

ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩІЙ НАВЧАЛЬНИЙ ЗАКЛАД»
МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
ІНСТИТУТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА
ДИЗАЙНУ
Кафедра комп'ютерних інформаційних систем та технологій

Покатілов Олександр Миколайович
(прізвище, ім'я, по батькові здобувача вищої освіти в називному відмінку)

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття ступеня бакалавра
на тему: «Порівняння підходів до управління кіберризиками у різних
країнах»

ТУчр-9-22-Б1КНТ (4.0д)

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 122 «Комп'ютерні науки»

Освітньо-професійна програма: «Комп'ютерні науки»

Рівень вищої освіти: перший (бакалаврський)

*Кваліфікаційна робота містить результати власних досліджень.
Використання ідей, результатів, текстів інших авторів мають посилання на
відповідне джерело*

(підпис) Покатілов О.М.
(прізвище та ініціали)

Науковий керівник

Старший викладач

(посада, науковий ступінь,
вчене звання)

(підпис) Маклюк О.В.
(прізвище та ініціали)

Київ – 2026 рік

ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД»
МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
ІНСТИТУТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА
ДИЗАЙНУ
Кафедра комп'ютерних інформаційних систем та технологій

Рівень вищої освіти: перший (бакалаврський) рівень
Ступінь вищої освіти: бакалавр
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 122 «Комп'ютерні науки»
Освітньо-професійна програма: «Комп'ютерні науки»

Завдання
на кваліфікаційну роботу здобувачу вищої освіти

Покатілову Олександру Миколайовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:

«Порівняння підходів до управління кіберризиками у різних країнах»

Керівник кваліфікаційної роботи

Старший викладач

(посада, науковий ступінь, вчене звання)

Маклюк Олег Володимирович

(прізвище, ім'я, по батькові)

2. Термін подання здобувачем кваліфікаційної роботи на попередній захист 15.05.2026 року

3. Вихідні дані до кваліфікаційної роботи (рекомендовані науковим керівником та відповідним методичним забезпеченням (окремі аспекти роботи, обсяги роботи):

Дослідити предметну область управління кіберризиками у державному та корпоративному середовищі. Розкрити сутність понять «кібербезпека», «кіберзагроза» та «кіберризик», визначити їхню роль у забезпеченні національної та інформаційної безпеки. Проаналізувати етичні та правові аспекти кібербезпеки, зокрема міжнародні стандарти та положення українського законодавства. Провести порівняльний аналіз підходів до управління кіберризиками у США (NIST Cybersecurity Framework, CISA), Європейському Союзі (ENISA, GDPR, директива NIS2) та країнах Азії (зокрема Китай, Південна Корея). Визначити особливості державного регулювання та корпоративних практик у цих країнах, їхні сильні сторони та можливості адаптації до українських реалій.

Обґрунтувати актуальність дослідження для України в умовах військової агресії та цифрової трансформації. Проаналізувати поточний стан кібербезпеки в Україні, окреслити ключові проблеми та виклики. Сформулювати практичні рекомендації щодо вдосконалення системи управління кіберризиками в Україні з урахуванням зарубіжного досвіду.

Розробити узагальнену модель управління кіберризиками, яка враховує технологічні, правові та організаційні аспекти, а також визначити перспективи її впровадження у національну систему протидії кіберзагрозам.

4. Необхідний графічний та аналітичний матеріал за темою дослідження:

-

5. Календарний план виконання кваліфікаційної роботи

№ п/п	Назва етапів виконання кваліфікаційної роботи	Строки виконання		Примітки
		Планові	Фактичні	
1	2	3	4	5
	Вступ	16.02.2026–02.03.2026		
	Розділ 1.	02.03.2026–16.03.2026		
	Розділ 2.	16.03.2026–06.04.2026		
	Розділ 3.	06.04.2026–22.04.2026		
	Висновки	До 30.04.2026		

6. Дата видачі завдання 28.08.2025 р.

Здобувач (ка) _____
(підпис)

Покатілов О.М.
(прізвище та ініціали)

Науковий керівник _____
(підпис)

Маклюк О.В.
(прізвище та ініціали)

АНОТАЦІЯ

Покатілов О.М. «Порівняння підходів до управління кіберризиками у різних країнах» – Рукопис.

Кваліфікаційна робота на здобуття першого (бакалаврського) рівня вищої освіти – Приватне акціонерне товариство «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»», Інститут комп'ютерно-інформаційних технологій та дизайну – Київ, 2026.

Актуальність теми дослідження зумовлена стрімкою цифровою трансформацією та зростанням кількості кібератак на державні установи, бізнес-структури та критичну інфраструктуру України. Управління кіберризиками стає стратегічним чинником національної безпеки, що потребує не лише технічних рішень, а й комплексного підходу з урахуванням правових, організаційних та етичних аспектів.

Мета роботи полягає у здійсненні порівняльного аналізу закордонних моделей управління кіберризиками (США, ЄС, країни Азії) та визначенні перспектив їх упровадження в українську систему протидії кіберзагрозам.

У кваліфікаційній роботі розкрито сутність понять «кібербезпека», «кіберзагроза» та «кіберризик», досліджено етичні та правові аспекти кібербезпеки, проаналізовано міжнародні стандарти та практики управління ризиками. Проведено порівняльний аналіз підходів у США (NIST Cybersecurity Framework, CISA), Європейському Союзі (ENISA, GDPR, директива NIS2) та країнах Азії (Китай, Південна Корея). Окреслено сучасний стан кібербезпеки в Україні та розроблено практичні рекомендації щодо вдосконалення системи управління кіберризиками з адаптацією зарубіжного досвіду.

Методи дослідження, використані у роботі: аналіз і узагальнення наукових джерел, аналітика, порівняльний аналіз міжнародних моделей управління ризиками, моделювання структури системи кіберзахисту, методи ризик-менеджменту.

Ключові слова: кібербезпека, кіберризик, кіберзагроза, управління кіберризиками, міжнародний досвід, Україна.

ANNOTATION

Pokatilov O.M. “Comparison of Approaches to Cyber Risk Management in Different Countries” – Manuscript.

Qualification work for obtaining the first (bachelor's) level of higher education – Private Joint-Stock Company “Higher Educational Institution ‘Interregional Academy of Personnel Management’”, Institute of Computer Information Technologies and Design – Kyiv, 2026.

The relevance of the research topic is determined by the rapid digital transformation and the growing number of cyberattacks on government institutions, business structures, and critical infrastructure in Ukraine. Cyber risk management is becoming a strategic factor of national security, requiring not only technical solutions but also a comprehensive approach that takes into account legal, organizational, and ethical aspects.

The aim of the qualification work is to conduct a comparative analysis of foreign models of cyber risk management (USA, EU, Asian countries) and to identify the prospects for their implementation in the Ukrainian system of countering cyber threats.

The qualification paper reveals the essence of the concepts “cybersecurity,” “cyber threat,” and “cyber risk,” examines ethical and legal aspects of cybersecurity, and analyzes international standards and risk management practices. A comparative analysis of approaches in the USA (NIST Cybersecurity Framework, CISA), the European Union (ENISA, GDPR, NIS2 Directive), and Asian countries (China, South Korea) has been carried out. The current state of cybersecurity in Ukraine has been outlined, and practical recommendations have been developed to improve the cyber risk management system with adaptation of foreign experience.

The research methods used in the work: analysis and synthesis of scientific sources, analytics, comparative analysis of international risk management models, modeling of cybersecurity system structures, risk management methods.

Keywords: cybersecurity, cyber risk, cyber threat, cyber risk management, international experience, Ukraine.

ВСТУП.....	7
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ КІБЕРРИЗИКАМИ..	10
1.1. Зміст та сутність понять «кібербезпека», «кіберзагроза» і «кіберризик»	10
1.2. Етичні та правові аспекти кібербезпеки.....	17
Висновки до розділу 1	26
РОЗДІЛ 2. ПОРІВНЯЛЬНИЙ АНАЛІЗ ПІДХОДІВ У РІЗНИХ КРАЇНАХ	28
2.1. Управління кіберризиками у США (NIST Cybersecurity Framework, CISA)	28
2.2. Досвід Європейського Союзу: ENISA, GDPR та директива NIS2	38
2.3. Державне регулювання та корпоративні практики у Китаї та країнах Азії	48
Висновки до розділу 2	60

ЗМІСТ

РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА РЕКОМЕНДАЦІЇ УПРОВАДЖЕННЯ ЗАКОРДОННОГО ДОСВІДУ БОРОТЬБИ З КІБЕРРИЗИКАМИ В УКРАЇНІ	62
3.1. Аналіз поточного стану кібербезпеки в Україні	62
3.2. Рекомендації щодо вдосконалення системи управління кіберризиками в Україні з адаптацією закордонного досвіду.....	73
Висновки до розділу 3	78
ВИСНОВКИ	80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	83

ВСТУП

У сучасних реаліях військової агресії росії, коли стрімка цифрова трансформація породжує низку важливих проблем, питання кібербезпеки набувають особливої ваги для України. Зростання кількості кібератак на державні установи, бізнес-структури та критичну інфраструктуру демонструє, що управління кіберризиками є не лише технічним завданням, а й стратегічним чинником національної безпеки. Саме тому дослідження зарубіжного досвіду та його адаптація до українських реалій має важливе значення для формування ефективної системи протидії кіберзагрозам.

Прагнення до інтеграції України у світовий цифровий простір, важливість адаптації національних стандартів до міжнародних та забезпечення стійкості інформаційних систем до ризиків визначає стратегічний напрям розвитку нашої держави. Це потребує не лише технічних рішень, а й комплексного підходу до управління кіберризиками, який враховує правові, організаційні та етичні аспекти. Зазначене вище і зумовлює **актуальність** обраної теми нашого дослідження *«Порівняння підходів до управління кіберризиками у різних країнах»*.

Об'єктом дослідження виступають процеси управління кіберризиками у державному та корпоративному середовищі.

Предмет дослідження – підходи до управління кіберризиками у різних країнах світу та можливості їх застосування в Україні.

Метою нашої кваліфікаційної роботи є здійснення порівняльного аналізу закордонних моделей управління кіберризиками та визначення перспектив їх упровадження в національну систему протидії кіберзагрозам.

Досягнення поставленої мети передбачає виконання наступних **завдань**:

- 1) розкрити сутність поняття «кіберризиками» та надати їх класифікацію;

- 2) порівняти підходи до управління кіберризиками у США, ЄС та країнах Азії;
- 3) проаналізувати поточний стан кібербезпеки в Україні;
- 4) сформулювати практичні рекомендації щодо вдосконалення системи управління кіберризиками в Україні.

Теоретична основа дослідження спирається на праці українських науковців (Ємельянов В., Бондар Г., Миненко С., Кочнева В., Бабич Є., Овандер Н., Орловський Б., Черноног О.), які досліджують проблеми кібербезпеки та інформаційного захисту, а також на роботи зарубіжних авторів (AbuHmed T., Mohaisen A., Nyang D., Ayush Mishra, Carroll Jami M., Ibo van de Poel, Kennedy A., Wang Xiaojun, Liu Zhen.), наукові пошуки котрих присвячені аналізу міжнародних стандартів та практики управління кіберризиками і проблемам кібербезпеки.

Методи дослідження: аналіз і узагальнення наукових джерел, аналітика, порівняльний аналіз міжнародних моделей управління ризиками, моделювання структури системи кіберзахисту, методи ризик-менеджменту.

Наукова новизна нашого дослідження полягає у систематизації та порівнянні підходів до управління кіберризиками у різних країнах (США, ЄС, країни Азії); на основі порівняльного аналізу пропонуються практичні рекомендації щодо упровадження позитивного досвіду зарубіжних країн, а також визначаються можливості їх адаптації до сучасних українських реалій.

Теоретичне значення нашої випускної кваліфікаційної роботи визначається поглибленням наукових уявлень про моделі управління кіберризиками у зарубіжних країнах та їх роль у забезпеченні кіберстійкості нашої держави.

Практичне значення дослідження полягає у розробці рекомендацій для щодо удосконалення системи управління кіберризиками та протидії кіберзагрозам.

Структура роботи. Робота складається зі вступу, трьох розділів та висновків до кожного з них, загальних висновків та списку використаних джерел (75 одиниць друкованої та електронної літератури українською й англійською мовами). Загальний обсяг дослідження становить 91 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ КІБЕРРИЗИКАМИ

1.1. Зміст та сутність понять «кібербезпека», «кіберзагроза» і «кіберризик»

Кібербезпека сьогодні розглядається як ключовий елемент системи національної безпеки держави. Вона визначається як сукупність організаційних, правових та технічних заходів, спрямованих на захист інформаційних ресурсів, комп'ютерних систем і мереж від несанкціонованого доступу, використання, модифікації чи руйнування. Її значення виходить далеко за межі технологічної сфери, адже кіберзагрози здатні впливати на політичну стабільність, економічну стійкість та соціальну безпеку.

До основних напрямів важливості кібербезпеки для держави належать:

- 1) Захист критичної інфраструктури. Енергетика, транспорт, фінансові системи та комунікаційні мережі є найбільш уразливими до кібератак. Їхня стійкість визначає здатність держави функціонувати у кризових умовах.
- 2) Політична безпека. Кібератаки можуть використовуватися як інструмент зовнішнього втручання чи дестабілізації, впливаючи на роботу урядових органів, виборчі процеси та державні реєстри.
- 3) Економічна стабільність. Наслідки атак включають фінансові втрати, порушення роботи підприємств, падіння довіри до банківської системи та інвестиційного клімату.
- 4) Захист прав громадян. Кіберзлочини часто спрямовані на персональні дані, що створює ризики для приватності, безпеки особи та довіри до цифрових сервісів.
- 5) Міжнародна співпраця. Оскільки кіберзагрози не мають кордонів, ефективна протидія можлива лише через обмін досвідом, спільні ініціативи та участь у глобальних програмах кіберзахисту [70, с. 775-784].

У науковій літературі *кібербезпека* визначається як сукупність заходів, спрямованих на захист інформаційних систем, мереж та даних від несанкціонованого доступу, використання, розкриття, руйнування чи модифікації. Вона охоплює технологічні, правові та організаційні аспекти, забезпечуючи безпеку цифрового середовища та захист прав людини [19, с. 185].

За визначенням корпорації IBM, *кібербезпека* – це практика захисту людей, систем і даних від кібератак за допомогою різних технологій, процесів і політик. На рівні підприємства кібербезпека є ключовою для загальної стратегії управління ризиками, а саме для управління кіберризиками. До поширених загроз і ризиків кібербезпеці належать програми-вимагачі та інші шкідливі програми, фішингові шахрайства, крадіжка даних і, останнім часом, атаки, що працюють на основі штучного інтелекту (ШІ) [71].

У науковому дискурсі поняття ризику має багатогранне трактування. Згідно з одним із визначень, ризик розуміється як ймовірність настання інциденту та його наслідків для певного об'єкта [64, с. 9]. Класичний підхід до управління ризиками базується на категорії загрози. У цьому контексті загроза визначається як точка взаємодії людей, Інтернету та комп'ютерних систем, що може призвести як до помилок, так і до навмисних дій. Якщо помилки можливо усунути шляхом підвищення обізнаності щодо важливості належного поводження з конфіденційною інформацією, то зловмисні впливи мають принципово інший характер.

Орієнко С. та Черней В. підкреслюють, що інформаційна безпека нерозривно пов'язана з діяльністю злочинних угруповань та транснаціональної організованої злочинності. Такі мережі функціонують у багатьох країнах, плануючи свої дії та досягаючи бізнес - цілей, які часто включають тяжкі злочини: торгівлю людьми, сексуальну експлуатацію, наркоторгівлю, насильницькі злочини, корупцію, торгівлю зброєю тощо. Важливо зазначити, що саме транснаціональна злочинність однією з перших усвідомила переваги

використання сучасних інформаційних технологій та комунікацій, а також надійних систем захисту.

Метою управління ризиками у сфері кібербезпеки є виявлення та усунення факторів, що можуть поставити під загрозу інформацію або порушити бізнес - процеси, шляхом застосування відповідних заходів безпеки з урахуванням рівня ризик-толерантності організації. У цьому контексті ризик-аналіз визначається як методологія, що дозволяє оцінити ймовірність негативних наслідків для технологічних процесів, промислових систем чи природних явищ [60, с. 149].

У сфері кібербезпеки ризик трактується як ймовірність настання несприятливої події, що включає два ключові параметри: ймовірність її реалізації та масштаб можливих наслідків. У математичному вимірі ризик може бути виражений як відхилення від очікуваного результату. Якщо у фінансовій сфері високий ризик іноді може бути виправданим через потенційно високі прибутки, то у галузі інформаційної безпеки, навпаки, необхідно прагнути до мінімізації ризиків, активно знижуючи рівень загроз та можливих збитків [65, с. 16].

Згідно з доповіддю «Global Risks» Світового економічного форуму за 2023 рік, серед глобальних ризиків, ранжованих за ступенем небезпеки у коротко - та довгостроковій перспективі, окреме місце посідає проблема поширеної кіберзлочинності та недостатнього рівня кіберзахисту, яка займає восьму позицію у рейтингу. У документі зазначається, що технології посилюватимуть цифрову нерівність, а ризики, пов'язані з кібербезпекою, залишатимуться постійним викликом. Технологічний сектор визначається як головний об'єкт промислової політики. Очікується, що державна підтримка, військові бюджети та приватні інвестиції забезпечать високі темпи розвитку й досліджень у сфері новітніх технологій протягом наступного десятиліття, зокрема у галузі штучного інтелекту [60, с. 149].

У сучасному дискурсі кібербезпеки термін «кіберзагроза» використовується для позначення будь - якої обставини чи події, що має потенціал негативно вплинути на діяльність організації, її активи, репутацію або окремих осіб через інформаційні системи. Йдеться про можливість несанкціонованого доступу, знищення, розкриття, модифікації даних чи відмови у доступі до ресурсів, що може призвести до порушення функціонування системи та завдання шкоди.

Згідно з підходами, закріпленими у стандартах NIST (зокрема, SP 800-30, SP 800-53, SP 800-137 та інших), *кіберзагроза* визначається як потенційна небезпека, що може бути реалізована через експлуатацію вразливостей інформаційних систем. Вона охоплює широкий спектр ризиків, починаючи з інцидентів, котрі загрожують окремим користувачам, і закінчуючи подіями, які здатні вплинути на функціонування цілих організацій чи навіть держав.

Таким чином, *кіберзагроза* є багатовимірним явищем, яке поєднує технологічні, організаційні та соціальні аспекти. Її сутність полягає не лише у можливості здійснення атаки, а й у потенціалі джерела загрози успішно використати вразливості системи. Усвідомлення цього дозволяє розглядати кіберзагрозу як ключовий елемент управління ризиками, що потребує постійного моніторингу, оцінки та розроблення превентивних заходів для забезпечення стійкості інформаційних ресурсів [29].

Отже, поняття кіберзагрози окреслює потенційні небезпеки для інформаційних систем та суспільства загалом. Однак для практичного управління безпекою важливо не лише ідентифікувати джерела загроз, а й оцінювати їхню ймовірність та можливі наслідки. Саме тому дедалі більшої ваги набуває поняття кіберризик, яке дозволяє кількісно та якісно вимірювати рівень небезпеки й формувати ефективні механізми протидії.

Поняття «*кіберзагроза*» тісно пов'язане із поняттям «*кіберризик*». Відтак, кіберзагроза виступає джерелом небезпеки, а кіберризик – її виміром у

правовому, економічному та організаційному контекстах. Усвідомлення цього взаємозв'язку дозволяє комплексно оцінювати рівень небезпеки та формувати ефективні механізми управління кібербезпекою.

У сучасному правовому полі поняття *«кіберризик»* поступово виходить на передній план у зв'язку з інтенсивною цифровізацією суспільства та зростанням масштабів кіберзагроз. Попри це, його дефініція залишається дискусійною, адже охоплює не лише технічні параметри, а й соціальні, економічні та правові виміри. Важливо усвідомлювати, що кіберризик має також юридичний характер, оскільки відображає ймовірність виникнення негативних правових наслідків у результаті неналежної чи непрофесійної діяльності у кіберпросторі.

В українському законодавстві, як і в положеннях ратифікованої *«Конвенції про кіберзлочинність»*, відсутнє чітке визначення цього терміна. У Законі України *«Про основні засади забезпечення кібербезпеки України»* використовуються інші категорії – *«кіберінцидент»*, *«кібератака»*, *«кібершпиунство»*, *«кібертероризм»*, які фактично є проявами кіберризиків, проте саме поняття *«кіберризик»* юридично не закріплене. Лише у підзаконних актах, зокрема у *«Стратегії кібербезпеки України»*, цей термін застосовується епізодично, зокрема у контексті розроблення методик оцінки кіберризиків чи упровадження системи страхування, але без надання офіційного тлумачення.

З огляду на це, розкриття змісту поняття *«кіберризик»* є актуальним завданням, адже воно формується на перетині трьох ключових площин:

- 1) технологічної – у вигляді вразливостей інформаційних систем;
- 2) соціальної – через злочинні наміри суб'єктів;
- 3) правової – як наслідок недосконалості регуляторних механізмів [10, с. 212].

За визначенням Інституту ризик-менеджменту (Institute of Risk Management), *«кіберризик»* означає будь-який ризик фінансових втрат, збоїв або пошкодження репутації організації внаслідок будь-якого збою її інформаційно-технологічних систем. Також зазначено, що ризики та можливості, які надають цифрові технології, пристрої та медіа, очевидні. Кіберризики ніколи не є

питанням виключно ІТ-команди. Функція управління ризиками в організації повинна мати глибоке розуміння постійно змінюваних загроз, а також володіти практичними інструментами й методиками для їхнього подолання [45].

Відповідно до CSRC (Computer Security Resource Center) «*кіберризик* – це ймовірність виникнення негативних наслідків для інформаційних систем, бізнес-процесів чи національної безпеки, що зумовлена залежністю від цифрових ресурсів та технологій. Він охоплює ризик фінансових втрат, порушення операційної діяльності або завдання шкоди внаслідок збоїв цифрових систем чи їх елементів, а також через несанкціонований доступ, використання, розкриття, модифікацію або знищення інформаційних ресурсів [29].

Орловський Б.М. інтерпретує *кіберризик* як ймовірність настання негативних наслідків у результаті реалізації кіберзагроз, що здатні завдати шкоди інформаційним системам, конфіденційності даних, фінансовій стабільності чи навіть національній безпеці. Він пропонує наступне визначення поняттю:

Кіберризик – це ймовірність виникнення негативних наслідків для суб'єктів кібербезпеки, національної безпеки, суспільства та держави, що обумовлена наявністю потенційних кіберзагроз та/або вразливостей інформаційних, комунікаційних та інформаційно - комунікаційних систем, а також недоліками їх захисту, які можуть призвести до порушення конфіденційності, цілісності та доступності інформаційних ресурсів, порушення стабільного функціонування зазначених систем і завдання шкоди законним інтересам фізичних та юридичних осіб, майну та критичній інфраструктурі [10, с. 212].

Структура кіберзагроз, що формують ризики у сфері кібербезпеки, є багатокомпонентною та охоплює різні типи атак і вразливостей. Одним із найпоширеніших явищ є фішингові атаки, які здійснюються шляхом надсилання підроблених електронних листів чи повідомлень з метою отримання конфіденційної інформації або спонукання користувачів перейти за

шкідливими посиланнями. Наслідком таких дій часто стає крадіжка даних чи зараження системи шкідливим програмним забезпеченням.

До особливо небезпечних належать атаки типу «ransomware», коли зловмисники блокують доступ до даних шляхом їх шифрування та вимагають викуп за ключ розшифрування. Подібні інциденти призводять до серйозних перебоїв у роботі організацій та значних фінансових втрат. У ширшому сенсі до категорії шкідливого програмного забезпечення (malware) належать віруси, «трояни», «черви» та інші програми, створені для завдання шкоди комп'ютерним системам і мережам.

Окрему групу становлять внутрішні загрози (insider threats), що походять від співробітників чи підрядників, які навмисно або ненавмисно зловживають своїм доступом до інформаційних ресурсів. Не менш небезпечними є цілеспрямовані довготривалі атаки (Advanced Persistent Threats, APTs), які здійснюються професійними хакерами протягом тривалого часу з метою отримання несанкціонованого доступу до конфіденційних даних.

З поширенням технологій Інтернету речей зростає ризик атак на IoT-пристрої, що можуть використовуватися для проникнення у корпоративні мережі або спричинення збоїв у їх функціонуванні. Подібні виклики актуальні й для хмарних сервісів, які, попри свою інтегрованість у сучасні бізнес-процеси, створюють нові ризики, пов'язані з витоком даних, перехопленням сервісів чи несанкціонованим доступом.

Важливим інструментом кіберзлочинців залишаються атаки соціальної інженерії, котрі базуються на маніпуляції людьми з метою отримання конфіденційної інформації або спонукання їх до дій, які шкодять безпеці. До категорії масових атак належать Distributed Denial of Service (DDoS), коли система чи мережа перевантажується трафіком і стає недоступною для користувачів. Такі атаки часто використовуються для дестабілізації бізнес-процесів або шантажу організацій.

I, нарешті, кібершпигунство, що полягає у викраденні конфіденційної інформації з метою отримання конкурентних чи політичних переваг окремими організаціями або державами.

Отже, спектр кіберзагроз є надзвичайно широким і охоплює як технічні, так і соціально-організаційні аспекти. Їх комплексне розуміння є необхідною умовою для ефективного управління кіберризиками та забезпечення стійкості інформаційних систем [60, с. 151].

1.2. Етичні та правові аспекти кібербезпеки

Взаємозв'язок між технологіями, правом та етикою набув важливого значення в академічному та публічному дискурсі в швидкозмінну цифрову епоху. У цьому підрозділі ми робимо спробу з'ясувати природу цих зв'язків, оцінити наслідки та надати уявлення про зміни в цій складній галузі шляхом ретельного вивчення складної динаміки, що оточує кіберправо та кіберетику.

Поширення технологій та міжнародний масштаб кіберпростору створюють безпрецедентні перешкоди для усталених правових структур. Як результат, необхідним є аналіз поточного стану кіберправа, що встановлює рамки для ретельного вивчення труднощів, що виникають через кіберзлочини, підкреслюючи необхідність ефективних правових баз для боротьби з цими ризиками та захисту прав людей [19, с. 186].

Законодавство у сфері кібербезпеки формувалося як відповідь на зростання масштабів та складності кіберзагроз. Перші нормативні ініціативи здебільшого виникали після резонансних інцидентів, що продемонстрували серйозні вразливості як у державному, так і в приватному секторах. Початкові закони мали фрагментарний характер: вони концентрувалися на окремих сферах чи проблемах, як то захист даних, протидія кіберзлочинності або забезпечення критичної інфраструктури, без створення комплексної та узгодженої нормативної бази. В останні роки спостерігається зсув у бік більш інтегрованих та комплексних правил кібербезпеки. Ці закони тепер охоплюють

широкий спектр питань, від захисту даних та конфіденційності до безпеки критичної інфраструктури та звітності про інциденти [34].

Будапештська конвенція про кіберзлочинність, ухвалена Радою Європи у 2001 році, стала першим міжнародним договором, що заклав правові основи боротьби з кіберзлочинами у глобальному масштабі. Її поява була зумовлена стрімким розвитком інформаційних технологій та зростанням кількості правопорушень у цифровому середовищі, які виходили за межі національних юрисдикцій. Конвенція визначила перелік дій, що підлягають криміналізації, серед яких незаконний доступ до комп'ютерних систем, перехоплення даних, втручання у роботу мереж, комп'ютерне шахрайство та порушення авторських прав. Важливим нововведенням стало закріплення процесуальних інструментів, які дозволяють правоохоронним органам ефективно збирати цифрові докази, здійснювати обшук та вилучення даних, а також перехоплювати комунікації у реальному часі.

Ця конвенція наголосила на необхідності міжнародної співпраці, створивши механізми швидкої взаємодії між державами, зокрема мережу «24/7», що забезпечує оперативний обмін інформацією. Її значення полягає не лише у встановленні єдиних стандартів кримінального права, але й у прагненні збалансувати боротьбу з кіберзлочинністю із захистом прав людини, включно з правом на приватність та свободою слова. Саме тому Будапештська конвенція стала орієнтиром, який використовується багатьма країнами як основа для розробки власного законодавства у сфері кібербезпеки [5].

Іншим фундаментальним документом є Загальний регламент про захист даних (GDPR), ухвалений Європейським Союзом у 2016 році, він набрав чинності у 2018 року. Цей документ визначив нові стандарти захисту персональних даних, які стали обов'язковими для всіх організацій, що здійснюють обробку інформації громадян ЄС. GDPR закріпив принципи прозорості та підзвітності, зобов'язавши компанії чітко пояснювати, як саме використовуються дані користувачів, а також надав громадянам низку нових прав, серед яких право на доступ до власної інформації, її виправлення,

видалення («право бути забутим») та право на передачу даних. Регламент встановив суворі вимоги щодо повідомлення про витoki даних та запровадив інститут Data Protection Officer, котрий призначений відповідальним за дотримання правил у кожній організації. Його вплив вийшов далеко за межі Європейського Союзу, адже GDPR став глобальним еталоном приватності, який наслідують інші країни, зокрема Бразилія, Японія, Південна Африка та США (через California Consumer Privacy Act). Важливою особливістю регламенту є запровадження значних штрафів за порушення – до двадцяти мільйонів євро або чотирьох відсотків від річного обороту компанії, що стимулює бізнес до відповідального ставлення до даних користувачів [3].

Підсумовуючи, можемо зазначити, що Будапештська конвенція та GDPR репрезентують два взаємодоповнювальні напрями розвитку міжнародного кіберправа. Конвенція зосереджена на кримінально - правових аспектах та боротьбі з кіберзлочинністю, а GDPR, у свою чергу, формує етичні та правові стандарти захисту персональних даних. Разом вони створюють комплексну основу для регулювання цифрового середовища, забезпечуючи гарантію безпеки та прав людини. Їхнє значення для глобального світового середовища полягає у формуванні правових механізмів, що дозволяють протидіяти кіберзагрозам, водночас підтримуючи довіру громадян до цифрових технологій та сприяючи розвитку демократичного суспільства у цифрову епоху.

Правові виклики кіберпростору репрезентують необхідність оновлення нормативних рамок та висувають питання моральних орієнтирів, що мають визначати розвиток та застосування кібербезпеки, адже ефективність правових механізмів значною мірою залежить від того, наскільки вони узгоджені з базовими цінностями, котрі формують етичний фундамент цифрового суспільства.

У сфері кібербезпеки можна виокремити кілька ключових кластерів цінностей, що відображають основні моральні орієнтири та відповідають на типові проблемні ситуації:

Першим кластером є безпека, яку можна розуміти як індивідуальну чи національну. До нього належать також кібербезпека, інформаційна безпека та інструментальні цінності (конфіденційність, цілісність і доступність даних). Основна мета цього кластера полягає у захисті людей та інших цінних об'єктів від шкоди, що може виникати внаслідок витоків інформації, втрати її цілісності, кіберзлочинності чи навіть кібервоєн.

Другий кластер – конфіденційність. Він охоплює моральну автономію, людську гідність, ідентичність, особистість, свободу, анонімність. Цінності цього кластера вимагають поваги до особистих даних та їхнього використання лише за поінформованої згоди. Вони є відповіддю на морально проблемні ситуації, пов'язані з таємним збором великих масивів даних чи їхньою несанкціонованою передачею третім сторонам.

Третій кластер визначає справедливість. Сюди входить рівність, доступність, свобода від упереджень, відсутність дискримінації, демократія та захист громадянських прав. Цей кластер підкреслює, що кіберзагрози та заходи протидії їм можуть впливати на різні групи нерівномірно, створюючи морально несправедливі умови. Крім того, посилення кібербезпеки може іноді обмежувати демократичні права та свободи, що потребує особливої уваги.

Четвертий кластер представляє підзвітність. Він охоплює прозорість, відкритість та пояснюваність. Підзвітність є важливою процедурною цінністю, адже заходи кібербезпеки, особливо урядові, можуть завдавати шкоди громадянам. Вона передбачає обов'язок звітувати за свої дії, а також відповідальність за неправомірну поведінку, включно з компенсацією чи штрафами.

Окрім наведених вище кластерів, існують й цінності, що залежать від конкретної сфери застосування кібербезпеки. Наприклад, у медичній галузі важливим є здоров'я, у державному секторі – національна безпека. Вони тісно пов'язані з технічними цінностями, такими як ефективність, зручність використання, зрозумілість, доступність даних, надійність, сумісність і зв'язність. Хоча ці технічні параметри мають інструментальний характер, вони

часто є морально значущими, оскільки забезпечують досягнення базових цінностей у конкретних сферах діяльності.

Отже, аналіз кластерів цінностей у кібербезпеці дозволяє стверджувати, що правові та технічні механізми мають бути узгоджені з етичними орієнтирами. Це забезпечує не лише ефективний захист від кіберзагроз, а й збереження фундаментальних прав і свобод людини. [44, с.50].

Окремим напрямом сучасних досліджень є аналіз етичних аспектів, пов'язаних із розвитком новітніх технологій. Штучний інтелект (AI), Інтернет речей (IoT) та блокчейн (Blockchain) наразі розширюють можливості кібербезпеки, і, крім того, створюють нові виклики правового та етичного характеру. Їхнє використання потребує ретельного аналізу, бо баланс між безпекою, приватністю та прозорістю стає дедалі складнішим.

Злочинність – це людська проблема, і кіберзлочинність не є винятком. Технології, включаючи генеративний штучний інтелект, – це просто ще один інструмент в арсеналі зловмисника. Компанії навчають свої моделі штучного інтелекту на величезних обсягах даних, зібраних з Інтернету. Ці моделі часто навчаються не лише на творчих зусиллях мільйонів реальних людей, але й існує ймовірність того, що вони навмисно чи ненавмисно збирають особисту інформацію, яка опинилася у відкритому доступі. Як наслідок, деякі з найбільших розробників моделей штучного інтелекту зараз стикаються з позовами, тоді як галузь загалом стикається зі зростаючою увагою з боку регуляторів.

Хоча зловмисники мало дбають про етику штучного інтелекту, легітимним компаніям легко мимоволі зробити те саме. Наприклад, інструменти для веб-скрапінгу можуть використовуватися для збору навчальних даних для створення моделі виявлення фішингового контенту. Однак ці інструменти можуть не розрізняти особисту та анонімізовану інформацію, особливо у випадку графічного контенту. Набори даних з відкритим кодом, такі як LAION для зображень або The Pile для тексту, мають схожу проблему. Наприклад, у 2022 році каліфорнійська художниця виявила, що приватні медичні фотографії,

зроблені її лікарем, потрапили до набору даних LAION-5B, який використовувався для навчання популярного синтезатора зображень з відкритим кодом Stable Diffusion.

Не можна заперечувати, що недбала розробка вертикалізованих моделей штучного інтелекту (далі – ШІ) з урахуванням кібербезпеки може призвести до більшого ризику, ніж повна відсутність використання ШІ. Щоб запобігти цьому, розробники рішень безпеки повинні підтримувати найвищі стандарти якості даних та конфіденційності, особливо коли йдеться про анонімізацію або захист конфіденційної інформації. Такі закони, як Загальний регламент про захист даних (GDPR) Європи та Закон про конфіденційність споживачів Каліфорнії (CCPA), хоча й були розроблені до появи генеративного ШІ, служать цінними рекомендаціями для формування етичних стратегій ШІ [72].

Протягом останніх десятиліть було запропоновано низку етичних принципів, які постійно уточнюються та вдосконалюються, адже їхня роль полягає у формуванні довіри до систем штучного інтелекту та мінімізації ризиків, що виникають у процесі їхнього застосування.

Одним із ключових принципів є прозорість та пояснюваність. Системи штучного інтелекту повинні мати здатність пояснювати логіку своїх рішень, щоб користувачі могли зрозуміти процес їхнього формування та довіряти результатам. Не менш значущим є принцип справедливості та недискримінації, зокрема, алгоритми не повинні відтворювати або посилювати соціальні упередження, закладені у даних.

Захист конфіденційності даних становить ще один фундаментальний вимір етики ШІ. Системи мають обробляти інформацію безпечно та з повагою до приватності особи, дотримуючись міжнародних стандартів, зокрема положень Загального регламенту про захист даних (GDPR). Водночас важливим є питання підзвітності та відповідальності: необхідно чітко визначати, хто несе юридичні та моральні наслідки у випадку шкоди, спричиненої рішеннями системи. Це дозволяє уникати правової невизначеності та забезпечує прозорість у сфері регулювання.

Етичні принципи також включають вимогу користі та нешкідливості, що означає прагнення систем штучного інтелекту приносити благо людству, а не заподіяти шкоди. Важливим є й принцип співпраці та людського нагляду, котрий передбачає, що штучний інтелект має залишатися інструментом, який доповнює людські рішення, а не повністю їх замінює.

Не можна оминати й питання безпечного розвитку. Системи штучного інтелекту повинні бути захищені від атак та вразливостей, адже їхнє порушення може призвести до масштабних негативних наслідків. Нарешті, важливим етичним орієнтиром є справедливий розподіл переваг: користь від застосування штучного інтелекту має бути доступною широким верствам суспільства, а не концентруватися у руках небагатьох. Це передбачає рівний доступ до технологій та можливостей навчання, що сприяє зменшенню цифрової нерівності [18, с. 38-54].

Підсумовуючи вищевикладене, можемо констатувати, що етичні принципи штучного інтелекту формують основу для його відповідального розвитку. Вони забезпечують баланс між інноваційністю та гуманістичними цінностями, сприяють формуванню довіри до технологій і визначають рамки їхнього застосування у критично важливих сферах. Саме завдяки цим принципам ШІ може стати не лише потужним інструментом прогресу, але й чинником сталого та справедливого розвитку цифрового суспільства.

Інтернет речей (ІоТ), що стрімко розширюється та інтегрує дедалі більшу кількість пристроїв і систем, ставить перед суспільством складні питання конфіденційності та етики. Його трансформаційний потенціал полягає у створенні нових можливостей для медицини, транспорту, енергетики та побуту, проте водночас він породжує ризики, які потребують ретельного розгляду. Баланс між інноваціями та захистом даних стає ключовим викликом сучасної цифрової доби.

Одним із найважливіших аспектів є конфіденційність даних. Пристрої ІоТ збирають величезну кількість інформації, котра часто включає персональні та конфіденційні відомості. Тому необхідно забезпечувати їх захист від

несанкціонованого доступу чи використання, застосовуючи надійне шифрування, контроль доступу та методи анонімізації. Водночас варто згадати й принцип інформованої згоди. Цей принцип передбачає, що користувачі повинні мати чітке уявлення про те, які саме дані збираються, як вони будуть використані та кому можуть бути передані. Лише прозорі механізми надання згоди здатні гарантувати реальний контроль людини над власною інформацією.

Принцип мінімізації даних також має фундаментальне значення. Системи IoT повинні збирати лише ті дані, які є необхідними для досягнення конкретної мети, адже надмірний обсяг інформації збільшує ризики порушення приватності. Питання безпеки у нашому дослідженні є ключовим, тому цей принцип розглядаємо як найважливіший. Пристрої IoT стають потенційними цілями для кібератак, тож їхнє порушення може мати серйозні наслідки для користувачів та інфраструктури. Тому виробники та постачальники послуг повинні приділяти пріоритетну увагу захисту всієї екосистеми (від апаратного забезпечення до програмних оновлень).

Етичний вимір використання даних виходить за межі конфіденційності. Організації, що впроваджують IoT - системи, мають враховувати суспільні цінності та уникати ситуацій, які можуть призвести до дискримінації чи упередженості. Відтак, прозорість алгоритмів і процесів прийняття рішень стає необхідною умовою для формування довіри. З цього випливає й питання підзвітності, насамперед компанії повинні брати на себе відповідальність за дані, які вони збирають і обробляють, проводити регулярні аудити та оцінки впливу на конфіденційність, а також дотримуватися міжнародних стандартів захисту даних.

Аспект освіти та обізнаності ґрунтується на тому, що підвищення цифрової грамотності користувачів дозволяє їм приймати обґрунтовані рішення та захищати власні права. Це сприяє формуванню суспільства, яке усвідомлює цінність конфіденційності та етичного використання технологій. Вирішальну роль відіграють уряди та регуляторні органи, які мають розробляти комплексні

та перспективні правила, що враховують специфіку IoT, водночас підтримуючи інновації та захищаючи права людини [63].

Отже, кіберетика є фундаментальним елементом сучасної цифрової культури, адже вона визначає моральні принципи та практики, що забезпечують безпечне, відповідальне й законне використання технологій. Її значення полягає у формуванні довіри, захисті прав людини та запобіганні зловживанням у кіберпросторі. Кіберетика стосується моральних принципів та найкращих практик, які керують відповідальним, безпечним та законним використанням комп'ютерів, мереж та цифрових технологій [46].

Висновки до розділу 1

Аналіз теоретичних основ управління кіберризиками дозволяє зробити кілька узагальнень, котрі мають значення для академічного дискурсу і для практичного застосування. Кібербезпека представляє собою технічну категорію, своєрідне багатовимірне явище, що охоплює політичні, економічні, соціальні та правові аспекти. Вона є базовим елементом національної безпеки, адже кібератаки здатні паралізувати критичну інфраструктуру, дестабілізувати політичні процеси та підірвати економічну стабільність. У цьому контексті кіберзагроза визначається як потенційна небезпека, що може бути реалізована через вразливості інформаційних систем, а кіберризик – це її вимір у правовій, економічній та організаційній площині.

Важливою рисою сучасного розуміння кіберризиків є його комплексність: він формується на перетині технологічних вразливостей, соціальних факторів та недосконалості правових механізмів. Саме тому управління ризиками у сфері кібербезпеки потребує системного підходу, що включає моніторинг, оцінку ймовірності та масштабів наслідків, а також розроблення превентивних заходів. Класичні методи ризик - аналізу, які застосовуються у фінансовій чи промисловій сферах, набувають нового змісту у цифровому середовищі, де навіть незначна вразливість може призвести до масштабних збитків.

Значна увага приділяється міжнародній кібербезпеці. Оскільки кіберзагрози не мають кордонів, ефективна протидія можлива лише через співпрацю держав, обмін досвідом та участь у глобальних програмах. Будапештська конвенція про кіберзлочинність стала першим кроком у цьому напрямі, заклавши правові основи боротьби з кіберзлочинами на міжнародному рівні. Водночас Загальний регламент ЄС про захист даних (GDPR) визначив нові стандарти приватності, які стали глобальним еталоном. Разом ці документи

демонструють, що правове поле має постійно адаптуватися до технологічних змін, забезпечуючи баланс між безпекою та правами людини.

Ми розглядаємо етичний аспект кібербезпеки як вкрай важливий. Він охоплює цінності безпеки, конфіденційності, справедливості та підзвітності, які мають бути інтегровані у правові та технічні механізми. Новітні технології, як то штучний інтелект, Інтернет речей, блокчейн, створюють нові моральні суперечності, що потребують осмислення. Зокрема, прозорість алгоритмів, інформована згода користувачів, мінімізація збору даних та справедливий розподіл переваг стають ключовими орієнтирами для формування довіри до цифрових систем.

Отже, кібербезпека сьогодні є міждисциплінарною сферою, яка поєднує технології, право та етику. Її ефективність залежить від здатності суспільства інтегрувати ці виміри у єдину систему управління ризиками. Лише комплексний підхід, що враховує технічні, правові та моральні аспекти, здатний забезпечити стійкість інформаційних систем і захист прав людини у цифрову епоху.

РОЗДІЛ 2. ПОРІВНЯЛЬНИЙ АНАЛІЗ ПІДХОДІВ У РІЗНИХ КРАЇНАХ

2.1. Управління кіберризиками у США (NIST Cybersecurity Framework, CISA)

Управління кіберризиками, яке також називають управлінням ризиками кібербезпеки, – це процес виявлення, визначення пріоритетів, управління та моніторингу ризиків для інформаційних систем.

Управління кіберризиками стало важливою частиною зусиль з управління ризиками підприємства. Компанії в різних галузях промисловості сьогодні залежать від інформаційних технологій для виконання ключових бізнес-функцій, що наражає їх на ризик кіберзлочинців, помилок співробітників, стихійних лих та інших загроз кібербезпеці. Ці загрози можуть вивести з ладу критично важливі системи або завдати шкоди іншим чином, що призводить до втрати доходу, крадіжки даних, довгострокової шкоди репутації та штрафів з боку регуляторних органів.

Ці ризики неможливо усунути, але програми управління кіберризиками можуть допомогти зменшити вплив та ймовірність загроз. Компанії використовують процес управління ризиками кібербезпеки, щоб точно визначити свої найважливіші загрози та вибрати правильні заходи IT-безпеки для захисту інформаційних систем від кібератак та інших цифрових і фізичних загроз на основі своїх бізнес-пріоритетів, IT-інфраструктури та рівня ресурсів [72].

Управління кіберризиками у Сполучених Штатах Америки має системний та інституційно закріплений характер, що відображає стратегічну важливість цифрової безпеки для держави та бізнесу. Центральну роль у цьому процесі відіграє Національний інститут стандартів і технологій (NIST), який розробив Cybersecurity Framework – універсальний інструмент для оцінки, управління та мінімізації кіберризиків. Ця рамка стала базовим орієнтиром для організацій різних секторів, адже вона поєднує технічні, організаційні та правові аспекти

безпеки, пропонуючи стандартизований підхід до ідентифікації загроз, захисту систем, виявлення інцидентів та відновлення після атак.

Паралельно з діяльністю NIST важливу роль у сфері кібербезпеки виконує Агентство з кібербезпеки та безпеки інфраструктури (CISA), яке координує захист критичної інфраструктури, надає рекомендації приватному сектору та органам влади, а також здійснює моніторинг і реагування на масштабні інциденти. Взаємодія між NIST та CISA створює комплексну модель управління ризиками, де стандарти та методики поєднуються з практичними заходами і державною політикою. Такий підхід дозволяє США формувати внутрішню стійкість до кіберзагроз та задавати глобальні стандарти у сфері кібербезпеки. Тож розглянемо детально досвід США у сфері управління кіберризиками з метою виявлення можливостей подальшого застосування й впровадження у систему управління кіберризиками нашої країни.

У Стратегії національної безпеки США 2015 року (NSS 2015) президент Обама зазначає, що однією з восьми головних сфер, на які країна має виділити обмежені оборонні ресурси, є «забезпечення доступу до спільних просторів», включаючи кіберпростір. «Процвітання та безпека дедалі більше залежать від відкритого, сумісного та надійного Інтернету... наша економіка, безпека та здоров'я пов'язані через мережеву інфраструктуру, на яку спрямовані зловмисні урядові, кримінальні та окремі суб'єкти» (Національна стратегія безпеки Б.Обами, 2015). Однак з неї не зовсім незрозуміло, як досягти безпечного кіберпростору. Цілі, а також засоби контролю на найближче та довгострокове майбутнє не описані. Без чіткого обговорення цілей, шляхів та засобів постає питання чи є NSS 2015 стратегією. Крім того, у сфері кібербезпеки спостерігається конкуренція між різними урядовими департаментами та агентствами США, кожне з яких претендує на провідну роль у визначенні стратегії захисту кіберпростору. Поточна політика та виконавчі накази передбачають залучення Міністерства внутрішньої безпеки, Міністерства оборони, Міністерства юстиції, Міністерства торгівлі, Агентства національної

безпеки та Ради національної безпеки, які виконують ключові, а не допоміжні функції [68, с. 7].

Сьогодні Національна стратегія кібербезпеки США зосереджена на п'яти стовпах захисту критичної інфраструктури: виявлення, руйнування та ліквідація чинників, що здійснюють загрози; підвищення стійкості та безпеки ринку; інвестування в майбутню стійкість; та створення міжнародних партнерств зі спільними цілями. План реалізації Національної стратегії кібербезпеки зосереджений на критичній інфраструктурі, що підтримує енергетичний, фінансовий, охорону здоров'я, інформаційні технології та виробничий сектори.

Національна стратегія кібербезпеки США у відповідь на занепокоєння щодо критичної інфраструктури призвела до створення двох основних документів щодо кібербезпеки, які були розроблені спільно з кількома іншими союзниками. Агентство з кібербезпеки та безпеки інфраструктури (CISA) розробило документ «Зміна балансу ризиків кібербезпеки: принципи та підходи для безпечного програмного забезпечення за проектуванням» за спільною згодою з Агентством національної безпеки (АНБ), Федеральним бюро розслідувань (ФБР) та 15 міжнародними урядовими установами, щоб надати міжнародним постачальникам дорожню карту очікуваної кібергігієни, необхідної для їхніх продуктів [27]. Спираючись на документ «Зміна балансу ризиків кібербезпеки: принципи та підходи для безпечного програмного забезпечення за проектуванням», CISA, ФБР та АНБ зустрілися з організаціями з кібербезпеки з Австралії, Канади, Нової Зеландії та Великої Британії та спільно створили документ «Аргументи на користь безпечного для пам'яті програмного забезпечення: чому як керівникам вищої ланки, так і технічним експертам потрібно серйозно ставитися до безпечного для пам'яті кодування» як ключове питання, визначене в попередньому керівництві [25].

Ці дві організації, спільно очолювані США, допомогли запровадити міжнародну норму кібербезпеки, яка наполягає на тому, щоб міжнародні виробники програмного забезпечення демонстрували безпеку продукції та прозорість у продуктах, які вони продають. Ці спільні документи швидко

показали, як світова спільнота може об'єднатися для вирішення проблем кібербезпеки, які існують десятиліттями. Це призвело до того, що двадцять найбільших міжнародних постачальників програмного забезпечення створили робочу групу з мінімально життєздатного безпечного продукту (MSVP) для вирішення вимог, встановлених цими документами; CISA приєдналася до цієї робочої групи, щоб допомогти сформувати закупівлі, договірний контроль, самооцінювання та життєвий цикл розробки системи (SDLC) з цими постачальниками.

Рада національної безпеки США (NSC) повинна використовувати кадровий резерв CISA, Національного інституту стандартів і технологій (NIST), Міністерства оборони (DoD), ФБР та АНБ для покращення виявлення, обміну інформацією, стандартів безпеки та впровадження не лише для урядового та комерційного секторів США, але й для допомоги нашим союзникам та партнерам. Міністерство оборони та Офіс директора бюро національної розвідки (ODNI) досягли значних успіхів у покращенні безпеки, інтегруючи вдосконалення з архітектурою нульової довіри (ZTA), управлінням ризиками ланцюга поставок (SCRM), безпекою ланцюга поставок програмного забезпечення, Радою з огляду безпеки кібербезпеки (CSRB), посібниками з реагування на інциденти та вразливості в галузі кібербезпеки та стандартами національних систем безпеки (NSS) Міністерства оборони. NSC повинна координувати свої дії через CISA для розробки спільних зусиль, які не лише принесуть користь критичній інфраструктурі США, але й допоможуть союзникам та партнерам [21, с. 8].

NIST Cybersecurity Framework (CSF 2.0) є базовим інструментом управління кіберризиками, який був оновлений у 2024 році для врахування нових технологічних викликів та потреб бізнесу. Його головна мета полягає у створенні універсальної моделі, що дозволяє організаціям різних секторів (як державних установ, так і приватних компаній) системно ідентифікувати, оцінювати та мінімізувати ризики кібербезпеки. CSF 2.0 ґрунтується на п'яти ключових функціях: Управління (Govern), Визначення (Identify), Захист (Protect),

Виявлення (Detect), Реагування (Respond) та Відновлення (Recover), котрі утворюють цикл безперервного управління ризиками та забезпечують стійкість інформаційних систем [75, с. 73-76].

CSF 2.0 не лише задає концептуальні рамки управління кіберризиками, але й пропонує технологічні інструменти та методики, що дозволяють організаціям інтегрувати безпеку у всі бізнес-процеси. Він поєднує функції управління ризиками з практичними прикладами впровадження, забезпечуючи універсальність та адаптивність для різних секторів економіки. Функція Управління (Govern): визначає політику, стратегію та очікування у сфері кібербезпеки. Вона інтегрує кіберризики у ширшу систему Enterprise Risk Management (ERM), забезпечуючи узгодженість між технічними заходами та корпоративними цілями.

Організаційні профілі (Profiles): дозволяють порівнювати поточний стан безпеки з цільовим, визначати прогалини та формувати план дій. Це створює основу для безперервного вдосконалення системи кіберзахисту.

Рівні зрілості (Tiers): характеризують ступінь формалізації управління ризиками – від часткових (Tier 1) до адаптивних (Tier 4). Вони допомагають організаціям оцінити власну готовність та визначити напрям розвитку [59, с. 3-27].

Сучасна версія NIST Cybersecurity Framework (CSF 2.0) не обмежується лише концептуальними положеннями управління ризиками, а пропонує конкретні технологічні підходи та інструменти, що дозволяють організаціям ефективно інтегрувати кібербезпеку у всі бізнес-процеси. Вона враховує нові виклики цифрової епохи, як, наприклад, поширення хмарних сервісів і віддаленої роботи і зростання залежності від глобальних ланцюгів постачання програмного забезпечення та апаратних компонентів. Саме тому у CSF 2.0 особливу увагу приділено технологіям, які забезпечують стійкість систем, підвищують рівень довіри до цифрових продуктів та створюють умови для довгострокового розвитку кіберзахисту:

1)Архітектура нульової довіри (Zero Trust Architecture, ZTA). CSF 2.0 рекомендує застосування цього підходу, який передбачає постійну перевірку користувачів та пристроїв незалежно від їхнього розташування. Це особливо актуально для хмарних сервісів та віддаленої роботи [58].

2)Управління ризиками ланцюга постачання (Supply Chain Risk Management, SCRM). Управління ризиками ланцюга постачання стало ключовим елементом CSF 2.0. Організації мають враховувати загрози, пов'язані з використанням стороннього програмного забезпечення та апаратних компонентів, і застосовувати принципи Безпека за проєктом (Secure by Design) та Безпека за замовчуванням (Secure by Default) [27].

3)Автоматизовані платформи управління ризиками (Enterprise Risk Management Platforms, ERM): системи на кшталт RSA Archer, MetricStream чи Qualys TruRisk інтегрують кіберризики у корпоративні програми управління ризиками підприємства (Enterprise Risk Management, ERM). Вони застосовують штучний інтелект для аналізу великих масивів даних, прогнозування інцидентів та оптимізації процесів реагування [31].

Агентство з кібербезпеки та безпеки інфраструктури (Cybersecurity and Infrastructure Security Agency, CISA) є ключовим органом у США, який відповідає за захист критичної інфраструктури та координацію дій між державним і приватним секторами. Засноване у 2018 році при Міністерстві внутрішньої безпеки (DHS), CISA виконує роль «національного агентства кіберзахисту», співпрацюючи з урядом, промисловістю та громадськістю для захисту від кібератак та фізичних загроз. На відміну від NIST, що формує стандарти та методології, CISA реалізує практичні заходи, зокрема відповідає за моніторинг загроз, реагування на інциденти і розробку міжнародних рекомендацій для постачальників програмного забезпечення. Саме діяльність CISA забезпечує прикладний вимір кібербезпеки, який доповнює концептуальні рамки NIST.

CISA відіграє ключову роль у захисті технологій та систем, які забезпечують роботу таких важливих послуг, як енергетика, транспорт, охорона здоров'я, зв'язок та державні операції. Воно виступає водночас регуляторним та координаційним органом, головне завдання якого полягає у забезпеченні стійкості критичної інфраструктури США до динамічних та багатопланових загроз. Його діяльність охоплює кілька ключових напрямів: а) Кіберзахист (розробка та поширення рекомендацій, попереджень і спеціалізованих інструментів, що допомагають організаціям запобігати кіберінцидентам та ефективно реагувати на них); б) захист інфраструктури (мінімізація ризиків для фізичних і цифрових активів, які мають критичне значення для національної безпеки та економічної стабільності); в) реагування на надзвичайні ситуації (координація загальнонаціональних зусиль у відповідь на кібер- та фізичні загрози, котрі впливають на функціонування життєво важливих послуг; г) обмін інформацією (виконання функції координаційного центру для обміну розвідувальними даними про загрози між урядовими структурами та приватним сектором, що сприяє формуванню спільної картини ризиків) [26].

Окрім традиційних завдань із захисту критичної інфраструктури та реагування на кіберзагрози, Агентство з кібербезпеки та безпеки інфраструктури (CISA) дедалі більше зосереджується на викликах, пов'язаних зі штучним інтелектом. Його діяльність ґрунтується на законодавчо закріплених повноваженнях та значних бюджетних ресурсах, що дозволяє координувати національні та міжнародні зусилля у сфері цифрової безпеки. Саме ці аспекти створюють практичний вимір кіберзахисту, який доповнює концептуальні рамки NIST CSF 2.0.

У бюджетному запиті на 2025 рік фінансування агентства перевищило 3 млрд доларів США, що свідчить про стратегічну вагу його діяльності. Такий масштаб ресурсів дозволяє CISA реалізовувати комплексні програми захисту, інвестувати у нові технології та підтримувати довгострокові проєкти у сфері цифрової безпеки.

У 2023–2024 роках CISA представило Дорожню карту ШІ (AI Roadmap), яка визначає напрями відповідального використання штучного інтелекту у критичній інфраструктурі. Основні положення цієї стратегії включають:

- оцінку ризиків, пов'язаних із впровадженням ШІ у державному та приватному секторах;
- розробку найкращих практик для безпечних систем ШІ;
- створення колаборації з кібероборони (Joint Cyber Defense Collaborative, JCDC) для протидії загрозам, пов'язаним із ШІ;
- формування професійної компетентності співробітників у сфері ШІ та формування кадрового резерву для майбутніх викликів [32].

Отже, сучасна діяльність CISA виходить за межі класичного управління кіберризиками. Вона охоплює стратегічне фінансування, міжнародну співпрацю та формування політики у сфері штучного інтелекту. Це дозволяє агентству виступати не лише як координатор кіберзахисту, але й як глобальний лідер у формуванні стандартів безпеки цифрових технологій.

Попри розробку концептуальних рамок та стратегій управління кіберризиками, реальна ефективність системи кіберзахисту визначається здатністю держави та організацій реагувати на конкретні інциденти. Саме масштабні атаки останніх років стали каталізаторами для вдосконалення політик та інструментів кібербезпеки у США. Серед них особливе значення мають атака на SolarWinds (2020) та Colonial Pipeline (2021), які продемонстрували вразливість критичної інфраструктури та необхідність комплексної взаємодії між CISA, NIST та іншими урядовими структурами.

Наприклад, у грудні 2020 року було виявлено масштабну атаку на ланцюг постачання програмного забезпечення SolarWinds Orion, яку здійснили актори, пов'язані з російською службою зовнішньої розвідки. Зловмисники інтегрували шкідливий код у легітимні оновлення, що дозволило їм отримати доступ до мереж урядових установ США та приватних компаній. Реакція була негайною: CISA видало Emergency Directive 21-01, яка зобов'язала федеральні агентства

відключити уражені системи, а також створило Об'єднану координаційну групу з кібербезпеки (Cyber Unified Coordination Group) для координації дій разом із Федеральним бюро розслідувань, Офісом директора національної розвідки та Агентством національної безпеки. Паралельно NIST оновило рекомендації щодо управління ризиками ланцюга постачання, інтегрувавши уроки SolarWinds у нову редакцію CSF 2.0, а CISA опублікувало технічні інструкції з виявлення та усунення компрометації, включно з методами обходу багатофакторної автентифікації [39].

Не менш показовим став інцидент із Colonial Pipeline у травні 2021 року, коли група DarkSide здійснила атаку програмою - вимагачем на найбільший паливний трубопровід США. Компанія була змушена тимчасово зупинити роботу, що призвело до перебоїв у постачанні пального на Східному узбережжі та панічних закупівель. У відповідь CISA разом із ФБР створили Спільну робочу групу з протидії програмам-вимагачам (Joint Ransomware Task Force), запустили портал «stopransomware.gov» як єдине джерело актуальних рекомендацій, а також заснували Об'єднану платформу співпраці у сфері кібероборони (Joint Cyber Defense Collaborative, JCDC) для обміну інформацією в реальному часі. NIST, зі свого боку, розробив додаткові методичні матеріали щодо управління ризиками ransomware та інтегрував їх у CSF 2.0, тоді як TSA видала нові директиви для операторів трубопроводів, CISA, у свою чергу, організувало співпрацю понад двох десятків компаній для посилення захисту промислових систем [28].

Згадані приклади показали, що кіберзагрози можуть мати системний і довготривалий вплив на державу та суспільство. Вони стали «моментами прозріння», коли кіберризики перестали бути абстрактною проблемою і перетворилися на фактор, що безпосередньо впливає на економіку, політику та повсякденне життя. Взаємодія між CISA та NIST у цих випадках продемонструвала дві взаємодоповнюючі моделі, зокрема оперативне реагування та практичні заходи з боку CISA і стандартизацію та методологічну

підтримку з боку NIST. Саме поєднання цих підходів забезпечує комплексність американської системи кіберзахисту та її здатність формувати глобальні стандарти у сфері цифрової безпеки.

США сьогодні фактично задають глобальні стандарти у сфері кібербезпеки: ініціативи NIST та CISA стали орієнтирами для міжнародних партнерів, а документи на кшталт «Зміна балансу кіберризиків: принципи та підходи до безпечного програмного забезпечення за проєктуванням» (Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software) та «Аргументи на користь безпечного для пам'яті програмного забезпечення» (The Case for Memory Safe Software) визначають правила для світових постачальників технологій.

Міжнародний вплив США у сфері кібербезпеки проявляється у тому, що розроблені ними стандарти та рекомендації поступово перетворюються на універсальні норми для світового ринку цифрової безпеки. Національний інститут стандартів і технологій (NIST) зі своїм Cybersecurity Framework та Secure Software Development Framework (SSDF), а також Агентство з кібербезпеки та безпеки інфраструктури (CISA) з його ініціативами Secure by Design і Secure by Default стали базовими орієнтирами для урядів і компаній у різних країнах.

Особливо показовою є співпраця США з державами альянсу «п'ять очей» (Five Eyes) – Австралією, Канадою, Великою Британією та Новою Зеландією. Саме ці країни разом із CISA, FBI та NSA у 2023 році опублікували спільний документ «Зміна балансу кіберризиків: принципи та підходи до безпечного програмного забезпечення за проєктуванням» (Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software), який закликав виробників програмного забезпечення інтегрувати безпеку на етапі проєктування та розробки продуктів. У жовтні 2023 року цей документ був оновлений і підписаний уже 17 міжнародними партнерами, включно з Німеччиною, Нідерландами, Ізраїлем, Сінгапуром, Японією та іншими країнами, що свідчить про його глобальне значення [24; 25; 27].

Ще одним прикладом є ініціатива Memory Safe Software, яка отримала підтримку від CISA та агентств «Five Eyes». У цьому документі наголошується на необхідності переходу від небезпечних мов програмування, таких як C та C++, до сучасних мов із вбудованими механізмами безпеки, як то Rust, C#, Go, Java. Цей заклик має стратегічний характер, адже проблеми з пам'яттю становлять до 70% усіх вразливостей у програмному забезпеченні, і саме США разом із союзниками визначають напрямок розвитку індустрії, стимулюючи глобальних виробників до створення «дорожніх карт» переходу на безпечні мови програмування [54].

Отже, стандарти та рекомендації, що походять із США, поступово формують міжнародну нормативну базу кібербезпеки. Вони не лише визначають технічні вимоги, а й задають політичні та економічні орієнтири для світового ринку. Це дозволяє говорити про США як про державу, що фактично встановлює «правила гри» у глобальному цифровому просторі, поєднуючи власні національні інтереси з формуванням міжнародних норм і практик.

2.2. Досвід Європейського Союзу: ENISA, GDPR та директива NIS2

Європейський Союз поступово формує комплексну архітектуру управління кіберризиками, яка поєднує нормативні акти, технічні стандарти та інституційну підтримку. Центральну роль у цьому процесі відіграє Європейське агентство з кібербезпеки (ENISA), що забезпечує методичні рекомендації, технічні положення та координацію між державами - членами. Водночас Загальний регламент про захист даних (GDPR) задає правові рамки для обробки персональних даних, а директива NIS2 встановлює обов'язкові вимоги до управління ризиками для критичних секторів і цифрових послуг. У сукупності ці інструменти створюють багаторівневу систему, яка прагне підвищити стійкість європейського цифрового простору та сформувати довіру громадян і бізнесу.

Важливо, що ЄС не обмежується деклараціями. ENISA у 2025 році опублікувало технічні рекомендації щодо імплементації NIS2, які охоплюють 13 ключових доменів, які включають аспекти політики безпеки та управління ризиками, а також криптографію (перетворення зрозумілого тексту (plaintext) у незрозумілий (ciphertext) за допомогою алгоритмів і ключів, щоб сторонні не могли його прочитати.), безпеки ланцюгів постачання та контролю доступу. Варто відмітити, що GDPR став глобальним еталоном у сфері захисту даних, вплинувши на законодавство за межами ЄС. Відтак, європейський досвід демонструє прагнення до гармонізації правових і технічних підходів, що дозволяє не лише зменшувати кіберризики, а й формувати міжнародні стандарти цифрової безпеки.

Акт про кіберсолідарність – це крок вперед після Спільного повідомлення про кіберзахист (JOIN(2022) 49) для Ініціативи ЄС про кіберсолідарність з такими цілями: посилити спільні можливості ЄС щодо виявлення, ситуаційної обізнаності та реагування, поступово створити резерв кібербезпеки на рівні ЄС з послугами від надійних приватних постачальників та підтримати тестування критично важливих об'єктів.

За даними Європейської комісії, «кібероперації все більше інтегруються в гібридні та військові стратегії, що має значний вплив на ціль. Зокрема, військовій агресії Росії проти України передувала та супроводжується стратегією ворожих кібероперацій, що є переломним моментом у сприйнятті та оцінці колективної готовності ЄС до кризового управління в галузі кібербезпеки та заклик до термінових дій».

«Загроза можливого масштабного інциденту, який спричинить значні порушення та пошкодження критичної інфраструктури, вимагає підвищеної готовності на всіх рівнях екосистеми кібербезпеки ЄС. Ця загроза виходить за рамки військової агресії Росії проти України та включає постійні кіберзагрози з боку державних та недержавних суб'єктів, які, ймовірно, триватимуть, враховуючи численність державно-правових, кримінальних та хактивістських суб'єктів, залучених до поточної геополітичної напруженості».

Цілі Закону ЄС про кіберсолідарність реалізуються за допомогою наступних дій:

1. Розгортання загальноєвропейської інфраструктури Центрів операцій безпеки (Європейський кіберщит) для створення та вдосконалення спільних можливостей виявлення та ситуаційної обізнаності.

2. Створення Механізму кібернадзвичайних ситуацій для підтримки держав-членів у підготовці, реагуванні та негайному відновленні після значних та масштабних інцидентів у сфері кібербезпеки. Підтримка реагування на інциденти також буде надана європейським установам, органам, службам та агентствам Союзу (EUIBA).

3. Створення Європейського механізму розгляду інцидентів у сфері кібербезпеки для розгляду та оцінки конкретних значних або масштабних інцидентів [36].

Хоча ЄС постійно зміцнює свою позицію в галузі кібербезпеки за допомогою таких нормативних актів, як NIS 2, DORA та Закон про кіберстійкість, Закон про кіберсолідарність служить іншій меті: колективній готовності, швидкому реагуванню та загальноєвропейським можливостям кіберзахисту. Це новий вимір колективної кіберстійкості.

Незважаючи на чинні нормативні акти щодо кібербезпеки, ЄС виявив прогалину в реагуванні на інциденти в режимі реального часу, транскордонній солідарності та скоординованій кіберзахисті. Закон про кіберсолідарність заповнює цю прогалину. Цей Закон відображає нову еру колективної оборони в кіберпросторі, гарантуючи, що кібератаки є не лише національною проблемою, а й відповідальністю всього ЄС.

Директива NIS 2 (Директива ЄС 2022/2555) є базовою рамкою ЄС для управління ризиками кібербезпеки та звітності про інциденти для важливих та необхідних організацій. Вона розширює сферу застосування оригінальної Директиви NIS, роблячи зобов'язання щодо кібербезпеки обов'язковими для ширшого кола секторів.

Ключова відмінність полягає в тому, що хоча NIS 2 накладає зобов'язання щодо кібербезпеки на важливі організації, Акт про кіберсолідарність встановлює загальноєвропейські механізми реагування та готовності до кібернадзвичайних ситуацій. На відміну від NIS 2, який вимагає від організацій впроваджувати управління ризиками кібербезпеки та повідомляти про інциденти, Закон про кіберсолідарність зосереджується на оперативному реагуванні на рівні ЄС через такі ініціативи, як Механізм надзвичайних ситуацій у сфері кібербезпеки та Резерв ЄС з кібербезпеки.

Акт про кіберсолідарність створює Європейську систему оповіщення про кібербезпеку для моніторингу в режимі реального часу та обміну розвідувальною інформацією, що не вимагається NIS 2. Хоча NIS 2 сприяє співпраці, він зосереджується на дотриманні вимог всередині організацій, тоді як Закон про кіберсолідарність посилює транскордонну солідарність, гарантуючи, що країни ЄС можуть допомагати одна одній у разі масштабних кіберзагроз [37].

Акт про цифрову операційну стійкість (DORA, Регламент ЄС 2022/2554) спеціально розроблений для фінансового сектору, спрямований на покращення управління ризиками в галузі ІКТ для банків, страхових компаній та інвестиційних фірм. Він встановлює суворі вимоги до кібербезпеки та стійкості для фінансових установ, а також зобов'язання щодо звітності та тестування для сторонніх постачальників послуг ІКТ.

На відміну від DORA, який застосовується лише до фінансових установ, Акт про кіберсолідарність поширюється на всі сектори, забезпечуючи структуровану систему реагування на надзвичайні ситуації в масштабах ЄС. У той час як DORA зобов'язує окремі фірми захищати свою діяльність та повідомляти про надзвичайні ситуації, Акт про кіберсолідарність створює колективну структуру управління кризами, яка мобілізує ресурси по всьому ЄС у разі масштабної атаки [36].

Ще одна ключова відмінність полягає в обміні інформацією про загрози. DORA запроваджує специфічні для сектору заходи розподілу ризиків для фінансових установ.

Акт про кіберстійкість (Cyber Resilience Act, Regulation EU 2024/2847) має на меті забезпечити, щоб цифрові продукти, включно з апаратним та програмним забезпеченням, відповідали мінімальним вимогам кібербезпеки. Він зосереджується на безпеці продуктів, а не на оперативному реагуванні.

Фундаментальна відмінність полягає в тому, що Акт про кіберстійкість є превентивним, встановлюючи зобов'язання щодо «безпеки за проєктуванням» для виробників цифрових продуктів, тоді як Акт про кіберсолідарність спрямований на протидію масштабним кібератакам та реагування на надзвичайні ситуації. Акт про кіберстійкість забезпечує більшу захищеність підключених пристроїв, програмного забезпечення та продуктів Інтернету речей (IoT), а Акт про кіберсолідарність, в свою чергу, створює механізми для пом'якшення наслідків та реагування на великі кіберкризи. Отже, Акт про кіберсолідарність стосується кризового реагування та оперативної співпраці [42].

У ЄС принцип «*lex specialis derogat legi generali*» (лат.) означає, що коли на одну й ту саму ситуацію поширюються дві правові норми, застосовується та, яка є більш конкретною. Тобто спеціальний закон має перевагу над загальним, оскільки він встановлює точніші правила для окремих випадків і звужує дію ширшого регулювання.

Застосовуючи цей принцип до Акта про кіберсолідарність, слід оцінити, чи вводить він більш конкретні норми, які мають перевагу над чинними законами у сфері кібербезпеки [41].

Акт про кіберсолідарність має перевагу над Директивою NIS2, оскільки вводить специфічні механізми екстреного реагування, яких бракує NIS2. Якщо NIS2 вимагає від організацій самостійно управляти кіберризиками та звітувати про виявлені загрози, то Акт про кіберсолідарність створює операційні механізми на рівні ЄС, включно з Механізмом кібернадзвичайних ситуацій

(Cybersecurity Emergency Mechanism), Резервом кібербезпеки ЄС (EU Cybersecurity Reserve) та Європейською системою кіберсповіщення (European Cybersecurity Alert System).

Оскільки ці положення виходять за межі підходу NIS2 до управління ризиками та дотримання вимог, Акт про кіберсолідарність має пріоритет у питаннях реагування на масштабні кіберінциденти, виступаючи спеціальним правовим інструментом для управління кібербезпекою в умовах надзвичайних ситуацій.

Акт про кіберсолідарність не має переваги над Актом про цифрову операційну стійкість (Digital Operational Resilience Act, DORA), оскільки DORA залишається галузевим актом, спрямованим на фінансовий сектор, тоді як Акт про кіберсолідарність поширюється на всі індустрії та урядові структури. DORA встановлює індивідуальні заходи управління ризиками та стійкості для фінансових установ, тоді як Акт про кіберсолідарність забезпечує колективну рамку реагування ЄС. Таким чином, DORA залишається спеціальним законом для фінансового сектору, а Акт про кіберсолідарність є радше доповненням, ніж заміщенням.

Акт про кіберсолідарність також не має переваги над Актом про кіберстійкість (Cyber Resilience Act), оскільки ці регламенти охоплюють різні сфери: Акт про кіберстійкість регулює безпеку продуктів та цілісність програмного забезпечення, тоді як Акт про кіберсолідарність зосереджується на оперативній кібербезпеці, кризовому реагуванні та колективних механізмах захисту ЄС.

Оскільки між цими законами немає прямого конфлікту, Акт про кіберстійкість залишається спеціальним законом для безпеки цифрових продуктів, а Акт про кіберсолідарність – спеціальним законом для реагування на кіберкризи [43].

Акт про кіберсолідарність формує правові механізми реагування на масштабні кіберзагрози, формуючи технічну інфраструктуру, яка має забезпечити оперативну стійкість Європейського Союзу. Центральним

елементом є створення Європейського кіберщита (European Cyber Shield) – мережі Центрів операцій безпеки (Security Operations Centres, SOC's), що інтегрують дані з національних систем моніторингу. Ці центри застосовують алгоритми машинного навчання для аналізу журналів подій та мережевого трафіку, зокрема методи виявлення аномалій (Isolation Forest, кластеризація K-Means) та глибинні нейронні мережі (LSTM) для прогнозування послідовностей атак. Такий підхід дозволяє виявляти нетипові патерни у реальному часі та забезпечує раннє попередження про загрози, що виходять за межі окремих держав.

Європейський кіберщит є ключовим елементом Акта про кіберсолідарність, спрямованим на створення інтегрованої інфраструктури для моніторингу, виявлення та реагування на кіберзагрози. Він функціонує як мережа Центрів операцій безпеки, що об'єднують національні та регіональні ресурси в єдину систему. Технічна модель кіберщита базується на трьох рівнях: збір даних, аналітика та реагування [20].

На першому рівні SOC's здійснюють збір телеметрії з різних джерел: журнали подій операційних систем, мережевий трафік, дані з сенсорів критичної інфраструктури, а також інформацію з honeypots, які симулюють вразливі вузли для відстеження тактик зловмисників. Цей масив даних надходить у централізовані сховища, де застосовуються алгоритми попередньої обробки (нормалізація, видалення шуму та кореляція подій).

Другий рівень – аналітичний, де використовуються алгоритми машинного навчання та штучного інтелекту. Для виявлення аномалій застосовуються методи кластеризації (K-Means, DBSCAN) та моделі ізоляційних лісів (Isolation Forest), які дозволяють ідентифікувати нетипові патерни у трафіку. Для прогнозування послідовностей атак використовуються рекурентні нейронні мережі (LSTM), здатні аналізувати часові ряди подій. Крім того, інтегруються системи на основі глибинного навчання для виявлення складних атак типу Advanced Persistent Threats (APT), які маскуються під легітимну активність.

Третій рівень – реагування, де SOCs застосовують автоматизовані механізми блокування та ізоляції. Використовуються платформи SOAR (Security Orchestration, Automation and Response), що дозволяють створювати сценарії реагування (playbooks). Наприклад, при виявленні DDoS-атаки система може автоматично активувати алгоритми rate - limiting та traffic scrubbing, перенаправляючи трафік через спеціалізовані фільтрувальні вузли. У випадку зараження вузла SOC може ізолювати його від мережі та запустити процедури відновлення на основі резервних копій.

Особливістю Європейського кіберщита є його пан'європейська інтеграція: SOCs у різних країнах обмінюються даними через захищені канали, формуючи єдину картину загроз. Це дозволяє виявляти атаки, які мають транскордонний характер, та координувати реагування на рівні ЄС. Технічна архітектура передбачає використання кореляційних рушіїв (Correlation Engines), які поєднують інформацію з різних джерел у єдину базу знань, доступну для ENISA та CERT-EU.

Отже, Європейський кіберщит є політичним проєктом, проте представляє собою високотехнологічну систему, яка поєднує алгоритмічні методи аналізу даних, автоматизацію реагування та колективну інфраструктуру захисту. Його функціонування забезпечує перехід від фрагментарного управління кіберризиками до централізованої моделі, здатної протидіяти масштабним загрозам у реальному часі [61, с. 1-12].

Механізм кібернадзвичайних ситуацій (Cybersecurity Emergency Mechanism) базується на платформах оркестрації та автоматизації реагування (SOAR). Ці системи дозволяють створювати сценарії реагування (playbooks), що автоматично блокують шкідливі IP - адреси, ізолюють уражені вузли чи запускають процедури відновлення. Використання алгоритмів кореляції подій та інтеграція моделей штучного інтелекту, включно з великими мовними

моделями (LLMs), забезпечує адаптивність реагування та скорочує час між виявленням і нейтралізацією атаки з годин до хвилин.

Механізм кібернадзвичайних ситуацій (Cybersecurity Emergency Mechanism) є ключовим інструментом Акта про кіберсолідарність, який забезпечує оперативне реагування Європейського Союзу на масштабні кібератаки. Його завдання полягає у швидкій мобілізації ресурсів, координації між державами - членами та застосуванні автоматизованих технологій для нейтралізації загроз.

Технічна архітектура цього механізму базується на використанні платформ оркестрації та автоматизації реагування (SOAR – Security Orchestration, Automation and Response). Ці системи інтегрують дані з різних джерел (SOCs, CERT - EU, національних центрів кібербезпеки) і формують цілісне уявлення про небезпечну ситуацію. На основі цієї інформації запускаються сценарії реагування, які автоматично виконують низку дій, як то блокування IP-адреси, ізоляцію заражених вузлів, активацію резервних систем чи перенаправлення трафіку через фільтрувальні вузли.

Алгоритмічна складова включає кілька рівнів. Тут застосовуються кореляційні рушії (Correlation Engines), які зіставляють події з різних джерел, виявляючи взаємозв'язки між атаками. Крім того, використовуються методи машинного навчання для класифікації загроз, зокрема алгоритми Random Forest та Support Vector Machines, котрі дозволяють визначати тип атаки (DDoS, ransomware, phishing) на основі ознак трафіку та поведінки системи, а також для аналізу великого обсягу журналів подій та прогнозування розвитку атаки інтегруються моделі глибокого навчання (CNN, LSTM) [47, с. 365].

Особливу роль відіграє використання LLMs (Large Language Models), які застосовуються для генерації адаптивних сценаріїв реагування. Наприклад, модель може автоматично створити інструкцію для ізоляції сегмента мережі або

запропонувати оптимальний порядок дій для відновлення системи після атаки. Це забезпечує гнучкість реагування та врахування контексту конкретної кризи.

Практичне значення механізму кібернадзвичайних ситуацій полягає у скороченні часу реагування. Якщо традиційні процеси раніше вимагали координації між різними органами вручну, то SOAR-платформи дозволяють виконувати ключові дії автоматично. Наприклад, при виявленні масованої DDoS-атаки система може негайно активувати алгоритми rate-limiting та traffic scrubbing, а у випадку зараження шкідливим ПЗ просто ізолювати вузол та запустити процедуру відновлення з резервних копій.

Отже, Механізм кібернадзвичайних ситуацій включає правові рамки і високотехнологічні інструменти, що створює платформу колективного реагування країн ЄС на масштабні кіберзагрози. Він демонструє перехід від реактивної моделі до проактивної та автоматизованої системи захисту, де алгоритми та штучний інтелект відіграють ключову роль у забезпеченні кіберстійкості європейського простору [41].

Реагування Європейського Союзу на кіберзагрози має комплексний характер і поєднує технічні, політичні та організаційні інструменти. Одним із показових прикладів є атака на систему SolarWinds, яка зачепила й європейські інституції. У відповідь ЄС активував механізми кібердипломатії, зокрема так званий Cyber Diplomacy Toolbox, що дозволив координувати політичну реакцію та забезпечити обмін індикаторами компрометації між CERT - EU та національними центрами реагування. Цей випадок став каталізатором для розробки сценаріїв кризового управління в рамках мережі EU-CyCLONe, яка нині регулярно проводить симуляції масштабних атак на критичну інфраструктуру [31].

Як приклад, висвітлимо також випадок із масованою DDoS-атакою на вебсайт Європейського парламенту у 2022 році. Тоді технічне реагування

здійснювалося через застосування алгоритмів rate-limiting та traffic scrubbing, що дозволило швидко відновити доступність ресурсу. Цей інцидент продемонстрував потребу у створенні Європейської системи кіберсповіщення, яка нині інтегрує honeypots та системи виявлення вторгнень для раннього попередження про загрози.

Практичне використання платформ SOAR є важливим елементом, що забезпечує автоматизацію реагування на ризики і загрози. У рамках навчань EU - CyCLONe відпрацьовуються сценарії, де системи автоматично блокують шкідливі IP - адреси, ізолюють заражені вузли та запускають процедури відновлення. Інтеграція моделей штучного інтелекту, включно з великими мовними моделями, дозволяє створювати адаптивні інструкції для кризових ситуацій, що значно скорочує час між виявленням і нейтралізацією атаки.

Підсумовуючи зазначимо, що реагування ЄС на кіберзагрози демонструє перехід від фрагментарних дій до колективної та проактивної моделі кіберстійкості. Синтез правових рамок, дипломатичних інструментів і високотехнологічних платформ створює основу для захисту європейського цифрового простору від масштабних атак, які дедалі частіше мають транскордонний характер [66].

2.3. Державне регулювання та корпоративні практики у Китаї та країнах Азії

З кінця 1990-х років Китай проводить політику «інформатизації, яка передбачає впровадження цифрових технологій у всі важливі сфери економічного та соціального життя, а також в державну діяльність. У 2014 році створення Центральної керівної групи з кібербезпеки та інформатизації під головуванням президента Сі Цзіньпіна вивело цифрову політику на найвищий рівень пріоритетності та сприяло «стратегії кібердержави». Визначені плани швидко набули популярності: у 2020 році керівництво визначило дані як новий

фактор виробництва, нарівні із землею, капіталом та працею. Чотирнадцятий п'ятирічний план містив кілька пунктів щодо інформатизації загалом, цифрового управління і цифрової економіки.

Інформатизація відображає технократичну, сцієнтистську ідеологію, яку Комуністична партія Китаю (КПК) дотримується десятиліттями. Цей погляд принципово передбачає, що соціальна реальність є складною, але зрозумілою системою, що ґрунтується на об'єктивних законах, подібних до законів фізики. Інформаційно-комунікаційні технології (ІКТ) обіцяють забезпечити можливості збору даних та обчислювальну потужність, необхідні для реалізації цього бачення та забезпечення ефективного та результативного управління. Таким чином, технологічний порядок денний є вирішальним елементом спроб КПК адаптуватися до викликів «нової ери», проголошеної головою Сі [30, с. 111-112].

Але інформатизація – це лише половина цифрової трансформації, адже щоб ці нові можливості реалізували свій потенціал, вони мають бути безпечними. За словами Сі, кібербезпека та інформатизація – це «два крила на одному тілі та два колеса одного транспортного засобу». Він заявив, що кібербезпека невіддільна від національної безпеки, питання, яке швидко набуло пріоритетності, про що свідчить запровадження Закону про національну безпеку та створення Ради національної безпеки [52, с. 762-763].

До 2016 року Пекін опублікував Національну стратегію кібербезпеки, Стратегію міжнародного кіберспівробітництва та Закон про кібербезпеку, щоб сформувати ядро комплексного управління кібербезпекою, формування якого досі триває. Цей режим складається з низки адміністративних та відомчих нормативних актів, виданих Державною радою, Адміністрацією кіберпростору Китаю (САС) та пов'язаними з ним міністерствами, а також технічних стандартів та саморегулювальних конвенцій галузевих асоціацій та торгових організацій. Для їх ефективного впровадження, окрім розширення існуючих агентств та технічних органів з кібербезпеки, були здійснені інвестиції у вищу освіту та дослідницькі установи, а також проводяться пропагандистські заходи,

такі як щорічний Тиждень кібербезпеки, для підвищення обізнаності серед населення в цілому [56, с. 183-126].

Перший проект Закону про кібербезпеку було опубліковано в липні 2015 року. Він був розроблений у тісній співпраці між САС, МПТ та MPS, а також у співпраці із зацікавленими компаніями, включаючи банки, операторів критичної інфраструктури, інтернет-провайдерів, фірмами з кібербезпеки та виробниками обладнання. Проект поклав на САС відповідальність за загальне планування та координацію кібербезпеки за допомогою МПТ, MPS та інших відповідних відомств. Замість того, щоб включити конкретні суттєві положення, він створював мандати для адміністративних органів або включав уже існуючі регуляторні процеси, такі як MLP. Відображаючи постійну увагу до питань, пов'язаних з інформацією, як найважливішої частини кібербезпеки, він включав суворі обмеження на виробництво онлайн-контенту як єдине суттєве положення в першому розділі закону.

Розділ 2 стосується можливостей кібербезпеки. Він зобов'язав усі галузеві міністерства складати конкретні плани кібербезпеки для своїх секторів та створювати стандарти кібербезпеки, залучаючи широке коло цифрових підприємств. Міністерства та місцеві органи влади також були зобов'язані розробляти плани розвитку, розширювати інвестиції та субсидії в промисловість, дослідження та розробки, а також застосування та індустріалізацію, проводити пропаганду та освіту з кібербезпеки серед широкої громадськості та покращувати викладання кібербезпеки в освітніх програмах ЗВО.

Розділ 3 зосереджений на безпечних мережевих операціях. Перший, загальний розділ, включав багатосторонні проекти (MLP) до режиму csl, зобов'язував отримувати згоду на використання персональних даних та пов'язані з цим зобов'язання щодо повідомлення про порушення, запровадив вимоги до перевірки та сертифікації кібербезпеки, зобов'язав реєстрацію реальної особи для надання певних послуг доступу до мережі та телекомунікацій, зобов'язав онлайн-операторів створювати плани дій у

надзвичайних ситуаціях на випадок інцидентів безпеки, а також забороняв хакерство та розкриття інструментів або засобів хакерства [30, с. 117-118].

Закцентуємо увагу на критичній інформаційній інфраструктурі. Закон охоплює базові інформаційні мережі, що надають такі послуги, як публічне листування та радіо- та телевізійне мовлення; важливі інформаційні системи для важливих галузей промисловості, таких як енергетика, транспорт, водозбереження та фінанси, а також сфери державних послуг, зокрема електроенергетику, водопостачання та газопостачання, медичне та санітарне обслуговування, а також соціальне забезпечення; військові мережі та мережі урядових справ для державних органів на рівні міст-підрайонів; а також мережі та системи, що належать або управляються постачальниками мережевих послуг з величезною кількістю користувачів.

Оператори ініціативної інтеграції (КІІ) повинні були створити спеціальні відділи управління безпекою, регулярно навчати та оцінювати персонал з кібербезпеки, створювати резервні копії для важливих систем у разі стихійних лих та розробляти плани реагування на надзвичайні ситуації. Крім того, оператори КІІ повинні були зберігати особисту інформацію та інші важливі дані, зібрані та отримані під час операцій у Китаї. Нарешті, вони повинні були проводити щорічний аудит безпеки своїх мереж та подавати відповідну звітність регуляторним органам [33].

Китай має найбільшу кількість користувачів у мережі Інтернет та найбільшу мережу у світі. Підтримка кібербезпеки Китаю є не лише потребою самої країни, але й має велике значення для підтримки глобальної кібербезпеки і навіть миру. Китай прагне захищати національний суверенітет, безпеку та інтереси розвитку кіберпростору, сприяти розвитку Інтернету на благо людства, а також сприяти мирному використанню та спільному управлінню кіберпростором.

Захист національної безпеки – пріоритетний напрямок розвитку державної кібербезпеки і протидії кіберзагрозам. Запобігати, припиняти та карати відповідно до закону будь-які дії використання Інтернету для вчинення

державної зради, сецесії, заколоту, підривної діяльності або підбурювання до підриву режиму народно-демократичної диктатури; запобігати, припиняти та карати відповідно до закону будь-які дії з використання Інтернету для крадіжки, розголошення державної таємниці та інших дій, що загрожують національній безпеці; запобігати, припиняти та карати відповідно до закону будь-які іноземні сили, що використовують Інтернет для здійснення інфільтрації, саботажу, підривної діяльності та сепаратизму.

Захист критичної інформаційної інфраструктури є спільною відповідальністю уряду, підприємств та всього суспільства. Компетентні, операційні підрозділи та організації повинні вживати необхідних заходів для забезпечення безпеки критичної інформаційної інфраструктури відповідно до вимог законів, нормативних актів та інституційних стандартів, а також поступово впроваджувати оцінку ризиків перед використанням, зокрема, вимагається посилення оцінки ризиків критичної інформаційної інфраструктури; посилення захисту безпеки веб-сайтів партійних та урядових установ та ключових сфер, низових партійних та урядових установ. Створюється впорядкований механізм обміну інформацією про мережеву безпеку між урядом, промисловістю та підприємствами, а також відповідальність підприємств у галузі захисту критичної інформаційної інфраструктури [23].

Національний центр реагування на загрози в Китаї (CNCERT/CC) являє собою основу державної системи кібербезпеки, створену у 2002 році під егідою Міністерства промисловості та інформаційних технологій. Його основне завдання полягає у моніторингу та аналізі кіберзагроз, координації реагування на небезпечні ситуації та забезпеченні інформаційного обміну між державними органами, операторами критичної інформаційної інфраструктури та приватними компаніями. CNCERT/CC виконує функції національного центру раннього попередження, формує щорічні звіти про стан кібербезпеки та розробляє рекомендації для підвищення стійкості цифрових систем.

З технічного боку CNCERT/CC застосовує комплексні методи виявлення та нейтралізації атак. Центр використовує системи глибокого аналізу трафіку, кореляційні рушії для зіставлення подій з різних джерел, а також алгоритми машинного навчання для класифікації загроз. У випадку масованих DDoS-атак або зараження шкідливим програмним забезпеченням CNCERT/CC координує застосування технологій rate-limiting, traffic scrubbing та ізоляції уражених вузлів. Важливим напрямом є інтеграція платформ SOAR, які дозволяють автоматизувати реагування та скоротити час між виявленням і нейтралізацією атак.

Окрім внутрішньої діяльності, CNCERT/CC активно співпрацює на міжнародному рівні, беручи участь у глобальних мережах реагування, таких як FIRST та APCERT. Це забезпечує обмін індикаторами компрометації, спільне відпрацювання сценаріїв реагування та узгодження стандартів кіберзахисту. Відтак, CNCERT/CC виступає не лише як національний центр технічної координації, але й як інституція, що формує китайську модель кіберстійкості, поєднуючи державне регулювання, корпоративні практики та міжнародну взаємодію [57].

Deep Packet Inspection (DPI) – це технологія аналізу мережевого трафіку, яка дозволяє досліджувати заголовки пакетів та їхній вміст, забезпечуючи виявлення загроз, контроль політик та оптимізацію роботи мережі. Вона базується на алгоритмах пошуку шаблонів, машинному навчанні та апаратних прискорювачах, що робить її ключовим інструментом сучасних систем кіберзахисту.

DPI працює на рівні Layer 7 (Application Layer) моделі OSI, що дозволяє аналізувати протоколи HTTP, SMTP, FTP, DNS та інші. На відміну від традиційних фільтрів, котрі перевіряють лише IP-адреси та порти, DPI здатний виконувати глибокий контент-аналіз, зокрема, здійснювати пошук сигнатур шкідливого коду та виявляти аномалії у поведінці користувачів. Основні

технічні завдання включають в себе: сигнатурний пошук (regular expression matching, Aho–Corasick, Wu–Manber); аналіз поведінки за допомогою алгоритмів машинного навчання (Random Forest, SVM, CNN, LSTM). оптимізацію продуктивності через використання апаратних прискорювачів TCAM (Ternary Content Addressable Memory), FPGA та багатоядерних процесорів.

- 1) DPI застосовує різні алгоритми:
- 2) Aho–Corasick – ефективний пошук множини шаблонів у потоці даних.
- 3) Bloom Filters – швидка перевірка наявності елементів у множині.
- 4) Deep Learning Models – CNN та LSTM для класифікації трафіку та виявлення zero-day атак [50, с. 8-12].

Програмні реалізації включають Snort, Suricata, Bro/Zeek, які інтегрують DPI для IDS/IPS систем. У середовищах SDN (Software-Defined Networking) DPI реалізується через мову програмування P4, що дозволяє гнучко описувати правила аналізу пакетів на рівні контролера.

У системах на основі Suricata правила DPI виглядають як регулярні вирази для виявлення шкідливих HTTP-запитів. У середовищі SDN на P4 можна описати програму, яка аналізує заголовки та payload, наприклад:

```
p4
parser parse_http {
    extract(hdr.http);
    if (hdr.http.method == "POST") {
        apply(dpi_check);
    }
}
```

Цей код дозволяє інтегрувати DPI-функції безпосередньо у програмовані комутатори [16].

SOAR - платформи активно інтегруються у китайську державну та корпоративну систему кіберзахисту. Китайська модель поєднує жорстке регулювання (CSL, DSL, PIPL) із технічними рішеннями, які дозволяють автоматизувати реагування на загрози у масштабах критичної інфраструктури.

У китайських SOC - центрах SOAR використовується для інтеграції з національними системами моніторингу, зокрема CNCERT/CC. Це означає, що плейбуки реагування не лише блокують IP-адреси чи ізолюють заражені вузли, а й автоматично формують звітність для регуляторних органів. Алгоритмічно такі платформи поєднують rule - based engines із машинним навчанням, як, наприклад, моделі CNN та LSTM застосовуються для класифікації трафіку та виявлення zero - day-атак, а графові алгоритми – для побудови зв'язків між загрозами у різних секторах (енергетика, транспорт, фінанси).

Програмні реалізації у Китаї часто базуються на модифікованих open - source рішеннях (TheHive+Cortex, Shuffle), але інтегровані у національні стандарти безпеки. Кодова база здебільшого орієнтована на Python, що дозволяє створювати кастомні плейбуки. Наприклад, у випадку виявлення шкідливого трафіку SOAR-система може викликати API китайських фаєрволів (наприклад, Huawei або NSFOCUS) для блокування, а паралельно – системи управління загрозами API для створення запису у внутрішньому реєстрі. У середовищах SDN та NFV, які активно розвиваються в рамках програми «Made in China 2025», SOAR інтегрується через мову P4, що дозволяє описувати правила DPI та запускати автоматичні процедури реагування безпосередньо на рівні комутаторів [30, с. 111–145].

Великі мовні моделі (LLMs) у Китаї розглядаються як стратегічна технологія, що має подвійне значення. Це інструмент розвитку штучного

інтелекту для освіти, науки та промисловості, але це є і ключовим елементом кібербезпеки та інформаційного суверенітету КНР.

Архітектурно LLM базуються на трансформерних нейронних мережах, які дозволяють моделі працювати з мільярдами параметрів, аналізувати контекстні залежності у тексті та генерувати адаптивні відповіді. У сфері кіберзахисту це означає можливість автоматичного аналізу журналів подій, класифікації загроз, виявлення аномалій та формування інструкцій для систем оркестрації реагування (SOAR). Китайські дослідницькі центри активно займаються fine - tuning LLM на спеціалізованих корпусах (логах IDS/IPS), даних з DPI - систем, звітах CNCERT/CC, що дозволяє моделі працювати у вузькому домені кібербезпеки.

Технічні аспекти використання LLM у Китаї включають оптимізацію продуктивності через методи параметричної компресії (LoRA, quantization), що дає змогу запускати моделі у корпоративних середовищах із обмеженими ресурсами. Алгоритмічно LLM застосовують механізми attention для побудови багатовимірних контекстних представлень, а також інтегруються з графовими базами даних для виявлення складних атак, які мають багаторівневу структуру.

У практиці SOC - центрів LLM можуть отримати вхідні дані про небезпечну ситуацію, класифікувати її як «phishing» чи «malware», згенерувати Python-код для SOAR-плейбуку, а також сформувати звіт для регуляторного органу. Це забезпечує перехід від статичних систем реагування до динамічних, де модель сама пропонує оптимальні дії залежно від контексту атаки [74, с. 45–67].

Програмні реалізації LLM у Китаї представлені кількома ключовими проєктами. ERNIE (Baidu) – це модель, оптимізована для китайської мови та технічних текстів, яка використовується у державних і корпоративних платформах. PanGu- α (Huawei) являє собою масштабну модель, інтегровану в

хмарні сервіси Huawei Cloud, що застосовується для аналізу промислових даних і кіберзахисту критичної інфраструктури. MOSS (Fudan University) – відкрита модель для китайської мови, яка використовується у дослідницьких проєктах і навчальних середовищах. Усі вони мають API-інтерфейси, що дозволяють інтегрувати їх у SOC-центри, системи моніторингу та платформи реагування. Важливо, що китайські LLM розробляються з урахуванням вимог законодавства про кібербезпеку (CSL, DSL, PIPL), що передбачає локалізацію даних, контроль доступу та обов'язкову звітність перед державними органами. Отже, LLM у Китаї виступають не лише як технологія штучного інтелекту, а й як інструмент управління кіберризиками [69].

Японія має одну з найбільш збалансованих моделей кібербезпеки в Азії: держава встановлює чіткі закони (UCAL, APPI), а корпоративний сектор активно впроваджує стандарти METI та IPA. Це поєднання правового регулювання, корпоративних практик і технічних рішень (SOAR, DPI, LLM) формує японську модель кіберстійкості.

Японія вибудувала власну модель кібербезпеки, яка поєднує державне регулювання, корпоративну відповідальність та технічні інновації. На відміну від китайської централізованої системи, японський підхід базується на партнерстві між урядом і приватним сектором. Важливим кроком стало ухвалення закону UCAL (Act on the Prohibition of Unauthorized Computer Access), що криміналізує несанкціонований доступ до комп'ютерних систем, а також APPI (Act on the Protection of Personal Information), який встановлює високі стандарти захисту персональних даних. Ці закони створюють правову основу для боротьби з кіберзлочинністю та забезпечення приватності, а їхнє застосування координується через спеціалізовані агентства, зокрема Information-technology Promotion Agency (IPA) [53, с. 246-249].

Корпоративні практики в Японії формуються під впливом Міністерства економіки, торгівлі та промисловості (METI), яке разом з IPA розробило Cybersecurity Management Guidelines. Цей документ орієнтований на керівників

компаній і вимагає інтеграції кібербезпеки у систему корпоративного управління. Японські корпорації, такі як NEC, Fujitsu та Hitachi, впроваджують внутрішні SOC-центри, проводять регулярні аудити та застосовують PDCA-цикли для постійного вдосконалення систем захисту. Особлива увага приділяється безпеці ланцюгів постачання: великі компанії перевіряють постачальників на відповідність стандартам кіберзахисту, що стало особливо актуальним після глобальних атак на supply chain [55].

З технічного боку японські SOC-центри активно інтегрують платформи SOAR для автоматизації реагування на загрози. Це дозволяє скоротити час між виявленням загрози та її нейтралізацією, особливо у фінансовому секторі та телекомунікаціях. Deep Packet Inspection (DPI) використовується у мережах NTT та KDDI для виявлення шкідливого трафіку та забезпечення якості обслуговування. Алгоритми Aho–Corasick та Bloom Filters застосовуються для швидкого аналізу пакетів, а моделі машинного навчання – для класифікації аномалій. Великі мовні моделі (LLMs) також знаходять своє місце у японській кібербезпеці: дослідницькі центри RIKEN та університети Токіо й Осаки працюють над адаптацією трансформерних моделей для автоматичного аналізу логів, класифікації загроз та генерації звітів [48].

Міжнародний кейс японської кіберстратегії полягає у співпраці з APCERT та FIRST, що забезпечує обмін індикаторами компрометації та спільне відпрацювання сценаріїв реагування. Уряд підтримує концепцію «Cybersecurity for Society», яка поєднує державні та приватні ініціативи, підкреслюючи, що кібербезпека є не тільки технічним завданням, а й соціальною відповідальністю.

Отже, японська модель кібербезпеки вирізняється балансом між правовим регулюванням, корпоративними практиками та технічними рішеннями. Вона менш централізована, ніж китайська, але більш орієнтована на добровільне дотримання стандартів і міжнародну співпрацю. Це робить її прикладом того, як можна поєднати високий рівень технологічного розвитку з демократичними принципами управління кіберпростором.

Південна Корея вибудувала комплексну нормативну систему, що охоплює різні сектори. Основними законами є Network Act (регулює інформаційно - комунікаційний сектор), PIPA (Personal Information Protection Act , захист персональних даних), EFTA (Electronic Financial Transactions Act, фінансовий сектор) та Act on the Protection of Information and Communications Infrastructure (захист критичної інфраструктури). Додатково діють Cyber Security Work Regulations Національної служби розвідки (NIS), які встановлюють стандарти для державного сектору [35].

У 2024 році уряд оновив Національну стратегію кібербезпеки та основний план, які визначають п'ять ключових цілей: посилення оборонних можливостей, розвиток міжнародної співпраці, кіберстійкість критичної інфраструктури, конкурентоспроможність у нових технологіях та створення операційної бази для реалізації цих завдань. Корейські компанії зобов'язані дотримуватися вимог Network Act та PIPA, що передбачає суворий контроль за обробкою даних і звітність про інциденти. У фінансовому секторі банки впроваджують SOC - центри з автоматизацією реагування через SOAR, що дозволяє скоротити час між виявленням загрози та її нейтралізацією. У телекомунікаціях (SK Telecom, KT, LG U+) застосовується Deep Packet Inspection (DPI) для виявлення шкідливого трафіку та забезпечення QoS. Алгоритми Aho–Corasick та Bloom Filters використовуються для швидкого аналізу пакетів, а моделі машинного навчання для класифікації загроз.

У 2026 році набув чинності AI Framework Act, який встановлює вимоги до безпеки високоризикових систем штучного інтелекту. Це прямо стосується великих мовних моделей (LLMs), які інтегруються у SOC - центри для автоматичного аналізу логів, класифікації загроз та генерації звітів. Дослідницькі інститути, такі як KISA (Korea Internet & Security Agency) та університети Сеула, працюють над адаптацією трансформерних моделей для кіберзахисту.

Південна Корея активно співпрацює з міжнародними організаціями, зокрема FIRST та APCERT, бере участь у спільних тренуваннях реагування на інциденти та обміні індикаторами компрометації. Це підкреслює її прагнення бути глобальним гравцем у сфері кіберстійкості. Модель кібербезпеки Південної Кореї відрізняється від китайської та японської тим, що поєднує жорстке законодавче регулювання з активним корпоративним впровадженням технічних рішень. Вона орієнтована на міжнародну співпрацю та інтеграцію новітніх технологій, включно з LLM, що робить її однією з найбільш динамічних у регіоні [67].

Висновки до розділу 2

Розділ 2 нашої випускної кваліфікаційної роботи присвячений порівняльному аналізу підходів до управління кіберризиками у різних країнах світу. У ньому розглянуто досвід США, ЄС, Китаю, Японії та Південної Кореї, які демонструють різні моделі поєднання державного регулювання, корпоративних практик та технічних рішень. Аналіз показує, що кібербезпека стала стратегічним пріоритетом для провідних держав, а їхні підходи відображають особливості політичних систем, економічних моделей та технологічного розвитку.

Американська модель управління кіберризиками має системний та інституційно закріплений характер. Центральну роль відіграє NIST Cybersecurity Framework (CSF 2.0), який забезпечує універсальний підхід до ідентифікації, захисту, виявлення та реагування на загрози. Паралельно діє CISA, що координує захист критичної інфраструктури та реалізує практичні заходи реагування. Важливим є поєднання концептуальних рамок (NIST) із прикладними діями (CISA), що створює комплексну модель кіберстійкості. США активно інтегрують нові технології (Zero Trust Architecture, Supply Chain Risk Management, автоматизовані платформи ERM) і задають глобальні стандарти у сфері кібербезпеки.

Китайська модель базується на централізованому державному контролі та ідеології «інформатизації». Ключову роль відіграє САС та законодавчі акти CSL, DSL, PIPL, які забезпечують сувору регуляцію даних і контенту. Важливим елементом є CNCERT/CC, що координує реагування на загрози та інтегрує технічні рішення (DPI, SOAR). Китай активно розвиває власні LLMs (ERNIE, PanGu-α, MOSS), які застосовуються для аналізу логів, класифікації загроз та автоматизації реагування. Доходимо до висновку, що китайська модель поєднує жорстке регулювання з технологічними інноваціями, але має акцент на інформаційному суверенітеті та контролі.

Що стосується японської моделі кібербезпеки та управління кіберризиками, то вона вирізняється балансом між державним регулюванням та корпоративною відповідальністю. Основними законами є UCAL та APPI, які забезпечують захист від несанкціонованого доступу та високі стандарти приватності. Важливу роль відіграють METI та IPA, які розробили Cybersecurity Management Guidelines для корпоративного сектору. Японські компанії (NEC, Fujitsu, Hitachi) впроваджують SOC - центри, застосовують PDCA - цикли та контролюють безпеку ланцюгів постачання. Технічні рішення включають SOAR, DPI та адаптацію LLM для аналізу логів. Японія активно співпрацює з APCERT та FIRST, що підкреслює її міжнародну орієнтацію.

Корейська модель поєднує жорстке законодавче регулювання та активне корпоративне впровадження технічних рішень. Основними законами є Network Act, PIPA, EFTA та AI Framework Act (2026), що встановлює вимоги до безпеки високоризикових систем III. У фінансовому секторі банки застосовують SOC-центри з SOAR, у телекомунікаціях (SK Telecom, KT, LG U+) використовується DPI, а дослідницькі інститути (KISA, університети Сеула) працюють над інтеграцією LLM у кіберзахист. Південна Корея активно співпрацює з міжнародними організаціями (FIRST, APCERT), що робить її одним із найбільш динамічних гравців у регіоні.

З опрацьованого матеріалу стає очевидним, що кібербезпека є стратегічним пріоритетом для провідних держав світу. Кожна країна формує власну модель управління ризиками, яка відображає її політичні та економічні особливості. Для України важливо знати ці підходи, адже вони демонструють різні шляхи досягнення кіберстійкості (від централізованого контролю до партнерських моделей, від акценту на національному суверенітеті до міжнародної співпраці). Основні положення розділу полягають у тому, що ефективна система кібербезпеки має поєднувати законодавчу базу, корпоративні практики та технічні інновації, а також враховувати глобальні стандарти й міжнародний досвід.

РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА РЕКОМЕНДАЦІЇ УПРОВАДЖЕННЯ ЗАКОРДОННОГО ДОСВІДУ БОРОТЬБИ З КІБЕРРИЗИКАМИ В УКРАЇНІ

3.1. Аналіз поточного стану кібербезпеки в Україні

Після розгляду досвіду США, Китаю, Японії та Південної Кореї стає очевидним, що ефективне управління кіберризиками потребує комплексного поєднання законодавчої бази, корпоративних практик та технічних інновацій. Для України, яка перебуває у стані постійних кіберзагроз, особливо з боку державних акторів, питання адаптації зарубіжного досвіду є стратегічним. Відтак, маємо на меті окреслити поточний стан кібербезпеки в Україні.

Сучасний стан кібербезпеки в Україні визначається поєднанням законодавчих ініціатив, інституційних механізмів та практичних викликів, що виникають у контексті гібридної війни та постійних кібератак. Україна стала однією з перших держав у Східній Європі, яка законодавчо закріпила основи кіберзахисту, ухваливши Закон «Про основні засади забезпечення кібербезпеки України». Цей документ визначив ключові принципи державної політики у сфері кібербезпеки, закріпив правові основи для створення системи реагування на інциденти та встановив відповідальність державних органів і суб'єктів господарювання за захист інформаційних ресурсів [12].

Інституційно система кіберзахисту України представлена Державною службою спеціального зв'язку та захисту інформації (ДССЗІ), яка координує діяльність у сфері кібербезпеки, та CERT-UA, що виконує функції національного центру реагування на комп'ютерні інциденти. Ці структури забезпечують моніторинг загроз, інформування про інциденти та координацію дій між державними органами та приватним сектором. Водночас їхня діяльність часто обмежена браком ресурсів, кадровим дефіцитом та необхідністю швидкої адаптації до нових технологічних викликів.

Військовий контекст останніх років суттєво загострив проблему кіберзахисту. Масовані атаки на енергетичну інфраструктуру, банківський сектор, державні реєстри та телекомунікаційні системи показали вразливість критичних інформаційних ресурсів. Приклади атак на енергетичні компанії у 2015–2016 роках, а також постійні спроби зламати державні реєстри та системи управління, засвідчили, що кібербезпека є не лише технічним, а й стратегічним питанням національної безпеки.

Основними проблемами сучасної української системи кіберзахисту є:

- недостатня інтеграція кіберризиків у систему національної безпеки та корпоративного управління;
- обмежені ресурси для впровадження сучасних технологій (SOAR, DPI, LLM), які вже активно застосовуються у США, Японії та Південній Кореї;
- дефіцит кваліфікованих кадрів, що зумовлює потребу у створенні спеціалізованих освітніх програм і центрів підготовки;
- слабка міжнародна координація, яка обмежує доступ до глобальних індикаторів компрометації та спільних тренувань реагування [8, с. 487-500].

Попри ці виклики, Україна має значний потенціал для розвитку кіберзахисту. Важливим кроком стало створення Національної стратегії кібербезпеки України (2021), яка визначає пріоритети у сфері захисту критичної інфраструктури, розвитку кадрового потенціалу та міжнародної співпраці. Водночас стратегія потребує оновлення з урахуванням нових реалій війни та глобальних тенденцій, зокрема, інтеграції принципів Zero Trust, управління ризиками ланцюга постачання та використання штучного інтелекту у сфері кіберзахисту.

Отже, поточний стан кібербезпеки в Україні можна охарактеризувати як перехідний: існує базова законодавча та інституційна основа, проте вона потребує суттєвого вдосконалення. Україна має унікальний досвід протидії масштабним кібератакам у воєнних умовах, але для побудови стійкої системи управління кіберризиками необхідно інтегрувати найкращі міжнародні

практики, розвивати власні технологічні рішення та забезпечувати системну підготовку кадрів [9].

Кібербезпека в Україні тісно пов'язана із захистом критичної інфраструктури, адже саме ці об'єкти (енергетика, транспорт, фінанси, охорона здоров'я та державні інформаційні системи) є найбільш вразливими до атак. Дослідження Ємельянова В.М. і Бондар Г.Л. підкреслює, що в умовах гібридної війни кібератаки стали інструментом стратегічного тиску, здатним паралізувати роботу цілих секторів економіки. Приклади атак на енергетичні компанії у 2015–2016 роках показали, що наслідки можуть мати не лише економічний, а й соціальний вимір, а саме перебої у постачанні електроенергії та загрози життю та здоров'ю громадян.

Важливим аспектом є те, що кіберзахист критичної інфраструктури потребує комплексного підходу. Погоджуємося, що недостатньо лише технічних рішень, а необхідна інтеграція кіберризиків у систему національної безпеки, створення чіткої моделі взаємодії між державними органами та приватним сектором, а також формування культури кібергігієни серед населення. Саме людський фактор часто стає слабкою ланкою, і тому освітні та просвітницькі програми мають стратегічне значення.

Окремо акцентуємо на проблему кадрового дефіциту. Україна потребує системної підготовки фахівців з кіберзахисту, здатних працювати із сучасними технологіями, що включає платформи автоматизації реагування (SOAR) та інструменти штучного інтелекту для аналізу логів та прогнозування загроз. Без розвитку людського капіталу навіть найкращі технічні рішення залишатимуться малоефективними.

Таким чином, кібербезпека в Україні має розглядатися як стратегічний пріоритет державної політики, а захист критичної інфраструктури — як ключовий елемент національної безпеки. Лише комплексний підхід, що включає законодавче вдосконалення, розвиток корпоративних практик, впровадження технічних інновацій та міжнародну співпрацю, здатен

забезпечити належний рівень кіберстійкості України у сучасних умовах [2, с. 493-523].

Прийняття Закону України № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» стало важливим етапом у розвитку національної системи кібербезпеки. Документ, ухвалений Верховною Радою 27 березня 2025 року та підписаний Президентом України 17 квітня 2025 року, закріплює нові механізми реагування на кіберзагрози та визначає відповідальність усіх суб'єктів у цій сфері.

Закон передбачає створення національної системи реагування на кіберінциденти, до складу якої увійдуть CERT - UA, а також галузеві та регіональні команди реагування, що формуватимуться органами державної влади та місцевого самоврядування. Це дозволяє перейти від фрагментарних заходів до комплексної моделі управління кіберризиками, де кожен рівень державного управління має власні інструменти реагування.

Серед ключових нововведень закону:

Національна система обміну інформацією про кіберзагрози. Вона забезпечує оперативний обмін даними між державними органами, приватним сектором та міжнародними партнерами, що підвищує ефективність виявлення та нейтралізації ризиків.

Введення штатних посад фахівців з кібербезпеки у державних установах та на об'єктах критичної інфраструктури. Це створює новий кадровий стандарт і гарантує постійну присутність професійних спеціалістів у ключових сферах.

Відмова від традиційних КСЗІ та перехід до процесу управління ризиками на основі профілів безпеки. Такий підхід відповідає сучасним міжнародним практикам (зокрема NIST CSF 2.0) і дозволяє гнучко адаптувати заходи захисту до конкретних умов.

Система оцінювання стану кіберзахисту через аудит без надмірного контролю з боку держави. Це сприяє формуванню культури відповідальності та саморегуляції, а не лише адміністративного тиску.

Закон також має освітній вимір. Кафедра технічних систем кіберзахисту ДУІКТ вже розпочала оновлення навчальних програм, зокрема дисципліни «Комплексні системи захисту інформації», з урахуванням нових законодавчих вимог. Це означає, що підготовка майбутніх фахівців буде орієнтована на актуальні знання та навички, необхідні для роботи у державних установах і на об'єктах критичної інфраструктури.

Таким чином, Закон № 4336-IX закріплює перехід України до сучасної моделі кіберзахисту, яка базується на управлінні ризиками, інтеграції кадрового потенціалу та створенні національної системи реагування. Він формує нову архітектуру кібербезпеки, де поєднуються законодавчі механізми, інституційні структури та освітні ініціативи. Це дозволяє Україні не лише посилити власну стійкість до кіберзагроз, а й наблизитися до міжнародних стандартів у сфері цифрової безпеки [11].

На Kyiv International Cyber Resilience Forum 2026 було представлено нову архітектуру реагування на кіберінциденти, яка стала важливим кроком у формуванні національної системи кіберзахисту України. Вона передбачає створення галузевих та регіональних CERT - команд, інтегрованих у єдину систему обміну інформацією, а також акцент на розвиток культури кібергігієни та системне навчання персоналу.

Презентована модель передбачає багаторівневу структуру реагування, де CERT - UA виступає центральним координатором, а галузеві та регіональні команди забезпечують оперативне реагування на місцях. Такий підхід дозволяє швидко локалізувати загрози, враховуючи специфіку окремих секторів, будь то енергетика, фінанси, транспорт чи охорона здоров'я. Важливе значення має національна система обміну інформацією про кіберзагрози, що забезпечує

синхронізацію дій між державними органами, приватними компаніями та міжнародними партнерами.

Особливу увагу на форумі приділили кібергігієні, а саме базовим аспектам безпечної роботи з інформаційними системами. Йдеться про регулярне оновлення програмного забезпечення, використання багатофакторної автентифікації, контроль доступу та мінімізацію людських помилок. Важливо, що кібергігієна розглядається не лише як технічний набір правил, а як культура поведінки, котра має бути інтегрована у всі рівні державного управління та корпоративного сектору.

Форум підкреслив необхідність системного навчання кадрів:

- регулярні тренінги та брифінги для співробітників;
- залучення зовнішніх експертів для підвищення кваліфікації;
- створення програм сертифікації для фахівців з кібербезпеки;
- інтеграція навчальних модулів у систему вищої освіти та професійної перепідготовки.

Це дозволяє формувати кадровий резерв, здатний працювати з сучасними технологіями, зокрема, системи моніторингу і платформи автоматизації реагування (SOAR) [51].

Наша країна поступово переходить від реактивної моделі кіберзахисту до проактивної системи управління ризиками, де ключову роль відіграють обмін інформацією, кібергігієна та системне навчання персоналу. Представлена архітектура реагування на інциденти є важливим кроком у формуванні стійкої національної системи кібербезпеки, здатної протистояти сучасним викликам гібридної війни та інтегруватися у глобальну інфраструктуру кіберзахисту.

Розвиток кібербезпеки в Україні останніми роками набув виразного технічного виміру. Поряд із законодавчими та інституційними змінами формується комплексна екосистема програмних рішень, систем моніторингу та інноваційних технологій, які забезпечують захист державних інформаційних ресурсів і критичної інфраструктури.

В центрі уваги – CERT-UA, що виконує функції національного центру реагування на інциденти. Його діяльність базується на використанні систем IDS/IPS (Intrusion Detection/Prevention Systems), таких як Snort та Suricata, які дозволяють аналізувати мережевий трафік у реальному часі та виявляти аномалії. Важливим доповненням стали SOAR - платформи (Security Orchestration, Automation and Response), що автоматизують процес реагування на інциденти. Завдяки сценаріям плейбуks система може самостійно блокувати шкідливі IP-адреси, ізолювати заражені вузли та формувати звіти для аналітиків. Це значно скорочує час між виявленням загрози та її нейтралізацією [22].

У сфері телекомунікацій активно застосовується Deep Packet Inspection (DPI), котрий застосовується для аналізу пакетів даних на рівні їх вмісту. Для оптимізації роботи використовуються алгоритми Aho–Corasick для швидкого пошуку сигнатур та Bloom Filters для економії пам'яті. Це забезпечує ефективне виявлення шкідливого трафіку та підтримку якості сервісу (QoS), що особливо важливо для операторів мобільного зв'язку та інтернет-провайдерів.

Окремим напрямом є розвиток криптографічних технологій. Українські науковці працюють над впровадженням постквантових алгоритмів (NTRU, Kyber), які мають забезпечити стійкість до атак квантових комп'ютерів. Важливим майданчиком для обговорення цих питань стала конференція UkrCrypto2026, де презентували нові підходи до zero-knowledge протоколів, блокчейн-технологій та стеганографії. Це свідчить про прагнення України інтегруватися у глобальні дослідження та створювати власні криптографічні рішення.

Не менш значущим вважаємо використання ШІ та машинного навчання у кіберзахисті. Українські дослідницькі центри адаптують великі мовні моделі (LLMs) для автоматичного аналізу логів, класифікації загроз та прогнозування інцидентів. Моделі на базі PyTorch та TensorFlow застосовуються для виявлення

аномалій у системних журналах і мережевому трафіку щоб сформувати проактивну систему захисту, котра реагує на атаки і передбачає їх [17].

Україна демонструє високий рівень протидії кіберзагрозам і водночас ділиться напрацьованими практиками з глобальною спільнотою. Представники Міністерства цифрової трансформації, ДП «Дія» та Проектного офісу Талліннського механізму (ТМРО) презентували український досвід на міжнародному форумі InCYBER у французькому Ліллі. Учасники з України не лише окреслили особливості протидії загрозам у реаліях кібервійни, а й визначили нові напрями співпраці з іноземними партнерами.

На дискусійних майданчиках форуму українська делегація активно взаємодіяла з колегами з Франції, Швеції та Молдови. Керівниця ТМРО Олеся Данильченко акцентувала на стратегічних підходах до управління кібервразливостями та посилення стійкості цифрових систем. Талліннський механізм, що вже об'єднав 14 держав, поступово перетворюється на міжнародний еталон співпраці у сфері кіберзахисту. Показовим є те, що Франція офіційно інтегрувала партнерство з Україною у власну національну кіберстратегію.

У спілкуванні з делегатами з Канади, Кенії, Казахстану та Таїланду українська команда обговорила конкретні заходи, які уряди застосовують для зменшення ризиків у кіберпросторі. Такі обговорення мають ключове значення для формування політик цифрового суверенітету, підвищення кіберстійкості та ефективного управління критичними вразливостями.

Під час двосторонніх зустрічей із представниками Міністерства кібербезпеки та цифрових технологій Квебеку увага була зосереджена на розвитку цифрової ідентичності, впровадженні суверенних рішень (sovereign cloud, sovereign AI), сучасних методах класифікації кіберризиків та створенні зручних державних сервісів за українським зразком.

Ключовим чинником кібербезпеки залишаються фахівці. У межах Талліннського механізму за підтримки Expertise France реалізуються освітні програми для працівників державних органів та критичної інфраструктури.

Зокрема, підвищується кваліфікація експертів центрів безпеки (SOC), які відповідають за оперативне виявлення та нейтралізацію загроз.

Участь України в таких масштабних заходах, як InCYBER, дозволяє не лише переймати найкращі практики, а й виступати ініціатором нових тенденцій. Спільно з партнерами наша держава формує сучасну архітектуру глобальної кібербезпеки, що враховує виклики війни та потреби цифрового суспільства [7].

Важливим кроком стало представлення на Kyiv International Cyber Resilience Forum 2026 нової архітектури реагування на кіберінциденти. Вона включає галузеві та регіональні CERT-команди, інтегровані у єдину систему обміну інформацією. Акцент зроблено на розвитку культури cyber hygiene та системному навчанні персоналу – від регулярних тренінгів до залучення зовнішніх експертів. Це формує кадровий резерв, здатний працювати із сучасними технологіями та забезпечувати стійкість критичної інфраструктури.

Таким чином, технічні та комп'ютерні «фішки» України у сфері кіберзахисту охоплюють широкий спектр рішень: від SOC - центрів із автоматизацією реагування та DPI-систем до криптографічних досліджень і використання штучного інтелекту. Вони формують сучасну екосистему кіберзахисту, яка відповідає міжнародним стандартам і водночас враховує реалії гібридної війни.

Криптографія є фундаментом сучасної кібербезпеки, а в умовах розвитку квантових технологій постає завдання створення алгоритмів, стійких до нових типів атак. Українські науковці активно працюють над впровадженням постквантових алгоритмів (NTRU, Kyber), які вже розглядаються як перспективні стандарти у світі. Важливим напрямом є також дослідження zero-knowledge протоколів, що дозволяють підтверджувати достовірність інформації без її розкриття, що особливо актуально для фінансових транзакцій та систем електронного голосування. Паралельно розвиваються блокчейн-рішення, які застосовуються для захисту ланцюгів постачання,

забезпечення прозорості державних реєстрів та створення децентралізованих систем зберігання даних. Конференція *UkrCrypto2026* стала майданчиком для презентації цих інновацій, демонструючи прагнення України інтегруватися у глобальні криптографічні дослідження.

Штучний інтелект поступово стає невід'ємною частиною української системи кіберзахисту. CERT-UA та корпоративні SOC-центри використовують LLMs (Large Language Models) для автоматичного аналізу логів та класифікації загроз. Це дозволяє швидко виявляти аномалії у системних журналах, прогнозувати потенційні атаки та формувати рекомендації для реагування. Наприклад, моделі на базі PyTorch застосовуються для виявлення підозрілих патернів у мережевому трафіку, що дає змогу зменшити кількість хибних спрацювань. AI також використовується для прогнозування інцидентів: аналізуючи історичні дані, система може передбачати ймовірність атак на конкретні об'єкти критичної інфраструктури. Це створює проактивну модель захисту, де загрози не лише фіксуються, а й передбачаються.

Україна поступово переходить від традиційних КСЗІ до сучасних систем управління ризиками. Новий закон № 4336-IX закріпив концепцію профілів безпеки, які дозволяють оцінювати рівень ризику для кожної установи чи об'єкта критичної інфраструктури. Це означає, що заходи кіберзахисту більше не є універсальними, а адаптуються до конкретних умов. Важливим елементом є аудит кіберзахисту, який проводиться без надмірного контролю з боку держави, але з акцентом на відповідальність самих організацій. Такі аудити дозволяють виявляти слабкі місця та формувати рекомендації для їх усунення. Інтеграція управління ризиками у корпоративне управління забезпечує системність: кіберризики розглядаються поряд із фінансовими та операційними ризиками, що робить бізнес-моделі більш стійкими.

Поєднання криптографічних інновацій, застосування штучного інтелекту та системного управління ризиками формує нову архітектуру кіберзахисту України. Це дозволяє не лише реагувати на загрози, а й створювати проактивну модель безпеки, яка відповідає міжнародним стандартам і враховує реалії

гібридної війни. Україна поступово переходить від базових механізмів до комплексної технічної екосистеми, де законодавчі, інституційні та технологічні елементи взаємодіють для забезпечення стійкості держави у цифрову епоху [4].

У період 2013–2024 років в Україні спостерігається суттєве зростання кількості зареєстрованих кримінальних правопорушень у сфері кібербезпеки: від 576 випадків у 2013 році до 3945 у 2024 році. Особливо різкий стрибок зафіксовано у 2017 році, коли кількість злочинів зросла до 2437, після чого рівень залишався стабільно високим. Така тенденція може свідчити як про реальне збільшення масштабів кіберзлочинності, так і про вдосконалення механізмів її реєстрації та обліку.

Позитивною є динаміка у частці кримінальних правопорушень, за якими особам було вручено повідомлення про підозру: цей показник зріс із 41% у 2013 році до 78% у 2024 році, що свідчить про підвищення ефективності слідчих органів. Найбільше зростання відбулося у 2016–2018 роках. Кількість справ, переданих до суду, також демонструє поступове збільшення – від 230 у 2013 році до 2328 у 2024 році. Водночас частка таких справ залишається нерівномірною: пікове значення у 2021 році (63%) змінилося спадом у 2022 році (47%), що вказує на потребу оптимізації судово - слідчого процесу та забезпечення його стабільності.

Для комплексної оцінки рівня кібербезпеки України важливим є використання міжнародних індикаторів, зокрема National Cyber Security Index (NCSI). Методологія індексу базується на вимірюванні готовності держав до протидії кіберзагрозам і управління кіберінцидентами за допомогою 49 індикаторів, згрупованих у 12 показників та 3 категорії. За останніми даними станом на 29.11.2023 Україна посідає 15-те місце серед 58 країн із результатом 80,84 балів.

Аналіз компонентів індексу свідчить про високий рівень стратегічної кібербезпеки: політика та наукові дослідження оцінені на 100%, що підтверджує

наявність ефективної нормативно - правової бази та наукового потенціалу. Водночас глобальний внесок у кібербезпеку (67%) та освіта й професійний розвиток (60%) потребують посилення, зокрема через розширення міжнародної співпраці та інвестування у підготовку кадрів.

Показники превентивної кібербезпеки також демонструють високий рівень: захист персональних даних оцінено на 100%, кібербезпеку цифрових інструментів – на 83%. Проте захист критичної інфраструктури (75%) та аналіз кіберзагроз (75%) потребують додаткових заходів. Найбільш проблемними залишаються показники реагування: управління кіберризиками (56%) та реагування на кіберінциденти (64%), що свідчить про необхідність вдосконалення кризового менеджменту та впровадження сучасних технологій, зокрема штучного інтелекту для прогнозування та нейтралізації атак.

Отже, Україна демонструє значні досягнення у сфері кібербезпеки, проте подальший розвиток має бути спрямований на розширення міжнародної співпраці, підготовку висококваліфікованих кадрів, посилення захисту критичної інфраструктури та вдосконалення механізмів управління кіберризиками. Це дозволить забезпечити стійкість цифрової екосистеми та підвищити рівень національної безпеки у глобальному кіберпросторі [8, с. 493-495].

3.2. Рекомендації щодо вдосконалення системи управління кіберризиками в Україні з адаптацією закордонного досвіду

Сучасні виклики у сфері кібербезпеки вимагають від нашої країни не тільки оперативного реагування на загрози, а й також системного вдосконалення механізмів управління кіберризиками. В умовах війни та стрімкої цифрової трансформації Україна вже продемонструвала здатність абсорбувати міжнародний досвід і водночас формувати власні рішення, починаючи з розбудови центрів моніторингу безпеки і до створення унікальних цифрових сервісів. Саме тому рекомендації, що ґрунтуються на аналізі

зарубіжних моделей та українських прогресивних практик, мають стати путівником для подальшого розвитку національної системи кіберзахисту.

Спираючись на опрацьований матеріал нашої кваліфікаційної роботи пропонуємо наступні дії:

1. Інституційно-правова підтримка

Наша держава вже закріпила базові положення у Законі «Про основні засади забезпечення кібербезпеки» та у Стратегії кібербезпеки України, втім поняття «кіберризик» досі не має чіткого визначення. Вважаємо, що необхідно:

- внести офіційне тлумачення терміна «кіберризик» у законодавство;
- узгодити українські стандарти з міжнародними (ISO/IEC 27005, NIST SP 800-30, ENISA Guidelines);
- створити єдину систему оцінки ризиків для державних органів і бізнесу.

2. Технічні рішення та алгоритми

Україна вже активно застосовує SOC-центри (Security Operations Centers), які працюють над виявленням атак у режимі реального часу. Вважаємо, що необхідно зосередитися на наступних кроках:

- розширити мережу SOC-центрів на регіональному рівні;
- впровадити алгоритми машинного навчання для автоматичного виявлення аномалій у трафіку:

На нашу думку, одним із ключових напрямів удосконалення системи кіберзахисту України є впровадження алгоритмів машинного навчання, здатних автоматично виявляти аномалії у мережевому трафіку. Такі методи дозволяють підвищити ефективність моніторингу та забезпечити своєчасне реагування на нові та складні загрози, які не завжди можуть бути ідентифіковані традиційними сигнатурними системами. Серед найбільш перспективних моделей пропонуємо: а) K-Means Clustering, що групує пакети за схожістю та

виділяє аномальні кластери; б) Isolation Forest, який ефективно виявляє рідкісні або нетипові події у великих масивах даних; в) Autoencoders, здатні навчатися на «нормальному» трафіку й сигналізувати про відхилення від очікуваних патернів; г) LSTM - мережі, які добре працюють із часовими рядами та дозволяють аналізувати послідовність мережевих запитів; д) Support Vector Machines (SVM), котрі застосовуються для класифікації трафіку на «нормальний» та «підозрілий».

Практичне застосування цих алгоритмів охоплює широкий спектр завдань, зокрема виявлення DDoS-атак через аналіз нетипових піків у кількості запитів; ідентифікацію фішингових кампаній за характерними патернами у HTTP - трафіку; знаходження шкідливих ботів у корпоративних мережах шляхом аналізу поведінкових характеристик; моніторинг внутрішніх загроз (insider threats), коли алгоритми здатні помічати нетипові дії співробітників у системі.

- використовувати системи SIEM (Security Information and Event Management) для централізованого збору та аналізу журналів подій;
- розробити національні платформи для обміну індикаторами компрометації (IoC) між державними та приватними структурами.

3. Програмні комплекси та інструменти

Україна вже має успішний приклад – цифровий додаток «Дія», що забезпечує цифрову ідентичність та доступ до державних сервісів. Відповідно цьому пропонуємо:

- розширити функціонал «Дії» для інтеграції модулів кіберзахисту (наприклад, перевірка безпеки пристрою користувача). Подальший розвиток платформи «Дія» має включати інтеграцію інструментів кіберзахисту, які забезпечуватимуть безпеку користувачів у режимі реальноого часу. Міркуємо, що таке рішення дозволить перетворити «Дію» на багатофункціональний сервіс, пропонуючи поєднання цифрової

ідентичності із захистом інформаційного середовища української спільноти. Наприклад, перед входом у «Дію» система може запускати швидкий сканер безпеки пристрою (перевірити чи є антивірус, чи оновлена ОС тощо). При використанні державних сервісів може відбуватися перевірка підозрілих дій (виявляти нетипові IP-адреси або масові запити) та можна інтегрувати додаток з національним SOC - центром (якщо пристрій користувача виявляє аномалії, дані автоматично надходять у систему моніторингу)

- створити державну платформу sovereign cloud, яка гарантуватиме збереження даних у межах країни (Data residency: суворе розмежування, щоб дані не покидали визначену територію; Jurisdictional control: визначення, хто має право доступу до даних і за яких умов; шифрування та ключі: ключі зберігаються локально, що унеможлиблює доступ іноземних органів; AI - операції: автоматичне виявлення аномалій, прогнозування проблем і самовідновлення систем; Резервування та disaster recovery: створення копій даних у кількох локальних дата-центрах для стійкості до аварій);
- розробити власні рішення у сфері sovereign AI для класифікації кіберризиків та прогнозування атак;
- впровадити системи багатофакторної автентифікації та біометричної ідентифікації для критичних сервісів.

4. Міжнародний досвід та його адаптація

Україна вже інтегрувалася у Талліннський механізм, який став глобальним бенчмарком кіберспівпраці. Проте, з огляду на опрацьовану інформацію і ретельний аналіз поточного стану проблеми, ми можемо рекомендувати:

- розширити участь у програмах ENISA та CISA для отримання доступу до методик оцінки ризиків;
- адаптувати досвід ЄС щодо GDPR для захисту персональних даних;
- запозичити китайські практики централізованого моніторингу критичної інфраструктури, але з урахуванням демократичних принципів;
- розвивати партнерства з країнами, що мають сильні позиції у сфері AI-based cybersecurity (Канада, Франція, Ізраїль).

5. Освітня та кадрова складова

Україна вже розпочала реалізацію програм за підтримки Expertise France, проте для подальшого розвитку ми можемо рекомендувати:

- створити національну програму сертифікації фахівців SOC та SIEM;
- запровадити курси з управління кіберризиками для держслужбовців;
- розробити симуляційні платформи для тренування реагування на атаки (cyber ranges). До них може ввійти віртуалізація та контейнеризація – середовище будується на базі віртуальних машин (VMware, Hyper-V) або контейнерів (Docker, Kubernetes), що дозволяє швидко розгортати різні конфігурації мереж. Моделювання атак – у систему інтегруються симулятори DDoS, фішингових кампаній, ransomware чи APT-атак. Це дає змогу відтворювати реальні сценарії загроз. Інструменти моніторингу, такі як SOC - модулі, SIEM - системи та IDS/IPS (наприклад, Splunk, Suricata, Snort) відстежують дії учасників і дають аналітику у реальному часі. Автоматизовані сценарії – платформа може запускати заздалегідь прописані «playbooks», як, наприклад, блокування IP, ізоляція вузлів, відновлення даних. Звертаємо увагу також на ШІ - модулі, які застосовуються для аналізу поведінки учасників та прогнозування ефективності їхніх дій.

6. Перспективи розвитку боротьби з кіберзагрозами і злочинами

Україна вже стала трендсеттером у сфері цифрових сервісів (приклад «Дії»). Наступним кроком має стати:

- створення національної архітектури кібербезпеки, що інтегрує державні та приватні ініціативи;
- розвиток штучного інтелекту для кіберзахисту, зокрема алгоритмів прогнозування атак. Наприклад, Recurrent Neural Networks (RNN, LSTM) – аналізують часові ряди мережевого трафіку, прогножуючи піки активності, які можуть свідчити про підготовку DDoS-атаки; Random Forest та Gradient Boosting – класифікують події за ймовірністю того, що вони є початком атаки, використовуючи історичні дані про інциденти; Bayesian Networks – моделюють залежності між різними типами загроз і дозволяють оцінити ймовірність їхнього розвитку у майбутньому; Graph Neural Networks (GNN) – застосовуються для аналізу взаємозв'язків між вузлами мережі, що допомагає виявляти приховані патерни атак (наприклад, ботнети); AutoML-платформи – автоматично підбирають оптимальні моделі для прогнозування атак на основі локальних дата-сетів.
- формування єдиного центру реагування на інциденти (CERT - UA) з розширеними повноваженнями;
- інтеграція українських рішень у глобальні платформи кіберзахисту.

Висновки до розділу 3

Аналіз перспектив щодо упровадження зарубіжного досвіду боротьби з кіберризиками в Україні засвідчив, що національна система кіберзахисту перебуває у стані активної трансформації. Україна вже має базову законодавчу та інституційну основу, проте вона потребує суттєвого вдосконалення з урахуванням сучасних викликів гібридної війни та глобальних тенденцій розвитку цифрової безпеки.

Прийняття Закону № 4336-IX стало важливим етапом у формуванні нової архітектури кіберзахисту, яка ґрунтується на управлінні ризиками та профілях безпеки. Це означає відмову від традиційних КСЗІ та перехід до більш гнучкої моделі, що адаптує заходи захисту до конкретних умов кожної установи чи об'єкта критичної інфраструктури. Важливим нововведенням є створення національної системи реагування на кіберінциденти, яка включає CERT-UA та галузеві й регіональні команди реагування. Це забезпечує комплексність і багаторівневість управління ризиками, а також підвищує ефективність обміну інформацією між державними органами, приватним сектором та міжнародними партнерами.

Особливе значення має інтеграція кіберризиків у систему національної безпеки та корпоративного управління, дозволяючи розглядати кіберризики поряд із фінансовими та операційними та формуючи більш стійкі бізнес-моделі та державні стратегії. Водночас акцент робиться на аудитах кіберзахисту, які проводяться без надмірного контролю з боку держави, але з підвищеною відповідальністю самих організацій. Такий підхід сприяє формуванню культури саморегуляції та відповідальності, що відповідає міжнародним практикам.

Технічний вимір розвитку кіберзахисту в Україні охоплює впровадження сучасних інструментів: систем IDS/IPS (Snort, Suricata), платформ автоматизації реагування SOAR, технологій Deep Packet Inspection із використанням

алгоритмів Aho–Corasick та Bloom Filters, а також криптографічних рішень, включно з постквантовими алгоритмами NTRU та Kyber. Важливим напрямом є застосування штучного інтелекту та машинного навчання, зокрема адаптація великих мовних моделей (LLMs) для аналізу логів, класифікації загроз та прогнозування інцидентів, що будує проактивну систему захисту, здатну реагувати на атаки й передбачати їх.

Міжнародна співпраця стала одним із ключових чинників розвитку української кібербезпеки. Участь у Талліннському механізмі, форумах InCYBER та Kyiv International Cyber Resilience Forum 2026 дозволила Україні переймати найкращі практики, а згодом і виступати ініціатором нових тенденцій. Український досвід протидії масштабним кібератакам у воєнних умовах став предметом уваги глобальної спільноти, партнерство з Францією, Швецією, Молдовою та іншими країнами інтегрувалося у міжнародні стратегії кіберзахисту.

Важливим аспектом залишається кадровий потенціал. Дефіцит кваліфікованих фахівців викликає необхідність системної підготовки кадрів, створення програм сертифікації та інтеграції навчальних модулів у систему вищої освіти. Підвищення кваліфікації експертів SOC - центрів, регулярні тренінги та залучення зовнішніх спеціалістів формують кадровий резерв, що може працювати із сучасними технологіями та забезпечувати стійкість критичної інфраструктури.

Отже, Україна поступово переходить від реактивної моделі кіберзахисту до проактивної системи управління ризиками. Поєднання законодавчих змін, інституційних механізмів, технічних інновацій та міжнародної співпраці формує нову архітектуру кібербезпеки, яка відповідає міжнародним стандартам і враховує реалії гібридної війни. Важливим є і те, що технічні рішення стають основою сучасної екосистеми кіберзахисту України, що дозволяє зміцнити стійкість держави до кіберзагроз, а також закріпити її роль як активного учасника глобальної інфраструктури цифрової безпеки.

ВИСНОВКИ

У сучасних умовах цифрової трансформації та гібридної війни питання кібербезпеки набувають стратегічного значення для України. Проведене дослідження підтвердило актуальність теми та необхідність системного управління кіберризиками, що охоплює правові, організаційні та технічні аспекти. Порівняльний аналіз зарубіжного досвіду дозволив окреслити сильні сторони різних моделей та визначити можливості їх адаптації до українських реалій.

Метою роботи було здійснити порівняльний аналіз закордонних моделей управління кіберризиками та визначити перспективи їх упровадження в Україні. На основі проведеного дослідження можна стверджувати, що поставлена мета досягнута, адже ми систематизували теоретичні підходи, розглянули практики США, ЄС та країн Азії, проаналізували стан кібербезпеки в Україні та сформулювали рекомендації щодо її вдосконалення.

Відповідно до поставленої мети нам вдалося вирішити низку завдань і дійти наступних висновків:

Розглянувши сутність понять «кібербезпека», «кіберзагроза» і «кіберризик», ми з'ясували, що кіберризик є ймовірністю настання негативних наслідків у результаті реалізації кіберзагроз. Він має багатовимірний характер, а саме технологічний, соціальний та правовий. Класифікація кіберризиків охоплює зовнішні та внутрішні загрози, шкідливе програмне забезпечення, фішингові атаки, програми-вимагачі, APT-атаки та інші прояви.

При порівнянні досвіду зарубіжних країн дослідження показало, що США застосовують NIST Cybersecurity Framework та практики CISA, які базуються на управлінні ризиками та стандартизації процесів. Європейський Союз розвиває ENISA, GDPR та директиву NIS2, що акцентують на захисті персональних даних та критичної інфраструктури. У Китаї та інших країнах Азії поєднуються

державне регулювання й корпоративні практики, що забезпечує комплексний контроль і швидко адаптацію до нових викликів.

Аналіз поточного стану кібербезпеки в Україні дає підстави стверджувати, що Україна має законодавчу основу («Про основні засади забезпечення кібербезпеки України», Закон № 4336 - IX), інституційні структури (ДССЗІ, CERT - UA) та Національну стратегію кібербезпеки. Водночас існують такі проблеми, як кадровий дефіцит, обмежені ресурси, недостатня інтеграція кіберризиків у систему національної безпеки та слабка міжнародна координація. Попри це, Україна володіє унікальним досвідом протидії масштабним кібератакам у воєнних умовах.

На основі опрацьованого матеріалу ми мали змогу сформулювати практичні рекомендації щодо вдосконалення системи управління кіберризиками в Україні, а саме:

1. перехід від традиційних КСЗІ до управління ризиками на основі профілів безпеки;
2. створення національної системи реагування на кіберінциденти з галузевими та регіональними CERT-командами;
3. розвиток кадрового потенціалу через освітні програми та сертифікацію фахівців;
4. посилення міжнародної співпраці та інтеграції у глобальні механізми кіберзахисту;
5. упровадження низки сучасних технологій, які формують технічний вимір кіберзахисту України та визначають перспективи його розвитку. Важливим напрямом є впровадження платформ SOAR (Security Orchestration, Automation and Response), що дозволяють автоматизувати процес реагування на кіберінциденти. Завдяки використанню сценаріїв плейбуks система може самостійно блокувати шкідливі IP - адреси, ізолювати заражені вузли та

формувати звіти для аналітиків, що значно скорочує час між виявленням загрози та її нейтралізацією.

Не менш значущим є застосування технології Deep Packet Inspection (DPI), яка забезпечує аналіз мережевих пакетів на рівні їхнього вмісту. Для оптимізації роботи використовуються алгоритми Aho–Corasick, що дозволяють швидко здійснювати пошук сигнатур, та Bloom Filters, які економлять пам'ять при обробці великих масивів даних. Це створює умови для ефективного виявлення шкідливого трафіку та підтримки якості сервісу, що особливо важливо для операторів мобільного зв'язку та інтернет-провайдерів.

Окремим напрямом розвитку є постквантова криптографія, яка має забезпечити стійкість до атак квантових комп'ютерів. Українські науковці працюють над впровадженням алгоритмів NTRU та Kyber, а також досліджують нові підходи до zero - knowledge протоколів, блокчейн - технологій та стеганографії. Це свідчить про прагнення інтегруватися у глобальні дослідження та водночас створювати власні криптографічні рішення, що відповідають майбутнім викликам.

Надважливим, на нашу думку, є використання штучного інтелекту та машинного навчання. Українські дослідницькі центри адаптують великі мовні моделі (LLMs) для автоматичного аналізу логів, класифікації загроз та прогнозування інцидентів. Моделі, побудовані на базі PyTorch та TensorFlow, можуть застосовуватися для виявлення аномалій у системних журналах і мережевому трафіку, що дозволяє формувати проактивну систему захисту, здатну не лише реагувати на атаки, а й передбачати їх.

Отже, наше дослідження підтвердило, що Україна поступово переходить від реактивної моделі кіберзахисту до проактивної системи управління ризиками. Мета роботи досягнута, а завдання – виконані. Ми показали, що адаптація зарубіжного досвіду у поєднанні з розвитком власних технологічних рішень і кадрового потенціалу формує нову архітектуру кібербезпеки України.

Це дозволить ефективно реагувати на сучасні загрози і створити стійку модель цифрової безпеки, яка відповідає міжнародним стандартам та реаліям гібридної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аалендер М., Маатен Е., Майгре М., Петеркоп Т. та ін. Посилення захисту критичної інфраструктури України: Стратегічні висновки й кращі міжнародні практики. Академія електронного управління, Таллінн. 2025. URL: https://ega.ee/wp-content/uploads/2025/06/ciip-ua-204x275mm-ua-webi.pdf?_gl=1*5wqc3c*_up*MQ..*_ga*OTg4NDg4MDM3LjE3Nzg5MTk3NDY.*_ga_9FXJ5SMCDK*czE3Nzg5MTk3NDYkbzEkZzAkdDE3Nzg5MTk3NDYkajYwJGwwJGgw
2. Ємельянов В.М., Бондар Г.Л. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Public Administration and Regional Development*. 2019, 5. С. 493-523
3. Загальний регламент про захист даних. GDPR Українською. URL: <https://www.gdpr.org.ua/>
4. Кібербезпека за новими правилами: Закон 4336-IX на практиці. URL: <https://biz.nv.ua/ukr/markets/zakon-4336-ix-yak-diyut-novi-pravila-kiberbezpeki-dlya-biznesu-50607682.html>
5. Конвенція про кіберзлочинність. {Конвенцію ратифіковано із застереженнями і заявами Законом № 2824-IV від 07.09.2005, ВВР, 2006, № 5-6, ст.71}. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
6. Лучик С. Кібертероризм як загроза інформаційній безпеці України. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/e6767c2d-97ae-446e-bc94-450b8bd5bccb/content>
7. Міністерство цифрової трансформації України. Офіційний веб-сайт. URL: <https://thedigital.gov.ua/news/progress/ukrayina-na-incyber-mintsyfra-podilylasia-dosvidom-kiberstiykosti-na-naybilshomu-kiberforumi-yevropy>
8. Миненко С., Кочнєва В., Бабич Є. Оцінка рівня кібербезпеки України в умовах війни. *Європейський науковий журнал Економічних та Фінансових інновацій*. 2024. №2 (14). С. 487-500

9. Овандер Н. Огляд міжнародних та українських стандартів з управління ризиками з погляду сучасних викликів та загроз. Економіка та суспільство. 2021. Вип. 27. DOI: <https://doi.org/10.32782/2524-0072/2021-27-26>
10. Орловський Б. М. Сучасні кіберризики: їх поняття, структура та застосування у сфері торгівельного мореплавства. *Правова держава*, 2025. №58. С. 210–219. DOI: <https://doi.org/10.18524/2411-2054.2025.58.331007>
11. Президент України підписав закон про кіберзахист державних інформаційних ресурсів. URL: https://duikt.edu.ua/ua/news-1-569-14204-prezident-ukraini-pidpisav-zakon-pro-kiberzahist-derzhavnih-informaciynih-resursiv_kafedra-cistem-tehnichnogo-zahistu-informacii
12. Про основні засади забезпечення кібербезпеки України. Закон. Рада. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
13. Сучасні інструменти боротьби з кібершахрайствами у банках : Монографія / О. В. Кузьменко, Г.М. Яровенко, С. В. Леонов та ін. ; за заг. ред. О. В. Кузьменко, Г. М. Яровенко. Суми: видавництво "Ярославна", 2018. 144 с.
14. Фернандо В. Управління ризиками кібербезпеки: основи та найкращі практики. URL: <https://visuresolutions.com/uk/alm-guide/%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F-%D1%80%D0%B8%D0%B7%D0%B8%D0%BA%D0%B0%D0%BC%D0%B8-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8/>
15. Черноног О. Стратегія кібероборони України. Збірник наукових праць BITI. 2017. № 4. С. 30-37.
URL: https://www.researchgate.net/publication/380979172_STRATEGIA_KIBEROBORONI_UKRAINI
16. AbuHmed T., Mohaisen A., Nyang D. A Survey on Deep Packet Inspection for Intrusion Detection Systems. URL: https://www.researchgate.net/publication/1913283_A_Survey_on_Deep_Packet_Inspection_for_Intrusion_Detection_Systems
17. ACM Digital Library. URL: <https://dl.acm.org/>

18. Ariel L'opez Gonz'alez, Mailyn Moreno-Espino, Ariadna Claudia Moreno Rom'an, Yahima Hadfeg Fern'andez, Nayma Cepero P'erez. Ethics in Artificial Intelligence: an Approach to Cybersecurity. *Inteligencia Artificial*. 2024. 27(73). Pp. 38-54. DOI: 10.4114/intartif.vol27iss73pp38-54.
19. Ayush Mishra, Ujwala Bendale. Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices. *International Journal of Law*, 2024. Vol. 10, Issue 1. Pp. 185-187.
URL: <https://www.lawjournals.org/assets/archives/2024/vol10issue1/10037.pdf>
20. Breton Thierry. A European Cyber Shield to step up our collective resilience | Opening of the International Cybersecurity Forum. 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2145
21. Carroll Jami M. The U.S. National Cybersecurity Strategy: A Vehicle with an International Journey. *European Conference on Cyber Warfare and Security*. 2024. 23(1). Pp.107-115. DOI:10.34190/eccws.23.1.2300
22. CERT-UA (офіційний сайт урядової команди реагування на комп'ютерні надзвичайні події України). URL: <https://cert.gov.ua/>
23. China's national cyberspace security strategy. URL: <https://dig.watch/resource/chinas-national-cyberspace-security-strategy>
24. CISA. *Joint Cyber Defense Collaborative (JCDC)* (2021). URL: <https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative>
25. CISA. The Case for Memory Safe Roadmaps: Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously, 2023. URL: <https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf>
26. CISA. ORCA Security. URL: <https://orca.security/glossary/cisa/>
27. CISA. Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software, 2023. URL: <https://www.govinfo.gov/content/pkg/FR-2023-12-20/pdf/2023-27948.pdf>

28. CISA. StopRansomware.gov – U.S. Government’s Official One-Stop Resource to Stop Ransomware (2021). URL: <https://www.cisa.gov/stopransomware>
29. Computer Security Resource Center.. URL: <https://csrc.nist.gov/>
30. Creemers R. Cybersecurity Law and Regulation in China: Securing the Smart State. *China Law and Society Review*. 2023. 6 (2021). C. 111–145
31. Cyber Diplomacy Toolbox. URL: <https://www.cyber-diplomacy-toolbox.com/>
32. Cybersecurity & Infrastructure Security Agency (CISA). Department of Homeland Security (DoHS). URL: <https://futureoflife.org/us-agency/cybersecurity-and-infrastructure-security-agency-cisa/>
33. Cybersecurity Law Of The People’s Republic Of China. URL: https://www.dataguidance.com/sites/default/files/en_cybersecurity_law_of_the_peoples_republic_of_china_1.pdf
34. Cybersecurity Laws and Regulations: Global Perspectives. Legal Vidhiya. URL: <https://legalvidhiya.com/cybersecurity-laws-and-regulations-global-perspectives/>
35. Cybersecurity 2026. South Korea. URL: <https://practiceguides.chambers.com/practice-guides/cybersecurity-2026/south-korea>
36. Cyber Solidarity Act (Proposal, 18.4.2023). URL: https://www.eu-cyber-solidarity-act.com/Article_21.html
37. Cyber Solidarity Act | Updates, Compliance. URL: <https://www.eu-cyber-solidarity-act.com/>
38. Dharmapurikar S., Krishnamurthy P., Sproull T., Lockwood J. Deep packet inspection using parallel Bloom filters. *IEEE Computer Society*. 2004. Pp.52-54. URL: https://www.researchgate.net/publication/3215373_Deep_packet_inspection_using_parallel_Bloom_filters
39. ED 21-01: Mitigate SolarWinds Orion Code Compromise. URL: <https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise-closed>

40. European Commission. Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. URL: <https://www.eur-lex.europa.eu>
41. European Commission. Proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (Cyber Solidarity Act). COM(2023) 209 final. URL: <https://www.eur-lex.europa.eu>
42. European Parliament and Council. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: <https://www.eur-lex.europa.eu>
43. European Parliament and Council. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). URL: <https://www.eur-lex.europa.eu>
44. Ibo van de Poel. Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security. *The Ethics of Cybersecurity*. Vol. 21. Pp. 45-71
45. Institute of Risk Management. Cyber risk. URL: <https://www.theirm.org/what-we-say/thought-leadership/cyber-risk/>
46. Introduction to Cyberethics. URL: <https://www.geeksforgeeks.org/cybersecurity/what-is-cyberethics/>
47. Ismail, R., Kurnia, R., Brata, Z. A., Nelistiani, G. A., Heo, S., Kim, H., & Kim, H. Toward robust security orchestration and automated response in security operations centers with a hyper-automation approach using agentic artificial intelligence. *Information*, 2025. 16(5), 365. DOI: <https://doi.org/10.3390/info16050365>
48. Japan Deep Packet Inspection and Processing Market Research Report. URL: <https://www.linkedin.com/pulse/japan-deep-packet-inspection-processing-market-research-qlrie>

49. JRTF: A Joint Ransomware Task Force by FBI and CISA. FBI Cyber Division. URL: https://www.linkedin.com/posts/fbicyber_fbi-activity-7231722587263815680-6ne9
50. Kennedy A., Wang Xiaojun, Liu Zhen. Ultra-High Throughput String Matching for Deep Packet Inspection. *Design, Automation and Test in Europe, 2010, Dresden, Germany, March 8-12*. DOI:10.1109/DATE.2010.5457172. URL: https://www.researchgate.net/publication/221340478_Ultra-high_throughput_string_matching_for_Deep_Packet_Inspection
51. Kyiv International Cyber Resilience Forum 2026 19-20th February. URL: <https://cyberforumkyiv.org/en>
52. Lampton, D. Xi Jinping and the National Security Commission: Policy coordination and political power. *Journal of Contemporary China*. 2015. 24, № 95. С. 759–777.
53. Matsubara Mihoko. Japan's Cybersecurity Policies. Japan in an Era of Geopolitics. Pp. 246-249. URL: <https://www.kas.de/documents/d/japan/22>
54. Microsoft Digital Defense Report 2020: Cyber Threat Sophistication on the Rise. URL: <https://www.microsoft.com/en-us/security/blog/2020/09/29/microsoft-digital-defense-report-2020-cyber-threat-sophistication-rise/>
55. Ministry of Economy, Trade and Industry (METI). Cybersecurity Management Guidelines for Japanese Enterprise Executives Ver. 3.0. 52 p. URL: https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v3.0_en.pdf
56. Min Jiang. Cybersecurity Policies in China. *CyberBRICS*. 2021. pp.183-226. DOI:10.1007/978-3-030-56405-6_5
57. National Computer Network Emergency Response Technical Team/Coordination Center of China. URL: <https://www.cert.org.cn/publish/english/index.html>
58. NIST. Cybersecurity Framework (CSF) та Secure Software Development Framework (SSDF). URL: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-218.pdf>

59. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024. 27 p. DOI: <https://doi.org/10.6028/NIST.CSWP.29>
60. Ohrimenco S., Cernei V. Cybersecurity risk. Economic Security in the Context of Systemic Transformations, international conference (3 ; 2023; Proceedings of International Conference "Economic Security in the Context of Systemic Transformations", 3rd Edition, December 7-8 2023 / drafting committee: Tatiana Bucos [et al.]: SEP ASEM, 2024. 271 p.: fig., tab. https://www.researchgate.net/publication/378746843_CYBERSECURITY_RISK
61. Otmar Lendl. The European Cyber Shield. URL: <https://www.cert.at/en/downloads/papers/the-european-cyber-shield>
62. Post-Quantum Cryptography. URL: <https://csrc.nist.gov/projects/post-quantum-cryptography>
63. Privacy and Ethical Considerations in IoT: Balancing Innovation and Data Protection. Nechnology Innovators. The New-age Knowledge Platform. URL: <https://www.technology-innovators.com/privacy-and-ethical-considerations-in-iot-balancing-innovation-and-data-protection/>
64. Refsdal, Atle, et al. Cyber-risk management. Springer International Publishing, 2015. p. 33-47.
65. Saffady W. Managing Information Risks: Threats, Vulnerabilities, and Response. Rowman & Littlefield Publishers, 2020. 257 p.
66. A snapshot of Cybersecurity in the EU. <https://www.eurelectric.org/wp-content/uploads/2024/11/A-Eurelectric-snapshot-of-Cybersecurity-2024-11-18-FINAL.pdf>
67. South Korean National Cybersecurity Strategy. URL: <https://dig.watch/resource/south-korean-national-cybersecurity-strategy>
68. Souza G. An Analysis of the United States Cybersecurity Strategy. Center for Development for Security Excellence Defense Security Service, 2015. 26 p.
69. Sun Y., Zhang Z., Wang X., and Li J. MOSS: An Open Conversational Large Language Model. *Machine Intelligence Research*. 2024. 21(5). DOI:[10.1007/s11633-024-1502-8](https://doi.org/10.1007/s11633-024-1502-8)

URL: https://www.researchgate.net/publication/380745738_MOSS_An_Open_Conversational_Large_Language_Model

70. Vakulyk O., Petrenko P., Kuzmenko I., Pochtovyi M., Orlovskiy R. Cybersecurity as a Component of The National Security of the State. *Journal of security and sustainability issues*. 2020. Vol.9. № 3. Pp. 775-784. DOI: [https://doi.org/10.9770/jssi.2020.9.3\(4\)](https://doi.org/10.9770/jssi.2020.9.3(4))

71. What is cybersecurity? IBM Corp. URL: <https://www.ibm.com/think/topics/cybersecurity#:~:text=Cybersecurity%20is%20the%20practice%20of,and%20specifically%2C%20cyber%20risk%20management>.

72. What is cyber risk management? IBM. URL: <https://www.ibm.com/think/topics/cyber-risk-management>

73. Zadeh A., Lavine B., Zolbanin H., Hopkins D. A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decision Analytics Journal*. 2023. Vol.9. URL: <https://doi.org/10.1016/j.dajour.2023.100328>

74. Zhang Y., Li H., Chen W., Zhao, J. Large Language Models in Cybersecurity Applications: Vulnerabilities and Defense Techniques. *Cybersecurity Advances*. 2024. 12. № 3. Pp. 45–67.

URL: https://www.researchgate.net/publication/393852332_Large_Language_Models_in_Cybersecurity_Applications_Vulnerabilities_and_Defense_Techniques.

75. Zhylin A., Beliaivsky V. Bakalynsky O. NIST CSF 2.0: New Cybersecurity Framework from the National Institute of Standards and Technology of the United States. *Ukrainian Scientific Journal of Information Security*, 2024, vol. 30, issue 1, pp. 73-76.