УДК 004.056
DOI: 10.31673/2409-7292.2025.020831

Гайдур Г.І., Гахов С.О., Скибун О.Ж.

ОЦІНКА СТАНУ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ ШІ

У даному дослідженні розглядається впровадження штучного інтелекту як інструменту для оцінки стану кібербезпеки критичної інфраструктури. Такий підхід є актуальним з огляду на зростаючу загрозу використання технологій штучного інтелекту кіберзлочинцями. Завдяки потужності штучного інтелекту стало можливим аналізувати великі масиви даних для виявлення шаблонів та аномалій, які свідчать про потенційні атаки, включаючи раніше невідомі їх варіанти. Це дозволяє забезпечити проактивний захист, що включає своєчасне попередження про загрози та перевірку цілісності даних, яка сприяє впевненому їх відновленню після атак.

Штучний інтелект також сприяє локалізації загроз через аналіз масштабу кібератак, визначаючи радіус їх поширення, що дозволяє ефективно ізолювати уражені системи та мінімізувати їхній вплив на інфраструктуру. Крім того, алгоритми штучного інтелекту оптимізують процес відновлення, скорочуючи час простою систем, зменшуючи збитки та забезпечуючи високу адаптивність до нових викликів кіберсередовища.

Враховуючи значну капіталоємність заходів, підхід до інтеграції штучний інтелект потребує ретельного вибору платформи, концепції та інструментарію. Розробка та впровадження рішень у сфері кіберзахисту здебільшого забезпечується міжнародними компаніями, що впливає на можливості використання таких технологій власниками та користувачами критичної інфраструктури. Таким чином, впровадження штучного інтелекту для оцінки стану кібербезпеки критичної інфраструктури є не лише перспективним напрямом кібербезпеки, але й обов'язковою умовою/вимогою для створення стійкої критичної інфраструктури, яка здатна ефективно адаптуватися до нових кіберзагроз/кібертак/кіберінцидентів.

Крім того запропоновано рекомендації щодо вибору моделі/платформи/інструментів ШІ для великих компаній – володіяльців/користувачів КІ у різних сферах економіки, оскільки питання вибору/використання моделей/платформ/інструментів ШІ вимагає долучення до критеріїв вибору такі чинники як вплив на стан національної безпеки та геополітичні стратегічні взаємовідносини між країнами

Ключові слова: уразливості, безпека держави, системи захисту, кібербезпека, кіберзахист, сталість та стійкість, критична інфраструктура, управління інформаційною безпекою, модель та інструменти, аналіз, оцінка стану безпеки, штучний інтелект.

Вступ

Сучасний етап цивілізаційного розвитку суспільства характеризується постійним зростанням як кількісних, так і якісних характеристик розвитку критичної інфраструктури. Так, «критична інфраструктура включає об'єкти, системи, мережі чи їх частини, руйнування або порушення функціонування яких може спричинити найтяжчі наслідки для соціальної та економічної сфер держави, підірвати її обороноздатність та національну безпеку», коли «у мирний час її діяльність забезпечує життєво-важливі функції суспільства, захищає базові потреби його членів та сприяє формуванню відчуття безпеки і захищеності» [1, с.11], а у військовий час ще і підтримує обороноздатність та сприяє координації військових дій. Критична інфраструктура насамперед відіграє ключову роль у забезпеченні базових умов існування населення завдяки постачанню життєво-важливих послуг. Тому її захист і стале функціонування є пріоритетом, адже будь-які порушення можуть мати катастрофічні наслідки для суспільства та національної безпеки. Стабільне функціонування критичної інфраструктури (далі – КІ) є фундаментом життєдіяльності всіх сфер економіки та суспільних відносин країни. У сучасних умовах впровадження новітніх технологій у процеси управління та технологічні операції підвищує уразливість управління та функціонування як об'єктів КІ, такі і окремої сфери економіки. Зважаючи на постійне ускладнення та автоматизацію усіх управлінських та технологічних процесів, залучення елементів штучного інтелекту (далі – ШІ), Інтернету речей (далі – IoT), робототехніки тощо. Водночас можливості ШІ починають все частіше використовуватися як для організації атак на об'єкти КІ, так і для створення ефективних систем їх захисту. Ось чому кібербезпека критичної інфраструктури стає невід'ємною складовою функціонування держави та бізнесу. У контексті зростання цифрових загроз ШІ виступає ключовим інструментом для оцінки та захисту кіберпростору. Адже його використання покращує аналіз ризиків, виявлення аномалій і прогнозування потенційних атак

у реальному часі, що в кінцевому результаті сприяє підвищенню стійкості та безпеки об'єктів КІ. Таким чином здійснення оцінки стану кібербезпеки критичної інфраструктури з використанням ШІ вимагає додаткової уваги з огляду на новизну.

Постановка проблеми

Останнім часом тема застосування елементів та можливостей ШІ стрімко набуває популярності, перетворюючись на справжній мейнстрім. Новітні технології ШІ активно впроваджуються на прикладному рівні всіма учасниками ІТ ринку, перш за все тими хто займається розробкою спеціалізованого програмного забезпечення, автоматизації процесів управління та виробництва. Проблематика сьогодення полягає у стрімкому зростанні кібервпливу на КІ з боку шахраїв та зловмисників, які використовують новітні технології, передове обладнання та спеціалізоване програмне забезпечення для здійснення своїх злочинних намірів в кіберпросторі. Ці дії несуть серйозні загрози безпеці інформаційних мереж/систем, збереженню даних, чутливої/конфіденційної інформації та функціонуванню важливих державних та приватних об'єктів, що потребує адекватної реакції та розробки ефективних механізмів захисту, перш за все кіберзахисту. Насамперед мова йде про інфраструктуру великих компаній, корпорацій, підприємств, установ від сталого функціонування яких залежить життя людей. Отже мова йде про сталість та стійкість функціонування такої інфраструктури під час кіберінцидентів. Так, «під стійкістю критичної інфраструктури розуміється її спроможність надійно функціонувати в нормальному режимі, адаптовуватися до умов, що постійно змінюються, протистояти й швидко відновлюватися після аварій і технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ» [1, с.12]. А тому вкрай важливо діяти на випередження, впроваджуючи інноваційні системи захисту, управління, тестування та проєктування із застосуванням сучасних інструментів, технологій, тенденцій тощо. На сьогодні однією з найбільш динамічно розвиваючих технологій є ШІ. Елементи ШІ знаходять застосування серед усіх учасників ІТ-ринку, включаючи зловмисників, які використовують їх у своїх цілях. Отже, протидіяти таким загрозам можливо лише через активне впровадження ШІ для забезпечення високого рівня кібербезпеки та кіберзахисту. Зокрема, питання оцінки стану кібербезпеки критичної інфраструктури з використанням ШІ є надзвичайно актуальним і потребує постійної уваги дослідників і експертів у сфері кібербезпеки, а також тестувальників і розробників програмного забезпечення. Використання штучного інтелекту для оцінки стану кібербезпеки критичної інфраструктури є надзвичайно важливим, оскільки людські можливості обробляти величезні обсяги даних є обмеженими. Завдяки ШІ стає можливим ефективний аналіз великих масивів інформації, що дозволяє своєчасно виявляти потенційні загрози та забезпечувати належний рівень захисту критично важливих об'єктів.

Аналіз останніх досліджень показав, що питання сталості та стійкості функціонування критичної інфраструктури, а також стану кібербезпеки критичної інфраструктури є досить актуальними серед сучасних дослідників та науковців, таких як: С. Гахов, С. Гончар, Ю. Дерйс, В. Дмітрієв, Я. Жахалов, І. Ткаченко, В. Козачок, Д. Ланде, Т. Литвинова, І. Мальцева, Я. Мануілов, Дж. Маккген, В. Овсяніков, С. Смирнов, І. Стьопочкіна, Ю. Черниш, Е. Фуллер тощо.

Незважаючи на значний обсяг проведених досліджень, питання застосуванням ШІ для оцінки стану кібербезпеки критичної інфраструктури залишається лише окремою складовою ширшої проблематики, що розглядається у статті. Це питання потребує подальшого вдосконалення та інтеграції нових підходів для забезпечення більш ефективного захисту критично важливих об'єктів.

Метою статті є дослідження питань використання ШІ під час оцінки стану кібербезпеки критичної інфраструктури.

Завданнями статті є:

– розгляд оцінки стану кібербезпеки критичної інфраструктури;

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025). Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. Сучасний захист інформації, 2(62), 31–41.
https://doi.org/10.31673/2409-7292.2025.020831

– розгляд використання ШІ в рамках оцінки стану кібербезпеки критичної інфраструктури;

– напрацювання пропозицій щодо використання ШІ в рамках оцінки стану кібербезпеки критичної інфраструктури.

Методи дослідження, використані у процесі написання статті, передбачають застосування загальнонаукових та емпіричних прийомів, що ґрунтуються на системному підході. Також у процесі роботи застосовувались такі загальні методи досліджень, як узагальнення та порівняння.

Виклад основного матеріалу дослідження

Подальший розвиток усіх сфер економіки визначається ускладненням процесів управління та виробництва через широке застосування цифрових технологій, комп'ютеризації, автоматизації, віртуального кіберпростору, ресурсів електронних комунікацій та глобальної мережі передачі даних. Вказане формує новий тип економіки та виробництва, що характеризується як цифровий. На фоні цього цифровізація, комп'ютеризація, автоматизація широко запроваджується на інфраструктурних об'єктах (для управління та для виробничих процесів), формуючи новий кіберпростір інфраструктури різних сфер економіки та суспільства. Разом з зростанням рівнів цифрової та віртуальної економіки та цифрового суспільства зростає і рівень впливу кіберінцидентів та кіберзагроз. В умовах сучасних викликів трансформується розуміння питань захисту та безпеки, де фізична безпека доповнюється кібербезпекою та кіберзахистом як всієї інфраструктури, так і її окремих складових – об'єктів інфраструктури. Особливу увагу слід приділяти КІ та її об'єктам, які формують нову реальність, в якій функціонують сучасна людина і держава. Від рівня стійкості КІ до кіберінцидентів та кібератак залежить не лише безпека та життя людей, але й стабільність функціонування держави загалом. Це потребує постійного вдосконалення «принципів та алгоритмів побудови надійного кіберзахисту, оперативного реагування на масштабні кіберризики» [2, с.145]. Адже «постійне удосконалення злочинних та хакерських посягань» на персональні дані, чутливу/конфіденційну інформацію» потребує практичного впровадження та посилення кіберзахисту інформаційно-комунікаційних і комп'ютерних систем, критичної інформаційної інфраструктури», що в свою чергу вимагає здійснення «оцінювання стану кібербезпеки» адже «оцінка ризиків кібербезпеки допомагає краще розуміти вразливість систем до кібератак, а також розставити пріоритети у витратах на забезпечення безпеки.» [2, с.145-146]. Крім того «в сучасних умовах таке поняття, як «ризик кібербезпеки» безпосередньо пов'язаний з автоматизацією робочого процесу, тому управління цими ризиками також має бути автоматизовано за допомогою відповідних програмних продуктів для цих цілей (аналіз вразливості, захист інформації, інше).» [2, 148].

Так, у «Зеленій книзі з питань захисту критичної інфраструктури в Україні», під КІ розуміється «система та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки.» [1, с.15]. У Європейській програмі захисту КІ, термін КІ визначається, як «фізичні та інформаційні технологічні об'єкти, мережі, послуги та активи, які, якщо їх перервати або знищити, справлять серйозний вплив на здоров'я, безпеку, безпеку чи економічний добробут громадян або ефективне функціонування урядів у країнах ЄС» [3]. На сьогодні важливим є створення таких умов за яких мережа/система/ІКС КІ продовжує функціонувати на мінімально-допустимому рівні, а команда реагування на кібкерінцидент/кібератаку працює над мінімізацією впливу (зовнішні та/або внутрішні подразники) негативних наслідків від кіберінциденту/кібератаки. При цьому захист КІ розглядається як «комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості КІ» [1, с.15]. А отже ефективна робота команди реагування на кіберінциденти залежить від комплексного підходу з реалізації заходів,

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025). Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. Сучасний захист інформації, 2(62), 31–41.
https://doi.org/10.31673/2409-7292.2025.020831

де будуть взаємопов'язаній нормативно-технічні, організаційно-технічні та кадрові заходи на об'єктовому, корпоративному та галузевому рівнях. Так, в рамках «Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти та кібератаки» «встановлюються вимоги до інформаційного обміну, координації та спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти та кібератаки», а також «надання шаблонів і порядку дій відповідальних осіб по виконанню покладених на них обов'язків в частині інформаційного обміну, координації та спільних дій під час реагування на кіберінциденти та кібератаки» [4, с.3]. В свою чергу питання організаційно-технічного захисту здійнюються відповідно до побудови організаційно-технічної моделі кіберзахисту, яка є «комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливостей комунікаційних систем» [5]. Так, «Порядком взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти та кібератаки» встановлюються вимоги щодо інформаційного обміну, координації дій та взаємодії між суб'єктами забезпечення кібербезпеки у разі виникнення кіберінцидентів або кібератак, а також «містить шаблони та алгоритми дій для відповідальних осіб, що визначають порядок виконання обов'язків, пов'язаних з реагуванням на інциденти та координацією зусиль між учасниками» [4, с.3]. Треба враховувати, що організаційно-технічний захист реалізується через побудову відповідної моделі кіберзахисту, яка «передбачає комплекс заходів, засобів та ресурсів, спрямованих на оперативне (кризове) реагування на кіберінциденти та кібератаки», а також «включає впровадження контрзаходів, що мають на меті мінімізацію вразливостей у комунікаційних системах» [5]. При цьому треба зважати, що створена модель кіберзазхситу не може бути статичною, адже кіберландшафт постійно трансформується, змінюються методи, механізми та інструменти кіберінцидентів та кіберзлочинів. Це пов'язано з тим, що «поширення ландшафту загроз та ускладнення інструментарію їх реалізації спонукає уряди провідних країн удосконалювати архітектуру національних систем кібезбезпеки, змінювати стратегію і тактику протидії кіберзагрозам» [2, с.144]. Так, для створення ефективної моделі кіберзахисту на усіх рівнях (обєктовий/корпоративний/галузевий) необхідно широке використання новітніх технологій, інструментів, апаратно-програмного забезпечення, кваліфікованих спеціалістів з кібербезпеки. Прикладом такого є бурхливий розвиток технологій використання можливостей ШІ, IoT, машинного навчання тощо.

Наприклад «за даними Spherical Insights, у 2022 році обсяг глобального ринку ШІ для кібербезпеки оцінювався у понад 15,25 млрд. доларів США, а до 2032 року має вирости до позначки у понад 96.81 млрд. доларів США», а тому «вже за два-три роки сферу кібербезпеки неможливо буде уявити без алгоритмів машинного навчання та нейромереж» [6]. Наведені вище орієнтовні прогнозні дані є лише оцінкою майбутнього, проте тенденція стрімкого зростання ринку ШІ є очевидною й нею не можна нехтувати. Важливо також враховувати комплекс технологій, які сприяють розвитку ШІ, зокрема машинне навчання, нейронні мережі та IoT. На сьогодні «ШІ у кібербезпеці вже перетворився на двосічне лезо, яке може бути як найбільшою загрозою, так і найефективнішим засобом захисту» оскільки «залежить від того, у чиїх руках опиняється цей інструмент» [6]. Реалії сучасності такі, що «хакери досить швидко опановують технології ШІ й активно використовують їх для кібератак за низкою напрямків» серед яких можна виділити такі: «автоматизація процесів зламу (пошук вразливостей, подолання засобів захисту); спрощення та автоматизація цільового фішингу для викрадення особистих даних; виготовлення дипфейків для шахрайства та соціальної інженерії; «отруєння даних» для виведення ладу ШІ-моделям для будь-яких завдань; спрощення розробки шкідливого софту» [6]. Незважаючи на виклики, що виникають, їх необхідно вирішувати по мірі надходження.

Так, результати «опитування понад 500 відповідальних керівників енергетичних компаній, проведеного компанією Siemens у 2019 році» [8, с.18] показали, що ШІ починає

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025). Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. Сучасний захист інформації, 2(62), 31–41.
https://doi.org/10.31673/2409-7292.2025.020831

використовуватися, але поки що не має повного домінування. Загальні результати цього опитування викладені у таб. 1 [8, с.]. Також необхідно зважати, що на сьогодні вказаний рівень використання ШІ буде вищим, адже технології постійно розвиваються та поширюються. Приклади реалізації нових моделей організації роботи енергетичних ринків у таб. 2. [8, с.21-22].

Таблиця 1

Застосування ШІ в енергетичних компанія [8, с.18]

Напрям використання ШІ в енергетичних компаніях	**Використання ШІ** (2019 рік)
Автоматизація машин та обладнання	30 %
Аналіз та прогнозування термінів технічного обслуговування	28 %
Оптимізація технологічних процесів, машин та програмного забезпечення	28 %
Моніторинг рівня безпеки та запобігання інцидентам	26 %
Автоматизація немеханічних процесів	24 %
Контроль якості	23 %
Спілкування з клієнтами/персоналізація	22 %
Планування та прийняття рішень	21 %
Кібербезпека	21 %
Продажі та маркетинг	21 %
Віртуальні системи, експертні системи, чат-боти	17 %
Логістика, ланцюжки постачання	16 %
Дизайн нових продуктів	11 %
Моделювання (цифрові моделі процесів)	11 %

Відтак, головним завданням, яке сьогодні стоїть перед кіберспільнотою, є створення гнучкої моделі кіберзахисту – з широким використанням технологій ШІ, машинного навчання, нейромереж та IoT – здатної ефективно протидіяти сучасним кіберзагрозам і забезпечувати можливість подальшої модернізації. Варто зауважити, що «серед галузей, які найкраще підготовлені до майбутніх викликів, домінують ті, що найбільше страждають від інцидентів кібербезпеки, проте водночас отримують найбільшу вигоду від ефективного стримування загроз» [9]. Так, активне протистояння кібератакам/кіберзагрозам дійсно позитивним чином впливає на увесь спектр організаційний/технічних/людських заходів, які забезпечують достатній рівень кіберзахисту на об’єктовому/корпоративному/галузевому рівнях.

Варто зазначити, що «серед галузей, які найкраще адаптовані до майбутніх викликів, переважають ті, що найбільше страждають від інцидентів кібербезпеки», оскільки «отримують значні переваги від ефективного стримування кіберзагроз/кіберінцидентів» [9]. Так, активна протидія кібератакам та кіберзагрозам позитивно впливає на весь комплекс організаційних-технічних, нормативно-правових заходів разом із підготовкою спеціалістів з кібербезпеки та загальною підготовкою спеціалістів компаній, які працюють з даними, в системі/мережі/ІКС. В кінцевому результаті це забезпечує високий рівень кіберзахисту на об’єктному, корпоративному та галузевому рівнях.

Група дослідників (О. Скіцько, П. Складанний, Р. Ширшов, М. Гуменюк, М. Ворохоб) розглядаючи «загрози та ризики використання штучного інтелекту» відзначають, що «ризики, породжені системами штучного інтелекту, багато в чому унікальні», адже вони . можуть бути навчені на даних, які можуть змінюватися з часом, іноді суттєво й несподівано, впливаючи на функціональність і надійність системи у спосіб, який важко зрозуміти», а складність самих систем штучного інтелекту «ускладнює виявлення збоїв і реагування на них» [7, с.9].

Важливим кроком до цього є застосуванням ШІ для оцінки стану кібербезпеки КІ. Так, до «ключових напрямків застосування алгоритмів машинного та глибокого навчання у сфері кіберзахисту» як: «автоматична обробка та аналіз звітів безпеки», «детектування вторгнень у систему», «моніторинг і аналіз трафіку», «боротьба із хибною тривогою», «оновлення інфраструктури», «прогнозування загроз», а до «переваг застосування ШІ в кібербезпеці»

можна віднести: «швидкість реагування», «автоматизація та економія ресурсів», «тестування систем та виявлення вразливостей», «розробка стратегій кіберзахисту» [6].

Таблиця 2

Технологічний розвиток та трансформація моделей організації роботи енергетичних ринків [8, с.21-22]

Новітні технології	**Бізнес-моделі**	**Дизайн ринку**	**Особливості роботи системного оператора**
Перетворення відновлюваної енергії в інші форми енергії: у тепло (*power-to-heat*), у газ (*power-to-hydrogen/methane*[36])	Агрегатори,[37] наприклад віртуальні електростанції (*Virtual power plants - VPPs*)	Скорочення періодичності фіксації значень (*time granularity*) даних щодо трансакцій на ринку (деталізація даних у часі)[38]	Майбутня роль оператора системи розподілу
Перетворення відновлюваної енергії у «накопичену енергію» (*power-to-power*) для зміщення поточного профіциту енергії у періоду дефіциту енергії[39]	Пірингова торгівля (*peer-to-peer (P2P)*)	Збільшення деталізації даних у просторі (*space granularity*) щодо трансакцій на ринку[40]	Співпраця між операторами систем передачі та розподілу
Акумуляторні батареї[41] на стороні споживача (за лічильником)	Енергія як послуга (*Energy-as-a-service - EaaS*)	Інноваційні рішення ринку допоміжних послуг	Віртуальні повітряні лінії
Акумуляторні батареї промислового рівня	Моделі оплати у міру використання (*Pay-as-you-go - PAYG*)	Переформатування ринку потужності	Удосконалене прогнозування генерації ВДЕ
Розумні зарядки електромобіля	Моделі власності громад (енергетичні кооперативи)	Ринкова інтеграція децентралізованих енергетичних систем (*distributed energy resources*)	Інноваційна робота гідроакумулюючих насосних станцій
Розумне обладнання (*Internet of Things*)		Регіональні/локальні ринки	Зміна пропускної спроможності ліній (*Dynamic line rating - DLR*)
ШІ та великі бази даних (*Artificial intelligence and big data*[42])		Чистий розрахунок (Net billing schemes)	Віртуальні лінії передачі (*Virtual power lines - VPLs*)
Блокчейн (*Blockchain*)		Багатозонні тарифи (Time-of-use tariffs)	
Мікромережі ВДЕ[43]			
Розумні мережі (*Smart Grids*)			

Опитування, проведене командою CISCO серед понад 8 000 респондентів, дозволило визначити «готовність до кібератак за п’ятьма ключовими напрямами, які є критично важливими для забезпечення безпеки сучасних організацій», а саме: «розвідка особистих даних (Identity Intelligence), стійкість мережі (Network Resilience), надійність машин (Machine Trustworthiness), вдосконалення хмарних технологій (Cloud Reinforcement), а також використання штучного інтелекту у заходах безпеки (AI Fortification)» [9].

Група дослідників (І. Ткаченко, В. Козачок, С. Гахов, В. Дмітрієв) наголошують на тому, що «впровадження оцінки стану кібербезпеки об’єктів критичної інформаційної інфраструктури в режимі реального часу, з використання індикаторів кіберзагроз на рівні прийняття рішень дозволить забезпечити інформацією загальнодержавний центр кібер-стійкості CRC (Cyber Resilience Center) у разі його створення» [10]. Вказане питання потребує всебічного опрацювання та швидкої реалізації, зважаючи на темпи впровадження нових

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025). Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. Сучасний захист інформації, 2(62), 31–41.
https://doi.org/10.31673/2409-7292.2025.020831

технологій, а також викликів щодо кібербезагроз. С. Гончар розглядаючи питання «оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури» обґрунтовує необхідність використання «поняття комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури» разом із використанням «методів обчислення сумарного ризику комплексного ризику», а також «алгоритмічне та програмне забезпечення обчислювальних систем для розрахунку зазначених ризиків» [11], що в цілому відповідає сучасним викликам, які постають перед володіяльцями/користувачами КІ в рамках кіберзахисту та кібербезпеки для сталого та стійкого функціонування мереж/систем/ІКС.

В свою чергу дослідників (О. Скіцько, П. Складанний, Р. Ширшов, М. Гуменюк, М. Ворохоб) наголошують на тому, що «оцінка ландшафту можливих ризиків та їх ідентифікація є важливим етапом управління ризиками, що виникають внаслідок використання систем ШІ» [7, с.14]. Вказаний процес є ітеративним і «спрямований на пошук нових типів ризиків та визначення їх основних характеристик для подальшої інтерпретації, аналізу і обробки», а «завдання ідентифікації ризиків полягає у виявленні аномалій у масивах даних, що стосуються діяльності у відповідній галузі застосування ризик-менеджменту», при цьому «аномалії можуть бути наслідком взаємозв'язків та взаємодій між об'єктами та суб'єктами діяльності, які створюють ще не визначені ризикові ситуації або потенційні джерела їх появи у майбутньому» [7 с.14].

На основі інформації та даних, представлених у таких документах ISACA як: Стан кібербезпеки за 2021–2023 роки; Звіт про стан кібербезпеки 2021– 2023 роки; Заключні думки щодо стану кібербезпеки у 2021–2023 роках [14] можна побачити динаміку впровадження ШІ за галузями (рис. 1) та застосування ШІ у сфері кібербербезпеки (рис. 2).

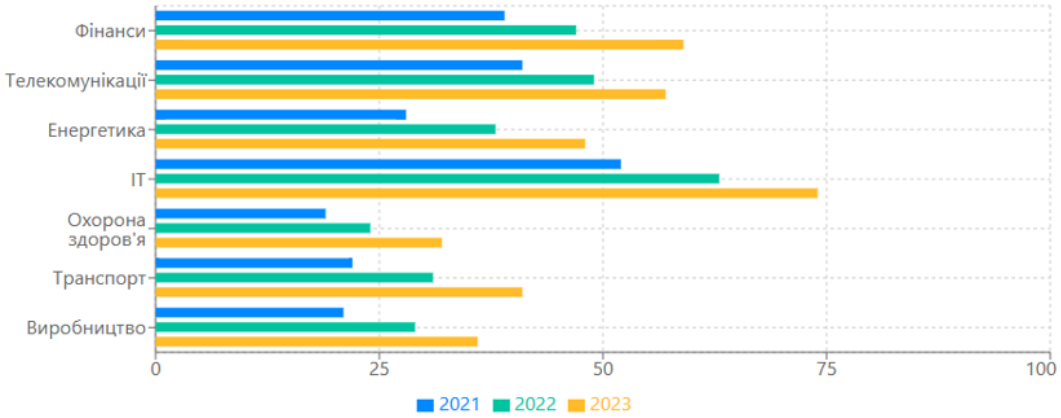

Рис. 1. Динаміка впровадження ШІ за галузями у 2021–2023 роках [14]

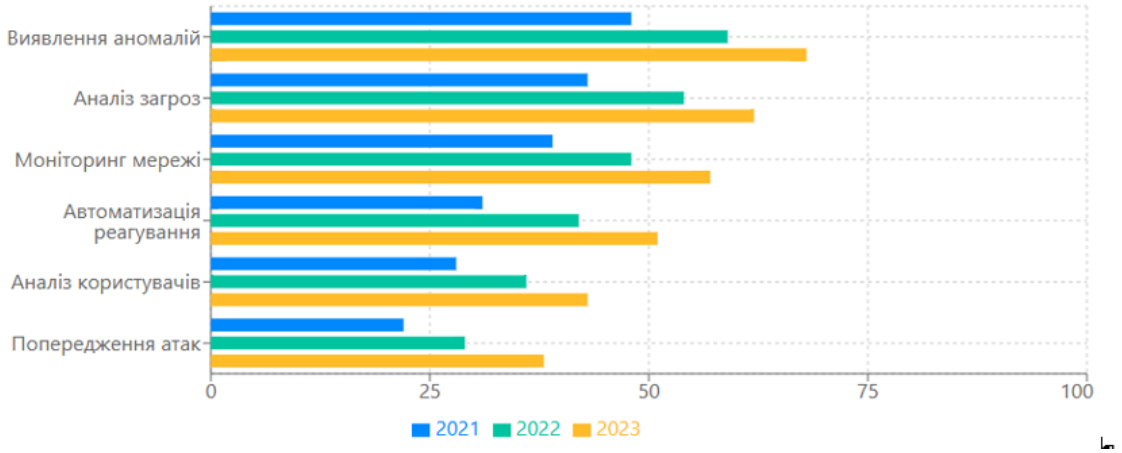

Рис. 2. Застосування ШІ у 2021–2023 роках у сфері кібербезпеки [14]

Заходи кіберзахисту охоплюють широкий спектр дій. Наприклад як зазначає Я. Мануйлов, цей перелік включає: «ідентифікацію – виявлення реальних та потенційних кіберзагроз для їх запобігання й нейтралізації; захист – розроблення та впровадження методів, засобів і процедур, спрямованих на забезпечення стабільності та надійності функціонування інформаційних, телекомунікаційних і технологічних систем; виявлення – моніторинг, збір та обробка даних про нетипові події у кіберпросторі; реагування – заходи для запобігання кіберінцидентам і кібератакам, мінімізації їх наслідків, удосконалення систем кіберзахисту з урахуванням реальних і потенційних ризиків; відновлення – відновлення функціонування систем після кібератаки, включно з поновленням пошкодженої або видаленої інформації, та створення умов для проведення розслідування.» [2, с.158-159]. Вказаний перелік показує складність питання побудови ефективної моделі кіберзахисту. При цьому слід враховувати, що заходи кіберзахисту постійно ускладнюються у відповідь на еволюцію кібератак. Це вимагає переходу на новий рівень технологічних можливостей, включаючи використання штучного інтелекту (ШІ), Інтернету речей (IoT), машинного навчання та нейромереж, що забезпечують ефективну адаптацію до зростаючих загроз.

Дж. Маккген, коментуючи «використання ШІ для забезпечення кібервідмовостійкості КІ», зазначає, що «сильна стратегія, побудована на основі ШІ, здатна мінімізувати збої та скоротити час простою без необхідності виплати викупу» адже на його думку «кібервідмовостійкість є ключовим елементом виживання, забезпечуючи структуру для ефективного виявлення загроз, аналізу атак, швидкого відновлення та адаптації до постійно змінюваних ризиків» [12]. Так, запровадження новітніх технологій дає змогу оптимізувати роботу команди реагування на кібератаки/кіберінциденти таким чином, що рутинна і монотонна робота з великими обсягами даних буде виконуватися ШІ.

Е. Фуллер у своєму дискурсі щодо «забезпечення запобігання витоку даних наступного покоління (DLP)» акцентує увагу на використанні передових технологій, таких як штучний інтелект і машинне навчання, у запобіганні витоку даних наступного покоління, а також підкреслює важливість процесу DLP (Data Loss Prevention) як одного з ключових механізмів захисту конфіденційної інформації, виділяючи при цьому використання моделі машинного навчання, яка дозволяє підвищити точність класифікації даних і виявлення загроз. Крім того, він звертає увагу на інноваційні рішення, впроваджені платформою Nightfall AI, що включають підтримку складних правил для детекторів, здатність працювати з текстом з багатьох типів файлів, масштабування системи для аналізу великих обсягів даних і реалізацію автоматичних дій для захисту [13]. Ця концепція особливо важлива в сучасному контексті зростаючих кіберзагроз, адже забезпечення безпеки даних потребує впровадження передових інструментів, здатних адаптуватися до нових викликів. Інтеграція ШІ та машинного навчання є логічним і необхідним етапом еволюції систем кіберзахисту, забезпечуючи швидку обробку великих обсягів даних, точність виявлення загроз і автоматизацію заходів захисту. Таким чином, впровадження таких технологій не лише мінімізує ризики витоку даних, але й закладає основу для створення більш стійкої й адаптивної інфраструктури. В свою чергу Дж. Макген підкреслює важливість штучного інтелекту у забезпеченні кіберстійкості даних КІ, зокрема через «виявлення шаблонів і аномалій для раннього попередження про загрози, перевірку цілісності даних для впевненості в їх відновлюваності, визначення масштабу атак шляхом аналізу мережевих журналів, а також оптимізацію стратегій відновлення після атак» [12]. Слід відзначити, що інтеграція ШІ в кібербезпеку бізнесу включає кілька ключових етапів: «визначення вимог – формулювання цілей і параметрів для впровадження рішень; проєктування – розроблення концепції й архітектури системи; технічна реалізація – виконання програмування, налаштування та інтеграції рішень у бізнес-процеси; контроль якості – тестування системи, перевірка її функціонування та відповідності вимогам; реліз та підтримка – запуск системи в експлуатацію та забезпечення її стабільної роботи з подальшою технічною підтримкою.» [6]. Так, на сьогодні вказані роботи є досить важливими з огляду на

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025). Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. Сучасний захист інформації, 2(62), 31–41.
https://doi.org/10.31673/2409-7292.2025.020831

необхідність вибору платформи, концепції та інструментарію ШІ. Зважаючи на значну капіталоємність цих заходів готові продукти та послуги з впровадження, адаптації та подальшого використання надаються міжнародними компаніями, що також впливає на поширення серед компаній, які виступають володіяльцями/користувачами КІ.

Дослідники (О. Скіцько, П. Складанний, Р. Ширшов, М. Гуменюк, М. Ворохоб) звертають увагу на такі загрози використання ШІ як: «посилення кібератак; етворення каналів витоку інформації з обмеженим доступом; атаки отруєння даних (*Data Poisoning,* DP)» та «містифікація даних» [7, с.10]. При цьому вони наголошують на тому включення неточних/помилкових/зловмисних даних «у навчальний набір» даних для ШІ може мати досить сумні наслідки. Нижче наводиться приклад, коли «спеціалістами компанії «Vulcan» була виявлена схильність генеративної СШІ ChatGPT до створення недостовірних (галюцінованих) фактів і даних (hallucinated facts and figures). Представлено схему реалізації загрози витоку інформації через недійсні пакети ШІ (рис. 3) в рамках такої загрози як «де за основу взято «містифікація даних» [7, с.10].

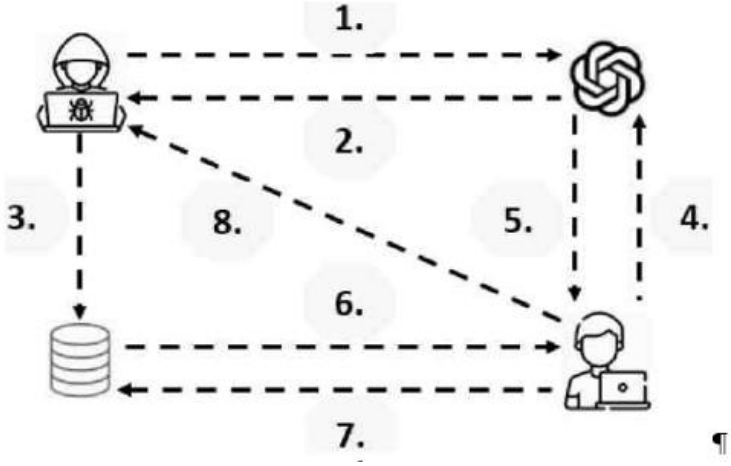

Рис. 3. Реалізація загрози витоку інформації через недійсні пакети СШІ

Так, «саме, ChatGPT в разі запиту рішень для кодування може пропонувати неіснуючі пакети (рис. 3, кроки 1, 2)», які «можуть бути використані зловмисниками для перетворення їх в замаскований шкідливий код, який завантажується в репозиторії кодів (крок 3), а коли «користувач, запитує у ChatGPT рекомендації щодо розробки (кроки 4, 5), в пропозиціях (кроки 6, 7) можуть з'явитися ці шкідливі пакети» і далі «ці недостовірні пакети ШІ потенційно перетворяться на канал витоку інформації користувач (крок 8)» [7, с.10]. Вказане є досить важливим і актуальним, зважаючи на постійні збільшення обсяги інформації.

Сучасне застосування ШІ та машинного навчання значно підвищує рівень виявлення кіберзагроз у системах/мережах/ІКС, і ця тенденція стабільно зберігається. Наш прогноз щодо ефективності виявлення кіберзагроз традиційними системами та системами з ШІ (з урахуванням апроксимації статистичних даних, в тому числі і даних, представлених ISACA [14]) представлений на графіку нижче (рис. 4).

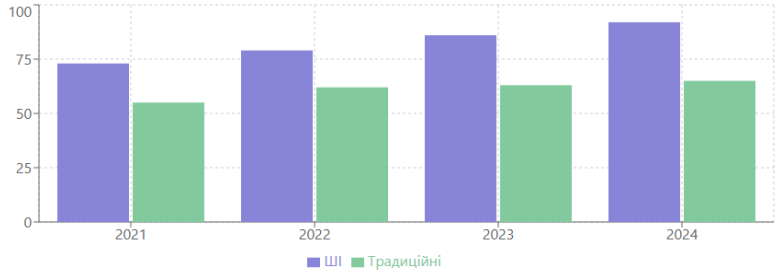

Рис. 4. Рівень виявлення загроз традиційними системами та системами з ШІ [14]

Отже, незважаючи на загальне зростання ефективності обох підходів, впровадження інструментів ШІ забезпечує вищий результат, що свідчить про його перевагу.

Крім того треба зважати на те, що питання вибору / використання моделей / платформ / інструментів ШІ вимагає/потребує долучення до критеріїв вибору такі чинники як вплив на стан національної безпеки та геополітичні стратегічні взаємовідносини між країнами (в рамках взаємодії на технічному, технологічному та комунікаційному рівнях).

Висновки і рекомендації

Застосування ШІ для кіберзахисту КІ є ключовим етапом у протидії сучасним кіберзагрозам/кібератакам/кіберінцидентам. Завдяки новим можливостям, які стають доступними (із використанням ШІ) аналіз великих масивів даних створюючи тим самим можливості для виявлення шаблонів та аномалій, що свідчать про потенційні атаки, включаючи невідомі раніше варіанти. Проактивний захист, забезпечений відповідними технологіями, методами/методиками та інструментами дозволяє своєчасно реагувати на кіберзагрози/кібератаки/кіберінциденти, гарантуючи при цьому перевірку цілісності даних, підтримуючи їхнє відновлення після кібератак. Алгоритми ШІ ефективно визначають масштаби кібератак, допомагаючи ізолювати кіберзагрози/кібератаки/кіберінциденти та мінімізувати їх вплив на корпоративні мережі/системи/ІКС КІ. Крім того, ці технології (використання ШІ) оптимізують процес відновлення, скорочуючи час простою та зменшуючи шкоду, водночас підвищуючи адаптивність корпоративної мережі/системи/ІКС КІ до нових викликів кіберсередовища.

Таким чином, впровадження ШІ сприяє створенню кіберстійкої КІ, яка здатна успішно протистояти зростаючим кібертакам/кіберзагрозам, забезпечуючи нові можливості для впровадження інноваційних стратегій захисту даних, чутливої конфіденційної корпоративної інформації, технологічної інформації/виробничих даних на об’єктах КІ та інформації, необхідної для управління системою/мережею/ІКС.

Що стосується надання конкретних рекомендацій, можна виділити таке. Так, в окремих сферах володіяльцями/користувачами КІ виступають великі компанії (наприклад енергетична сфера – Акціонерне товариство «Національна атомна енергогенеруюча компанія «Енергоатом», ГК «Нафтогаз України», обленерго; сфера виробництва та переробки с/х продукції – АТ ЗТ «Миронівський хлібопродукт», ТОВ «Кернел-трейд»; фармацевтична сфера – ПРАТ «Фармацевтична фірма «Дарниця»; електронні комунікації – ПрАТ «Київстáр», ПрАТ «ВФ Україна»), які мають складну, розгалужену багаторівневу мережу/ІКС і питання кіберзахисту та кібербезпеки стоїть досить актуально. А тому зважаючи на розміри цих компаній і критичність послуг, які вони надають, до питань інформаційної безпеки та кібербезпеки досить сейрозне відношення і прозуміння сучасних викликів з боку керівництва. Що сприяє побудові високоефективної системи кіберзахисту, впровадженню новітніх технологій, механізмів та інструментів.

З огляду на високий рівень критичності функціонування великих суб’єктів КІ на загальний рівень безпеки функціонування багатьох сфер нашої країни, питання вибору моделі/платформи/інструментів ШІ вимагає особливої уваги, оскільки важливими критеріями виступають не лише вартість та доцільність для ведення безпосереднього бізнесу, а і питання безпеки (у урахуванням геополітичних факторів).

Зважаючи на те, що відбувається постійний розвиток ШІ питання впровадження вимагає подальших розвідок.

Перелік посилань

1. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. мат-лів міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І. Кондратов; за заг. ред. О.М. Суходолі. Київ. : НІСД, 2015. 176 с. https://web.archive.org/web/20170215015327/http://www.niss.gov.ua/public/File/2016_book/Syxodolya_ost.pdf.

2. Мануілов Я.С. Питання розробки індикаторів оцінки стану кібербезпеки. Інформація і право. № 4(51) (2024). С.144-152. http://il.ippi.org.ua/article/view/318004.

3. Європейська програма захисту критичної інфраструктури. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260&frontOfficeSuffix=%2F

4. Протокол кризових комунікацій під час реагування на кібератаки та кіберінциденти : наказ МОЗ від 06.12.2023 № 20276. https://moz.gov.ua/uploads/10/51989-dn_2076_06122023_dod.pdf.

5. Положення про організаційно-технічну модель кіберзахисту : постанова Кабінету міністрів України від 29.12.2021 № 1426 (зі змінами). https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#n9

6. Застосування ШІ у кібербезпеці: роль та переваги. https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi?form=MG0AV3&form=MG0AV3

7. Скіцько О., Складанний П., Ширшов Р., Гуменюк М., Ворохоб М. Загрози та ризики використання штучного інтелекту. Кібербезпека: наука, освіта, техніка. № 2 (22), 2023. С.6-14.

8. Штучний інтелект в енергетиці : аналіт. доповідь / Суходоля О.М. Київ. : НІСД, 2022. 49 с. https://doi.org/10.53679/NISS-analytrep.2022.09

9. Готовність кібербезпеки: індекс Cisco у 2024 році. https://www.megatrade.ua/news/reviews/gotovnist-kiberbezpeki-indeks-cisco-u-2024-rotsi/

10. Ткаченко І.В., Козачок В.А., Гахов С.О., Дмітрієв В.Є. Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідковування кризових індикаторів. Сучасний захист інформації №1(41), 2020. С.54-57. https://journals.dut.edu.ua/index.php/dataprotect/article/view/2408/2309.

11. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія / С.Ф. Гончар. Київ.: Альфа Реклама, 2019. 176 с. https://www.researchgate.net/publication/337440032_Ocinuvanna_rizikiv_kiberbezpeki_informacijnih_sistem_ob'ektiv_kriticnoi_infrastrukturi.

12. MCGANN Jim. Cyber Resilience for Critical Infrastructure Using AI. https://www.cpomagazine.com/cyber-security/using-ai-to-build-cyber-resilience-for-critical-infrastructure/.

13. Fuller Evan How AI & Machine Learning Powers Next-Gen Data Leak Prevention (DLP). https://www.nightfall.ai/blog/how-ai-and-machine-learning-powers-next-gen-data-leak-prevention-dlp.

14. Офіційна сторінка ISACA. https: // www.isaca.org/search#q=State%20of%20Cybersecurity%202021%20-Report&sort=relevancy

Надійшла 13.04.2025