УДК 004.056.53:004.8]:334.716-021.412.1
DOI: 10.31673/2409-7292.2025.041203

Гайдур Г.І., Гахов С.О., Скибун О.Ж.

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПІДХОДИ, ОЦІНКА СТАНУ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У статті представлено розгорнутий аналіз сучасних підходів, оцінки поточного стану та перспектив розвитку штучного інтелекту (ШІ-технологій, ШІ-систем та інструментів ШІ) у забезпеченні кібербезпеки критичної інфраструктури як на галузевому/секторальному рівнях, так і на рівні окремих об'єктів. Підкреслено, що в умовах стрімкого зростання цифрової залежності та поширення гібридних загроз питання захисту критичної інфраструктури (енергетична, телекомунікаційна, транспортна, медична сфери, водопостачання тощо) набуває стратегічного значення для забезпечення національної безпеки, стійкості держави та стабільності суспільних процесів. Застосування ШІ (ШІ-технологій, ШІ-систем та інструментів ШІ) у сфері кібербезпеки критичної інфраструктури демонструє трансформаційний вплив на процеси виявлення, ідентифікації та нейтралізації кіберзагроз. Відзначено, що ШІ (ШІ-технології, ШІ-системи та інструменти ШІ) забезпечує суттєве підвищення швидкості обробки великих обсягів даних, дозволяє точно визначати аномальні дії у мережах, прогнозувати поведінкові патерни зловмисників і забезпечувати автоматизовану реакцію на інциденти. Водночас підкреслено, що складність захисту критичної інфраструктури зумовлена інтеграцією IT-систем із промисловими системами керування та операційними технологіями, які вимагають специфічних методів моніторингу, контролю та управління. Тісне переплетіння телекомунікаційних мереж із мережами виробничих процесів та процесів управління, ускладнює захист і формує потребу у спеціалізованих інструментах ШІ. Відзначено, що ключові підходи до застосування ШІ в кібербезпеці – зокрема, машинне навчання для раннього виявлення аномалій, автоматизовані технології SOAR для реагування на інциденти, а також методики оцінки вразливостей SCADA/ICS – вже успішно використовуються на практиці та доводять свою результативність в умовах реальних загроз. Окрему увагу приділено оцінюванню стану безпеки з використанням ШІ, що дозволяє не лише оперативно реагувати на активні атаки, а й прогнозувати можливі шляхи їх еволюції, забезпечуючи випереджувальний характер захисту. Розглянуто перспективні напрями розвитку ринку ШІ у сфері кіберзахисту критичної інфраструктури. Серед них виокремлено розширення застосування автономних кіберімунних систем, орієнтованих на створення самонавчальних і самокерованих середовищ безпеки; подальшу сегментацію ринку та розроблення спеціалізованих ШІ для окремих секторів критичної інфраструктури; інтеграцію ШІ у комплексні корпоративні екосистеми безпеки. Запропоновано низку рекомендацій, спрямованих на підвищення ефективності та стійкості системи кібербезпеки критичної інфраструктури. Серед ключових рекомендацій: активне впровадження гібридних систем «ШІ + людський контроль» для забезпечення оптимального поєднання автоматизації та експертної оцінки; регулярне оновлення та адаптація моделей ШІ до нових типів загроз; інвестування у розвиток людського капіталу шляхом навчання та підвищення кваліфікації спеціалістів у галузі ШІ та кібербезпеки; гармонізація національних підходів із міжнародними стандартами (зокрема NIST CSF та ISO/IEC 27001); формування державних програм інтеграції ШІ у систему захисту критичної інфраструктури; активне розширення міжнародної співпраці, орієнтованої на обмін інформацією про кіберзагрози та кращими практиками застосування ШІ. Підкреслено, що ефективна міжгалузева, міжсекторальна та міждержавна взаємодія експертних спільнот є ключовою умовою розбудови сучасної, адаптивної та стійкої системи кіберзахисту критичної інфраструктури, здатної протистояти зростаючим викликам цифрової епохи.

Ключові слова: кібербезпека, критична інфраструктура, кіберфізичні системи, штучний інтелект, машинне навчання, виявлення загроз, автоматизація реагування.

Вступ

Подальший розвиток інформаційних систем, мереж, інформаційно-комунікаційних систем вимагає використання значної кількості програмних продуктів, мобільних додатків, які функціонують на відповідних операційних системах. Як відзначають експерти AIxCC «програмне забезпечення є вразливим до кібератак, які можуть здійснюватися віддалено з будь-якої точки світу, підтвердженням цього є приклади численних атак останніх років висвітлили загрози для суспільства з боку зловмисних кіберсуб'єктів, що використовують вразливе програмне забезпечення, при цьому критична інфраструктура особливо вразлива до кібератак, враховуючи її велику поверхню атаки» [14]. Згідно з дослідженням CISA, «критична інфраструктура (далі – КІ) залишається основною мішенню для кіберзагроз та кібератак, а тому питання захисту КІ потребує уваги та вимагає залучення інноваційних підходів» [18, с.12], які базуються на нових сучасних технологіях, методах та інструментах. Наприклад, як відзначає Е. Карні «системи штучного інтелекту (далі – ШІ) здатні не лише

виявляти, але й виправляти вразливості для захисту коду, який лежить в основі критичної інфраструктури» [14]. Кібератаки на КІ (насамперед на енергетичну, транспортну сфери, сферу охорону здоров'я, а також на державні реєстри та бази відкритих даних) стають дедалі частішими, особливо в умовах гібридних війн, що є надзвичайно актуальним для України, коли військові дії відбуваються і на полі бою і в кіберпросторі.

Постановка проблеми

У сучасному цифровому середовищі кіберзагрози набули системного характеру, особливо щодо об'єктів критичної інфраструктури, що забезпечують функціонування держави, економіки та суспільства. Енергетичні системи, телекомунікаційні мережі, транспортні вузли та медичні установи дедалі частіше стають мішенню складних кібератак, здатних спричинити масштабні порушення життєво важливих процесів для населення, управління країною та обороноздатності країни.

У відповідь на зростаючу складність та динаміку загроз, технології ШІ демонструють значний потенціал у сфері кіберзахисту. Інтелектуальні системи на базі ШІ, машинного навчання здатні автоматично аналізувати поведінкові патерни, виявляти аномалії в реальному часі, прогнозувати ризики та адаптуватися до нових сценаріїв атак. Це відкриває можливості для побудови проактивних, самонавчальних механізмів захисту, що відповідають вимогам стійкості та надійності функціонування КІ в цілому та окремих об'єктів КІ. Як відзначають експерти Neoversity «ШІ стає ключовим інструментом для побудови системи захисту КІ (енергетика, транспорт, водоканали тощо), адже запровадження елементів ШІ дає змогу автоматично аналізувати поведінку промислових систем (OT/ICS), виявляти аномалії, що вказують на кібератаки та швидко реагувати на загрози» [13]. Вказане є «критично важливо для запобігання фізичним руйнуванням і збоям у роботі критично важливих об’єктів» [13], в першу чергу об’єктів КІ (ОКІ).

Таким чином, питання використання ШІ (інтеграції інтелектуальних технологій у системи кіберзахисту КІ в цілому та окремих ОКІ, що функціонують в умовах підвищених ризиків) потребує додаткового дослідження.

Аналіз результатів останніх досліджень показав, що питання сталості та стійкості функціонування критичної інфраструктури у контексті кібербезпеки є досить актуальними серед сучасних дослідників та науковців: Дж. Бейкер, Є. Галич, І. Зоря, Р. Іваненко, А. Ільєнко, С. Ільєнко, С. Казьмірук, К. Крайтон, Д. Котенко, Б, Леонов, А. Людтке, В. Назаренко, А. Марущак, І. Олішевський, О. Омельян, В. Павленко, Р. Пантюшенко, К. Пуаро, В. Симонов, П. Соловій, В. Устименко, Ю. Хлапонін, О. Федорченко, Н. Хенайн, Ю. Чайка, І. Яненкова, О. Яковенко, О. Ящик, тощо

Незважаючи на значний обсяг проведених досліджень, питання застосування ШІ (ШІ-технологій, ШІ-систем та інструментів ШІ) у нових методах, методиках та інструментах кібербезахисту КІ залишається лише окремою складовою ширшої проблематики.

Це питання потребує подальшого дослідження для можливості впровадження нових підходів для забезпечення більш ефективного захисту КІ в цілому та окремих ОКІ, що входять до її складу.

Мета статті

Метою статті є дослідити застосовується ШІ (ШІ-технологій, ШІ-систем та інструментів ШІ) для оцінки стану кібербезпеки КІ у контексті нових підходів використання та подальших перспектив, що відкриваються через нові можливості.

Завдання статті:

– розгляд стану кібербезпеки критичної інфраструктури;
– розгляд використання ШІ в заходах з кібербезпеки критичної інфраструктури;
– напрацювання пропозицій щодо використання ШІ в заходах кібербезпеки критичної інфраструктури.

Методи дослідження: у процесі написання статті застосовувались загальнонаукові та емпіричні прийоми, що ґрунтуються на системному підході, а також методи узагальнення та порівняння.

Виклад основного матеріалу дослідження

У сучасних умовах глобальної цифровізації та зростання кіберзагроз питання забезпечення кібербезпеки КІ набуває особливої актуальності. Оскільки КІ охоплює сукупність об'єктів, систем і мереж, функціонування яких є життєво важливим для національної безпеки, економічної стабільності, громадської безпеки та проживання населення. Порушення роботи на окремих ОКІ та/або на секторальному рівні КІ внаслідок кіберінцидентів може спричинити масштабні соціальні, економічні та екологічні наслідки. Так, «одним із основних чинників, які утворюють значну небезпеку ОКІ, є кіберзагрози та кібератаки» з боку хакерських угрупувань дії яких підтримуються на державному рівні та «базуються на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операціях», що «створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно окремих ОКІ та/або цілих секторів КІ» [6, с.157].

З огляду на зростаючу складність інформаційних систем, що обслуговують критичні галузі (насамперед енергетика, транспорт, зв’язок, водопостачання, тощо), питання їх захисту від кіберзагроз потребує системного підходу, міжвідомчої координації та впровадження сучасних технологій на всіх етапах. Водночас, ефективне управління ризиками у сфері кібербезпеки неможливе без чіткого розуміння структури критичної інфраструктури, її вразливостей та нормативно-правових засад захисту.

Перш за все слід відзначити, що на сьогодні в Україні вже сформовано і продовжує далі розвиватися відповідне нормативно-правове поле для реалізації державної політики в сфері забезпечення кібербезбеки та «створення і функціювання національної системи захисту критичної інфраструктури» [10], як є складової сфери національної безпеки. Перелік основних нормативних актів, які формують нормативно-правову базу у сфері захисту об'єктів критичної інфраструктури України представлено нижче у таб. 1 [7].

Відповідно до «Положення про організаційно-технічну модель кіберзахисту», яке затверджено постановою Кабінету Міністрів України від 29.12.2021 № 1426 «здійснення заходів з кіберзахисту передбачає: ідентифікацію (виявлення реальних і потенційних кіберзагроз для запобігання та їх нейтралізації); захист розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, комунікаційних, інформаційно–комунікаційних та технологічних систем; виявлення (проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі); реагування (вжиття заходів, спрямованих на запобігання кіберінцидентам, кібератакам, мінімізацію їх можливих наслідків (запобігання виникненню загроз життю або здоров’ю людей та заподіяння шкоди майну), удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності та співрозмірності можливостей таких систем реальним та потенційним ризикам); відновлення (поновлення штатного режиму функціонування інформаційно-комунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення передумов для проведення розслідування за наслідками кібератаки)» [9].

Вказаний перелік заходів є фундаментом для створення відповідної стратегії з кіберзахисту на рівні окремої корпорації, компанії, підприємства. Що виступає умовою для подальшої побудови корпоративної системи кіберзахисту. З огляду на певну уніфікацію та типізації процесів формування та реалізації відповідних політик з кібербезпеки на корпоративному рівні (відповідно до загальноприйнятних стандартів, рекомендацій, нормативно-правових та нормативно-технічних документів на міжнародному та національному рівнях) можна говорити про можливість створення секторальної та/або галузевої системи кіберзахисту.

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

Таблиця 1.

Нормативно-правова база у сфері захисту об'єктів критичної інфраструктури України [10]

Закони України	**Постанови Кабінету Міністрів України**		**НД Адміністрації Держспецзв'язку**
1. Закон України «Про критичну інфраструктуру»	1. Постанова КМУ від 19.06.2019 № 518, «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»	7. Постанова КМУ від 22.07.2022 № 821, «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури»	1. Наказ Адміністрації Держспецзв'язку від 15.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури»
2. Закон України «Про основні засади забезпечення кібербезпеки України»	2. Постанова КМУ від 09.10.2020 №1109, «Деякі питання об'єктів критичної інфраструктури»	8. Постанова КМУ від 04.08.2023 № 818, «Деякі питання паспортизації об'єктів критичної інфраструктури»	2. Наказ Адміністрації Держспецзв'язку від 06.10.2021 № 601 (із змінами, внесеними згідно з наказами Адміністрації Держспецзв'язку від 12.10.2021 № 616 та від 10.07.2022 №343) «Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури»
3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»	3. Постанова КМУ від 11.11.2020 № 1176, «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом»	9. Постанова КМУ від 28.04.2023 № 415, «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього»	3. Наказ Адміністрації Держспецзв'язку від 02.09.2023 № 793 «Про затвердження форм подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури»
4. Закон України «Про інформацію»	4. Постанова КМУ від 09.10.2020 № 943, «Деякі питання об'єктів критичної інформаційної інфраструктури»	10. Постанова КМУ від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»	4. Наказ Адміністрації Держспецзв'язку від 04.10.2023 № 877 «Про затвердження форми Плану захисту об'єкта критичної інфраструктури за проєктною загрозою національного рівня «кібератака/кіберінцидент»
5. Закон України «Про національну безпеку України»	5. Постанова КМУ від 14.10.2022 № 1175, «Деякі питання подання інформації у сфері захисту критичної інфраструктури»	11. Постанова КМУ від 04.04.2023 № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»	5. Наказ Адміністрації Держспецзв'язку від 01.12.2023 № 1011 «Про затвердження Рекомендацій з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент»
	6. Постанова КМУ від 14.10.2022 № 1174, «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури»	12. Постанова КМУ від 24.03.2023 № 257, «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»	6. Науково-практичний коментар до Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою КМУ від 29.12.2021 № 1426

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

При цьому необхідно зважати на необхідність «реалізацію ефективної системи кіберзахисту КІ та ОКІ поетапно за умови розгортання та вдосконалення її технологічної архітектури», а саме «поступове збільшення кількості функціональних компонентів у децентралізованому сегменті системи, їх інтеграцію з елементами централізованого управління, розвиток механізмів міжсистемної інформаційно-технологічної взаємодії» тим самим забезпечуючи «підвищення адаптивності, стійкості та оперативності реагування на кіберінциденти в умовах зростаючої складності загроз та динаміки цифрового середовища» [6, с.158-159].

На сьогодні технології ШІ стрімко впроваджуються у промислове використання і все частіше стають ключовим інструментом як для протидії кіберзагрозам, так і, потенційно, для застосування під час створення кіберзагроз. Так, «використання штучного інтелекту допомагає ефективно боротися з кіберзагрозами і забезпечує високий рівень безпеки в цифровому середовищ», де «системи ШІ на базі алгоритмів машинного навчання та лінгвістичних нейромереж широко використовуються для захисту даних у сучасних інструментах», при цьому «традиційні системи ШІ опрацьовують відомі загрози, але нові методи злому з’являються майже щодня», а «засоби на основі генеративних моделей ШІ стають ефективним інструментом для цього завдання» оскільки «вони не лише здатні виявляти певні патерни, але й генерувати контент, що є перспективним напрямком для розробки як антивірусів, так і комерційних засобів кібербезпеки» [3]. В свою чергу О. Федоренченко надає наступний перелік де використовується ШІ у сфері кібербезпеки, а саме: «виявлення аномалій у мережевому трафіку; автоматичного аналізу подій у кібепросторі; захисту від несанкціонованого доступу до інформаційних ресурсів; аналізу і структуризація інформації про кіберзагрози; реагування на кіберінциденти в режимі реального часу; прогнозування кібератак на основі аналізу великих масивів даних; розробки передових алгоритмів, які допомагають виявляти кібератаки та запобігання їх негативним проявам; машинного навчання на підставі набутого досвіду» [12, с.3]. Треба враховувати, що «на відміну від інформаційно-технологічних систем (IT–системи), які в основному займаються обробкою даних та зв'язком, OT-системи керують машинами, обладнанням та процесами (на виробництві, енергетиці, транспорті, постачанні та водовідведенні води, опаленні тощо), а Системи промислового керування (ICS) «мережі операційних технологій – це комп'ютеризовані системи, що мають вирішальне значення для контролю фізичних промислових операцій з високим рівнем ресурсів», які «контролюють критичну інфраструктуру разом із виробничими роботами» [29]. Так, «Operational Technology (OT) та Industrial Control Systems (ICS) – це «мозок» та «нервова система» промислових об'єктів» від яких залежать «фізичні процеси на виробництві та управління складовими елементами КІ (від подачі електроенергії до очищення води)» [11]. Але при цьому не треба недооцінювати важливість IT–систем, оскільки мережі електронних комунікацій виступають транспортними мережами передачі даних (управління КІ на рівні сектору/корпорації).

Отже ми маємо ситуацію, коли необхідно забезпечувати високий рівень кіберзахисту як IT-систем та і OT-систем, оскільки виробничі процеси все частіше автоматизуються , а їх управління може відбуватися віддалено. Водночас необхідно зважати на те, що «конвергенція IT- та OT-мереж принесла нові ризики кібербезпеки», коли «промислові процеси дедалі більше залежать від взаємопов'язаних систем та технологій OT, що робить їх вразливими до кібератак, шкідливого програмного забезпечення та інших форм експлуатації» [29].

Згідно з аналітичними висновками фахівців компанії Neoversity, сучасні системи оперативних технологій (OT) характеризуються низкою критичних вразливостей, що зумовлюють підвищений рівень ризику для ОКІ, а саме: «застарілість апаратного та програмного забезпечення: значна частина OT-систем функціонує на технологічних платформах, розроблених понад 10–20 років тому», а «для таких систем оновлення безпеки випускаються нерегулярно або взагалі не передбачені, що унеможливлює своєчасне усунення

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

виявлених вразливостей»; «обмеження щодо зупинки технологічного процесу: у виробничих середовищах із безперервним циклом роботи недопустимим є призупинення функціонування технологічного обладнання для встановлення оновлень та/або перезавантаження систем, що створює додаткові ризики кібербезпеки»; «фізичні наслідки кібератак: компрометація ОТ-системи може спричинити аварійні події, а це «робить ОТ-інфраструктуру привабливою ціллю для суб'єктів з деструктивними намірами, включаючи терористичні кіберугруповання та/або дії держава-агресора»; «втрата ізольованості мереж; історично ОТ-системи функціонували в ізольованих середовищах, без доступу до глобальних мереж», але «сучасні вимоги до цифровізації, автоматизації та віддаленого управління зумовлюють інтеграцію ОТ-компонентів до корпоративних ІТ-мереж» а це «суттєво розширює поверхню атаки та відкриває нові вектори загроз» [11].

В свою чергу експерти Axians UK зазначають, що забезпечення кібербезпеки в ОТ-системах стикається з низкою специфічних викликів, які обумовлені особливостями архітектури ОТ-середовищ та процесами конвергенції з інформаційними технологіями (ІТ): «застарілість та обмеженість функціоналу безпеки: більшість ОТ-систем побудовані на базі застарілих технологій, які не мають вбудованих механізмів захисту та/або мають їх у обмеженому обсязі, що ускладнює інтеграцію сучасних засобів кіберзахисту»; «складність та неоднорідність середовища: ОТ-інфраструктура, як правило, включає широкий спектр пристроїв, протоколів та рішень від різних постачальників, що ускладнює впровадження уніфікованих політик безпеки та засобів контролю; «зростаюча зв'язність та конвергенція з ІТ-середовищем: підключення ОТ-систем до корпоративних ІТ-мереж, Інтернету та сторонніх платформ розширює поверхню атаки та створює нові вектори загроз», а «конвергенція ІТ- та ОТ-компонентів розмиває межі між раніше ізольованими доменами, що призводить до виникнення міждоменних вразливостей»; «вразливість до кіберзагроз: ОТ-системи є чутливими до широкого спектру атак, зокрема експлуатації вразливостей, що можуть спричинити фізичні пошкодження, порушення технологічних процесів або інші критичні інциденти»; «баланс між безпекою та операційною надійністю: забезпечення належного рівня захисту в умовах вимог до безперервного контролю та реагування в реальному часі становить суттєвий виклик для фахівців з кібербезпеки; «недостатній рівень обізнаності персоналу: людський фактор залишається критичним елементом у забезпеченні безпеки ОТ-середовищ», що «проблеми потребує впровадження програм навчання, підвищення обізнаності та формування культури безпеки»; «нормативні вимоги та стандартизація: дотримання галузевих стандартів, таких як NERC-CIP, IEC 62443 та NIST SP 800-82, вимагає постійного моніторингу, оцінювання та підтримки відповідних засобів контролю безпеки»; «обмежена видимість та моніторинг: відсутність повноцінної видимості ОТ-мереж та систем ускладнює процеси виявлення, аналізу та реагування на інциденти безпеки»; «операційні обмеження та мінімізація простоїв: вимоги до безперебійної роботи технологічного обладнання та виробничі графіки обмежують можливості впровадження заходів безпеки та технічного обслуговування», а «забезпечення балансу між цілями безпеки та операційними імперативами є складним завданням для команд, відповідальних за кіберзахист ОТ-середовищ» [27].

З огляду на комплексний характер загроз, що постають перед ОТ-системами, забезпечення кібербезпеки ОКІ потребує системного підходу, який поєднує технічні, організаційні та нормативні складові елементи. Такий підхід повинен враховувати специфіку технологічного середовища, динаміку його взаємодії з інформаційними мережами (ІТ-системами).

При цьому «головним завданням технологічної інфраструктури кіберзахисту є оперативний та ефективний захист кіберпростору в частині протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, в тому числі шляхом: збору, аналізу, оцінювання, узагальнення та поширення інформації про кіберінциденти; надання методичної допомоги іншим суб'єктам кіберзахисту; взаємного інформування суб'єктів кіберзахисту про

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

нові реальні та потенційні загрози; створення умов для відповідального та довіреного обміну інформацією між суб'єктами кіберзахисту всіх секторів кіберзахисту» [6, с.159].

У контексті національної політики безпеки, зокрема відповідно до положень «Зеленої книги з питань захисту критичної інфраструктури в Україні», «пріоритетним є впровадження сучасних технологій виявлення, моніторингу та реагування на інциденти, а також адаптація міжнародних стандартів до національного регуляторного середовища» при цьому «ефективна протидія загрозам вимагає технічного переоснащення, формування стійких процедур управління ризиками, підвищення обізнаності персоналу та забезпечення міжвідомчої координації» [18]. При цьому необхідно зважати на те, що «ШІ володіє здатністю аналізувати та обробляти великі обсяги даних, а також виявляти та уникати ризики, що пов'язані з кіберзагрозами, завдяки своїм можливостям самонавчання» коли «алгоритми машинного навчання аналізують величезні обсяги даних, сприяючи виявленню аномалій у мережевому трафіку та ідентифікації потенційно небезпечних вразливостей» бо «чим більше даних надається, тим більше ШІ навчається, поліпшуючи свої можливості прогнозування», а це означає, що «методи машинного навчання відіграють ключову роль у процесах забезпечення кібербезпеки» [12, с.3-4].

Сучасні технології ШІ відкривають нові можливості для захисту критичної інфраструктури через кілька ключових напрямків, серед яких можна виділити такі: виявлення загроз, автоматизація реагування, оцінка вразливостей. Важливим застосуванням ШІ є виявлення кіберзагроз у реальному часі. Як зазначають експерти Агентства з кібербезпеки та безпеки інфраструктури США (CISA) «системи на основі машинного навчання здатні аналізувати аномалії в мережевому трафіку та виявляти потенційні загрози з точністю до 95%» [19, с.23]. Розроблений ними інструмент оцінки кібербезпеки (The Cyber Security Evaluation Tool (CSET) «забезпечує систематичний, дисциплінований та повторюваний підхід до оцінки стану безпеки організації, допомагає організаціям оцінити рівень кібербезпеки своїх інформаційних та операційних систем», а «його основна мета – виявити вразливості, порівняти поточний стан безпеки з міжнародними стандартами та надати рекомендації щодо покращення» [4],[5]. Також, «рамках Меморандуму про співробітництво між Держспецзв'язку та Агентством з кібербезпеки та безпеки інфраструктури Сполучених Штатів (CISA) інструмент оцінки кібербезпеки (CSET) був перекладений українською мовою і адаптований до потреб українських держорганів та операторів критичної інфраструктури» [1],[2]. Для «аналізу та інтерфейсу користувача для допомоги в оцінці систем промислового керування (ICS) і інформаційних технологій (IT) мережевої безпеки» надає «доступ до бази знань щодо вимог, нормативних актів і практик щодо кібербезпеки ICS», а також до «колекції рішень для пом'якшення вразливостей», тому за допомогою цього інструменту (CSET) можна проводити оцінку кібербезпеки кіберсистем управління підприємством і промисловістю» [1],[2]. Крім того технології глибокого навчання дозволяють ідентифікувати невідомі атаки (zero-day exploits), які традиційні системи безпеки можуть пропустити.

Поведінковий аналіз (UEBA – User and Entity Behavior Analytics) використовує ШІ для ідентифікації інсайдерських загроз. Так, за даними Hyperproof «організації, що впровадили UEBA, зафіксували зменшення часу виявлення внутрішніх загроз на 60%» [28]. При цьому «автоматизація процесів реагування на інциденти (платформи SOAR (Security Orchestration, Automation and Response) використовують ШІ для швидкого реагування на інциденти) скорочує час реакції з годин до хвилин, що критично важливо для захисту критичної інфраструктури» [27, с. 8]. Важливо, що автоматизоване оновлення політик безпеки на основі аналізу нових загроз дозволяє підтримувати актуальний рівень захисту; **о**цінка вразливостей: ШІ активно використовується для сканування конфігурацій систем і прогнозування ризиків, що особливо актуально для застарілих систем SCADA (Supervisory Control and Data Acquisition) та ICS (Industrial Control Systems), які використовуються в енергетиці та промисловості. Відповідно до рекомендацій Міністерства внутрішньої безпеки США (DHS),

«регулярний аналіз вразливостей за допомогою ШІ-інструментів має бути інтегрований у загальну стратегію кібербезпеки компаній КІ» [26, с. 15].

Водночас слід зважати на те, що за висновками аналітичного агентства Конгресу США (GAO), «завданням підрозділів внутрішньої безпеки компанії/корпорації/підприємства, серед іншого, є здійснення заходів з покращення керівництва з оцінки ризиків, пов'язаних із застосуванням ШІ у секторах КІ» [16, с.1]. Наразі можна відзначити наступні виклики щодо впровадження ШІ в кібербезпеку КІ та ОКІ: технічні виклики: «якість даних залишається критичним фактором для ефективної роботи ШІ-систем», а тому «недостатня якість даних для навчання моделей ШІ може призвести до помилкових спрацювань у 30-40% випадків» [16, с. 28]. (GAO); організаційні виклики: «складність інтеграції ШІ в застарілі системи та гостра нестача кваліфікованих фахівців створюють перешкоди для широкого впровадження технологій (за оцінкою McKinsey «глобальний дефіцит фахівців з кібербезпеки та ШІ становить понад 3 мільйони спеціалістів» [27, с.15]; етичні виклики: «проблеми конфіденційності та надмірної автоматизації потребують уваги: оскільки «використання ШІ в кібербезпеці має балансувати між ефективністю захисту та дотриманням прав людини на приватність» [15, с. 45].

В свою чергу експерти Gartner відзначають, що «використання моделей GenAI та сторонніх моделей великих мов (LLM) має свої переваги», але водночас «існують ризики для користувачів, які вимагають нових практик безпеки», а саме: «виявлення аномалій контенту: неприйнятне або зловмисне використання; некерований корпоративний контент, що передається через підказки, ставить під загрозу конфіденційність введених даних; галюцинації або неточні, незаконні, порушуючи авторські права та небажані чи ненавмисні виходи, що ставлять під загрозу прийняття рішень або завдають шкоди бренду»; «захист даних: витік даних, цілісність та порушення конфіденційності контенту та даних користувачів у середовищах розміщених постачальників; неможливість керувати політиками конфіденційності та захисту даних у зовнішніх середовищах; складність проведення оцінок впливу на конфіденційність та дотримання регіональних норм через принцип «чорної скриньки» сторонніх моделей»; «безпека застосунків зі штучним інтелектом: атаки з використанням підказок для зловмисників, включаючи зловживання бізнес-логікою та прямі та непрямі введення підказок; векторні атаки на бази даних; доступ хакера до станів та параметрів моделі» [24].

Слід також звернути увагу на використання працівниками, співробітниками на своїх робочих місцях не тільки «інструменти, які спеціально розроблені для кібербезпеки», а і інструменти, незалежні від предметної області» адже «використання LLM на ширшому робочому місці може включати потенційне розкриття конфіденційних даних та галюцинації, пов'язані зі штучним інтелектом» [11]. Таким чином спеціалісти з кібербезпеки та ІТ стурбовані «проблемою тіньового ШІ, несанкціонованих інструментів ШІ та програм ШІ, які використовуються без їх відома та/або схвалення», що «створює значні ризики, включаючи витік даних та порушення вимог, оскільки ці тіньові інструменти ШІ часто не мають належних заходів безпеки та нагляду» [11]. Запобігти поширенню вказаної тенденції можна через запровадження чітких рекомендацій щодо переліку інструментів ШІ, які можна користуватися на робочому місці усіма працівниками компанії, які мають доступ до корпоративної інформаційної мережі, а також ведення постійного моніторингу з боку підрозділів ІТ та безпеки. Реалізувати це можна шляхом «розгортання системи моніторингу мережі та встановлення загальнокорпоративної політики щодо прийнятного використання інструментів ШІ на робочому місці» [11]. Для зростання ефективності запропонованих механізмів вбачається у налагодженні, на постійній основі, заходів з підвищення рівня кібергігієни та кіберграмотності серед працівників компанії.

Таким чином «ШІ вимагає надійних регуляторних систем управління ризиками, пов'язаними зі ШІ, які можуть враховувати складні наслідки використання ШІ для

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

кібербезпеки, конфіденційності та етики» [8]. Наразі «23% респондентів використовують NIST Cybersecurity Framework (наприклад NIST CSF) для управління ризиками, пов'язаними зі штучним інтелектом»; «16% опитаних використовують NIST AI RMF для боротьби з ризиками, пов'язаними з генеративним ШІ» [8]. Більш детальна інформація щодо фреймворків, які використовуються для управління ризиками, пов'язаними з генеративним ШІ представлена на рис.1 [8].

Водночас необхідно враховувати занепокоєння бізнесу через прямий вплив, який ШІ може мати на критичні операційні аспекти, та суворе регуляторне середовище, в якому вони працюють [подвійні переваги]. Нижче представлені результати опитування щодо занепокоєнням ризиками для бізнесу, пов'язаними із ШІ (рис. 2) [8].

Подальше збільшення рівня присутності ШІ (ШІ-технології, ШІ-системи, інструменти ШІ) в кібербезпеці вимагає від компаній/корпорацій/організацій «використовувати переваги ШІ для підвищення безпеки та операційних можливостей, а також бути обізнаними (і готовими) до ризиків, які додатково виникають під час використання ШІ» [8].

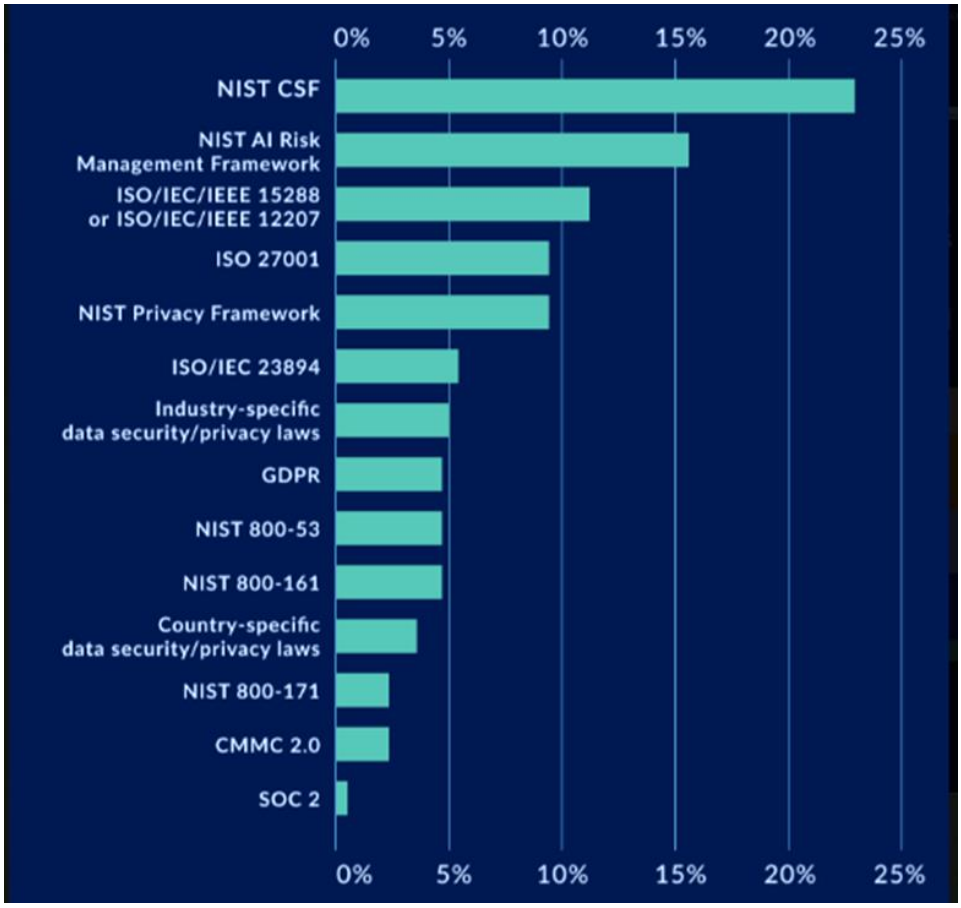

Рис. 1. Результати використання фреймворків для управління ризиками, пов'язаними з генеративним ШІ [8]

Цьому сприятиме здійснення оцінювання поточного стану програми кібербезпеки (на рівні корпорації, компанії, організації) з можливістю подальшого визначення прогалин, які потрібно усунути. Так, «процес стратегічного планування починається з формування бачення кібербезпеки, що ґрунтується на реальних рушійних силах, пов'язаних з бізнесом, технологіями та ширшим економічним середовищем» разом із виявленням прогалин в можливостях» [17]. Наразі експерти Gartner пропонують наступну «комбінацію різних типів оцінювання», а саме: «оцінювання ефективності контролю для визначення зрілості впровадження контролю, порівнюючи його з аналогічними системами та узгоджуючи з

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

галузевими стандартами; оцінка вразливостей та тести на проникнення для оцінки технічної інфраструктури; оцінка ризиків для збалансування інвестицій у засоби контролю відповідно до фактичних ризиків; останні результати аудиту; оцінювання управління програмами для оцінки та порівняння рівня зрілості політик, процесів та програм кібербезпеки; витрати на кібербезпеку та контрольні показники персоналу для порівняння ресурсів з аналогічними компаніями» [17]. На сьогодні оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ включає аналіз ризиків за допомогою прогнозних моделей ШІ. Наприклад Департамент внутрішньої безпеки США розробив «Дорожню карту ШІ», яка визначає пріоритетні напрямки використання технологій для оцінки та захисту критичної інфраструктури [21, с.10]. Крім того моніторинг кіберфізичних систем у реальному часі стає можливим завдяки застосуванню графових нейронних мереж для аналізу зв'язків між подіями. Так, за даними Capitol Technology University «використання графових нейронних мереж дозволяє виявляти складні патерни атак, які охоплюють кілька систем одночасно» [23]. При цьому слід відмітити, що серед платформ на основі ШІ, які використовуються для захисту критичної інфраструктури, виділяються такі: Darktrace, IBM QRadar та Splunk. В свою чергу, спеціалізовані рішення, такі як Nozomi Networks, орієнтовані саме на захист промислових систем управління (ICS). Відповідно до результатів огляду ENISA «інтеграція ШІ-платформ з існуючими системами безпеки підвищує ефективність виявлення загроз на 40-70%» [15, с. 34]. А тому можна говорити про те, що практична реалізація впровадження / застосування / використання елементів ШІ для кібербезпеки КІ та ОКІ дає змогу корпораціям / компаніям отримувати позитивний досвід з огляду на демонстрацію високого рівня ефективності.

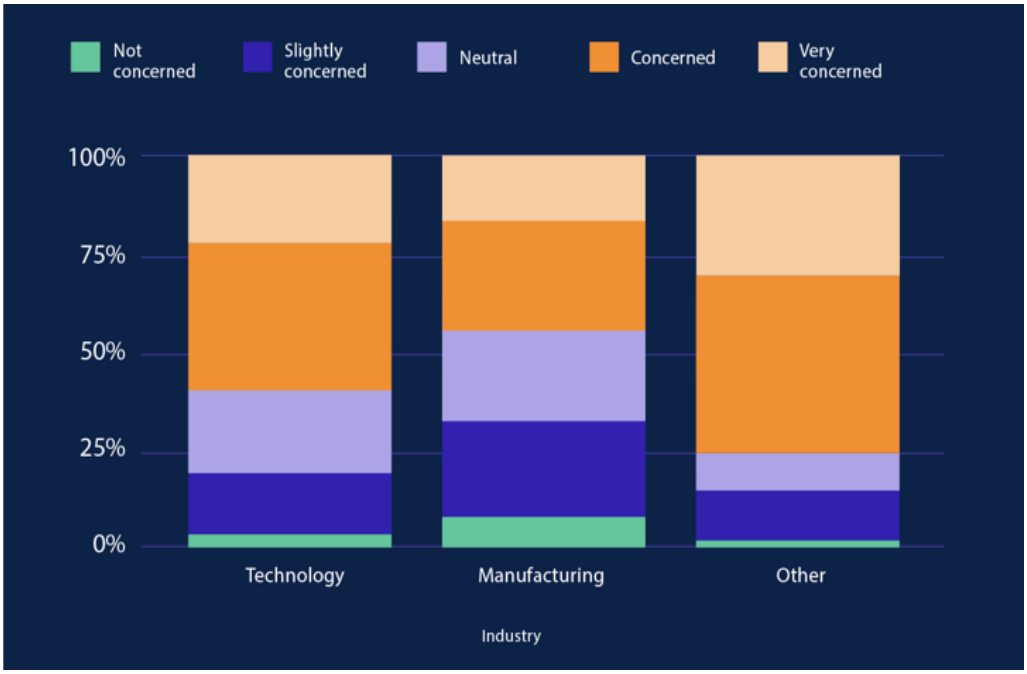

Рис. 2. Результати опитування щодо занепокоєнням ризиками для бізнесу, пов'язаними із ШІ [8]

Подальший розвиток та поширення технологій ШІ (ШІ-технології, ШІ-системи, інструменти ШІ) в сфері кібербезпеки КІ та ОКІ необхідно розглядати у контексті технологічних трендів, глобальних ініціатив та локального контексту. І так, по-перше, технологічні тренди: «інтеграція ШІ з Інтернетом речей на базі мобільного зв’язку 5G», що створить передумови для «широкого впровадження ШІ-систем захисту для Інтернету речей, які застосовуються в КІ та на ОКІ» [20]. Також треба зважати на те, що «когнітивні системи безпеки зможуть самостійно адаптуватися до нових типів загроз без необхідності постійного

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

оновлення людиною» [14]. По-друге, «пріоритетом розвитку ШІ-систем захисту буде формування тісних взаємовідносин на секторальному рівні КІ та ОКІ, яке проходитиме на базі міжнародної співпраці» [21, с. 8]. По-третє, зростання рівня задіяння «потенціалу ШІ-систем у протидії гібридним загрозам країн, що перебувають під кіберагресією матиме як актив, так і загрозу» [22].

Подальший розвиток ШІ (ШІ-технологій, ШІ-систем та інструментів ШІ) в сфері кібербезпеки відбуватиметься на кількох напрямах, серед яких можна виділити такі: технічно-технологічний, нормативно-правовий та регуляторний, людський (морально-етичний, освітній) тощо.

На сьогодні «ШІ не лише вдосконалює продукти, але й трансформує робочі процеси в компаніях, які займаються питаннями безпеки» [11]. Наприклад компанії «Fortinet, Netskope та GitLab публічно оголосили про інтеграцію ШІ у свою діяльність за напрями: розвідка загроз, операції з безпеки та процес DevSecOps» [11]. В свою чергу компанія Gartner пропонує власний «інтерактивний інструмент (Gartner AI Use Case Insights), який допомагає ефективно виявляти, оцінювати та визначати пріоритети варіантів використання ШІ для потенційного розвитку», коли «клієнти можуть шукати серед понад 500 варіантів використання (застосування ШІ в певних галузях) та понад 380 тематичних досліджень (прикладів з реального світу) на основі галузі, бізнес-функції та оцінки Gartner потенційної бізнес-цінності», а «отримати доступ до цього інтерактивного інструменту» можна за посиланням: https://tools.gartner.com/use-case-insights [24].

М. Вудард, віце-президент з управління продуктами безпеки додатків у Digital.ai наголошує, що «моніторинг загроз за допомогою ШІ, а саме розпізнавання образів, виявлення аномалій та загальна класифікація даних, стане необхідним для команд безпеки, щоб виявляти найнагальніші загрози, аби своєчасно вжити належних заходів щодо їх пом'якшення» [11].

В той же час експерти компанії Gartner прогнозують, що «до 2030 року превентивні рішення з кібербезпеки становитимуть 50% витрат на IT-безпеку, порівняно з менш ніж 5% у 2024 році, замінивши автономні рішення для виявлення та реагування (DR) як кращий підхід до захисту від кіберзагроз», адже технології превентивної кібербезпеки «використовують передовий ШІ та машинне навчання (ML) для передбачення та нейтралізації загроз до їх реалізації» та «включають такі можливості як: прогнозна розвідка про загрози, передовий обман та автоматизований захист від рухомих цілей» [24]. Наступними важливими складовим подальшого розвитку використання ШІ в кібербезпеці за інформацією від Gartner будуть: «автономна кіберімунна система (ACIS)» та «перехід від універсального рішення до більш цілеспрямованих та ефективних превентивних рішень у сфері кібербезпеки» [24]. Так, «автономна кіберімунна система (ACIS) є найвищою еволюцією превентивної кібербезпеки для складної, швидкозростаючої глобальної сітки поверхні атак (GASG)» в умовах, коли «розробка та розгортання інтелектуальних, децентралізованих, тактичних автономних кіберуімунних систем ACIS – це не просто амбітні цілі, а абсолютний імператив для захисту нашого дедалі більш взаємопов'язаного світ» [24]. Подальший «перехід від універсального рішення до більш цілеспрямованих та ефективних превентивних рішень у сфері кібербезпеки» дасть змогу зосередитись постачальникам рішень безпеки використання ШІ (ШІ-технологій, ШІ-систем та інструментів ШІ) в кібербезпеці на «нішових» областях «для формування окремих сегментів ринку завдяки глибокому розумінню унікальних викликів безпеки», адже «жоден окремий постачальник рішень безпеки не може ефективно вирішити всі проблеми GASG, партнерство та сумісність між спеціалізованими рішеннями стануть ще більш важливими» [24].

Висновки та рекомендації

У контексті зростаючої цифрової взаємозалежності та гібридних загроз, захист критичної інфраструктури набуває стратегічного значення. До таких об'єктів належать енергетичні системи, телекомунікаційні мережі, транспортні вузли, водопостачання та

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

медичні установи – тобто ті компоненти, безперебійна робота яких є життєво важливою для національної безпеки та стабільності суспільства.

Перш за все, використання ШІ (ШІ-технологій, ШІ-систем, інструментів ШІ) трансформує підходи до кібербезпеки критичної інфраструктури, забезпечуючи безпрецедентні швидкість і точність виявлення та нейтралізації загроз. Також необхідно відзначити, що питання забезпечення кібербезпеки критичної інфраструктури ускладняється тим, що у зв'язку із наявністю виробничих процесів та необхідності контролю за технологіями виробництва питання кібербезпеки та кіберзахисту поширюється не лише на інформаційно-комунікаційні системи (IT–системи), а і промислові системи керування (ICS) та операційні системи (OT–системи). Це пов'язано із тісним поєднанням телекомунікаційних мереж передачі даних та виробничих мереж у контексті побудови віддаленої системи управління та контролю за виробничими процесами, а також адміністративного управління на корпоративному рівні та/або на галузевому/секторальному рівнях критичної інфраструктури в цілому та/або об'єктів критичної інфраструктури. Оцінка стану безпеки з використанням ШІ (ШІ-технологій, ШІ-систем, інструментів ШІ) дозволяє не лише реагувати на поточні інциденти, але й прогнозувати майбутні загрози, що є критично важливим для захисту критичної інфраструктури та об'єктів критичної інфраструктури.

Дослідження показало, що ключові підходи застосування ШІ (ШІ-технологій, ШІ-систем, інструментів ШІ), а саме виявлення загроз через машинне навчання, автоматизація реагування за допомогою SOAR-платформ та оцінка вразливостей систем SCADA/ICS, вже демонструють свою ефективність у практичній площині.

Подальші прогнози щодо ринку послуг ШІ (ШІ-технологій, ШІ-систем, інструментів ШІ) стосуються: поширення побудови автономних кіберімунних систем (ACIS) в рамках корпоративних екосистем з кібербезпеки; подальша сегментація та зосередження уваги на окремі елементи, напрями та сектори, які потребують спеціалізованих рішень з кібербезпеки.

На основі проведеного дослідження представлено до уваги такі рекомендації щодо подальшого розвитку кібербезпеки критичної інфраструктури:

– *широке використання гібридних систем* (ШІ + людський нагляд) для забезпечення балансу між автоматизацією та експертним контролем;

– *регулярне оновлення моделей ШІ* для адаптації до нових загроз з урахуванням динамічного характеру кіберпростору;

– *інвестування у людський капітал: навчання/підготовка/підвищення кваліфікації фахівців* із кібербезпеки, ШІ-технологій та ШІ-систем;

– *широке використання міжнародних стандартів* (наприклад NIST Cybersecurity Framework, ISO/IEC 27001) для уніфікації підходів до захисту критичної інфраструктури;

– *створення національних програм* з інтеграції ШІ (ШІ-технологій , ШІ-систем, інструментів ШІ) у систему захисту критичної інфраструктури з урахуванням специфіки гібридних загроз;

– *розвиток міжнародної співпраці* для обміну даними про кіберзагрози та кращими практиками застосування ШІ.

При цьому треба відзначати, що активна співпраця фахівців та експертів в сфері кібербезпеки на секторальному та/або міждержавному рівнях створює передумови для побудови більш ефективної системи захисту критичної інфраструктури.

З огляду на динамічний характер впливу ШІ (ШІ-технологій, ШІ-систем, інструментів ШІ) на кібербезпеку критичної інфраструктури, дослідження питань забезпечення їх сталого та стійкого функціонування в умовах триваючої військової агресії з боку рф, разом із елементами кібервійни, набуває особливої актуальності та потребує подальших наукових досліджень.

Перелік посилань

1. Держспецзв'язку презентували інструмент оцінки кібербезпеки для українських організацій. 2024. https://ain.ua/2024/09/30/instrument-ocinki-kiberbezpeki/.

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

2. Держспецзв'язку провела презентацію інструменту оцінки кібербезпеки CSET (Cybersecurity Evaluation Tool) та провела практичне заняття з його використання. 2024. https://delo.ua/telecom/derzspeczvyazku-prezentuvala-novii-instrument-ocinki-kiberbezpeki-436947/.

3. Зоря І.С., Марущак А. В. застосування штучного інтелекту для виявлення та реагування на кіберзагрози. 2024. http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf?sequence=3&isAllowed=y .

4. Інструмент оцінки кібербезпеки (CSET). https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset.

5. Інструмент оцінки кібербезпеки CSET. https://csirt.csi.cip.gov.ua/uk/pages/cset .

6. Мануілов Я.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. Інформація і право. № 1(44)/2023. С.154-163.

7. Нормативно-правова база у сфері захисту об'єктів критичної інфраструктури України. https://csirt.csi.cip.gov.ua/uk/pages/cio.

8. Подвійні переваги штучного інтелекту в кібербезпеці: висновки зі звіту Benchmark Survey за 2024 рік. 2024. https://hyperproof.io/resource/ai-in-cybersecurity-2024-benchmark-report/.

9. Про затвердження Положення про організаційно-технічну модель кіберзахисту : постанова Кабінету Міністрів України від 29.12.2021 № 1426. https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text.

10. Про критичну інфраструктуру : закон України від 16.11.2021 № 1882-IX. Відомості Верховної Ради (ВВР), 2023, № 5, ст.13. https://zakon.rada.gov.ua/laws/show/1882-20#Text.

11. Пуаро К. Огляд тенденцій кібер-штучного інтелекту: підготовка до 2025 року. 2024. https://www.infosecurity-magazine.com/news-features/cyber-ai-trends-review-preparing/.

12. Федорченко О.С. Роль штучного інтелекту у забезпеченні кібербезпеки України: сучасний стан та перспективи розвитку. Інформація і право. № 3(54)/2025. С.139-146. DOI: https://doi.org/10.37750/2616-6798.2025.3(54).340521. http://il.ippi.org.ua/article/view/340521 .

13. Як AI захищає критичну інфраструктуру України: все про кібербезпеку OT/ICS. 2025. https://neoversity.com.ua /blog/yak-ai-zahishchaie-kritichnu-infrastrukturu-ukrayini-vse-pro-kiberbezpeku-ot-ics.

14. AIxCC: AI Cyber Challenge / Defense Advanced Research Projects Agency. Arlington, VA : DARPA, 2024. https://www.darpa.mil/research/programs/ai-cyber .

15. Artificial Intelligence and Cybersecurity / European Union Agency for Cybersecurity. Athens : ENISA, 2024. 62p. https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity .

16. Artificial Intelligence: DHS Needs to Improve Risk Assessment Guidance for Critical Infrastructure Sectors / U.S. Government Accountability Office. Washington, DC : GAO, 2024. 42p. (GAO-25-107435). https://www.gao.gov/ assets/gao-25-107435.pdf .

17. Assess the current state of the cybersecurity program and identify capability gaps. (Оцінити поточний стан програми кібербезпеки та виявити прогалини в можливостях) 2024. https://www.gartner.com/en/ cybersecurity/ topics/cybersecurity-roadmap.

18. CISA's 2024 Year in Review / Cybersecurity and Infrastructure Security Agency. Washington, DC : CISA, 2024. 80p. https://www.cisa.gov/sites/default/files/2024-12/CSAC%20Annual%20Report_20241210.pdf .

19. Crichton, K. Securing Critical Infrastructure in the Age of AI / K. Crichton, J. Baker, A. Luedtke // Center for Security and Emerging Technology. Washington, DC : CSET, 2024. 58p. https://cset.georgetown.edu/wp-content/uploads/CSET-Securing-Critical-Infrastructure-in-the-Age-of-AI.pdf.

20. Cyber AI Trends Review: Preparing for 2025 / Infosecurity Magazine. London : Infosecurity Magazine, 2025. https://www.infosecurity-magazine.com/news-features/cyber-ai-trends-review-preparing/.

21. DHS Artificial Intelligence Roadmap / Department of Homeland Security. Washington, DC : DHS, 2024. 36p. https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf .

22. DHS Highlights AI as a Threat and Asset to Critical Infrastructure in New Priority Guidance / Nextgov/FCW. Washington, DC : Nextgov/FCW, 2024. https://www.nextgov.com/cybersecurity/2024/06/dhs-highlights-ai-threat-and-asset-critical-infrastructure-new-priority-guidance/397524/ .

23. Emerging Threats to Critical Infrastructure: AI Driven Cybersecurity Trends for 2025 / Capitol Technology University. Laurel, MD : Capitol Technology University, 2024. https://www.captechu.edu/blog/ai-driven-cybersecurity-trends-2025 .

24. Gartner states that in the GenAI era, the future of cybersecurity lies in prevention rather than detection and response. 2025. https: // www.gartner.com/en/newsroom / press-releases / 2025-09-18-gartner-says-that-in-the-age-of-genai-preemptive-capabilities-not-detection-and-response-are-the-future-of-cybersecurity.

25. Idaho National Laboratory. Cyber Security Evaluation Tool (CSET) User Guide. https://inl.gov/wp-content/uploads/2020/06/CSET-User-Guide.pdf.

26. Safety and Security Guidelines for Critical Infrastructure Sector Owners and Operators / Department of Homeland Security. Washington, DC : DHS, 2024. 24p. https://www.dhs.gov/sites/default/files/2024-04/24_0426_ dhs_ai-ci-safety-security-guidelines-508c.pdf .

27. The Cybersecurity Provider's Next Opportunity: Making AI Safer / McKinsey & Company. New York : McKinsey & Company, 2024. https: // www.mckinsey.com / capabilities / risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer .

© Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025) Штучний інтелект у кібербезпеці критичної інфраструктури: підходи, оцінка стану та перспективи розвитку. Сучасний захист інформації, 4(64), 24–37. https://doi.org/10.31673/2409-7292.2025.041203

28. The Dual Edges of AI in Cybersecurity: Insights from the 2024 Benchmark Survey Report / Hyperproof. Seattle, WA : Hyperproof, 2024. https://hyperproof.io/resource/ai-in-cybersecurity-2024-benchmark-report/ .

29. What is Operational Technology (OT) Cyber Security?. https://www.axians.co.uk/glossary/what-is-operational-technology-security/#:~:text=Operational%20Technology%20(OT)%20security%2C,vulnerabilities%20from%202017%20to%202020.

Надійшла 17.09.2025

УДК 004.056.5:004.415.53
DOI: 10.31673/2409-7292.2025.041204

Hashko A.O, Bondarchuk A.P.

AUTOMATED METHOD FOR VERIFYING THE CORRECTNESS OF THE EXECUTION OF SMART CONTRACTS IN THE BLOCKCHAIN NETWORK

The article examines an automated method for verifying the correctness of smart contracts in the Solana blockchain network. The relevance of the research is driven by the growing popularity of Web3 applications and the need to ensure their security, as even minor errors in smart contract code can lead to significant financial losses. The primary goal is to develop an automated verification methodology for smart contracts that can detect vulnerabilities such as the absence of founder rights verification, arithmetic operation errors, and missing transaction check signatures. Using static analysis techniques in the Rust programming language, the authors propose an approach that enables rapid analysis-taking less than three minutes per contract-and automatic generation of reports on identified vulnerabilities. The methodology is based on analyzing external data flows through smart contracts, allowing for the early detection of potential threats. To automate the process, Python and Bash scripts are employed, integrating with cloud services such as Amazon Web Services to scale the analysis. Testing results on real Web3 applications demonstrate the effectiveness of the methodology, particularly in reducing analysis time and improving the accuracy of error detection. An important aspect of the research is the continuous updating of knowledge bases and analysis tools, enabling the consideration of new types of attacks and vulnerabilities. The article also highlights the importance of interoperability between different blockchain networks, which remains a challenging task but is a key element for the future development of Web3. The research results show that the proposed methodology is promising for scaling and adapting to new challenges in blockchain ecosystems such as Solana. Thus, the developed approach to automated smart contract verification not only enhances the security of Web3 applications but also contributes to their further development, ensuring stability and reliability in the dynamic evolution of blockchain technologies.

Keywords: blockchain, smart contract, Solana, information system, Rust, automated verification, optimization, security, decentralization.

Introduction

Despite optimistic forecasts in IT research that reveal blockchain's potential for creating decentralized societal structures, the practical implementation of these ideas faces significant challenges. A key obstacle to mass adoption is the vulnerabilities and errors inherent in the blockchain networks themselves and, specifically, in smart contract mechanisms [1-2].

In contrast to first-generation blockchains like Bitcoin, which are limited in functionality, second and third-generation platforms (Ethereum, Solana, Cardano) offer more complex capabilities. However, their complexity introduces new risks. For instance, the shift to consensus algorithms like Proof-of-Stake (PoS), which underlies the smart contracts of Ethereum and Solana, while solving the energy efficiency problems of its predecessor (Proof-of-Work), introduces new threats such as 51% attacks (in PoS) or the complexity of ensuring network security under delegated staking conditions [5-6].

The main threat lies in the implementation of smart contracts. Their core idea-the automatic execution of agreement terms without intermediaries-is simultaneously their main "Achilles' heel." The most dangerous errors are:

1. Logical Vulnerabilities: The contract's source code may contain errors that allow malicious actors to steal funds or disrupt the agreement's logic. History knows numerous cases of million-dollar losses due to such bugs;