Технічні науки

УДК 004.056:343.9

Сисоєнко Світлана Володимирівна

кандидат технічних наук, доцент,

доцент кафедри інформаційної безпеки та комп'ютерної інженерії

Черкаський державний технологічний університет

Sysoienko Svitlana

PhD in Engineering, Associate Professor,

Associate Professor of the Department of Information Security

and Computer Engineering

Cherkasy State Technological University

ORCID: 0000-0002-0009-337X

Бевза В'ячеслав Ігорович

бакалавр за спеціальністю 125 «Кібербезпека»

НУ «Одеська юридична академія»

Bevza Viacheslav

Bachelor's degree in Cybersecurity, specialty 125

National University "Odesa Law Academy"

ORCID: 0009-0007-2695-969X

Слатвінська Валерія Миколаївна

доктор філософії, асистент кафедри кібербезпеки

НУ «Одеська юридична академія»

Slatvinska Valeriia

Doctor of Philosophy, Assistant Professor of the Department of Cybersecurity

National University "Odesa Law Academy

ORCID: 0000-0002-6082-981X

Лада Наталія Володимирівна
кандидат технічних наук, провідний науковий співробітник
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки (м. Черкаси)
Lada Nataliia
PhD in Engineering, Leading Researcher
State Research Institute for Testing and Certification of Arms and Military Equipment (Cherkasy)
ORCID: 0000-0002-7682-2970

МЕТОДИ ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ КІБЕРЗАГРОЗ
METHODS OF DETECTING AND NEUTRALIZING CYBER THREATS

Анотація. *У дослідженні розглядаються методи виявлення та нейтралізації кіберзагроз для захисту критичної інфраструктури у 2025 році. Розглядаються сигнатурний аналіз, аномальний аналіз з прийняттям рішень ШІ, гібридні підходи, активні, пасивні та проактивні методи реагування. Пропонується інтеграція ШІ, великих даних та SOAR-систем для ефективного протистояння APT, ransomware й DDoS-атакам. Оцінка, що здійснюється через регулярні аудити та адаптація до особливостей секторів механізмів що забезпечують стабільність, надійність та швидкість захисту.*

Ключові слова: *кібербезпека, кіберзагрози, інформаційні впливи, загрози в кібербезпеці.*

Summary. *The study examines methods of detecting and neutralizing cyber threats to protect critical infrastructure in 2025. It considers signature analysis, anomaly analysis with AI decision-making, hybrid approaches, active, passive and proactive response methods. It suggests the integration of AI, big data, and SOAR systems to effectively counter APT, ransomware, and DDoS attacks.*

Evaluation, carried out through regular audits and adaptation of mechanisms to the specifics of the sectors to ensure the stability, reliability and speed of protection.

Key words: *cybersecurity, cyber threats, information influences, threats in cybersecurity.*

Постановка проблеми. Забезпечення кібербезпеки критичної інфраструктури у 2025 році вимагає ефективних методів виявлення та нейтралізації кіберзагроз, враховуючи їхню зростаючу складність і технологічну витонченість. Критична інфраструктура, що охоплює енергетику, транспорт, телекомунікації, водопостачання, охорону здоров'я та урядові системи, є основою функціонування суспільства, а її захист від таких загроз, як APT (Advanced Persistent Threats), ransomware, DDoS-атаки та AI-driven малваре, потребує системного підходу. Сучасні кіберзагрози характеризуються високим рівнем адаптивності та здатністю до еволюції, що вимагає впровадження інноваційних методів виявлення та нейтралізації на основі штучного інтелекту, машинного навчання та автоматизованих систем реагування.

Аналіз останніх досліджень. Дослідження в області кібербезпеки об'єктів критичної інфраструктури, зокрема потужністю сучасних інформаційних технологій та розвиток законодавчої бази щодо забезпечення безпеки показує про збільшений інтерес до інтеграції інноваційних рішень управління. Дорогий Я.Ю. та Цуркан В.В. [1] наголошують на відомій ключовій ролі захисту об'єктів інфраструктури під час військових загроз, зокрема в Україні, розглядаючи сучасні кіберзагрози як кібердиверсії та шпигунство, і на підставі чого розробляються рекомендації щодо покращення заходів захисту, підкреслюючи необхідність комплексного підходу, який передбачає організаційні й управлінські рішення.

Богдана Б. [2] віддає особливу увагу розвитку критичної інформаційної інфраструктури як основному об'єкту кібербезпеки і розглядає аспекти стійких систем захисту для забезпечення безпеки та поінформованості суспільства, зазначаючи, що згідно з сучасними вимогами, фахівці повинні поєднувати у собі сучасні технології, наприклад, штучний інтелект, для підвищення ефективності захисту. Скіцько О.І. [3] досліджує актуальні питання захисту кібербезпеки об'єктів критичної інфраструктури з метою перевірки наявних прогалин в законодавчо-нормативній базі та необхідності швидкої адаптації до нових видів загроз, вказуючи на особливості розробки керуючих підходів, на підставі яких можна побачити динаміку кіберзагроз й особливості різних секторів.

Комплексний підхід до правових аспектів кібербезпеки критичної інформаційної інфраструктури України представлений у дослідженні Коваліва М., Скриньковського Р., Назара Ю., Єсімова С., Красницького І., Кайдровича Х., Князя С., Кемської Ю. [4], де пропонується вдосконалення законодавчої бази шляхом опрацювання міжнародних стандартів, що вносить вклад у створення добре підготовлених спеціалістів з управлінських рішень щодо захисту інфраструктури. Скіцько О. та Ширшов Р. [5] поглиблюють дослідження нормативно-правової частини щодо кіберзахисту, підкреслюючи необхідність встановлення досить чіткої процедури і стандартів захисту об'єктів критичної інфраструктури, демонструючи, яким чином виведені рішення управління можуть допомогти державним організаціям та приватному сектору.

Технологічні аспекти підвищення рівня кібербезпеки розглядає Давидюк А. [6], який аналізує застосування нових засобів і методів, зокрема за допомогою штучного інтелекту та автоматизації для спостереження та реагування на кіберзагрози, показуючи перспективу застосування інноваційних технологій для розробки адаптивних засобів захисту, який міг бути інтегрований у управліннями стратегії. Богом'я В. та Галунько В. [7]

розглядають питання правового регулювання кібербезпеки захисту критичної інфраструктури, пропонуючи внести зміни до законодавчої бази для забезпечення швидкої дії в разі виникнення інцидентів та наголошуючи на співпраці сучасних технологій та управлінських рішень.

Міжнародний досвід представлений у роботі Ojo B., Ogborigbo J.C., Okafor M.O. [8], де представлені інновації в рамках сучасних рішень розвитку компаній і високоефективної інфопромисловості, являючи собою приклад комбінації штучного інтелекту, IoT і блокчейна як важливої складової для кібербезпеки. Sarkar A. [9] вивчає ефективні методи кібербезпеки для критичної інфраструктури через підхід до об'єднання науки про дані та машинного навчання в процеси, які стосуються інтеграції штучного інтелекту та великих даних у процеси управління ризиками, підкреслюючи, що сучасні управління методи повинні брати до уваги швидке зростання складності кіберзагроз.

Стандарти ISO/IEC 27001:2022 [10] та ISO/IEC 27011:2024 [11] продовжують залишатися основним джерелом інформації щодо принципів управління інформаційною безпеки та кіберзахистом, зокрема для керівників телекомунікаційних організацій, при цьому аналіз цих стандартів свідчить, що інтеграція нових світових управлінських рішень із міжнародним регулюванням може збільшити ефективність захисту критичної інфраструктури, але необхідна адаптація до локальних умов й особливості окремих секторів.

Виклад основного матеріалу. Методи виявлення кіберзагроз у контексті захисту критичної інфраструктури класифікуються за принципом аналізу та обробки інформації на три основні категорії, кожна з яких має специфічні характеристики ефективності та застосування. Сигнатурний аналіз представляє собой традиційний підхід, який базується на порівнянні мережевого трафіку чи поведінки системи з відомими сигнатурами атак, що зберігаються в спеціалізованих базах даних, таких як Snort або Suricata [3,

6], і виявляється ефективним для виявлення відомих загроз, зокрема ransomware типу WannaCry чи DDoS-атак з чіткими патернами поведінки, забезпечуючи високу точність виявлення до 99% для каталогізованих загроз.

Аналіз аномалій на базі штучного інтелекту представляє собой сучасний підхід до виявлення відхилень від нормальної поведінки систем чи користувачів за допомогою машинного навчання та статистичних методів, як це реалізовано в системах типу Darktrace [2; 9], що особливо підходить для виявлення нових загроз, таких як експлойти нульового дня чи AI-driven атаки, де традиційні сигнатури відсутні, забезпечуючи адаптивність до еволюціонуючих методів кіберзлочинців. Гібридний аналіз поєднує переваги сигнатурного підходу та аналізу аномалій, як це реалізовано в IBM QRadar або Splunk [8; 9], дозволяючи одночасно виявляти як відомі, так і невідомі загрози, що робить його оптимальним для комплексного захисту критичної інфраструктури від APT і атак на ланцюги постачання.

Методи нейтралізації кіберзагроз диференціюються за рівнем автоматизації та характером втручання в роботу систем критичної інфраструктури. Активні методи нейтралізації передбачають автоматизоване реагування на загрози в реальному часі, включаючи блокування IP-адрес, ізоляцію скомпрометованих вузлів чи припинення шкідливих процесів через SOAR-системи [1; 6], що використовується для швидкого реагування на DDoS-атаки чи ransomware з часом відповіді 1-2 секунди. Пасивні методи характеризуються генерацією оповіщень для операторів критичної інфраструктури без автоматичних дій, із подальшим ручним аналізом і реагуванням, як це реалізовано в Elastic Stack [5; 7], що виявляється ефективним для складних атак типу APT, які потребують експертної оцінки та детального аналізу.

Проактивні методи нейтралізації представляють собою превентивні заходи, що включають симуляцію атак через пентестинг чи систематичне оновлення систем для усунення вразливостей до їхньої потенційної

експлуатації [4; 11], забезпечуючи захист від експлойтів нульового дня та інсайдерських загроз через створення багаторівневої системи безпеки. Ключові методи виявлення демонструють різну ефективність залежно від типу загроз та специфіки критичної інфраструктури, при цьому сигнатурний аналіз використовує бази даних сигнатур для зіставлення з подіями в системі, забезпечуючи високу точність для відомих загроз до 99%, але виявляючись неефективним проти нових атак з точністю менше 10% для експлойтів нульового дня.

Аналіз аномалій на базі штучного інтелекту застосовує машинне навчання, зокрема нейронні мережі LSTM, для побудови базової моделі поведінки критичної інфраструктури та виявлення відхилень [2, 9], демонструючи здатність виявляти невідомі загрози з точністю до 95% при достатніх обсягах тренувальних даних, проте характеризуючись високим рівнем хибнопозитивних результатів до 15% та потребою в значних обчислювальних ресурсах. Кореляція подій через SIEM-системи, такі як Splunk, аналізує взаємозв'язки між подіями в системі критичної інфраструктури для виявлення складних атак [8; 10], забезпечуючи виявлення APT і атак на ланцюги постачання через аналіз патернів з точністю до 90%, але вимагаючи значних обчислювальних ресурсів для обробки до 1 млн подій за секунду.

Таблиця 1

Порівняльна характеристика методів виявлення та нейтралізації кіберзагроз критичної інфраструктури

Метод	Принцип роботи	Точність виявлення (%)	Час реагування	Типи загроз	Основні переваги	Обмеження
Сигнатурний аналіз	Порівняння з базою відомих сигнатур	99 (відомі) / 10 (нові)	Миттєво	Ransomware, DDoS	Висока точність, низькі хибнопозитивні	Неефективний для нових загроз

Аналіз аномалій (ШІ)	Машинне навчання на базі поведінки	95 (при достатніх даних)	1-5 хвилин	APT, експлойти нульового дня	Адаптивність, виявлення невідомих загроз	15% хибнопозитивних, потреба в даних
Гібридний аналіз	Комбінація сигнатур та аномалій	90	30 секунд - 2 хвилини	Комплексні атаки, APT	Баланс точності та адаптивності	Високі обчислювальні ресурси
Автоматичне блокування	Блокування джерела загрози в реальному часі	95	1-2 секунди	DDoS, ransomware	Швидкість реагування	5% блокування легітимного трафіку
Ізоляція вузлів	Відключення скомпрометованих компонентів	98	5-10 секунд	Malware, інсайдерські загрози	Обмежує поширення загроз	10% зниження доступності
Проактивний патч-менеджмент	Превентивне усунення вразливостей	80	Години-дні	Експлойти вразливостей	Запобігає атакам	Простої систем до 2 годин

Ключові методи нейтралізації кіберзагроз демонструють різноманітні підходи до локалізації та усунення загроз для критичної інфраструктури. Автоматичне блокування реалізується через блокування джерела загрози в реальному часі за допомогою NGFW типу Palo Alto чи IPS-систем [1; 8], забезпечуючи швидкість реагування за 1-2 секунди та ефективність проти DDoS і ransomware, проте характеризуючись можливим блокуванням легітимного трафіку в до 5% випадків. Ізоляція скомпрометованих вузлів передбачає відключення інфікованих компонентів критичної інфраструктури від мережі для локалізації загрози [6; 9], обмежуючи поширення ransomware чи APT з ефективністю до 98%, але спричиняючи тимчасове порушення роботи критичної інфраструктури з зниженням доступності до 10%.

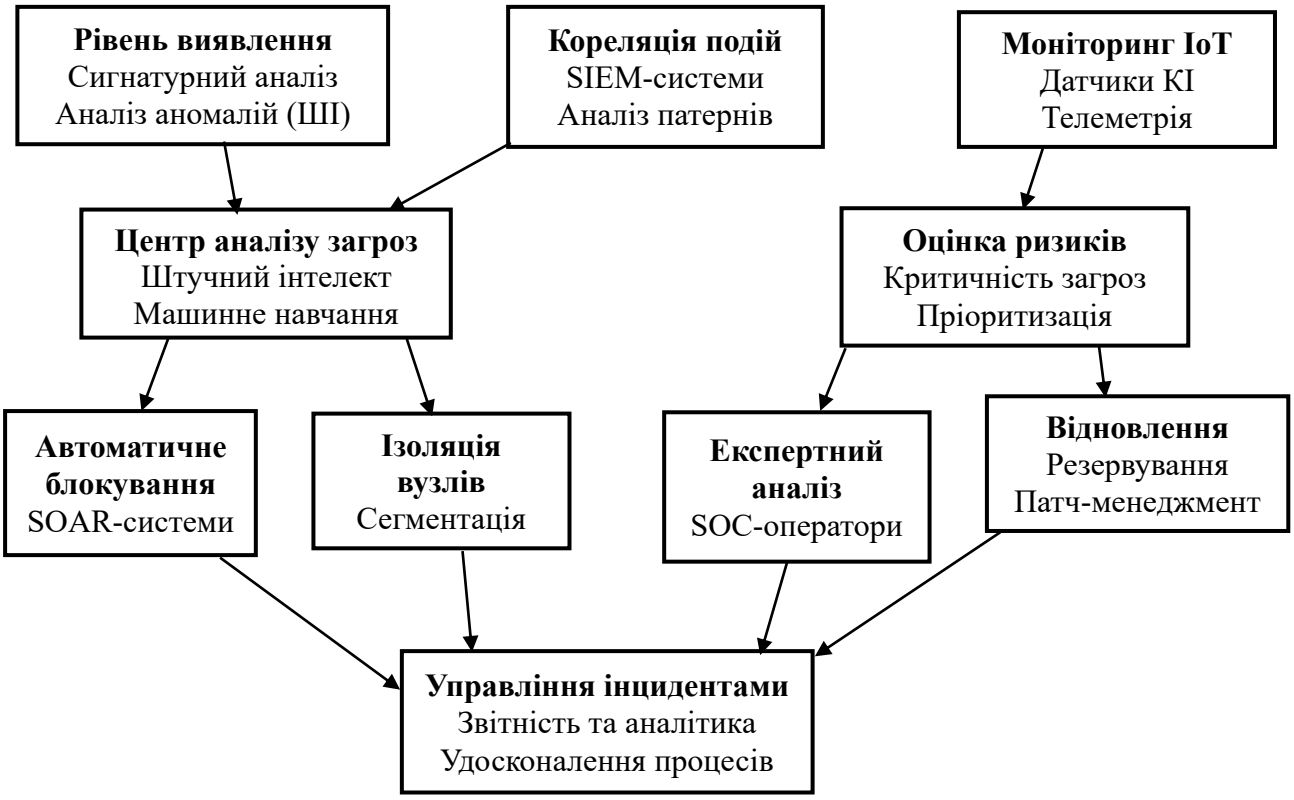

Рис. 1. Багаторівнева архітектура систем виявлення та нейтралізації кіберзагроз критичної інфраструктури

Представлена багаторівнева архітектура на рис. 1 демонструє інтеграцію різних методів виявлення та нейтралізації кіберзагроз у єдиній системі захисту критичної інфраструктури, де перший рівень забезпечує первинне виявлення загроз через сигнатурний аналіз, аналіз аномалій та моніторинг IoT-пристроїв, другий рівень здійснює глибокий аналіз та оцінку ризиків з використанням штучного інтелекту, третій рівень реалізує різноманітні методи нейтралізації від автоматичного блокування до експертного аналізу, а четвертий рівень забезпечує централізоване управління інцидентами та удосконалення процесів захисту.

Оновлення та патч-менеджмент представляють собою проактивне усунення вразливостей шляхом систематичного оновлення систем критичної інфраструктури до їхньої потенційної експлуатації кіберзлочинцями [4; 10; 11], забезпечуючи запобігання експлойтам

нульового дня з зменшенням ризику на 80%, проте потребуючи планових зупинок систем для оновлення тривалістю до 2 годин, що вимагає ретельного планування та координації з операторами критичної інфраструктури.

Станом на 2025 рік методи виявлення та нейтралізації кіберзагроз для критичної інфраструктури інтегрують передові технології для підвищення ефективності захисту. Штучний інтелект використовується в аналізі аномалій і кореляції подій для прогнозування атак із горизонтом до 30 хвилин з точністю до 92% у системах типу Darktrace [2; 6; 9], дозволяючи операторам критичної інфраструктури готуватися до потенційних інцидентів та превентивно активувати захисні механізми. Аналіз великих даних дозволяє обробляти до 10 ТБ даних із критичної інфраструктури щоденно, виявляючи складні патерни APT у SIEM-системах типу Splunk [8, 9], що забезпечує виявлення довготривалих кампаній кіберзлочинців, які можуть тривати місяцями без виявлення традиційними методами.

Автоматизація через SOAR-системи зменшує час реагування до 1-2 секунд для DDoS і ransomware, інтегруючи процеси виявлення та нейтралізації в єдиний автоматизований workflow [1; 6; 8], що критично важливо для критичної інфраструктури, де навіть короткочасні збої можуть мати катастрофічні наслідки для суспільства. Квантово-стійке шифрування захищає канали передачі даних від майбутніх квантових атак [10; 11], що особливо важливо для проактивних методів захисту та забезпечення довгострокової безпеки критичної інфраструктури в умовах розвитку квантових обчислень.

Аналіз ефективності різних методів виявлення та нейтралізації демонструє специфічні характеристики кожного підходу в контексті захисту критичної інфраструктури. Сигнатурний аналіз забезпечує високу ефективність 99% для відомих загроз, але демонструє низьку ефективність 10% для нових атак [3; 5], що робить його ефективним компонентом

багаторівневої системи захисту, але недостатнім як єдиний метод виявлення в умовах постійно еволюціонуючого ландшафту кіберзагроз. Аналіз аномалій на базі штучного інтелекту демонструє ефективність 95% для невідомих атак при достатній якості тренувальних даних, проте характеризується чутливістю до якості даних і рівнем хибнопозитивних результатів 15% [2; 9], що потребує додаткових засобів фільтрації та верифікації виявлених аномалій для мінімізації впливу на операційну діяльність критичної інфраструктури.

Висновки. Проведений аналіз методів виявлення та нейтралізації кіберзагроз для критичної інфраструктури станом на 2025 рік демонструє необхідність комплексного підходу, що включає сигнатурний аналіз, аналіз аномалій на базі штучного інтелекту, гібридний підхід, автоматичне блокування, ізоляцію вузлів і проактивний патч-менеджмент як взаємодоповнюючі компоненти багаторівневої системи кіберзахисту. Інтеграція сучасних технологій штучного інтелекту, аналізу великих даних та автоматизації процесів реагування через SOAR-системи значно підвищує ефективність захисних механізмів, дозволяючи адаптуватися до нових типів загроз, таких як AI-driven атаки, квантові загрози та складні APT-кампанії.

Кожен із розглянутих методів має специфічні переваги та обмеження, що обумовлює необхідність їхнього комбінованого застосування в системах кіберзахисту критичної інфраструктури для досягнення оптимального балансу між швидкістю виявлення, точністю ідентифікації загроз, ефективністю нейтралізації та мінімізацією впливу на операційну діяльність об'єктів критичної інфраструктури. Подальший розвиток методів виявлення та нейтралізації кіберзагроз має бути спрямований на підвищення адаптивності систем захисту, зменшення кількості хибнопозитивних спрацьовувань, інтеграцію квантово-стійких технологій та розвиток проактивних підходів до прогнозування та попередження кіберінцидентів у критичній інфраструктурі.

Література

1. Дорогий Я. Ю., Цуркан В. В. Кібербезпека критичної інфраструктури під час військової загрози. *Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні: матеріали XII міжн. наук.-практ. конф.,* 21-22 листопада 2024 р. Київ. 3 с. DOI: https://doi.org/10.5281/zenodo.14591061; URI: https://ela.kpi.ua/handle/123456789/71649 (дата звернення: 20.07.2025).

2. Богдана Б. Критична інформаційна інфраструктура як об'єкт забезпечення кібербезпеки. *Актуальні питання у сучасній науці.* 2025. DOI: 10.52058/2786-6300-2025-3(33)-473-482; URL: https://is.gd/sRQlCU (дата звернення: 20.07.2025).

3. Скіцько О.І. Актуальні питання забезпечення кібербезпеки об'єктів критичної інфраструктури. *Юридичний науковий електронний журнал.* № 10. 2024. С. 312-315. DOI: https://doi.org/10.32782/2524-0374/2024-10/71; URL: http://lsej.org.ua/10_2024/73.pdf (дата звернення: 20.07.2025).

4. Ковалів М., Скриньковський Р., Назар Ю., Єсімов С., Красницький І., Кайдрович Х., Князь С., Кемська Ю. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. Traek*toriâ Nauki - Path of Science*. 2021. No 4, Vol. 7. С. 2011–2018. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3731 (дата звернення: 20.07.2025).

5. Скіцько О., Ширшов Р. Нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична).* 2024. С. 73-79. DOI:10.32782/2311-8040/2024-2-11; URL: http://journals.lvduvs.lviv.ua/index.php/law/article/view/870 (дата звернення: 20.07.2025).

6. Davydiuk A. Впровадження нових засобів і методів підвищення рівня кібербезпеки об'єктів критичної інфраструктури. *Ukrainian Information Security Research Journal.* 2023. 25. С. 122-132. DOI: 10.18372/2410-7840.25.17937; URL: https://is.gd/0p4SaE (дата звернення: 20.07.2025).

7. Богом'я В., Галунько В. Правове регулювання кібербезпеки в контексті захисту критичної інфраструктури. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 2024. 4. P. 35–42, DOI: https://doi.org/10.32782/IT/2024-4-5; URL: https://journals.politehnica.dp.ua/index.php/it/article/view/705 (дата звернення: 20.07.2025).

8. Ojo B., Ogborigbo J. C., Okafor M. O. Innovative solutions for critical infrastructure resilience against cyber-physical attacks. 2024. URL: 10.30574/wjarr.2024.22.3.1921; DOI: https://doi.org/10.30574/wjarr.2024.22.3.1921 (дата звернення: 20.07.2025).

9. Sarkar A. Safeguarding the Backbone of Modern Society: Cybersecurity Strategies for Critical Infrastructure in the Digital Age. *International Journal of Scientific Research in Computer Science Engineering and Information Technology.* 2025. 11(2). P. 1631-1644. DOI: 10.32628/CSEIT25112535; URL: https://is.gd/OKxCKU (дата звернення: 20.07.2025).

10. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems. URL: https://www.iso.org/standard/27001 (дата звернення: 20.07.2025).

11. ISO/IEC 27011:2024 - Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations. URL: https://www.iso.org/standard/80584.html (дата звернення: 20.07.2025).