УДК 004.056.5:004.738.5:004.8
DOI: 10.31673/2409-7292.2025.012201

Смолєв Є.С.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРОБЛЕМИ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ОРГАНІЗАЦІЇ: МОЖЛИВОСТІ ШТУЧНОГО ІНТЕЛЕКТУ В АНАЛІЗІ ТРАФІКУ

У високотехнологічному глобальному інтегрованому середовищі актуалізується проблема забезпечення надійності інформації, що супроводжується імплементацією високих стандартів щодо протоколів безпеки та захисту конфіденційності. Дослідження присвячене аналітиці потенціалу інструментарію штучного інтелекту в аналізі трафіку як основи вирішення проблеми вторгнень в інформаційну систему організації. Особливої ваги зазначена проблема набуває на тлі активізації внутрішніх та зовнішніх загроз військового часу в Україні. Роз'яснено дефініцію інформаційної безпеки в контексті надійно захищеного інформаційного простору, що забезпечує стійкість до деструктивного впливу загрозливих факторів. Обґрунтовано актуальність проблеми вторгнень в інформаційні системи, що зумовлена стрімким розвитком процесів цифровізації. З'ясовано, що інструментарій штучного інтелекту (ШІ) дозволяє формувати управлінські рішення значно вищого рівня ефективності, що дає змогу оперативно ідентифікувати загрози кібератак, оптимально реагувати на інциденти в сфері інформаційної безпеки, автоматизувати процеси оцінки ризику та наслідків кібер-інцидентів. Доведено функціональність технологій штучного інтелекту через мінімізацію впливу людського фактору, адже інструментарій ШІ дає змогу фактично вповні виключити його з процесу забезпечення захисту інформаційної безпеки, залишаючи в межах компетенції функціонал корекції та моніторингу. Проаналізовано основні типи сучасних рішень в галузі інформаційної безпеки на основі ШІ, що ефективно ідентифікують та нівелюють кібератаки, у тому числі – в превентивному контексті. Обґрунтовано, що активізація використання технологій ШІ на нинішньому етапі розвитку суспільства зумовлена можливістю інтеграції комплексних захисних мір протидії внутрішнім та зовнішнім загрозам інформаційної безпеки. У статті доведено, що використання потенціалу штучного інтелекту в аналізі трафіку з метою попередження та вирішення проблеми вторгнень в інформаційну систему організації дозволяє своєчасно ідентифікувати та знешкоджувати існуючі загрози, попереджувати потенційні ризики та оптимізувати протоколи інформаційної безпеки.

Ключові слова: інформаційна безпека, штучний інтелект, кібератака, трафік, аналітика, інформаційна система, вторгнення.

Вступ і формулювання проблеми

Загальною тенденцією сучасного глобального розвитку є формування інтегрованого інформаційного суспільства. Євроінтеграційні потуги України зумовлюють активізацію її залученості до зазначеного процесу на тлі глобальної цифровізації. Власне, саме інформаційному фактору відводиться на сьогодні першочергова роль у концепції стійкого розвитку як окремих організацій, так і держави, в цілому.

Основною компонентою алгоритму управління процесами суспільного розвитку позиціонується розширений та максимально оперативний доступ інформаційного забезпечення, що породжує супутні виклики кіберзагроз. Масова інтеграція інноваційних систем інформаційно-комунікаційного поля вимагає ефективних рішень в контексті цифрової безпеки. При цьому, одним із найбільш перспективних чинників забезпечення інформаційної безпеки вбачається інструментарій штучного інтелекту.

Штучний інтелект являє собою комплекс технологічних рішень, що має на меті імітацію когнітивного функціоналу людини. Штучний інтелект відкриває безапеляційно нові можливості технологічних інновацій в безпековій сфері. Інтеграція елементів ШІ в цифровій фінансовій сфері розширює можливості для підвищення рівня інклюзивності, безпеки, доступності та інноваційності останньої. Дієва концепція трансферу ШІ до бізнес-сектору повинна сприяти стійкості фінансових інституцій, стимулювати інвестиційну діяльність, гарантувати належний рівень безпеки фінансових операцій.

Імплементація технологій ШІ до фінансової системи дозволяє приймати ефективні управлінські рішення на підґрунті оптимального адаптаційного реагування в умовах ринкової динаміки та забезпечення нових конкурентних можливостей для бізнесу. І першочергова роль

у цьому відводитиметься саме інструментарію ШІ. Його функціонал в контексті вирішення проблеми вторгнень повинен мати на меті:

- оперативну та достовірну ідентифікацію загроз для інформаційних систем;
- використання різноманітних методів та засобів захисту інформації;
- формування надійних бар'єрів для проникнення;
- визначення «вузьких» локацій в існуючій системі захисту інформації.

У загальному, стратегія забезпечення інформаційної безпеки повинна передбачати сукупність методів та засобів захисту інформаційних активів. Цифровізація у глобальному контексті вимагає не лише підвищення рівня цифрової компетентності суспільства та практики акумуляції інформації на цифрових платформах, але й детермінує кібербезпеку як пріоритетну проблему.

Створення єдиного інформаційного простору організації з залученням інструментарію ШІ дає можливість відстеження потенційних ризиків у режимі реального часу, а також максимальної цифровізації документообігу та ефективного контролінгу. На підтвердження, концепція Індустрії 4.0 пропонує інноваційний потенціал для модернізації фінансового аналізу саме із залученням спектру цифрових інструментів, у тому числі, ШІ.

Аналіз останніх досліджень і публікацій

Дослідженню питань інтеграції потенціалу штучного інтелекту в контексті інформаційної безпеки присвячені низка напрацювань сучасних науковцівсобливості модернізації інтегрованих у проєкт «Цифрова держава» систем репрезентовані в межах дослідження О. Скибуна [1]. Науковцями І. Ревак і Р. Грень [2]досліджуються сучасні методи практичної боротьби з кіберзлочинністю в контексті державного та корпоративного рівнів. Дослідник І. Сопілко [3] розглядає нормативно-правове забезпечення системи захисту інформації та актуалізує потребу гармонізації секторального законодавчого поля в Україні комплементарно вимогам та нормам міжнародних стандартів. Г. Ситник, О. Зубчик, М. Орел [4] досліджують специфіку вдосконалення національної концепції стратегічного планування розвитку національного безпекового сектору в умовах інформатизації суспільства.

Проблематика апгрейду безпекових систем у контексті використання цифрового інструментарію досліджується В. Зянько, Т. Нечипоренко [5], Н. Козій, О. Синиця [6], О. Карій та ін. [7], O. Maslyhan та ін. [8], М. Тарасюк, О. Кощєєв [9], N. Moșteanu [10]. Низкою авторів, у тому числі, M. Soltanifar та ін. [11], I. Handayani, R. Agustina [12], A. Ghezzi, A. Cavallo [13] аналізуються аспекти розвитку кіберзахисту за посередництвом технологій ШІ.

Водночас, спостерігається певна фрагментарність щодо розвитку ролі технологій ШІ у секторі інформаційної безпеки. Розширена аналітика даної проблематики дозволить глибше своєчасно ідентифікувати ключові виклики та адаптувати стратегії подальшого розвитку цифрових технологій захисту.

Мета та завдання дослідження. Метою статті є аналіз потенціалу інструментарію штучного інтелекту в аналізі трафіку як основи вирішення проблеми вторгнень в інформаційну систему організації.

Для досягнення вказаної мети передбачено розв'язання наступних завдань:

- роз'ясненити дефініцію інформаційної безпеки в контексті надійно захищеного інформаційного простору;
- виділити основні функції інструментарію штучного інтелекту (ШІ) в сфері інформаційної безпеки;
- проаналізувати основні типи сучасних рішень в галузі інформаційної безпеки на основі ШІ;
- визначити пріоритетні напрямки протидії внутрішнім та зовнішнім загрозам інформаційної безпеки на основі аналізу трафіку за допомогою ШІ.

© Смолєв Є.С. (2025). Загальна характеристика проблеми вторгнень в інформаційну систему організації: можливості штучного інтелекту в аналізі трафіку. Сучасний захист інформації, 1(61), 145–152. https://doi.org/10.31673/2409-7292.2025.012201.

Основна частина

В умовах активної глобалізації інформаційна безпека позиціонується одним із найбільш впливових факторів гарантії безпечного середовища стійкого суспільного розвитку. Серед пріоритетних стратегій оптимізації безпеки інформаційного забезпечення варто виділити наступні:

- систематична аналітика інноваційних технологій ідентифікації загроз;
- інтеграція зусиль фахівців із кіберзахисту для виконання аудиту безпеки, впровадження технологій, розроблення захисних стратегій;
- впровадження стратегічних програм кіберстійкості;
- імплементація міжнародних стандартів безпеки, розширення напрямів міжнародної взаємодії, обміну досвідом, спільних навчальних проєктів;
- інтеграція інноваційних технологій захисту, шифрування та багатофакторної аутентифікації.

Для створення сучасних комплексних систем захисту інформації (КСЗІ) на сьогодні активно використовуються можливості штучного інтелекту та інноваційних технологій, аутсорсинг та моніторинг. Базовими принципами організації КСЗІ є системність, гнучкість управління, безперервність захисту, відкритість алгоритмів та простота застосування [11].

Пріоритетні завдання, які має успішно вирішувати КСЗІ в секторі проблеми вторгнень в інформаційну систему організації, передбачають:

- ефективне управління доступом до конфіденційних даних;
- захист інформаційних даних та контролінг діяльності користувачів системи;
- гарантування цілісності критичних ресурсів системи;
- управління засобами захисту.

Прогресивним рішенням для України в даному контексті стала ратифікація 23.02.2023 р. Угоди про участь країни у програмі ЄС «Цифрова Європа» (2023), що пропонує інноваційний формат можливостей для розвитку цифрового суспільства.

Штучний інтелект являє собою складну систему взаємозв'язків для формування інформаційних системних утворень. До основних технологій ШІ на сьогодні належать машинне навчання, когнітивістика, глибоке навчання, NLP (Natural Language Processing) та інші. Загалом, сучасні рішення ШІ впроваджуються за напрямками розпізнавання та синтезу мови, а також інтелектуальних систем підтримки прийняття рішень [3].

Необхідність інтеграції інструментарію штучного інтелекту в безпекову сферу зумовлена, першочергово, дефіцитом кваліфікованих фахівців із кіберзахисту та необхідністю оперативного реагування на існуючі та потенційні кіберзагрози. Водночас, сфера застосування ШІ наразі стрімко розширюється та набуває значущої ролі в питаннях кібербезпеки.

З його посередництвом відбувається аналіз великих даних з метою виявлення нових загроз та, зокрема, прогнозування атак нульового дня, виявлення певних закономірностей та проведення кластеризації даних. Із метою ефективної обробки значних обсягів інформації практично активно застосовуються нейронні мережі та кластеризація [7]. Штучний інтелект активно залучається до процесу відслідковування та прогнозування загроз.

Системи на основі інструментарію штучного інтелекту позиціонуються як ефективні засоби для виявлення та реагування на фішингові атаки та інші види соціальної інженерії, для ідентифікації та реагування на атаки розподіленої відмови в обслуговуванні. При цьому визначається джерело та тип атаки, а також шляхи мінімізації шкоди. Орім того, як свідчить практика, технології, що функціонують на основі ШІ, доцільно використовувати з метою виявлення та нейтралізації експлойтів нульового дня, тобто тих, що зорієнтовані на раніше невідомі вразливості програмного забезпечення [8].

Сучасний рівень технологічного розвитку зумовлює необхідність в пошуку інноваційних можливостей інструментарію ШІ. Системи виявлення вторгнень (IDS) на базі штучного інтелекту використовують розширені алгоритми для ідентифікації аномальної поведінки, що

© Смолєв Є.С. (2025). Загальна характеристика проблеми вторгнень в інформаційну систему організації: можливості штучного інтелекту в аналізі трафіку. Сучасний захист інформації, 1(61), 145–152. https://doi.org/10.31673/2409-7292.2025.012201.

зумовлює більш надійне та комплексне рішення безпеки. Метою функціонування таких систем є виявлення зловмисної активності та оперативне сповіщення фахівців із безпеки про потенційні загрози.

Серед переваг IDS на основі штучного інтелекту варто виділити здатність до ідентифікації специфічних інноваційних загроз, недоступних для традиційних IDS (наприклад, атаки нульового дня), а також функцію аналітики знаних обсягів інформації в режимі реального часу для ефективного та оперативного виявлення загроз. IDS на основі ШІ можуть динамічно навчитися на даних, які вони акумулюють, коригуючи базові алгоритми ідентифікації. Автоматизуючи ідентифікацію та аналітику потенційних загроз, IDS на базі ШІ зменшують робоче навантаження на фахівців із безпеки, вивільняючи ресурс для створення системи превентивного захисту [10].

Така концепція функціонування дозволяє IDS на базі ШІ працювати на випередження та виявляти нові загрози, перш ніж вони зможуть завдати будь-якої шкоди. В цілому, системи виявлення вторгнень на основі штучного інтелекту забезпечують комплексне рішення питання інформаційної безпеки.

Іншим важливим проблемним питанням технократичного сьогодення є потреба в запобіганні втраті даних (DLP) для оптимізації кібербезпеки. Такі рішення дають можливість організаціям вчасно ідентифікувати, ефективно керувати та оптимально захищати інформативні дані від випадкової або зловмисної втрати [12].

Рішення DLP із застосуванням штучного інтелекту акумулюють передові підходи до аналітики, машинне навчання та обробку природної мови для виділення шаблонів і аномалій у інформаційних масивах, а також превентивне попередження щодо потенційно можливих втрат даних або ризику їх нецільового використання. Застосування рішень DLP на базі ШІ відкриває можливості щодо виявлення використання конфіденційних даних з несанкціонованою метою, запобігати передачі даних у несанкціоновані місця призначення та контролювати дії користувачів, котрі мають доступ до конфіденційної інформації, а також попереджати організації про потенційно можливі витоки даних.

Серед позитивних наслідків застосування рішень DLP із підтримкою ШІ варто виділити високу швидкість реагування на загрози, мінімізацію витрат на керування інформаційною безпекою, зменшення ризику втрати даних чи їх несанкціонованого використання, економія часового ресурсу на регулярний моніторинг та аудит безпеки. Завдяки властивості оперативної ідентифікації загроз та сповіщення організації про потенційну втрату даних або неправильне використання, DLP-рішення на основі ШІ позиціонуються як вагомий інструмент оптимізації системи кібербезпеки.

Проте, не зважаючи на суттєві переваги та інноваційні можливості ШІ в сфері кіберзахисту, існують певні ризики та недоліки використання ШІ в системах інформаційної безпеки. В першу чергу, хакери можуть залучати можливості ШІ для автоматизації процесу пошуку та експлуатації вразливостей у мережах та додатках, скануючи значні обсяги даних в короткі часові проміжки та ідентифікуючи слабкі місця у безпеці. Також, наразі спостерігається активізація соціальної інженерії, та як ШІ можна використовувати для створення персоніфікованих фішингових повідомлень та шахрайських кампаній, котрі оптимально адаптуються під легітимні запити та повідомлення. ШІ може значно підвищити ефективність брутфорс-атак, добираючи паролі та ключі швидше, ніж традиційні програми.

Окрім того, ймовірним залишається застосовування ШІ з метою розробки складних для ідентифікації шкідливих програм, здатних безпроблемно обійти системи виявлення загроз та антивірусні програми. ШІ дає можливість хакерам приховувати місце розташування та джерело атаки, що суттєво ускладнює процес їх виявлення та переслідування кіберполіцією.

ШІ може використовуватись в злочинних намірах з метою аналітики даних про потенційну жертву для точного націлення атаки та вибору оптимального часу для її реалізації, щоб максимізувати збитки або уникнути викриття.

© Смолєв Є.С. (2025). Загальна характеристика проблеми вторгнень в інформаційну систему організації: можливості штучного інтелекту в аналізі трафіку. Сучасний захист інформації, 1(61), 145–152. https://doi.org/10.31673/2409-7292.2025.012201.

Актуальність вище зазначених ризиків використання можливостей ШІ в злочинних кіберцілях зумовлює необхідність прогресивного інноваційного розвитку засобів і методів захисту від кіберзагроз [5]. Системи на основі ШІ повинні оперативно сповіщати про небезпеки, розпізнавати нові типи зловмисного програмного забезпечення, захищати критично важливі масиви інформаційних даних.

Необхідно відзначити, що для машинного навчання необхідні набори інформативних даних, і в окремих випадках їх збір, акумуляція та застосування можуть відбуватись всупереч аксіомам щодо конфіденційності даних, тому вбачається необхідним передбачення проблеми такого роду та превентивне її вирішення. Іншим «підводним каменем» можуть виступати системи на основі ШІ, які роблять доступ до вихідних даних практично неможливим після завершення навчання. Анонімізація точок інформативних даних позиціонується як метод, що на сьогодні вимагає глибшого вивчення задля уникнення спотворення логіки програм.

Очевидним також є факт дефіциту експертів щодо забезпечення кібербезпеки на основі штучного інтелекту. Ефективність засобів мережевої безпеки значно зросте за умов наявності кваліфікованих співробітників, що здатні ефективно їх обслуговувати та налаштовувати, виконуючи управлінську функцію. Таким чином, команди фахівців у перспективі залишаться невід'ємною частиною відділів кібербезпеки, адже вагомою складовою системи прийняття рішень стабільно мають критичне мислення і креативний підхід, що не характерно для інструментарію ШІ [8].

Індустрія кібербезпеки в перспективі вдосконалюватиме інноваційні підходи з залученням ШІ для оптимізації системи кіберзахисту. Першочергово, доцільним вбачається застосовування багаторівневого підходу до інформаційної безпеки, запровадження передових методів навчання для розуміння інноваційної складності сучасних загроз, покращення моніторингу, виявлення та реагування на загрози за допомогою інструментарію ШІ. Такий підхід дозволить більш ефективно протидіяти загрозам, в тому числі у превентивному векторі захисту.

Сучасний стан розвитку інформаційного середовища переконує, що аналітика процесу взаємодії традиційних базових підходів до інформаційної безпеки та технологій ШІ дозволяє в широкому спектрі відтворити багатофакторність концепції синергії такого плану, в тому числі впровадження автоматичних систем захисту та попередження кіберзагроз. При цьому, технології ШІ в кібербезпеці позиціонуються як складна динамічна система, котра проявляє успішність функціонування в синергії технологічного, інтелектуального та інноваційного векторів.

Властивість систем ШІ прогнозувати ризики є надзвичайно важливою, так як вони можуть передбачити потенційний час виникнення порушення, оцінити прогностичні збитки та обрати способи їх відшкодування, беручи до уваги інвентаризацію IT-активів і визначаючи рівень загрози. Такий підхід до прогнозування, отриманий на основі аналітики засобами ШІ, позиціонується як дієвий засіб зміцнення кібербезпеки організації шляхом автоматизацій захисту областей, де системи та пристрої особливо вразливі.

Організації, які ефективно впроваджують технології штучного інтелекту для продуктивної аналітики та поведінкового аналізу, суттєво підвищують рівень ефективності ідентифікації атак, скорочуючи час реагування та витрат на організацію безпеки. Диференціювати технології поведінкового аналізу та предикативної аналітики доцільно за двома напрямами: за сценаріями використання та за функціональним чи технологічним типом (рис.1).

Основними типами технологій штучного інтелекту в системі інформаційної безпеки на сьогодні є:

1. NDR (Network Detection and Response) – аналітичні платформи, що спроможні ефективно ідентифікувати атаки на мережевому рівні. У даному випадку, за посередництвом ШІ, на основі бази даних та статистики щодо кіберзагроз, ідентифікуються потенційні загрози

© Смолєв Є.С. (2025). Загальна характеристика проблеми вторгнень в інформаційну систему організації: можливості штучного інтелекту в аналізі трафіку. Сучасний захист інформації, 1(61), 145–152. https://doi.org/10.31673/2409-7292.2025.012201.

в мережевому трафіку, із подальшим автоматичним оперативним реагуванням, що реалізовується шляхом зміни конфігурації мережевих пристроїв.

2. EDR (Endpoint Detection and Response) – платформи ідентифікації атак, що можуть ефективно виявляти та класифікувати загрози, а також самостійно реагувати на них. Іноді виконується розмітка даних за допомогою засобів ШІ даних та подальший контроль їх переміщення, що дозволяє ефективно виявляти внутрішні загрози.

3. TIP (Threat Intelligence Platform) – платформи попереднього детектування загроз та реагування на них. Даний продукт функціонує на основі індикаторів компрометації (IoC) та великої кількості різних даних (Data Lake).

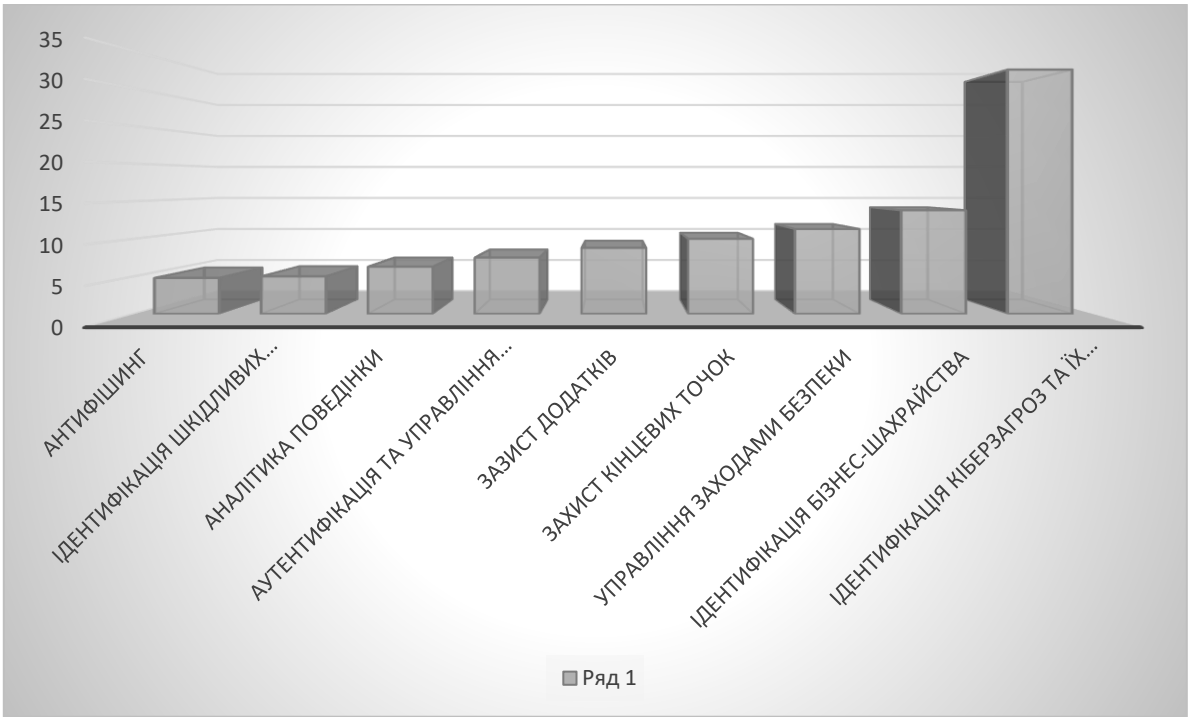

Рис. 1. Диференціація технологій штучного інтелекту за сценаріями використання
Джерело: [11,12]

4. SIEM (Security Information and Event Management) – рішення, що дозволяють в режимі реального часу аналізувати безпекові процеси та оперативно виявляти інциденти. Застосування технологій штучного інтелекту в даних продуктах дозволяє своєчасно ідентифікувати аномалії.

5. UEBA (User and Entity Behavior Analytics) – системи поведінкового аналізу користувачів та інформаційних сутностей. Основний сценарій – автоматичне виявлення аномалій в поведінкових моделях, з їх подальшою класифікацією за допомогою штучного інтелекту.

5. SOAR (Security Orchestration and Automated Response) – системи, що дозволяють виявляти загрози інформаційній безпеці та автоматизувати реагування на інциденти.

7. Засоби захисту додатків (Application Security) – автоматичний збір інформації про вразливі місця, атаки та зараження, та заснована на його результатах автоматизація захисних дій: сканування на вразливість, зміна правил захисту для веб-додатків, виявлення загроз та зміна ризикової моделі.

8. Антифрод (Antifraud) – системи, які дають змогу ідентифікувати загрози в бізнес-процесах та попереджати шахрайські операції в режимі реального часу шляхом визначення відхилень від встановлених процесів.

Результати

Результати дослідження концентрують увагу на властивості штучного інтелекту швидко осягати різноманітні ІТ-тенденції за допомогою алгоритмів машинного навчання та змінювати свої алгоритми відповідно до найновіших даних чи інформації.

Подібним чином штучний інтелект у сфері кібербезпеки використовується для складних мереж даних, які можуть швидко виявляти загрози безпеці та знищувати їх без участі людини. Окрім того, вчені розглядають перевагу використання штучного інтелекту у кіберзахисті за рахунок мінімізації потреб у людському факторі, що значно знижує ймовірність виникнення помилки. Водночас, ШІ в кібербезпеці не переймає весь функціонал експертів з інформаційного захисту, а лише оптимізує процес виявлення загроз та оперативного нівелювання небезпечних дій у мережі.

Таким чином, наукова позиція сучасності віддзеркалює висновки даного дослідження, що позиціонують технології ШІ як формувальника міцного альянсу між людиною та машиною, що оптимізує суспільні процеси, нівелює загрози кібербезпеці та зорієнтований на превентивний захист інформаційної безпеки. На сьогодні можна спрогнозувати зростання ролі засобів ШІ в процесі цифрової трансформації суспільства. Такий підхід дасть можливість значно підвищити рівень інформаційної безпеки, а також сприятиме формуванню ефективної конвергенції штучного інтелекту та кібербезпеки.

Висновки і рекомендації

Штучний інтелект став важливою частиною системи реалізації захисту інформації, пропонуючи ефективний критичний аналіз та дієву ідентифікацію загроз. В дослідженні встановлено, що штучний інтелект у сфері безпеки може ідентифікувати пріоритети ризиків, оперативно виявляти зловмисне програмне забезпечення в мережі, скеровувати реагування на інциденти та попереджати можливі атаки ще до їх виникнення.

Системи штучного інтелекту відіграють ключову роль у покращенні протоколів інформаційної безпеки, при цьому виключаючи ризики людського фактору. Окрім того, в процесі дослідження вдалося виділити ризики та виклики застосування штучного інтелекту в системах інформаційної безпеки, основні серед яких – ймовірність використання потенціалу ШІ кіберзлочинцями та загроза несанкціонованого витоку інформації.

У статті вдалося проаналізувати основні типи технологій ШІ, застосовувані в системі кібербезпеки. Окрім того, обґрунтовано високу ефективність систем підтримки прийняття рішень за допомогою технологій штучного інтелекту, а також попередження ризиків та автоматизації захисту. Очевидно, що ШІ спроможний створювати адаптивні системи безпеки, які можуть оперативно та ефективно реагувати на змінні загрози та атаки в реальному часі. При цьому, такі системи можуть автоматично коригувати правила та політики безпеки, щоб більш ефективно захищати мережі та дані.

Таким чином, поєднання можливостей штучного інтелекту та кібербезпеки відкриває можливості трансформації парадигми у сфері цифрової безпеки. В результаті розвитку можливостей такого симбіотичного зв'язку з’являються безпрецедентні можливості для протистояння кіберзагрозам. Висока аналітична точність технологій ШІ в синергії з його оперативним реагуванням на нові виклики позиціонує їх як рушійну силу перспективної кібербезпеки майбутнього.

Технології штучного інтелекту ефективно справляються з розшифруванням закономірностей та аномалій, тому можуть бути інструментом моніторингу загроз. Надійна стратегія інформаційної безпеки також допомагає захистити персональні дані населення та державні дані та алгоритми, що стає важливішим у міру розгортання нових моделей штучного інтелекту.

Перелік посилань

1. Skibun, O. Zh. (2021). Cybersecurity of electronic communications systems of public authorities of Ukraine. Visnyk of the National Academy of Public Administration. Series “Public Administration”, 1 (100), 30-39.

© Смолєв Є.С. (2025). Загальна характеристика проблеми вторгнень в інформаційну систему організації: можливості штучного інтелекту в аналізі трафіку. Сучасний захист інформації, 1(61), 145–152. https://doi.org/10.31673/2409-7292.2025.012201.

2. Revak, I. O., & Gren, R. T. (2021). Features of the formation of secure cyberspace in the context of the development of the digital economy. Innovative Economy, 3-4, 164-169. http://dspace.lvduvs.edu.ua /handle/1234567890/4099.

3. Sopilko, I. (2021). Information security and cybersecurity: a comparative legal aspect. Scientific works of the National Aviation University. Series: Legal Bulletin "Air and Space Law", 2 (59), 110-115. https://er.nau.edu.ua/handle/NAU/53733.

4. Sytnyk, H.P., Zubchyk, O.A., Orel, M.H. (2022). CONCEPTUAL UNDERSTANDING OF THE PECULIARITIES OF MANAGING INNOVATION-DRIVEN DEVELOPMENT OF THE STATE IN THE CURRENT CONDITIONS. Science and Innovation,18(2), 3-15. DOI: https://doi.org/10.15407/scine18.02.003

5. Зянько, В.,& Нечипоренко, Т. (2023). Штучний інтелект у фінансовому секторі України: драйвер розвитку та фактор модернізації. Innovation and Sustainability, 3, 6–21.

6. Козій, Н.С., & Синиця, О. О. (2020). Інфраструктура фінансового ринку України в умовах цифрової економіки. Економічний простір, 154, 156–160.

7. Карій, О.І., Лемішовська, О.С., & Воськало, Н.М. (2021). Обліково-аналітичний інструментарій в управлінні ризиками і забезпеченнями капіталу комерційного підприємства. Причорноморські економічні студії, 65, 104–111.

8. Maslyhan, O., Liba, N., Korolovych, O., Vovchenko, O., & Kvasnytska, R. (2022). Modelling the Performance of the Financial Market. Economic Affairs, 67(04), 631-642.

9. Тарасюк, М.В., & Кощеєв, О.О. (2017). Інновації в глобальній цифровій фінансовій сфері: оцінка трансформацій. Актуальні проблеми міжнародних відносин, 131, 94–110.

10. Moșteanu, N. R. (2019). International Financial Markets face to face with Artificial Intelligence and Digital Era. Theoretical and Applied Economics, 3, 123−134.

11. Soltanifar, M., Hughes, M., & Göcke, L. (2021). Digital entrepreneurship: Impact on business and society. Springer Nature. https://library.oapen.org/handle/20.500.12657/47272

12. Handayani, I., & Agustina, R. (2022). Starting a digital business: Being a millennial entrepreneur innovating. Startupreneur Business Digital (SABDA Journal), 1(2), 126-133. https://journal.pandawan.id/sabda/article/view/113

13. Ghezzi, A., & Cavallo, A. (2020). Agile business model innovation in digital entrepreneurship: Lean startup approaches. Journal of business research, 110, 519-537. https://doi.org/10.1016/j.jbusres.2018.06.013

Надійшла 08.02.2025