# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ ПРАВООХОРОННИХ ОРГАНІВ

***Балтовський Олексій Анатолійович***
*доктор технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ*

У сучасних умовах трансформації глобального інформаційного середовища, інтенсивної цифровізації суспільних процесів та стрімкого розвитку кіберфізичних систем особливої актуальності набуває проблема забезпечення належного рівня кібербезпеки інформаційно-аналітичних систем правоохоронних органів. Динаміка розвитку цифрових технологій, інтеграція засобів автоматизованого аналізу даних у діяльність суб'єктів сектору безпеки і оборони, а також зростання масштабів використання інформаційно-комунікаційних технологій у сфері кримінального аналізу формують нові виклики для національної системи кібербезпеки. Вказані процеси супроводжуються не лише розширенням функціональних можливостей інформаційно-аналітичних платформ, але й суттєвим підвищенням рівня їх вразливості до деструктивних інформаційних впливів, кібератак, несанкціонованого доступу, маніпуляцій з даними та інтелектуальних форм кіберзлочинності [3].

Інформаційно-аналітичні системи правоохоронних органів у сучасних умовах функціонують як складні багаторівневі організаційно-технічні комплекси, що забезпечують накопичення, інтеграцію, оброблення, інтерпретацію та прогнозування інформації, необхідної для підтримки управлінських рішень, виявлення кримінальних загроз, аналізу ризиків та протидії транснаціональній злочинності. Такі системи характеризуються високим рівнем інформаційної насиченості, багатокомпонентною структурою, інтеграцією розподілених баз даних, використанням хмарних сервісів, засобів Big Data-аналітики, геоінформаційних технологій, систем підтримки прийняття рішень та автоматизованих механізмів моніторингу. У зв'язку з цим забезпечення їх кіберстійкості стає

не лише технічним, але й стратегічним завданням державної політики у сфері безпеки [1,2].

Особливого значення набуває використання технологій штучного інтелекту та інтелектуального аналізу даних як інструментів підвищення ефективності функціонування систем кіберзахисту. Концептуально штучний інтелект у сфері кібербезпеки слід розглядати як комплекс методів і алгоритмів, здатних здійснювати автоматизоване виявлення аномалій, моделювання поведінкових патернів, класифікацію кіберзагроз, прогнозування потенційних інцидентів, аналіз ризиків та підтримку прийняття управлінських рішень у режимі реального часу. Інтелектуальний аналіз даних, у свою чергу, виступає фундаментальним методологічним інструментарієм виявлення прихованих закономірностей, причинно-наслідкових зв'язків, латентних залежностей та структурних характеристик інформаційних потоків, що циркулюють у цифровому середовищі правоохоронних органів.

Сучасний етап розвитку кіберзагроз характеризується переходом від традиційних форм комп'ютерних атак до складних адаптивних моделей кібернетичного впливу, які використовують механізми соціальної інженерії, генеративного штучного інтелекту, автоматизованих бот-мереж, поліморфного шкідливого програмного забезпечення та технологій маскування цифрової активності. В умовах постійного ускладнення архітектури кібератак класичні сигнатурні підходи до виявлення загроз демонструють обмежену ефективність, оскільки орієнтовані переважно на відомі шаблони поведінки. Саме тому пріоритетного значення набуває впровадження інтелектуальних систем аналізу, здатних до самоадаптації, машинного навчання та прогнозування нових типів загроз.

Використання методів машинного навчання у сфері забезпечення кібербезпеки дозволяє реалізувати принципово новий рівень автоматизації процесів аналізу інформації. Алгоритми supervised learning забезпечують класифікацію мережевої активності на основі попередньо сформованих наборів даних та дозволяють виявляти шкідливі сценарії поведінки користувачів або системних процесів. Методи unsupervised learning спрямовані на виявлення аномалій у великих масивах неструктурованих даних та забезпечують ідентифікацію потенційних кіберінцидентів без необхідності попереднього маркування інформації. Технології reinforcement learning дозволяють системам кіберзахисту

адаптуватися до змін середовища та оптимізувати механізми реагування на інциденти шляхом накопичення досвіду функціонування [3].

Особливу роль у забезпеченні кібербезпеки інформаційно-аналітичних систем правоохоронних органів відіграють нейромережеві технології. Глибокі нейронні мережі забезпечують можливість аналізу великих обсягів мережевого трафіку, лог-файлів, інформаційних журналів та поведінкових характеристик користувачів з метою виявлення нетипових сценаріїв активності. Використання рекурентних нейронних мереж дозволяє здійснювати часовий аналіз послідовностей подій, що є надзвичайно важливим у контексті прогнозування етапів розвитку складних кібератак. Конволюційні нейронні мережі можуть застосовуватися для виявлення шкідливого програмного забезпечення шляхом аналізу структурних характеристик файлів та цифрових артефактів.

Інтелектуальний аналіз даних у діяльності правоохоронних органів має міждисциплінарний характер та поєднує елементи системного аналізу, математичного моделювання, теорії ризиків, теорії прийняття рішень, криптографії, комп'ютерної лінгвістики та когнітивної аналітики. Використання Data Mining-технологій дозволяє здійснювати глибоку обробку інформації, виявляти латентні взаємозв'язки між подіями, суб'єктами та цифровими об'єктами, формувати прогностичні моделі кіберзагроз та оцінювати рівень інформаційних ризиків. У контексті кримінального аналізу це створює передумови для переходу від реактивної моделі забезпечення безпеки до проактивної концепції попередження кіберзлочинності.

Суттєвий науковий та практичний інтерес становить використання технологій штучного інтелекту у процесі аналізу поведінкових характеристик користувачів інформаційно-аналітичних систем. Поведінкова аналітика базується на побудові цифрових профілів користувачів, моделюванні типових сценаріїв взаємодії із системою та виявленні відхилень від нормативної поведінки. Такий підхід дозволяє своєчасно ідентифікувати ознаки внутрішніх загроз, компрометації облікових записів або спроб несанкціонованого доступу. Особливої актуальності це набуває в умовах використання віддалених форм доступу до інформаційних ресурсів та інтеграції мобільних платформ у систему службової діяльності правоохоронних органів.

Одним із ключових напрямів застосування інтелектуальних технологій є автоматизація процесів реагування на кіберінциденти. У сучасних умовах традиційні моделі реагування часто не забезпечують необхідної швидкості прийняття рішень через значні обсяги інформації та високий рівень динамічності кіберзагроз. Використання технологій SOAR та SIEM у поєднанні з алгоритмами штучного інтелекту дозволяє автоматизувати процеси кореляції подій, аналізу журналів безпеки, виявлення аномалій та формування рекомендацій щодо реагування на інциденти. Це суттєво підвищує оперативність діяльності аналітичних підрозділів та забезпечує мінімізацію часу між виявленням загрози та реалізацією заходів протидії.

Не менш важливим аспектом є використання штучного інтелекту для прогнозування кіберризиків. Прогностичні моделі, побудовані на основі аналізу історичних даних, поведінкових патернів та характеристик мережевої активності, дозволяють визначати потенційно критичні ділянки інформаційної інфраструктури, прогнозувати ймовірність виникнення інцидентів та формувати ризик-орієнтовані стратегії кіберзахисту. Застосування системного аналізу у поєднанні з методами машинного навчання створює передумови для комплексної оцінки стійкості інформаційно-аналітичних систем до зовнішніх і внутрішніх загроз [4].

У контексті функціонування правоохоронних органів особливого значення набуває проблема забезпечення достовірності та цілісності інформації, що обробляється в інформаційно-аналітичних системах. В умовах гібридних загроз та інформаційних операцій противника маніпуляція цифровими даними може мати критичні наслідки для процесів прийняття управлінських рішень. Технології штучного інтелекту дозволяють здійснювати автоматизовану верифікацію інформації, виявляти ознаки фальсифікації даних, аналізувати цифрові сліди втручання та формувати механізми забезпечення інформаційної довіри. У цьому аспекті особливої актуальності набуває використання алгоритмів аналізу цифрових аномалій, криптографічних методів контролю цілісності та блокчейн-технологій.

Проблематика впровадження штучного інтелекту у сферу кібербезпеки інформаційно-аналітичних систем правоохоронних органів має також виражений правовий та етичний вимір. Автоматизація процесів прийняття рішень, використання алгоритмів

прогнозування поведінки та аналізу персональних даних потребують дотримання принципів законності, пропорційності, прозорості та недискримінаційності. У зв'язку з цим важливого значення набуває формування нормативно-правових механізмів регулювання використання технологій штучного інтелекту у діяльності правоохоронних структур, визначення меж автоматизації аналітичної діяльності та забезпечення належного рівня контролю за функціонуванням інтелектуальних систем [1-3].

Складність сучасного кіберпростору обумовлює необхідність формування інтегрованої архітектури кіберзахисту, що базується на принципах адаптивності, масштабованості, багаторівневості та прогнозованості. У цьому контексті інформаційно-аналітичні системи правоохоронних органів мають трансформуватися у комплексні когнітивні платформи, здатні забезпечувати автоматизоване сприйняття, інтерпретацію та прогнозування кіберзагроз. Використання технологій штучного інтелекту дозволяє реалізувати концепцію інтелектуальної кібероборони, в межах якої система не лише реагує на інциденти, але й здійснює постійний аналіз цифрового середовища, моделює потенційні сценарії атак та формує превентивні механізми протидії.

Перспективним напрямом розвитку систем кібербезпеки є використання когнітивних моделей аналізу інформації. Когнітивна аналітика дозволяє інтегрувати механізми машинного навчання, семантичного аналізу, оброблення природної мови та системного моделювання для виявлення прихованих взаємозв'язків між подіями, суб'єктами та інформаційними потоками. У діяльності правоохоронних органів це створює можливості для автоматизованого аналізу великих масивів текстової інформації, OSINT-даних, соціальних мереж, цифрових комунікацій та інших джерел інформації з метою виявлення ознак підготовки кіберзлочинів або координації протиправної діяльності.

Важливим елементом сучасної системи кібербезпеки є інтеграція засобів штучного інтелекту з технологіями аналізу великих даних. Big Data-підхід дозволяє здійснювати оброблення значних обсягів структурованої та неструктурованої інформації у режимі реального часу, забезпечуючи можливість комплексного аналізу цифрового середовища. Для правоохоронних органів це означає формування нових можливостей щодо оперативного виявлення

кіберзагроз, прогнозування криміногенних тенденцій та підтримки стратегічного управління ризиками.

Одним із найбільш складних викликів у сфері кібербезпеки є проблема протидії адаптивним інтелектуальним атакам, що використовують алгоритми штучного інтелекту для обходу традиційних механізмів захисту. У зв'язку з цим особливої актуальності набуває концепція AI-driven cybersecurity, яка передбачає використання інтелектуальних механізмів для забезпечення автоматизованої протидії інтелектуальним загрозам. Реалізація такої концепції потребує створення комплексних систем кібермоніторингу, здатних до самоадаптації, автономного аналізу інформації та безперервного навчання.

Науково-методологічна основа застосування штучного інтелекту у сфері кібербезпеки має базуватися на системному підході, який передбачає розгляд інформаційно-аналітичних систем як складних відкритих систем із багаторівневою структурою взаємозв'язків. Використання методів системного аналізу дозволяє здійснювати декомпозицію складних процесів забезпечення кібербезпеки, визначати критичні елементи інфраструктури, аналізувати потоки інформації та оцінювати рівень стійкості системи до деструктивних впливів. Поєднання системного підходу з алгоритмами штучного інтелекту створює концептуальні передумови для формування адаптивних моделей кіберзахисту нового покоління [4].

Таким чином, використання штучного інтелекту та інтелектуального аналізу даних у забезпеченні кібербезпеки інформаційно-аналітичних систем правоохоронних органів є стратегічним напрямом розвитку сучасної системи безпеки держави. Інтелектуальні технології забезпечують можливість автоматизації процесів аналізу інформації, прогнозування кіберризиків, виявлення аномалій, підтримки прийняття управлінських рішень та формування проактивних механізмів протидії кіберзагрозам. Їх впровадження сприяє підвищенню ефективності діяльності правоохоронних органів, зміцненню стійкості інформаційної інфраструктури та розвитку сучасних підходів до кримінального аналізу в умовах цифрової трансформації суспільства. Перспективи подальших досліджень у даному напрямі пов'язані з удосконаленням методів когнітивної аналітики, розвитком адаптивних систем кіберзахисту, інтеграцією генеративного штучного інтелекту у процеси аналізу інформації, а також формуванням комплексних

міждисциплінарних моделей забезпечення кібербезпеки у діяльності правоохоронних органів [4].

**Список використаних джерел:**

1. Балтовський О.А., Форос Г.В., Пядишев В.Г., Сіфоров О.І. Системи підтримки прийняття рішень: навчальний посібник. Одеса: РВВ ОДУВС. 2022. 176 с.

2. Сучасні підходи щодо адаптивного автоматизованого управління складними системами в умовах невизначеності: монографія. /Кокошко В.С та ін.; за заг. ред. Форос Г.В. Одеса: ОДУВС, 2020. 180 с.

3. Шульга Є.М. Калугін В. Ю. Вдосконалення інформаційного забезпечення діяльності правоохоронних органів України. Матеріали круглого столу «Імплементація ILP моделі в Україні», 15 березня 2023 року. ОДУВС, 2023, С. 84-85

4. .Ханькевич А.М. Імплементація ilp моделі поліцейської діяльності у внутрішній безпековий сектор держави – з чого починати? Наукові перспективи № 5(35) 2023 с. 185-186/

## ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ ТА КІБЕРБЕЗПЕЦІ:АНАЛІТИЧНІ, ТЕХНОЛОГІЧНІ ТА ПРАВОВІ АСПЕКТИ

***Борисович Надія Олександрівна***
*здобувач вищої освіти бакалавра*
*1 курс, 1 група, «Правоохоронна діяльність»*
*Одеського державного університету внутрішніх справ*
*Науковий керівник:* ***Меликов Руслан***
*Науковий співробітник науково-дослідної лабораторії*
*з актуальних питань кримінального аналізу*
*доктор філософі в галузі права*

Сучасний розвиток інформаційних технологій суттєво впливає на діяльність правоохоронних органів та систему забезпечення національної безпеки держави. Одним із найбільш перспективних напрямів модернізації правоохоронної діяльності є використання технологій штучного інтелекту у кримінальному аналізі та кібербезпеці. Впровадження інтелектуальних систем дозволяє