Додатково, слід вказати на конкретні галузі, де інтелектуальні системи вже успішно використовуються для кібербезпеки, такі як фінансовий сектор, медична сфера та промисловість. Це демонструє широкий спектр можливостей цих систем у різних контекстах та надає конкретних прикладів їхнього впливу.

Зосередження на можливостях навчання та адаптації інтелектуальних систем, їх здатність вдосконалювати алгоритми відповіді на нові загрози та змінюючіся умови, робить їх динамічним інструментом кібербезпеки. Також слід розглянути вплив на бізнес-процеси, зменшення ризиків та витрат на забезпечення кібербезпеки в організаціях.

Важливим аспектом є взаємодія інтелектуальних систем з людьми, яка може включати виявлення загроз та надання рекомендацій для прийняття рішень. Це підкреслює роль цих систем у впровадженні більшій кількості сторін у процесах кібербезпеки та створенні дієвих стратегій.

В заключенні, важливість інтелектуальних систем у кібербезпеці проявляється в їхній здатності швидко та ефективно виявляти, аналізувати та реагувати на кіберзагрози. Ці системи стають важливим інструментом для забезпечення безпеки та стійкості в інформаційному просторі, де вимоги до захисту від кіберзагроз надзвичайно високі.

Інтелектуальні системи є ключовим елементом в забезпеченні ефективності та стійкості сучасної кібербезпеки. Їхню роль можна розглядати з різних перспектив, враховуючи основні аспекти їхнього внеску у забезпечення інформаційної безпеки.

Аналіз та виявлення загроз стають більш ефективними завдяки використанню інтелектуальних систем, які використовують алгоритми машинного навчання та аналізують великі обсяги даних для точного виявлення аномалій. Це дозволяє реагувати на потенційні загрози миттєво, запобігаючи можливим атакам та забезпечуючи безпеку інформаційних ресурсів.

Важливою характеристикою інтелектуальних систем є їхня здатність реагувати в реальному часі на кіберзагрози. Швидкість реакції та аналізу дозволяє їм ефективно виявляти та усувати загрози до виникнення значних збитків чи втрат.

Співпраця та обмін інформацією між інтелектуальними системами створюють спільний фронт для протидії кіберзагрозам. Це поліпшує загальну кібербезпеку шляхом ефективного використання інформації та координації заходів захисту.

Створення інтелектуальних стратегій кібербезпеки є ще однією важливою функцією цих систем. Вони використовують аналітичні дані та інсайти для планування оптимальних заходів захисту, розробляючи цілісні підходи, які враховують різноманітні аспекти кіберзагроз.

Оптимізація заходів захисту інформаційних ресурсів стає легшою завдяки використанню інтелектуальних систем у кібербезпеці. Це дозволяє ефективно використовувати ресурси та мінімізувати витрати на управління кібербезпекою.

В цілому, інтелектуальні системи відіграють визначальну роль у підвищенні кібербезпеки, забезпечуючи швидке виявлення та реагування на кіберзагрози, забезпечуючи стійкість інформаційного середовища та підтримуючи загальну безпеку інформаційних ресурсів.

Інтелектуальні системи також відіграють важливу роль у вдосконаленні процесу реагування на кіберзагрози через використання розуміючих алгоритмів та навчання на основі досвіду. Це дозволяє системам навчатися на ходу, адаптуючи свої стратегії та методи захисту до постійно змінюючогося ландшафту кіберзагроз.

Застосування інтелектуальних систем в кібербезпеці є необхідністю в умовах розвитку нових методів атак та появи продвинутих загроз. Їхні аналітичні та прогностичні можливості дозволяють побудувати більш гнучкі та реактивні стратегії відповіді на кіберзагрози.

Ще однією важливою функцією інтелектуальних систем у кібербезпеці є створення прогностичних моделей. За допомогою аналізу великих обсягів даних вони можуть передбачати можливі майбутні кіберзагрози, що надає можливість приймати ефективні запобіжні заходи та підготовити інфраструктуру до можливих атак.

Такий комплексний підхід до кібербезпеки залежить від інтеграції інтелектуальних систем у всі аспекти захисту інформаційних ресурсів. Вони не

лише виявляють та реагують на загрози, але й активно співпрацюють для створення більш сильних та витончених стратегій захисту.

Цей підхід до кібербезпеки, заснований на інтелектуальних системах, дозволяє створити адаптивне та ефективне середовище захисту від кіберзагроз, де вчасна реакція, аналіз та прогнозування є важливими складовими для забезпечення безпеки та стійкості.

Інтелектуальні системи активно залучаються до аналізу великого обсягу даних для виявлення найтонших аномалій та невідповідностей, які можуть свідчити про кіберзагрози. Це важливо не лише для реакції на вже існуючі загрози, але й для попередження майбутніх атак.

Однією з ключових переваг інтелектуальних систем у кібербезпеці є їхній потенціал виявляти та аналізувати нові, раніше невідомі типи загроз. Такий підхід є критично важливим у світі швидкого розвитку кіберзлочинності, де атаки надходять у нових формах та варіантах.

Крім того, інтелектуальні системи сприяють ефективному виявленню та аналізу цільованих атак, спрямованих на конкретні об'єкти або організації. Їхні алгоритми можуть розпізнавати характеристики цільованих атак, що допомагає забезпечити додатковий рівень захисту для об'єктів з високим ризиком.

Інтелектуальні системи також відіграють важливу роль у виявленні та аналізі "нульових днів" – вразливостей, які стають відомими вперше тільки під час атаки. Їхні алгоритми здатні виявляти патерни та невідповідності, що свідчать про використання невідомих вразливостей.

Таким чином, інтелектуальні системи в кібербезпеці є не лише інструментом для реакції на вже існуючі загрози, але і активним учасником в пошуку та виявленні нових, раніше невідомих видів кіберзагроз. Вони грають визначальну роль у підтримці стійкості та безпеки в умовах постійно зростаючого ризику в кіберпросторі.

Інтелектуальні системи у кібербезпеці також важливі для розробки та вдосконалення технологій ідентифікації та аутентифікації. Вони можуть використовувати біометричні дані, поведінковий аналіз та інші аспекти для

надійної перевірки ідентичності користувачів та виявлення спроб несанкціонованого доступу.

Підвищення кібербезпеки також відбувається через використання інтелектуальних систем у сфері кібергігієни. Вони виявляють шкідливі програми, фішингові атаки та інші види шахрайства, що спрямовані на зловживання інформаційно-комунікаційними технологіями.

Крім того, інтелектуальні системи забезпечують аналіз трафіку та виявлення аномалій в мережі, що дозволяє ефективно виявляти та блокувати потенційно небезпечний зміст чи комунікації, що містять загрози для кібербезпеки.

Важливою аспектом їхньої ролі є також взаємодія з іншими складовими систем безпеки, такими як системи виявлення вторгнень (IDS), файерволи та антивіруси. Ця взаємодія сприяє створенню комплексних та повноцінних стратегій кіберзахисту.

Таким чином, інтелектуальні системи не лише виявляють загрози та реагують на них, але і глибоко інтегруються в інфраструктуру кібербезпеки, забезпечуючи багатоплановий та комплексний підхід до захисту інформаційних ресурсів. Їхні можливості виявлення нових загроз, аналізу та вдосконалення стратегій кібербезпеки роблять їх ключовим елементом сучасного кіберпростору.

1.3 Огляд існуючих інтелектуальних систем

Інтелектуальні системи виявлення загроз у сфері кібербезпеки є ключовим елементом сучасного оборонного комплексу. Огляд існуючих систем дозволяє краще зрозуміти їх функції, можливості та обмеження.

Системи виявлення вторгнень (IDS) відіграють ключову роль у забезпеченні кібербезпеки, надаючи засоби для виявлення та відстеження неавторизованих або шкідливих дій у мережі. Ці системи можуть бути розділені на дві основні категорії: системи виявлення вторгнень на основі сигнатур та системи аналізу поведінки.

Системи виявлення вторгнень на основі сигнатур це системи, які використовують підписи або сигнатури для ідентифікації вже відомих загроз. Якщо

трафік або активність збігається із відомими сигнатурами, система вважає це можливим вторгненням. Прикладами є Snort та Suricata.

Системи виявлення вторгнень на основі аналізу поведінки оцінюють поведінку систем та користувачів, шукаючи аномалії, які можуть свідчити про потенційні загрози. Вони використовують алгоритми машинного навчання та статистичний аналіз для виявлення нових та невідомих загроз.

Системи виявлення вторгнень є необхідним компонентом комплексної стратегії кібербезпеки, надаючи здатність оперативно реагувати на загрози та запобігати можливим атакам. Інтеграція інтелектуальних систем у ці процеси дозволяє покращити ефективність виявлення та відповіді на кіберзагрози.

Викликами та тенденціями в розвитку систем виявлення вторгнень є збільшення обсягу даних, адаптація до нових загроз, виявлення невідомих атак.

З великим обсягом мережевого трафіку та системних журналів системам IDS важко ефективно працювати без використання інтелектуальних методів обробки даних. Інтелектуальні системи дозволяють системам IDS бути більш гнучкими та швидше адаптуватися до нових видів кіберзагроз. Машинне навчання дозволяє IDS виявляти атаки, які не мають відомих сигнатур, забезпечуючи важливий етап захисту від нових загроз.

У деяких системах IDS використовуються алгоритми глибокого навчання, які можуть аналізувати складні зв'язки та шаблони у великих обсягах даних. Це дозволяє виявляти навіть найвитонченіші та непомічені раніше атаки, забезпечуючи підвищений рівень кібербезпеки.

Системи виявлення вторгнень з інтелектуальним підходом виявляються надзвичайно корисними для забезпечення кібербезпеки. Їх здатність адаптуватися до нових загроз, виявлення невідомих атак і зменшення кількості помилкових спрацьовувань робить їх ефективним інструментом в сфері кіберзахисту.

Інтелектуальні Системи Запобігання Вторгнень (IPS) відіграють ключову роль у сфері кібербезпеки, забезпечуючи ефективний захист мережевих інфраструктур від різноманітних загроз. Системи IPS виявляють та запобігають вторгненням до комп'ютерних систем та мереж, використовуючи різні методи та

технології. Основні аспекти їхньої функціональності включають: сигнатурний аналіз, аномальний аналіз, захист від невідомих атак, проактивна аналітика та інтеграція з іншими системами.

Інтелектуальні системи запобігання вторгнень (IPS) є важливою складовою кібербезпекової архітектури, яка призначена для виявлення та запобігання різноманітним загрозам у мережевому середовищі. Основною метою IPS є захист мережі від несанкціонованого доступу, атак та інших кіберзагроз.

Ці системи використовують різноманітні методи виявлення, такі як аналіз пакетів даних, використання сигнатур для ідентифікації відомих атак, та аналіз поведінки для виявлення аномальних активностей. Інтеграція технологій глибокої інспекції пакетів (DPI) дозволяє IPS проводити детальний аналіз вмісту пакетів, що забезпечує виявлення та блокування важливого спектру загроз.

Однією з ключових переваг IPS є їхня здатність реагувати в реальному часі на потенційні атаки, надаючи миттєвий захист від загроз. Постійне оновлення сигнатур та правил дозволяє цим системам ефективно протистояти новим видам загроз, що постійно еволюціонують. Інтеграція з системами журналювання та аналітики (SIEM) дозволяє агрегувати дані та сповіщати про події на рівні всієї мережі.

IPS є необхідною складовою для забезпечення комплексного кіберзахисту, доповнюючи інші заходи безпеки та забезпечуючи протидію загрозам в режимі реального часу.

Сучасні системи IPS можуть ефективно використовувати алгоритми машинного навчання для розпізнавання атак, що використовують нестандартні методи або покладаються на аномальну поведінку.

Інтелектуальні системи виявлення вторгнень (IDS) та інтелектуальні системи запобігання вторгнень (IPS) є ключовими елементами кібербезпекового ландшафту, але вони виконують різні завдання та мають відмінності в поведінці.

Таблиця 1.1 – Різниця в Поведінці IDS та IPS Систем

№	Різниця	IDS	IPS
1	Задачі	Основною задачею IDS є виявлення аномальних або зловживальних дій у мережі. Вони генерують сповіщення або журнали про виявлені загрози, але не блокують трафік.	У відміну від IDS, IPS вживають заходів для запобігання або миттєвого реагування на виявлені загрози. Вони можуть блокувати або відхиляти трафік, що містить потенційну загрозу.
2	Реакція на загрози	IDS ідентифікує атаки, але його роль обмежена відправкою або журналуванням повідомлень про виявлені загрози.	IPS може автоматично вживати заходів для припинення атак, блокуючи або відхиляючи трафік, що містить загрозу.
3	Дозвіл та блокування	IDS не має можливості блокувати трафік або втручатися у мережевий обмін.	IPS може вживати заходів для блокування або відхилення трафіку, що допомагає негайно реагувати на атаки.
4	Ризики та переваги	IDS дозволяє виявляти атаки без блокування легітимного трафіку, але не забезпечує миттєвого реагування.	IPS може швидко реагувати на загрози, але може призвести до блокування легітимного трафіку, що може вплинути на нормальну роботу мережі.

Розуміння цієї різниці є ключем до правильного вибору та впровадження систем виявлення та запобігання вторгнень в залежності від потреб конкретної організації.

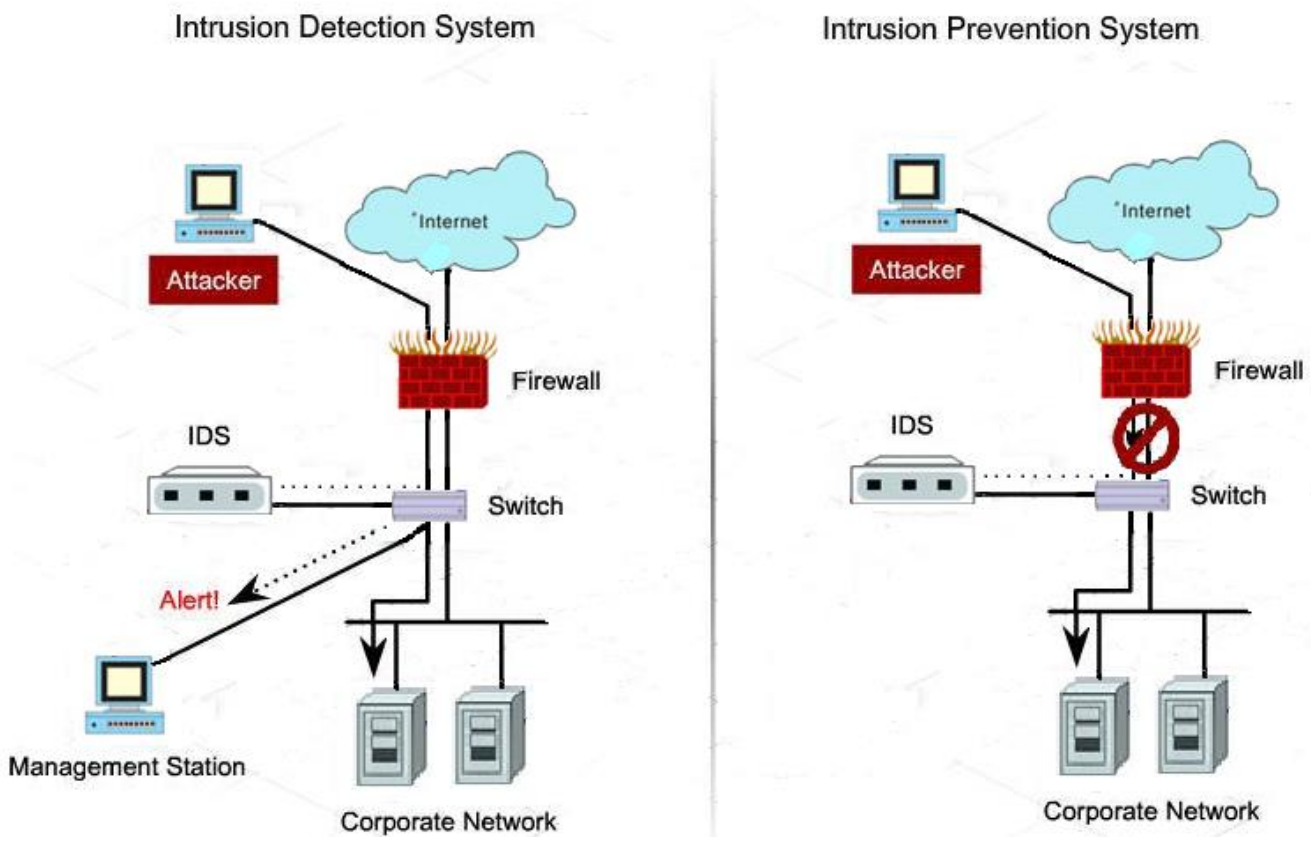

Рисунок 1.1 – Різниця в поведінці IDS та IPS систем

Системи аналізу журналів (SIEM) представляють собою важливий елемент в сфері кібербезпеки, забезпечуючи об'єднання та аналіз журнальних даних з різних джерел в реальному часі. SIEM використовується для виявлення та реагування на кіберзагрози та має наступні ключові характеристики:

SIEM автоматично збирає та аналізує журнальні дані з різних джерел, таких як сервери, мережеві пристрої, додатки та файли журналів. Кореляція даних дозволяє ідентифікувати зв'язки та шаблони між різними подіями, сповіщаючи про можливі загрози.

SIEM використовує аналіз поведінки та евристичні методи для виявлення аномальних подій або несподіваного змін у мережевому трафіку.

Система сповіщень SIEM надає інформацію про виявлені загрози та аномалії. Деякі SIEM можуть автоматично запускати заходи для реагування на ідентифіковані загрози.

SIEM веде журнали аудиту для відстеження та аналізу подій у випадку інцидентів, допомагаючи у вивченні та реагуванні на інциденти шляхом надання цілісної картини ситуації. Може інтегруватися з іншими системами кібербезпеки, такими як IDS, IPS, антивірусні програми та системи управління інцидентами, що створює комплексну систему безпеки для організацій.

SIEM відіграє ключову роль у виявленні та відповіді на інциденти безпеки, сприяючи покращенню реакції на загрози та забезпечуючи великий обсяг корисної інформації для аналізу.

Таблиця 1.2 - деякі додаткові аспекти SIEM

№	Аспект	SIEM
1	Кореляція даних	SIEM використовує механізми кореляції для об'єднання та аналізу різних типів журнальних подій. Це дозволяє виявляти складні атаки, які можуть залишати сліди в різних системах.
2	Аналіз поведінки	Деякі сучасні SIEM використовують аналіз поведінки для виявлення змін у звичайних паттернах роботи систем та користувачів, що може вказувати на атаку або компрометацію.
3	Інтеграція з Threat Intelligence	SIEM може інтегруватися з зовнішніми джерелами Threat Intelligence, щоб оновлювати бази даних ідентифікаторів загроз і виявляти нові типи атак.
4	Автоматизована реакція	Системи SIEM можуть автоматично запускати засоби захисту або вживати інші заходи реакції відповідно до зазначених правил.
5	Аудит та звітність	SIEM дозволяє вести аудит подій, а також генерувати звіти, які можуть бути використані для аналізу діяльності, дотримання стандартів безпеки та взаємодії з регуляторами.

Загалом, SIEM є потужним інструментом для кібербезпеки, який допомагає організаціям ефективно виявляти та вирішувати інциденти, забезпечуючи комплексний погляд на стан безпеки інформації.

UEBA (User and Entity Behavior Analytics) - це підхід до кібербезпеки, який використовує аналіз поведінки користувачів та сутностей для виявлення потенційних загроз безпеки. Системи Аналізу Поведінки Кібербезпеки (UEBA)

виявляють та аналізують аномальні зміни у поведінці користувачів та систем для виявлення потенційних загроз безпеки.

Таблиця 1.2 - деякі аспекти та функції UEBA

№	Аспект	UEBA
1	Моделювання поведінки	Створює базові профілі для користувачів та систем, використовуючи машинне навчання та аналіз історичних даних. Це дозволяє системі розпізнавати типові патерни поведінки.
2	Виявлення аномалій	UEBA аналізує поточну поведінку користувачів та систем і порівнює її з їх звичайними зразками. Якщо виявляються невідповідності або аномалії, система може сповістити адміністратора про потенційну загрозу.
3	Контекстуальний аналіз	UEBA враховує контекстні фактори, такі як час доби, географічне розташування та тип пристрою, щоб краще зрозуміти та фільтрувати події, зменшуючи кількість фальшивих позитивів.
4	Інтеграція з іншими рішеннями	Може інтегруватися з іншими системами кібербезпеки, такими як SIEM, для обміну інформацією та координації заходів з відповіді на інциденти.
5	Системи аналізу загроз	Може використовувати бази даних про загрози для виявлення і аналізування підозрілих дій або інцидентів, пов'язаних із відомими типами загроз.
6	Моніторинг привілеїв	Виявляє надмірні або неочікувані зміни привілеїв користувачів, що може свідчити про несанкціонований доступ або компрометацію облікових записів.

UEBA стає все більше важливим компонентом стратегій кібербезпеки, оскільки вона дозволяє організаціям активно виявляти загрози та реагувати на них до того, як завдано значні шкоди. Аналіз поведінки користувачів та сутностей, є стратегією кібербезпеки, що базується на вивченні та аналізі поведінки користувачів та інших об'єктів в інформаційних системах. В основі UEBA лежить використання методів машинного навчання для створення моделей поведінки, які дозволяють виявляти аномалії та потенційні загрози безпеки.

Однією з ключових характеристик UEBA є використання алгоритмів машинного навчання для створення профілів нормальної поведінки користувачів та сутностей. Ці моделі дозволяють системі розрізняти звичайні патерни

використання від аномалій, вчаться на основі активності та адаптуються до змін у середовищі.

UEBA виявляє аномалії шляхом аналізу дій та подій, які виходять за межі звичайних зразків. Це може включати в себе невідомий доступ до ресурсів, зміну звичайних робочих звичок або інші незвичайні активності. Використовуючи цей підхід, UEBA дозволяє виявляти загрози, які можуть залишитися непоміченими за допомогою традиційних методів захисту.

Основна перевага використання UEBA полягає в здатності виявляти нові, раніше невідомі загрози, а також в підвищенні точності та швидкості виявлення аномалій у порівнянні з традиційними методами.

ATD (Automated Threat Detection) представляють собою інтегровані рішення в галузі кібербезпеки, спрямовані на виявлення та аналіз загроз в інформаційних системах. Основна мета ATD полягає в автоматизації процесу виявлення та реагування на потенційні кіберзагрози.

ATD використовує різні методи та техніки для аналізу активності в мережі та системі. Однією з ключових функцій є використання розумних алгоритмів для ідентифікації аномальної поведінки та виявлення нових загроз. Ці системи часто використовують технології машинного навчання для вдосконалення аналітики та здатності виявляти еволюцію кіберзагроз.

Однією з переваг ATD є здатність виявляти загрози, які можуть бути неочевидними та важкими для виявлення традиційними методами. Також, вони можуть автоматично реагувати на виявлені загрози, спрощуючи завдання кібербезпеки для організацій. Важливою характеристикою ATD є його інтеграція з іншими системами кібербезпеки, такими як системи аналізу журналів та інші інструменти, щоб забезпечити повний огляд та відслідковування загроз в інформаційному середовищі.

Системи автоматизованого виявлення загроз визначаються своєю здатністю виявляти загрози в інформаційних системах за допомогою автоматизованих процесів та розширених аналітичних засобів. Основна функція ATD полягає в

тому, щоб виявляти аномальну або небезпечну активність, яка може вказувати на потенційні загрози безпеці.

Таблиця 1.3 - деякі аспекти та функції ATD

№	Аспект	ATD
1	Моніторинг мережі та систем	ATD веде постійний моніторинг активності в мережі та інформаційних системах для виявлення аномалій та незвичайної поведінки.
2	Виявлення загроз	Системи ATD використовують розумні алгоритми та механізми аналізу для ідентифікації потенційно небезпечної активності, яка може вказувати на наявність загроз.
3	Використання машинного навчання	Технології машинного навчання застосовуються для покращення аналітики та розпізнавання нових та еволюційних загроз.
4	Автоматизована реакція	ATD може автоматично реагувати на виявлені загрози, забезпечуючи швидку та ефективну відповідь.
5	Інтеграція з іншими системами	Ці системи легко інтегруються з іншими інструментами кібербезпеки, такими як IDS (Системи Виявлення Вторгнень), SIEM (Системи Управління Інформаційною Безпекою та Подіями), для створення комплексного заходу забезпечення безпеки.

Завдяки цим функціям ATD допомагає організаціям виявляти та вирішувати кіберзагрози шляхом швидкого реагування та застосування заходів безпеки.

2 ВПЛИВ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ НА ЕФЕКТИВНІСТЬ НАЦІОНАЛЬНОЇ КІБЕРОБОРОНИ

2.1. Застосування інтелектуальних систем у виявленні та аналізі кіберзагроз

Сучасне безпекове середовище невперше стикається із стрімкими технологічними змінами, які обумовлюють потребу у подальшому розвитку та посиленні спроможностей системи кібербезпеки. Згідно з "Стратегією забезпечення державної безпеки", однією з основних цілей державної політики у цій сфері є ефективна протидія кіберзагрозам. В цьому контексті особливою увагою визначається гнучка адаптація національної системи кібербезпеки до швидко змінюючогося цифрового середовища.

Однією з ключових стратегічних цілей є гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, як зазначено в "Стратегії національної безпеки України". В умовах цифрової трансформації важливо оптимізувати координацію суб'єктів системи кібербезпеки та забезпечити доступ до державних електронних ресурсів та інформаційних систем.

Це наголошує на необхідності розвитку та впровадження інтелектуальних систем виявлення та аналізу кіберзагроз. Зокрема, у "Стратегії кібербезпеки України" зазначено, що розширення кола держав, які зацікавлені в кіберрозвідці, підкреслює необхідність формування більш збалансованої та ефективної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища.

Щоб забезпечити ефективне функціонування інтелектуальних систем у виявленні та аналізі кіберзагроз, важливо створити ефективну систему обміну інформацією між суб'єктами забезпечення державної безпеки, як це визначено в "Стратегії забезпечення державної безпеки". Така система повинна включати механізми швидкого виявлення та реагування на кіберзагрози.

Важливим завданням є розробка системи раннього виявлення, прогнозування та запобігання гібридним загрозам, включаючи дезінформацію та інформаційні операції, як це визначено в "Стратегії інформаційної безпеки". Такий підхід

дозволяє ефективно протидіяти сучасним методам атак в інформаційному просторі, спрямованим на дестабілізацію національної безпеки.

Для підвищення ефективності інтелектуальних систем важливо вдосконалювати спроможності складових сил оборони щодо протидії загрозам в інформаційному просторі, зокрема за допомогою сучасних технологій розвідки та логістики. Враховуючи потужний розвиток кіберзагроз, забезпечення безпеки в цифровому просторі стає важливим аспектом національної безпеки, як стверджує "Стратегія кібербезпеки України".

Впровадження інтелектуальних систем у виявленні та аналізі кіберзагроз є стратегічним кроком для гарантування кіберстійкості та забезпечення ефективної кібербезпеки національного інформаційного простору. Застосування сучасних технологій у цій сфері дозволяє адаптуватися до швидкозмінюваного цифрового середовища та забезпечує нові можливості для цифровізації різних галузей суспільства.

Дієвість інтелектуальних систем у виявленні кіберзагроз може бути підтримана розвитком системи протидії дезінформації та інформаційним операціям, як це передбачено в "Стратегії інформаційної безпеки". Це включає в себе не лише виявлення штучно створеної інформації, але й розробку ефективних методів її стримування та запобігання.

Розвиток спеціалізованих сил оборони щодо протидії загрозам в інформаційному просторі, визначений в "Стратегії інформаційної безпеки", стає ключовим завданням для забезпечення безпеки в цифровому середовищі. Це включає удосконалення та розвиток систем управління, телекомунікацій та розвідки, спрямовані на ефективне виявлення та протидію кіберзагрозам.

Застосування інтелектуальних систем у виявленні та аналізі кіберзагроз також сприяє реалізації стратегічних завдань, визначених у "Стратегії кібербезпеки України". Зокрема, це охоплює забезпечення кіберстійкості національної інформаційної інфраструктури та адаптацію до змін безпекового середовища.

Враховуючи швидкі технологічні зміни та загрози в сфері кібербезпеки, ефективне використання інтелектуальних систем у виявленні та аналізі кіберзагроз

стає необхідною передумовою для гарантування безпеки та обороноздатності України в цифровому віці.

Важливою складовою ефективної стратегії виявлення та аналізу кіберзагроз є розробка та впровадження систем раннього виявлення. Це вимагає створення інтелектуальних алгоритмів, спроможних вчасно розпізнавати непередбачувані та нові форми кіберзагроз, забезпечуючи вчасне реагування на них.

Розглядаючи "Стратегію кібербезпеки України", слід враховувати потребу в гнучких системах адаптації до змін безпекового середовища. Це передбачає навчання інтелектуальних систем, використовуючи нейронні мережі та машинне навчання, щоб вони могли ефективно взаємодіяти з новими формами кіберзагроз та швидко адаптуватися до їхніх еволюційних змін.

Зазначена у "Стратегії інформаційної безпеки" необхідність створення системи протидії дезінформації та інформаційним операціям вимагає розробки інтелектуальних агентів, які здатні визначати та фільтрувати дезінформацію, а також виявляти джерела та поширювачі неправдивої інформації.

Загальна ефективність інтелектуальних систем у виявленні та аналізі кіберзагроз буде залежати від тісного співробітництва з органами кібербезпеки, державними структурами та приватним сектором. Спільні зусилля у розробці та впровадженні передових технологій гарантують створення інтегрованих та комплексних підходів до кібербезпеки національного інформаційного простору.

2.2. Роль та ефективність інтелектуальних систем у реагуванні на кібератаки та забезпеченні кіберстійкості

Інтелектуальні системи відіграють важливу роль у забезпеченні кіберстійкості та реагуванні на кібератаки, враховуючи прогресивний характер кіберзагроз у сучасному цифровому середовищі. Інтеграція технологій штучного інтелекту у цей контекст може бути вирішальною для виявлення та усунення загроз на ранніх етапах.

Відповідно до "Стратегії кібербезпеки України", інтелектуальні системи

повинні бути спрямовані на удосконалення кіберзахисту та ефективного взаємодії зі складовими силами оборони. Забезпечення кіберстійкості передбачає розвиток інтелектуальних алгоритмів, які здатні визначати та контролювати кіберзагрози у режимі реального часу.

В контексті "Стратегії інформаційної безпеки", інтелектуальні системи можуть бути використані для реагування на дезінформацію та інформаційні операції. Їхня роль полягає в аналізі великих обсягів даних, виявленні шаблонів дезінформації та вчасному розпізнаванні фейкових новин.

Інтелектуальні системи також можуть відігравати ключову роль у виявленні та нейтралізації кібератак, що визначено у "Стратегії воєнної безпеки України". Використання механізмів машинного навчання та аналізу великих обсягів даних дозволяє швидко реагувати на нові методи атак та розвивати стратегії кібероборони.

За словами доктора юридичних наук, професора Ніно Пацурія, "ШІ може допомогти в зборі та аналізі великих обсягів даних, що забезпечує більш швидкий та точний аналіз інформації, скорочуючи час, необхідний для прийняття рішення."

Згідно з "Стратегією розвитку оборонно-промислового комплексу України", важливим аспектом є реалізація інтегрованих рішень, які поєднують в собі кібербезпеку та захист від кібератак. Інтелектуальні системи можуть автоматизувати процеси виявлення, аналізу та реагування на кіберзагрози, забезпечуючи більш ефективну кібероборону.

Інтеграція інтелектуальних систем у військово-технічний комплекс, як визначено у "Стратегії розвитку оборонно-промислового комплексу України", відкриває можливості для розробки передових технологій кібероборони та посилення кіберстійкості Збройних Сил.

Інтелектуальні системи виконують ключову роль у впровадженні високоефективних стратегій реагування на кібератаки та забезпеченні кіберстійкості. Згідно з загальною концепцією кібербезпеки, їхнє застосування ускладнюється високим ступенем складності та різноманітністю кіберзагроз.

Інтелектуальні системи виявлення загроз у сфері кібербезпеки взаємодіють із

системами аналізу великих даних, щоб вчасно виявляти навіть найтонші аномалії та атаки в мережі. Вони базуються на алгоритмах машинного навчання, які, адаптуючись до змін у підходах кіберзлочинців, забезпечують сталу ефективність систем виявлення.

Роль інтелектуальних систем у реагуванні на кібератаки полягає в автоматизації процесів виявлення та аналізу відмінностей у поведінці мережі. Вони не лише виявляють потенційні загрози, але і надають операторам докладну інформацію для ефективного реагування. Це дозволяє зменшити час реакції та мінімізувати збитки внаслідок кібератак.

У забезпеченні кіберстійкості інтелектуальні системи грають важливу роль у виявленні вразливостей та удосконаленні заходів безпеки. Вони можуть аналізувати потенційні ризики та надавати рекомендації для вдосконалення систем безпеки, що допомагає попереджати можливі атаки та забезпечує стійкість до нових загроз.

Застосування інтелектуальних систем у виявленні та аналізі кіберзагроз є стратегічно важливим для національної кібербезпеки, дозволяючи ефективно протидіяти сучасним та майбутнім кіберзагрозам.

Однією з ключових функцій є виявлення кіберзагроз на ранніх етапах, навіть до того, як вони завдають значних збитків. Завдяки алгоритмам машинного навчання та аналізу великих обсягів даних, інтелектуальні системи здатні ідентифікувати невідомі та важкозасікливі атаки, забезпечуючи забезпечення ефективної реакції.

Ще однією важливою характеристикою ролі інтелектуальних систем у реагуванні на кібератаки є їхня здатність до автоматичної адаптації та вдосконалення. Це означає, що вони можуть навчатися на основі нових даних та аналізувати нові варіанти загроз, що з'являються. Такий підхід дозволяє інтелектуальним системам підтримувати високий рівень ефективності в умовах постійно змінюючихся кіберзагроз.

Крім того, інтелектуальні системи сприяють удосконаленню системи кіберстійкості. Вони можуть аналізувати структуру та вразливості інформаційних

систем, рекомендуючи та впроваджуючи заходи щодо підвищення безпеки. Це включає в себе не лише виявлення потенційних атак, але й розробку стратегій їх запобігання.

Таким чином, роль інтелектуальних систем у реагуванні на кібератаки та забезпеченні кіберстійкості полягає в їхній здатності виявляти, аналізувати та ефективно протидіяти кіберзагрозам, забезпечуючи оптимальний рівень захисту інформаційних ресурсів.

Ефективність використання інтелектуальних систем у вирішенні завдань національної кібербезпеки проявляється в кількох ключових аспектах.

Інтелектуальні системи виявляються важливим інструментом для аналізу та виявлення кіберзагроз. Їх здатність ефективно обробляти великі обсяги кіберінформації дозволяє виявляти потенційні загрози та вчасно реагувати на них.

У протидії кібератакам інтелектуальні системи використовують алгоритми машинного навчання та аналізу великих даних для розпізнавання та аналізу сучасних кіберзагроз. Це дозволяє ефективно виявляти атаки та розробляти стратегії протидії.

Застосування інтелектуальних систем сприяє автоматизації процесів у сфері національної кібербезпеки. Вони використовуються для виявлення аномалій та невідповідностей, що допомагає вчасно реагувати на події та запобігати можливим загрозам.

За висновками дослідження, опублікованого в статті "Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України", "ШІ може допомогти в автоматизації багатьох процесів у сфері оборони, зменшуючи ризик помилок та підвищуючи ефективність. "Також, "ШІ може бути використаний для розроблення та вдосконалення зброї, що забезпечить перевагу військам на полі бою. "

Інтелектуальні системи здобувають визнання як ключовий елемент в забезпеченні національної кібербезпеки. Згідно з дослідженням, проведеним у статті "Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України", вони виявляються дієвим інструментом у

вирішенні завдань цієї критично важливої галузі. Зокрема, висвітлено такі аспекти:

Аналіз і виявлення загроз: інтелектуальні системи відзначаються високою точністю та швидкістю аналізу великих обсягів кіберпростору. "ШІ може допомогти в зборі та аналізі великих обсягів даних, що забезпечує більш швидкий та точний аналіз інформації, скорочуючи час, необхідний для прийняття рішення," як зазначено в зазначеній статті.

Виявлення та протидія кібератакам: інтелектуальні системи виявляються дієвим інструментом у виявленні та протидії кібератакам. "Застосування ШІ може допомогти у попередженні катастроф та мінімізації ризиків для військового персоналу, забезпечуючи безпеку та захист держави," як відзначено у висновках згаданої статті.

Ефективне реагування на кіберзагрози: важливим елементом ефективності інтелектуальних систем у сфері кібербезпеки є їх здатність до автоматичного реагування на кіберзагрози та прийняття відповідних заходів для їх нейтралізації.

Ці аспекти підкреслюють важливість інтеграції інтелектуальних систем у стратегії національної кібербезпеки для забезпечення ефективного виявлення, протидії та реагування на сучасні кіберзагрози.

Важливим аспектом ефективності інтелектуальних систем у вирішенні завдань національної кібербезпеки є їх роль у реагуванні на нові, раніше невідомі загрози. Інтелектуальні системи, здатні виявляти аномальні патерни та адаптуватися до нових форм кіберзагроз, сприяють оперативному реагуванню та мінімізації можливих шкідливих наслідків.

Крім того, інтелектуальні системи вирішують завдання національної кібербезпеки шляхом підвищення кіберстійкості систем та інфраструктури. Вони виявляють вразливості та розробляють стратегії для їх усунення, а також надають можливість для постійного моніторингу та оновлення заходів безпеки.

Ефективність інтелектуальних систем у вирішенні завдань національної кібербезпеки також полягає в їх здатності адаптуватися до швидкозмінюючогося кіберпростору. Автоматичне навчання та аналіз великих обсягів даних дозволяють системам штучного інтелекту швидко реагувати на нові виклики та атаки,

забезпечуючи тривалий та надійний рівень кіберзахисту.

Узагальнюючи, інтелектуальні системи виявляються необхідним інструментарієм для забезпечення ефективної кібербезпеки нації, забезпечуючи виявлення, запобігання та реагування на кіберзагрози в сучасному інформаційному середовищі.

2.3 Тенденції розвитку технологій інтелектуальних систем

Один із основних напрямків тенденцій розвитку технологій інтелектуальних систем у сфері кібербезпеки полягає в пошуку нових методів застосування машинного навчання та штучного інтелекту. Моделі глибокого навчання стають все більш точними у виявленні складних кіберзагроз, а їхні здібності аналізувати величезні об'єми даних роблять їх ефективними в ідентифікації нових векторів атак.

За оцінкою MarketsandMarkets, в 2019-2026 рр. зростання ринку засобів ШІ для забезпечення кібербезпеки буде рости в середньому на 23,3% в рік, з $ 8,8 млрд до $ 38,2 млрд.

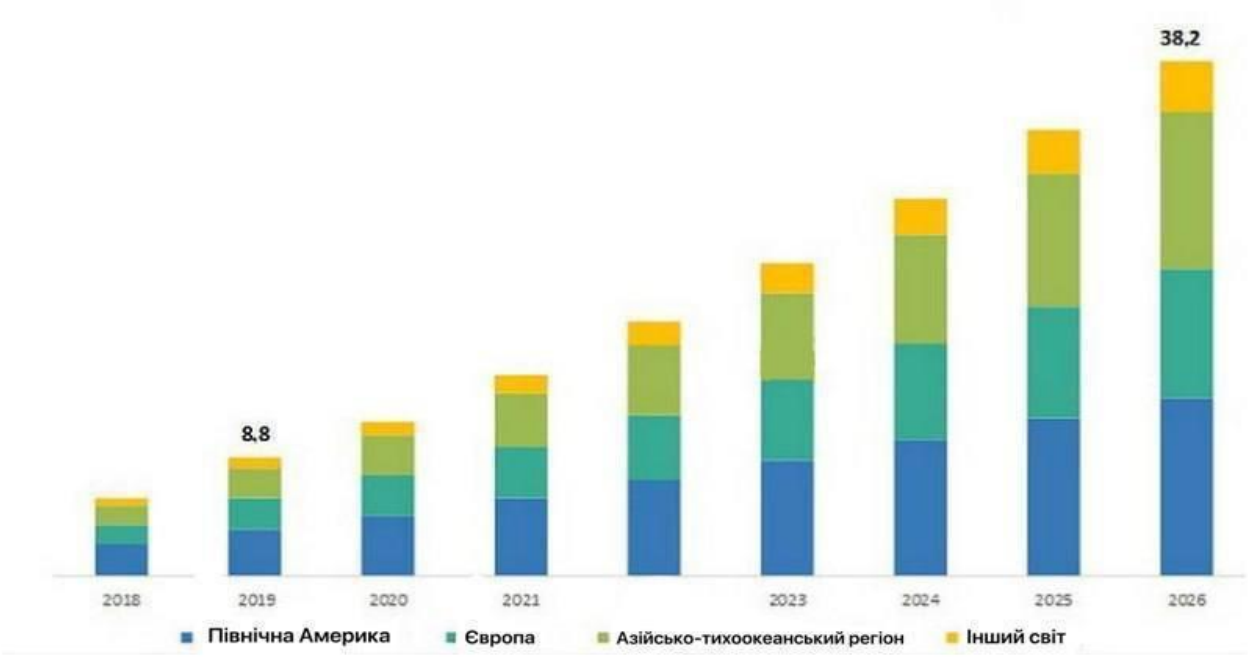

Рисунок 2.1 - Динаміка ринку засобів ШІ для кібербезпеки по регіонах, $ млрд.

З огляду на гостру нестачу досвідчених фахівців щодо забезпечення безпеки і величезні обсяги даних, з якими доводиться працювати організаціям, багато компаній вже використовують можливості штучного інтелекту (ШІ) для забезпечення кібербезпеки або планують зробити це.

Концепція "інтелектуальних хакерів" або "етичного хакінгу" стає більш поширеною. Такі спеціалісти використовують інтелектуальні системи для виявлення та усунення слабкі пункти в кіберзахисті. Вони ефективно використовують аналітику та симуляції атак для покращення систем безпеки.

Застосування квантових обчислень може стати революційним моментом у кібербезпеці. Квантові комп'ютери мають потенціал вирішувати складні математичні проблеми, на яких засновані сучасні алгоритми шифрування. Зокрема, це може вплинути на розвиток нових, стійких до квантових обчислень методів шифрування.

Зростаюча кількість підключених до мережі пристроїв у сфері Інтернету Речей (IoT) породжує нові виклики у сфері кібербезпеки. Тенденція до використання інтелектуальних систем для захисту та моніторингу цих пристроїв, а також розробка стандартів безпеки для IoT, стає все більш актуальною.

Однією з ключових тенденцій є розвиток технологій для захисту від маніпулювання алгоритмами машинного навчання. Атаки, спрямовані на зміну результатів роботи моделей штучного інтелекту, можуть бути важко виявити, тому розробка методів захисту від таких загроз є критичною.

Іншою важливою тенденцією у розвитку технологій інтелектуальних систем у сфері кібербезпеки є акцент на автоматизацію та орієнтованість на реагування в реальному часі. Розвиток систем, які можуть автоматично реагувати на виявлені загрози без значного втручання людини, стає ключовим елементом у забезпеченні ефективності кіберзахисту.

Технології обробки природної мови та аналізу текстів знаходять широке використання в інтелектуальних системах для виявлення кіберзагроз, оскільки багато атак відбувається через текстові взаємодії. Використання алгоритмів

машинного навчання для розпізнавання та класифікації загроз у текстових повідомленнях стає дедалі важливішим.

Впровадження технологій блокчейну також може внести свій внесок у забезпечення кібербезпеки. Застосування блокчейну може зробити системи більш стійкими до атак, спрямованих на зміну чи видалення даних, а також полегшити відстеження та перевірку подій у системі.

Розширення використання технологій глибокого навчання в області обнаруження загроз та реагування на них. Сучасні алгоритми можуть вивчати навіть неочікувані та важкі до узагальнення патерни атак, забезпечуючи вищу ефективність у порівнянні з традиційними методами.

Загальна тенденція до розвитку інтегрованих підходів, де різні типи інтелектуальних систем і технологій працюють разом, утворюючи комплексні рішення для забезпечення кібербезпеки, також є актуальною. Спільна робота різних систем може покращити виявлення, аналіз та реагування на кіберзагрози.

Такі тенденції свідчать про постійне вдосконалення технологій інтелектуальних систем з метою відповіді на зростаючі та еволюційні виклики у сфері кібербезпеки.

3 ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

3.1 Основні визначення

Машинне навчання - це процес, за допомогою якого машина навчається, будуючи логіку на основі заданої інформації та прогнозуючи результати на основі заданих вхідних даних. Існує три підкатегорії машинного навчання: контрольоване навчання, неконтрольоване навчання та навчання з підкріпленням. Навчання під контролем використовує набори даних і позначає правильні відповіді для навчання. Ці мітки визначають характеристики кожного набору даних. Коли модель завершує самонавчання, вона може робити прогнози і судження про нові дані і ситуації. Навчання без вчителя не потребує такого специфічного набору даних. Як тільки модель отримує набір даних, вона автоматично знаходить закономірності та взаємозв'язки і формує кластери всередині них. Однак цей тип навчання нічого не передбачає. Коли додаються нові дані, модель або відносить їх до одного з існуючих кластерів, або створює новий кластер. Навчання з підкріпленням - це здатність системи взаємодіяти з навколишнім середовищем і визначати найкращий результат.

Аналогічно, після навчання він готовий передбачати нові дані, що надходять на вхід. Глибоке навчання (ГН) - це тип алгоритму машинного навчання, який використовує кілька рівнів для поступового вилучення ознак вищого рівня з вихідних даних.

Основні відмінності між ML та ANN полягають у наступному: Алгоритми ML майже завжди вимагають структурованих даних, тоді як ANN-мережі базуються на рівні штучних нейронних мереж (ШНМ). Зазвичай ML вимагає втручання людини для досягнення більших результатів на великих масивах даних, тоді як ШНМ цього не роблять:

Одним з основних понять ML є ШНМ; ШНМ використовуються для досягнення більших результатів на великих масивах даних; ШНМ використовуються для досягнення більших результатів на великих масивах даних;

ШНМ використовуються для досягнення більших результатів на великих масивах даних; ШНМ використовуються для досягнення більших результатів на великих масивах даних; ШНМ використовуються для досягнення більших результатів на великих масивах даних.

134No 4(12), 2021ISSN 2663-4023АНМ - це модель, заснована на принципах організації та функціонування людського мозку (тобто мережі нейронів у живому організмі). Іншими словами, алгоритм нейронної мережі намагається створити функцію, яка відображає входи до бажаних виходів. Нейронні мережі (НМ) зазвичай складаються з шарів (рис. 1). Шар складається з ряду взаємопов'язаних "вузлів", включаючи "функцію активації". Шаблони подаються в мережу через "вхідний шар", який передає дані одному або декільком "прихованим шарам", де відбувається фактична обробка за допомогою зваженої системи "зв'язків". Потім прихований шар надсилає дані до "вихідного шару", де виводиться відповідь.

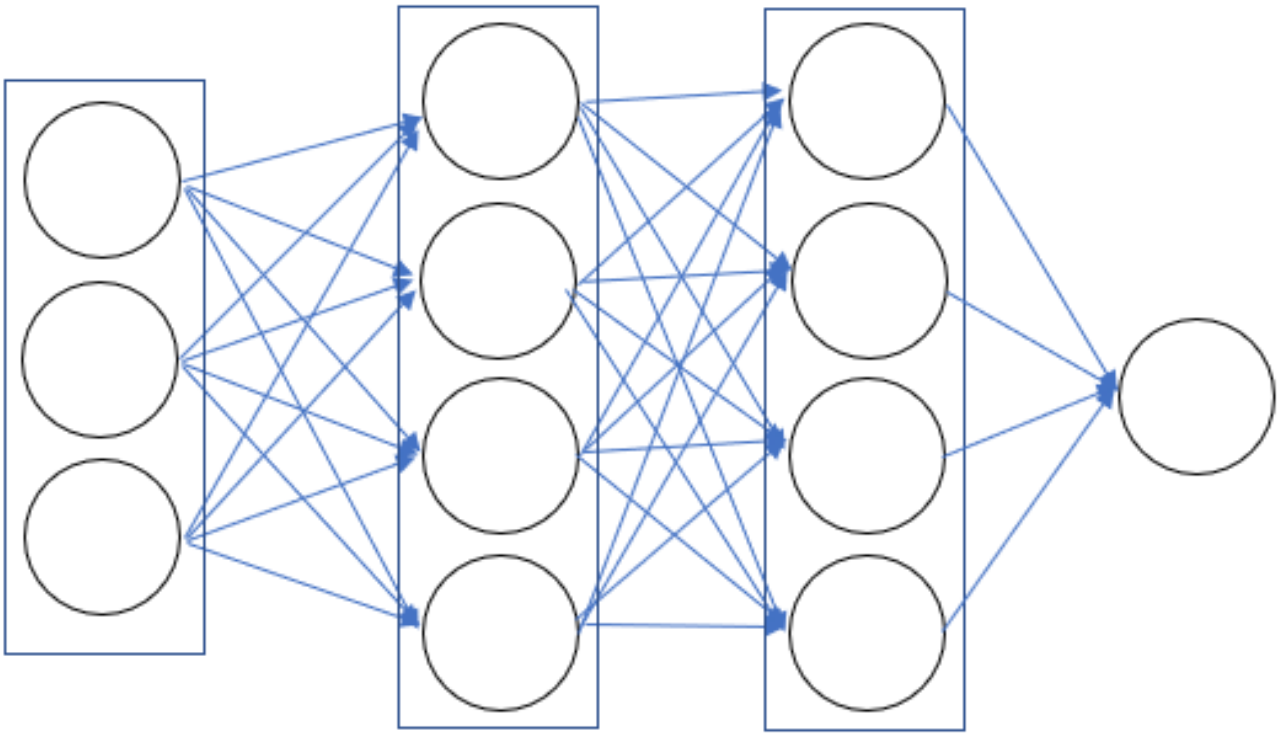

Рисунок 3.1 - Приклад нейронної мережі

3.2 Використання специфічних алгоритмів машинного навчання в кібербезпеці

Алгоритми машинного навчання забезпечують фундамент для побудови сучасних систем кібербезпеки. У цьому підрозділі ми розглянемо три основні класи алгоритмів: глибокі нейронні мережі, методи ансамблю та методи кластеризації.

Глибокі нейронні мережі (Deep Neural Networks, DNN) складаються з великої кількості шарів нейронів, що дозволяє їм навчатися складним патернам у даних. Кожен нейрон виконує нелінійну трансформацію вхідного сигналу, що можна описати як:

$$y_i = f\left(\sum_{j=1}^{n} w_{ij}x_j + b_i\right)$$

де y_i – вихід нейрона i-го шару,

x_j – вхідний сигнал від нейрона j-го шару,

w_{ij} – ваговий коефіцієнт,

b_i – зміщення,

f – нелінійна функція активації, така як Rectified Linear Unit:

$$f(x) = max(0, x)$$

Для задач класифікації використовується функція softmax на вихідному шарі:

$$P(y = j|x) = \frac{exp\ exp\ (y_i)}{\sum_{k=1}^{K} exp(y_k)}$$

Де $P(y = J|x)$ - ймовірність належності зразка xx до класу j, K – кількість класів.

Метод ансамблю (Ensemble Methods) об'єднують прогнози декількох моделей для покращення загальної точності. Одним із популярних методів є Random Forest, який складається з набору дерев рішень, кожне з яких навчається на випадковій підмножині даних. Прогноз здійснюється шляхом голосування:

$$y = \left(h_1(x), h_2(x), \cdots, h_N(x)\right)$$

Де h_1 - окреме дерево рішень, NN – кількість дерев.

Метод кластеризації (Clustering Methods) використовується для виявлення аномалій шляхом групування схожих об'єктів. Один із популярних методів – k-means, який мінімізує суму квадратів відстаней між точками та центроїдами їх кластерів:

$$J = \sum_{i=1}^{k} \quad \Sigma_{x \epsilon C_i} ||x - \mu_i||^2$$

Де C_i - кластер, x – точка, що належить до цього кластера, μ_i - центроїд кластера i.

Для реалізації глибоких нейронних мереж використовуються фреймворки, такі як TensorFlow або PyTorch. Прикладом є виявлення шкідливих програм на основі їх поведінкових ознак. Архітектура мережі може включати декілька згорткових (convolutional) і повнозв'язних (fully connected) шарів.

Точність мережі обчислюється як:

$$Accuracy = \frac{TP + TN}{TP + TN + FN}$$

де *TP* – істинно позитивні результати, *TN* – істинно негативні результати, *FP* – хибно позитивні, *FN* – хибно негативні.

Метод ансамблю - Random Forest реалізується за допомогою бібліотек, таких як scikit-learn. Для виявлення вторгнень у мережу використовується набір дерев рішень, які навчаються на різних підмножинах даних, що забезпечує стійкість до переобучення.

Показник F1-score для оцінки ефективності розраховується як:

$$F1=2 \cdot \frac{Precision * Recall}{Precision + Recall}$$

Де $\text{Precision} = \frac{TP}{TP+FP}$

$\text{Recall} = \frac{TP}{TP+FN}$

Метод кластеризації застосовується для кластеризації мережевого трафіку. Реалізація виконується за допомогою алгоритму Lloyd’s, який ітеративно оновлює центроїди та призначення точок до кластерів.

Ефективність кластеризації оцінюється за допомогою середньої відстані до центроїда:

Average Distance = $\frac{1}{N}\sum_{i=1}^{N} \quad \left||x_i - \mu c(i)|\right|$

Де $c(i)$ – індекс кластера, до якого належить точка x_i.

Традиційні методи кіберзахисту, такі як сигнатурний аналіз та евристичний аналіз, мають обмеження у виявленні нових загроз. Машинне навчання, навпаки, здатне адаптуватися до нових видів атак, виявляючи патерни, які не можна знайти за допомогою традиційних методів.

Таблиця 3.1 – Порівняння традиційних методів з машинним навчанням

№	Показник	Традиційні методи	Машинне навчання
1	Точність	Середня	Висока
2	Виявлення нових загроз	Обмежене	Висока
3	Швидкість обробки	Висока	Середня
4	Адаптивність	Низька	Висока

Перед вибором алгоритму машинного навчання важливо чітко визначити специфіку задачі кіберзахисту та умови її використання. Це включає аналіз типу даних, що доступні для аналізу, їх обсяг, структуру, основні цілі моделі (класифікація, виявлення аномалій, прогнозування) та реальні умови, такі як обмеження щодо обчислювальних ресурсів та часу обробки.

Глибокі нейронні мережі (DNN) є потужним інструментом для аналізу великих обсягів даних і виявлення складних патернів. Вони добре працюють з великими наборами даних, що містять мільйони зразків, і ефективні для задач, де необхідно виявляти складні патерни, такі як поведінковий аналіз шкідливих програм. Для задач, що потребують високої точності класифікації, наприклад, виявлення шкідливого програмного забезпечення або фішингових атак, DNN забезпечують високі результати. Реалізація таких мереж може бути здійснена за допомогою фреймворків, таких як TensorFlow або PyTorch, а архітектура може включати згорткові шари для аналізу зображень або сигналів та рекурентні шари для обробки послідовних даних. Важливо враховувати, що навчання мережі потребує значних обчислювальних ресурсів, тому необхідно мати доступ до GPU.

Методи ансамблю (Ensemble Methods) об'єднують прогнози кількох моделей для покращення загальної точності та стійкості до переобучення. Вони добре працюють з даними, що мають високу варіативність та складні патерни, і забезпечують високу стійкість до переобучення, що особливо важливо при наявності обмеженого обсягу даних для навчання. Для задач, де необхідна висока точність і стійкість до шуму, такі як виявлення вторгнень у мережу, ці методи є оптимальними. Реалізація ансамблевих методів, таких як Random Forest або Gradient Boosting, може бути здійснена за допомогою бібліотек, таких як scikit-learn. Кількість моделей у ансамблі налаштовується в залежності від обсягу даних та обчислювальних можливостей. Поєднання прогнозів різних моделей для отримання кінцевого результату забезпечує високу точність класифікації.

Методи кластеризації (Clustering Methods) використовуються для групування схожих об'єктів та виявлення аномалій. Вони ефективні для задач, де необхідно виявляти аномальні патерни в даних, такі як нетипова активність у мережевому трафіку, і дозволяють виявляти нові види загроз, що не можна знайти за допомогою сигнатурних методів. Для задач, де дані не мають чіткої структури і їх потрібно кластеризувати для подальшого аналізу, методи кластеризації є найбільш підходящими. Реалізація k-means для кластеризації мінімізує суму квадратів відстаней між точками та центроїдами їх кластерів, а алгоритми, такі як DBSCAN або Gaussian Mixture Models, можуть використовуватися для кластеризації даних з різною густиною. Налаштування кількості кластерів залежить від специфіки задачі та властивостей даних.

Використання комбінованих підходів, що поєднують декілька алгоритмів, може забезпечити ще вищу ефективність у виявленні та нейтралізації загроз. Наприклад, поєднання глибоких нейронних мереж та методів ансамблю дозволяє використовувати DNN для початкової обробки даних та виявлення складних патернів, а методи ансамблю – для кінцевої класифікації. Також методи кластеризації можуть комбінуватися з алгоритмами на основі правил для детального виявлення аномалій після попереднього аналізу даних. Прикладом є поєднання DNN для аналізу мережевого трафіку та Random Forest для класифікації

результатів, що дозволяє підвищити точність та зменшити кількість хибно позитивних результатів.

Для успішного впровадження алгоритмів машинного навчання у системи кібербезпеки слід дотримуватись певних етапів. Це включає збір та підготовку даних, забезпечення їх високої якості та різноманітності для навчання моделей, використання належних алгоритмів та їх налаштування відповідно до специфіки задачі, проведення ретельного тестування моделей на валідаційних та тестових наборах даних для оцінки їх ефективності. Постійний моніторинг продуктивності моделей у реальних умовах та регулярне оновлення моделей на основі нових даних та змін у поведінці загроз є критично важливими для забезпечення високого рівня захисту.

Використання метрик, таких як точність (accuracy), F1-score, середня відстань до центроїда (для кластеризації) для оцінки ефективності моделей, допомагає забезпечити надійну та ефективну роботу систем кібербезпеки. Використання хмарних обчислювальних платформ для масштабованості та обробки великих обсягів даних, а також забезпечення доступності високопродуктивних обчислювальних ресурсів, таких як GPU, є ключовими факторами успіху.

Вибір оптимального алгоритму машинного навчання залежить від специфіки задачі кіберзахисту, обсягу та типу даних, а також вимог до швидкості та точності обробки. Використання різних алгоритмів та їх комбінацій дозволяє ефективно вирішувати складні задачі виявлення та нейтралізації загроз, забезпечуючи високий рівень захисту інформаційних систем. Ці рекомендації допоможуть вибрати та налаштувати алгоритми машинного навчання для побудови ефективних систем кібербезпеки, здатних адаптуватися до нових викликів та загроз у цифровому світі.

3.3 Використання штучного інтелекту та машинного навчання у кібербезпеці для виявлення загроз

Інтеграція штучного інтелекту та машинного навчання у системи кібербезпеки забезпечує значні переваги в виявленні та запобіганні кіберзагрозам. Розвиток цих технологій відкриває нові можливості для створення інтелектуальних систем виявлення загроз, аналізу аномалій та автоматичного реагування на інциденти. Цей підрозділ розглядає деталі та приклади застосування ШІ в різних аспектах кібербезпеки, ґрунтуючись на сучасних дослідженнях та практичних впровадженнях.

Інтелектуальні системи виявлення загроз є одними з найбільш значущих застосувань ШІ у кібербезпеці. Вони використовують методи машинного навчання для аналізу мережевого трафіку, ідентифікації потенційних загроз та автоматичного реагування на них. Методики, такі як кластеризація, класифікація та глибоке навчання, дозволяють виявляти підозрілу активність, яка може залишитися непоміченою традиційними методами.

Нейронні мережі є основою для багатьох сучасних систем виявлення загроз. Вони навчаються на великому обсязі даних про мережевий трафік та події, що дозволяє їм виявляти аномалії. Один з методів, що використовується, — це рекурентні нейронні мережі (RNN), які добре підходять для обробки послідовних даних, таких як мережевий трафік.

Для навчання моделі на історичних даних мережевого трафіку та прогнозування аномалій використовуються архітектури, такі як LSTM (Long Short-Term Memory). Ці моделі можуть запам'ятовувати довготривалі залежності у послідовностях даних, що дозволяє виявляти складні аномалії в мережевому трафіку. Детальний код реалізації наведено у Додатку А. В цьому додатку демонструється використання LSTM для аналізу мережевого трафіку. Модель навчається на історичних даних і використовується для прогнозування майбутніх значень трафіку, що дозволяє виявляти аномалії, які можуть свідчити про потенційну загрозу.

Крім нейронних мереж, для виявлення загроз часто використовуються інші алгоритми класифікації, такі як Support Vector Machine (SVM) або Random Forest. Вони дозволяють створювати моделі, здатні розрізняти нормальну і аномальну

активність. Наприклад, Random Forest використовується для навчання моделі на історичних даних мережевого трафіку, що дозволяє класифікувати аномальну активність в реальному часі. Детальний код реалізації наведено у Додатку Б. В цьому додатку демонструється використання Random Forest для класифікації мережевого трафіку. Модель навчена на історичних даних і використовується для виявлення аномальної активності в реальному часі.

Системи поведінкового аналізу користувачів та інформаційних сутностей (UEBA) використовують ШІ для виявлення аномалій у поведінкових моделях користувачів та пристроїв. Ці системи дозволяють виявляти відхилення від нормальної поведінки, що може свідчити про внутрішні або зовнішні загрози.

Моніторинг поведінки користувачів може включати аналіз їхньої активності в системі, часу роботи, доступу до файлів та інших дій. Наприклад, якщо користувач починає завантажувати велику кількість конфіденційних файлів у неробочий час або здійснює доступ до систем, до яких раніше не мав доступу, система UEBA може ідентифікувати таку поведінку як потенційну загрозу.

Для цього використовуються моделі машинного навчання, які аналізують великі обсяги даних про поведінку користувачів та виявляють аномальні патерни. Наприклад, нейронні мережі можуть бути використані для створення моделей поведінки користувачів, що дозволяє виявляти аномалії в режимі реального часу. Детальний код реалізації наведено у Додатку В. В цьому додатку демонструється використання нейронної мережі для аналізу поведінки користувачів. Модель навчається на історичних даних про дії користувачів і використовується для виявлення аномалій у поведінці в реальному часі.

Платформи попереднього детектування загроз (TIP) використовують великі обсяги даних та індикатори компрометації для ідентифікації загроз на ранніх етапах. Застосування ШІ дозволяє ефективно аналізувати ці дані, виявляючи загрози та автоматично реагуючи на них.

Такі платформи збирають та аналізують дані з різних джерел, включаючи журнали подій, мережевий трафік, дані від сторонніх постачальників безпеки та інші інформаційні потоки. Використання методів глибокого навчання дозволяє

створювати складні моделі для виявлення загроз, що можуть залишатися непоміченими традиційними методами.

Для цього застосовуються конволюційні нейронні мережі (CNN), які здатні ефективно обробляти та аналізувати великі обсяги даних. Вони навчаються на історичних даних та використовуються для виявлення потенційних загроз у режимі реального часу. Детальний код реалізації наведено у Додатку Г. В цьому додатку демонструється використання конволюційних нейронних мереж (CNN) для аналізу великих обсягів даних, зібраних платформами попереднього детектування загроз. Модель навчається на історичних даних та використовується для виявлення потенційних загроз.

Інтеграція ШІ у системи кібербезпеки забезпечує значне покращення ефективності виявлення загроз, автоматизації процесів та зменшення кількості хибних спрацьовувань. Однак існують також виклики, пов'язані з необхідністю постійного оновлення моделей та адаптації до нових загроз. Майбутні дослідження можуть зосередитися на покращенні алгоритмів МН, інтеграції різних джерел даних та створенні більш інтерактивних і адаптивних систем кібербезпеки.

3.4 Аналіз програм на основі штучного інтелекту в якості комп’ютерних засобів захисту інформації

Загальна концепція багаторівневої інтегрованої структури для машинного навчання в інтелектуальних службах кібербезпеки включає кілька етапів обробки від початкових даних подій безпеки до кінцевих служб. Потік починається з необроблених даних подій безпеки, зібраних з різних джерел. Далі ці дані проходять етап підготовки та попередньої обробки для подальшої обробки алгоритмами машинного навчання. На наступному етапі застосовуються методи машинного навчання, де модель навчається виявляти шаблони та аномалії, що можуть свідчити про потенційні загрози. Отримані результати спрощуються модулем постобробки та вдосконалюються з урахуванням специфічних вимог шляхом інтеграції предметно-специфічних знань. Потім модуль аналізу

актуальності та оновлення моделі безпеки підтримує актуальність моделі шляхом завантаження новітніх шаблонів безпеки, керованих даними. На завершальному етапі модуль планування реагування та прийняття рішень використовує отриману інформацію для вжиття необхідних заходів щодо запобігання кібератакам.

Машинне навчання в кібербезпеці також використовується для класифікації зразків, прогнозуючи їх зловмисність з певним рівнем впевненості. Ефективність таких моделей оцінюється за точністю та результатами. Якщо класифікатор зловмисного програмного забезпечення правильно визначає зразок як зловмисний, це є позитивним виявленням. При розгляді моделей для аналізу шкідливих файлів, справжній позитивний результат означає правильне визначення файлу як шкідливого, тоді як справжній негатив означає правильне визначення нешкідливого файлу. Помилковий позитивний результат означає неправильне визначення нешкідливого файлу як шкідливого, а помилковий негатив означає неправильне визначення шкідливого файлу як нешкідливого. Хоча справжні спрацьовування мають ключове значення для виявлення загроз, помилкові спрацьовування теж важливі, оскільки вони впливають на ефективність системи, потребуючи додаткових ресурсів для розслідування кожного випадку та можуть порушити роботу критичних програм через автоматичні програми відновлення.

Під час налаштування моделей захисту даних необхідно збалансувати справжні та помилкові позитивні результати. Зниження порогу для справжніх позитивних результатів може збільшити кількість помилкових позитивних результатів, що вплине на продуктивність. Мета розробки високопродуктивних моделей машинного навчання полягає у максимізації ефективності виявлення, збільшуючи кількість справжніх позитивних виявлень та зменшуючи кількість помилкових спрацьовувань. Досягнення такого балансу може бути складним завданням, оскільки класифікатори зловмисного програмного забезпечення часто мають справжні позитивні показники близько 99%, збалансовані з помилковими позитивними показниками значно нижче 1%.

Таблиця 3.2 – Помилкові позитивні та помилкові негативні результати

Передбачені значення	**Справжні значення**

	Позитивні	**Негативні**
Позитивні	Справжні позитивні	Помилкові позитивні
Негативні	Помилкові негативні	Справжні негативні

Наступним етапом є розвідка загроз – збір і аналіз інформації про потенційні або поточні атаки, які загрожують організації. Концепція аналізу загроз передбачає аналіз та інтерпретацію даних для виявлення загроз, пошуку прогнозних індикаторів і впровадження захисних заходів. Роль штучного інтелекту в розвідці загроз полягає в автоматизації процесу збору, зберігання та аналізу даних. Розвідка загроз на основі штучного інтелекту використовує машинне навчання та інші методи штучного інтелекту для аналізу шаблонів і виявлення аномалій, які вказують на потенційні загрози. Для виявлення загроз сьогодні використовуються наступні бібліотеки штучного інтелекту та методи кодування. Scikit-learn, TensorFlow та PyTorch пропонують готові функції та інструменти для створення моделей машинного навчання.

Ці бібліотеки можна використовувати для реалізації різних алгоритмів машинного навчання для виявлення загроз, наприклад випадковий ліс, дерево рішень та нейронні мережі. Практики кодування також відіграють важливу роль у впровадженні аналізу загроз на основі штучного інтелекту. Перегляд коду, модульне тестування та постійна інтеграція збільшують якість і надійність моделей штучного інтелекту. Сьогодні використовується декілька наборів даних у сфері кібербезпеки, таких як NSL-KDD, DARPA, CAIDA, MAWI, ADFA IDS, CERT, EnronSpam, SpamAssassin, Malware Genome project, Virus Share, VirusTotal, Comodo, Contagio, Microsoft тощо. Дані набори даних містять приклади різних типів кібератак і можуть використовуватися для навчання та тестування продуктивності систем аналізу загроз з використанням штучного інтелекту. Наприклад, для завантаження набору даних NSL-KDD у фрейм для аналізу даних і машинного навчання за допомогою програмної бібліотеки pandas, використовується наступний код:

```
```python
import pandas as pd
```
```

```
df = pd.read_csv('NSL-KDD/KDDTrain+.txt')```
```

Впровадження методів штучного інтелекту та машинного навчання може значно підвищити продуктивність систем виявлення загроз. Наприклад, системи виявлення вторгнень можуть ідентифікувати різноманітні кіберзагрози та атаки, навіть невідомі атаки нульового дня, і реагувати в режимі реального часу на основі вимог користувачів. Додатково можна використовувати бібліотеки, такі як Keras, високорівневий API для нейронних мереж, написаний на Python і здатний працювати поверх TensorFlow, CNTK або Theano. Pandas, програмна бібліотека, яка пропонує структури даних і операції для роботи з числовими таблицями та часовими рядами, написана на мові програмування Python для обробки та аналізу даних. Numpy, бібліотека для мови програмування Python, що додає підтримку великих багатовимірних масивів і матриць разом із великою колекцією математичних функцій високого рівня для роботи з цими масивами.

Нижче наведено приклад програми реалізації бібліотеки для реалізації простої нейронної мережі та виявлення загроз:

```
import pandas as pd
import numpy as np
from keras.models import Sequentiel
from keras.layers import Dense
data = pd.read_csv('NSL-KDD/KDDTrain+.txt')
X = data.drop('label', axis=1)
Y=data['label']
model = Sequentiel()
model.add(Dense(12, input_dim=8, activation = 'relu'))
model.add(Dense(8, activation = 'relu'))
model.add(Dense(1, activation = 'sigmoid'))
model.compile(loss='binary_crossent', optimizer='adam', metrics=[accuracy])
model.fit(X, Y, epochs=150, bathc_size=10)
```

У представленій частині коду на першому етапі завантажується та попередньо оброблюється набір даних. На наступному етапі визначається проста нейронна мережа з одним вхідним шаром, одним прихованим шаром і одним вихідним шаром. Відбувається компіляція моделі за допомогою двійкової функції перехресних ентропійних втрат і оптимізатора 'Adam', а потім адаптація моделі до даних. Вихідні дані моделі визначаються як передбачення того, чи є вхідні дані

загрозою чи ні. В даному випадку наведено лише простий приклад фактичної реалізації, і залежно від конкретних вимог і контексту програма може бути більш комплексною і складною.

Автоматизоване реагування на інциденти (API) передбачає використання автоматизованих систем для виявлення інцидентів безпеки та реагування на них. Штучний інтелект може покращити API, забезпечивши виявлення загроз у реальному часі, автоматичне їх блокування і постійне навчання на основі минулих інцидентів.

Нижче приведено приклад використання ШІ для вдосконалення API за допомогою Python і бібліотеки Scikit-learn для машинного навчання:

```
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
import pandas as pd
data = pd.read_csv('security_data.csv')
X = data.drop('threat_detected', axis=1)
Y = data['threat_detected']
X_train, X_test, Y_train, Y_test = train_test_split(X, Y, test_size=0.2, random_state=42)
clf = RandomForestClassifier(n_estimators=100)
clf.fit(X_train, Y_train)
y_pred = clf.predict(X_test)
for i in range(len(Y_pred)):
    if Y_pred[i] == 1:
        print(f'Threat detected in data point {X_test.iloc[i]}. Initiating automated response.')
```

Коли система штучного інтелекту виявляє загрозу, відбувається запуск повідомлення про те, що загроза була визначена у відповідному пакеті даних, і здійснюється автоматична реакція на неї. Крім того, штучний інтелект може покращити виявлення фішингу, аналізуючи електронні листи або веб-сайти та визначаючи характеристики, які можуть вказувати на спробу фішингу.

Нижче наведено приклад використання ШІ для виявлення фішингу за допомогою Python і Natural Language Toolkit (NLTK) для аналізу тексту:

```
import nltk
from sklearn.featureextraction.text import  CountVectorizer
from sklearn.naive_bayes import MultinomialNB
from sklearn.model_selection import train_test_split
import pandas as pd
data pd.read_csv('phishing_data.csv')
X = data['email_text']
Y = data['is_phishing']
X_train, X_test, Y_train, Y_test = train_test_split(X, Y, test_size=0.2, random_state=42)
Vectorizer = CountVectorizer()
X_train_counts = vectorizer.fit_transform(X_train)
clf = MultinomialNB()
clf.fit(X_train_counts, Y_train)
X_test_counts = vectorizer.transform(X_test)
Y_pred = clf.predict(X_test_counts)
for I in range(len(Y_pred)):
    if Y_pred[i] == 1:
        print(f'Phishing attempt detected in email: {X_test.iloc[i]}.')
```

Система штучного інтелекту виявляє спроби фішингу, аналізуючи текстовий вміст електронних листів. При виявленні фішингу система надсилає сповіщення про наявність шкідливого повідомлення в конкретному листі. Шкідливе програмне забезпечення може включати віруси, хробаків, троянські програми, програми-вимагачі та інші небезпечні програми. Штучний інтелект може покращити виявлення таких програм, аналізуючи їх характеристики та визначаючи функції, що можуть свідчити про їх присутність.

Нижче наведено приклад використання ШІ для покращення виявлення шкідливого програмного забезпечення за допомогою Python і бібліотеки TensorFlow для глибокого навчання:

```
import tensorflow as tf
from sklearn.model_selection train_test_split
import pandas as pd
data pd.read_csv('malware_data.csv')
X = data.drop('is_malware', axis=1)
Y = data['is_malware']
X_train, X_test, Y_train, Y_test = train_test_split(X, Y, test_size=0.2, random_state=42)
model = tf.keras.models.Sequential([
    tf.keras.layers.Dense(128, activation 'relu'),
    tf.keras.layers.Dense(64, activation 'relu'),
    tf.keras.layers.Dense(1, activation 'sigmoid')
])
model.compile(optimizer='adam', loss='binary_crossent', metrics=['accuracy'])
model.fit(X_train, Y_train, epochs=5)
y_pred model.predict(X_test)

for i in range(len(y_pred)):
    if y_pred[i] >= 0.5:
        print(f'Malware detected in software: {X_test.iloc[i]}.')
```

Система штучного інтелекту виявляє шкідливі програми на основі характеристик програмного забезпечення і при виявленні загрози запускає автоматичне сповіщення. Представлена робота демонструє значний потенціал використання штучного інтелекту для посилення заходів в галузі кібербезпеки. Аналіз загроз на основі штучного інтелекту може покращити виявлення загроз і час реагування, забезпечуючи надійний захист від кібератак.

Крім того, застосування штучного інтелекту в кібербезпеці не тільки призводить до збільшення випадків виявлення загроз, але й має позитивний вплив автоматизованого реагування на інциденти. Наведені моделі можуть аналізувати загрози та реагувати на них у реальному часі, скорочуючи час, необхідний для зниження ефективності потенційних кібератак. Визначено, що штучний інтелект також може покращити виявлення фішингу та шкідливих програм. Аналізуючи закономірності та аномалії в даних, моделі штучного інтелекту можуть виявити й позначити потенційне шкідливе програмне забезпечення, додаючи нові можливості для систем кібербезпеки.

ВИСНОВОК

Інтелектуальні системи виявлення загроз кібербезпеки є ключовим елементом у забезпеченні безпеки інформаційних систем та мереж. Вони базуються на сучасних методах машинного навчання та дозволяють ефективно виявляти та аналізувати кіберзагрози в реальному часі.

Розробка та впровадження інтелектуальних систем кіберзахисту включає декілька етапів: збір даних про загрози, їх попередня обробка, навчання моделей машинного навчання, тестування та впровадження системи у реальне середовище. Використання різноманітних алгоритмів машинного навчання (наприклад, нейронних мереж, методів кластеризації) дозволяє значно підвищити точність і швидкість виявлення загроз.

Практичний аналіз ефективності інтелектуальних систем показує, що використання машинного навчання дозволяє виявляти складні та нові загрози, які важко виявити традиційними методами. Порівняння з відомими рішеннями демонструє, що інтелектуальні системи забезпечують вищу точність та адаптивність до нових видів атак.

Результати дослідження показали, що розроблені методи та моделі машинного навчання дозволяють значно покращити захист інформаційних систем. Вони здатні швидко адаптуватися до нових загроз та забезпечувати високий рівень безпеки при мінімальних затратах ресурсів.

Рекомендації для подальших досліджень включають:

1. Розширення бази даних загроз для покращення навчання моделей.
2. Дослідження можливостей інтеграції інтелектуальних систем в існуючі платформи кібербезпеки.
3. Вивчення впливу нових алгоритмів машинного навчання на ефективність виявлення загроз.
4. Розробка методів захисту від атак на самі системи машинного навчання, щоб забезпечити їх надійність та стійкість до зовнішніх впливів.

Загалом, інтелектуальні системи виявлення загроз кібербезпеки є перспективним напрямком розвитку сучасних технологій кіберзахисту. Вони дозволяють ефективно виявляти нові та складні загрози, підвищуючи рівень безпеки інформаційних систем та мереж. Подальші дослідження та вдосконалення цих систем є необхідними для забезпечення надійного захисту в умовах постійно змінюваного кіберпростору.

ПЕРЕЛІК ПОСИЛАНЬ

1. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека”. Правова інформатика. № 2(42)/2014. С. 54-62. URL: http://ippi.org.ua/sites/default/files/14boavpk.pdf
2. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Постанова Кабінету Міністрів України; Порядок від 04.04.2023 № 299 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/299-2023-%D0%B
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19
4. Стратегія кібербезпеки України: цілі та пріоритети. Матеріал з АРМІЯ INFORM URL: https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/
5. Перетин штучного інтелекту та кібербезпеки: Формування нової ери захисту. Матеріал з Ranktracker. URL: https://www.ranktracker.com/uk/blog/the-intersection-of-ai-and-cybersecurity-shaping-a-new-era-of-protection/
6. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України; Концепція від 02.12.2020 № 1556-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1556-2020-%D1%80
7. Гбур З. В. Використання штучного інтелекту в інформаційній безпеці України. *Державне управління: удосконалення та розвиток*. 2022. № 1. – URL: http://www.dy.nayka.com.ua/?op=1&z=2601
8. Мєшков В. І. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах / В. І. Мєшков, В. О. Віролайнен // Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», м. Київ, 21-23 травня 2015. – Київ : НТУУ «КПІ». – 2015. – С. 195-198. URL: https://ela.kpi.ua/handle/123456789/17609

9. Snort System Requirements. Матеріал з Flylib URL: https://flylib.com/books/en/3.100.1.199/1/
10. Understand what is SNORT, its features, different modes, and usage of SNORT rules. Матеріал з Fortinet URL: https://www.fortinet.com/resources/cyberglossary/snort
11. Веселков Н.Л. Марченко В.В. Можливості та перспективи використання Open-Source технологій виявлення вторгнень в сферах малого та середнього бізнесу України, м. Київ 2021, С. 21-25 URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2499/2399
12. The Role of AI in Cybersecurity: Anticipating and Preventing Attacks. Матеріал з bdodigital URL: https://www.bdodigital.com/insights/cybersecurity/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks#:~:text=AI%20plays%20a%20crucial%20role,help%20predict%20future%20attack%20vectors.
13. WIPO Technology Trends 2019 – Artificial Intelligence. Матеріал з WIPO URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf
14. Савченко В. А., Шаповаленко О. Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації. 2020. Т. 4, № 44. С. 6–11 URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2456/2356
15. Al Musawi, Ahmad. Introduction to Machine Learning. Матеріал з ResearchGate URL:https://www.researchgate.net/publication/323108787_Introduction_to_Machine_Learning
16. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning forcybersecurity. In 2018 10th International Conference on Cyber Conflict (CyCon) С. 371-390. URL: https://www.ccdcoe.org/uploads/2018/10/Art-19-On-the-Effectiveness-of-Machine-and-Deep-Learning-for-Cyber-Security.pdf
17. Ivanichenko, Y., Sablina, M., & Kravchuk, K. (2021). ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ В КІБЕРБЕЗПЕЦІ. *Електронне фахове наукове*

видання «Кібербезпека: освіта, наука, техніка», *4*(12), С. 132–142. https://doi.org/10.28925/2663-4023.2021.12.132142

18. Sharma, B., Mangrulkar, R. (2019). Deep learning applications in cyber security: a comprehensive review, challenges and prospects. International Journal of Engineering Applied Sciences and Technology, 4(8), С. 148-159 URL: https://www.researchgate.net/publication/339561219_DEEP_LEARNING_APPLICATIONS_IN_CYBER_SECURITY_A_COMPREHENSIVE_REVIEW_CHALLENGES_AND_PROSPECTS
19. Методи штучного інтелекту в кібербезпеці [Електронний ресурс] : навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: І.В. Стьопочкіна, О.М. Новіков. – Електронні текстові дані (1 файл: 19,9 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. С. 82 URL: https://ela.kpi.ua/bitstreams/9fee52b6-83fc-4e99-8541-c2767f634c7c/download
20. Шевченко, А. Аналіз застосування методів машинного навчання на основі штучних нейронних мереж для виявлення кіберзагроз / Андрій Шевченко, Герман Застело, Євген Шпачинський // Information Technology and Security. – 2019. – Vol. 7, Iss. 1 (12). С. 79–90. URL: https://ela.kpi.ua/bitstreams/0612dd40-88d4-47c6-b1b4-c35770d031c5/download

Додаток А

```
import numpy as np
from keras.models import Sequential
from keras.layers import LSTM, Dense
from sklearn.preprocessing import MinMaxScaler
# Завантаження даних
data = np.load('network_traffic_data.npy')
scaler = MinMaxScaler(feature_range=(0, 1))
data = scaler.fit_transform(data)
# Підготовка даних для LSTM
def create_dataset(data, look_back=1):
    X, Y = [], []
    for i in range(len(data)-look_back-1):
        a = data[i:(i+look_back), 0]
        X.append(a)
        Y.append(data[i + look_back, 0])
    return np.array(X), np.array(Y)
look_back = 10
X, Y = create_dataset(data, look_back)
# Переформатування даних
X = np.reshape(X, (X.shape[0], X.shape[1], 1))
# Створення та навчання моделі LSTM
model = Sequential()
model.add(LSTM(100, input_shape=(look_back, 1)))
model.add(Dense(1))
model.compile(loss='mean_squared_error', optimizer='adam')
model.fit(X, Y, epochs=20, batch_size=1, verbose=2)
# Використання моделі для прогнозування
predictions = model.predict(X)
```

Додаток Б

```
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score
# Завантаження та підготовка даних
X = np.load('network_features.npy')
y = np.load('network_labels.npy')
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=42)
# Створення та навчання моделі Random Forest
clf = RandomForestClassifier(n_estimators=100, random_state=42)
clf.fit(X_train, y_train)
# Прогнозування та оцінка моделі
y_pred = clf.predict(X_test)
print('Accuracy:', accuracy_score(y_test, y_pred))
```

Додаток В

```
from sklearn.preprocessing import StandardScaler
from keras.models import Sequential
from keras.layers import Dense
# Завантаження даних
user_data = np.load('user_behavior_data.npy')
scaler = StandardScaler()
user_data = scaler.fit_transform(user_data)
# Створення моделі для аналізу поведінки
model = Sequential()
model.add(Dense(64, input_dim=user_data.shape[1], activation='relu'))
model.add(Dense(32, activation='relu'))
model.add(Dense(1, activation='sigmoid'))
model.compile(loss='binary_crossentropy', optimizer='adam', metrics=['accuracy'])
# Навчання моделі
X_train, X_test, y_train, y_test = train_test_split(user_data[:, :-1], user_data[:, -1],
test_size=0.3, random_state=42)
model.fit(X_train, y_train, epochs=10, batch_size=10, verbose=2)
# Прогнозування та оцінка моделі
scores = model.evaluate(X_test, y_test)
print(f"Accuracy: {scores[1]*100}%")
```

Додаток Г

```
from keras.layers import Conv1D, MaxPooling1D, Flatten
from keras.models import Sequential
from keras.layers import Dense
# Завантаження та підготовка даних
data = np.load('threat_intelligence_data.npy')
scaler = MinMaxScaler(feature_range=(0, 1))
data = scaler.fit_transform(data)
# Створення моделі для аналізу даних
model = Sequential()
model.add(Conv1D(filters=64, kernel_size=2, activation='relu',
input_shape=(data.shape[1], 1)))
model.add(MaxPooling1D(pool_size=2))
model.add(Flatten())
model.add(Dense(100, activation='relu'))
model.add(Dense(1, activation='sigmoid'))
model.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])
# Навчання моделі
X_train, X_test, y_train, y_test = train_test_split(data[:, :-1], data[:, -1], test_size=0.3,
random_state=42)
X_train = X_train.reshape(X_train.shape[0], X_train.shape[1], 1)
X_test = X_test.reshape(X_test.shape[0], X_test.shape[1], 1)
model.fit(X_train, y_train, epochs=10, batch_size=64, verbose=2)
# Оцінка моделі
scores = model.evaluate(X_test, y_test)
print(f"Accuracy: {scores[1]*100}%")
```