ISSN 1998-7927(print) ISSN 2664-6498 (online)

DOI: https://doi.org/10.33216/1998-7927-2026-303-5-87-100

УДК 004.056:005.334(477+4-6ЄС)

ОЦІНКА РІВНЯ КІБЕРЗАХИСТУ В ОРГАНІЗАЦІЯХ УКРАЇНИ ТА КРАЇН ЄС: ПОРІВНЯЛЬНИЙ АНАЛІЗ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ

Сердюков К.С.

ASSESSMENT OF THE LEVEL OF CYBER PROTECTION IN ORGANIZATIONS OF UKRAINE AND EU COUNTRIES: COMPARATIVE ANALYSIS AND DIRECTIONS FOR IMPROVEMENT

Serdiukov K.S.

Стрімке зростання кількості та складності кіберзагроз безпосередньо впливає на стабільність функціонування організацій у різних секторах економіки. В умовах цифрової трансформації та інтеграції України до європейського кіберпростору особливої ваги набуває порівняльний аналіз рівня кіберзахисту з країнами ЄС для виявлення наявних розривів і слабких місць. Результати такого дослідження є важливими для формування ефективної державної та корпоративної політики у сфері кібербезпеки та підвищення кіберстійкості організацій. Метою дослідження є здійснення порівняльного аналізу рівня кіберзахисту в організаціях України та країн Європейського Союзу на основі визначених критеріїв та індикаторів, а також обґрунтування напрямів його вдосконалення з урахуванням сучасних міжнародних стандартів і найкращих практик у сфері кібербезпеки. У дослідженні використано комплекс загальнонаукових і спеціальних методів пізнання, що забезпечують всебічний аналіз рівня кіберзахисту в організаціях України та країн ЄС. Зокрема, застосовано системний підхід для розгляду кіберзахисту як цілісної багаторівневої системи, а також порівняльний аналіз для виявлення спільних рис і відмінностей у національних моделях кібербезпеки. Метод контент-аналізу використано для дослідження нормативно-правових актів і міжнародних стандартів у сфері кіберзахисту, тоді як індикаторний підхід дозволив оцінити рівень зрілості кіберзахисних систем організацій. Крім того, застосовано методи узагальнення та синтезу для формування обґрунтованих висновків і визначення напрямів удосконалення кіберзахисту. Розглянуто сутність кібербезпеки та кіберстійкості, сучасні підходи до їх забезпечення, а також основні міжнародні моделі оцінювання рівня кіберзахисту. Досліджено сучасні кіберзагрози та їх вплив на організації. Проаналізовано законодавчу базу України та ЄС у сфері кіберзахисту, зокрема NIS2, GDPR та українські нормативні акти, а також оцінити рівень їх гармонізації. Проведено порівняльний аналіз рівня кіберзахисту організацій України та країн ЄС. Оцінено вплив воєнних та кризових умов на кібербезпеку України. Визначено напрями вдосконалення кіберзахисту організацій. Сформульовано практичні рекомендації щодо підвищення кіберстійкості, впровадження сучасних технологій захисту та адаптації до стандартів ЄС. Наукова новизна дослідження полягає у систематизації підходів до порівняльної оцінки рівня кіберзахисту організацій України та країн ЄС на основі індикаторної моделі, а також у визначенні ключових розривів між національними та європейськими практиками.

Ключові слова: *цифрова трансформація, кіберпростір, кіберзагрози, кіберзахист, організація, нормативно-правова база, управління ризиками, інтеграція.*

Вступ. Сучасний етап розвитку цифрової економіки характеризується одночасним прискоренням цифрової трансформації та різким ускладненням кіберзагроз. В умовах гібридної війни кіберпростір фактично перетворився на окремий домен протистояння, де атаки на інформаційні системи державних органів, критичну інфраструктуру та бізнес-структури мають не лише технічний, а й стратегічний характер. Для України це питання

набуває особливої ваги, оскільки кібероперації використовуються як інструмент впливу поряд із традиційними військовими діями. Паралельно спостерігається стрімке зростання кількості та складності кібератак як в Україні, так і в країнах Європейського Союзу [1, с. 48]. Організації стикаються з масовими випадками шкідливого програмного забезпечення, фішингових кампаній, атак типу ransomware та цілеспрямованих APT-інцидентів. При цьому цифровізація бізнес-процесів, перехід до хмарних технологій та розширення віддаленої роботи створюють додаткові вразливості, які активно використовуються зловмисниками. У результаті питання ефективного кіберзахисту стає критичним як для державного сектору, так і для приватного бізнесу [2, с. 235].

У цих умовах кіберстійкість набуває статусу ключового елемента національної та економічної безпеки. Вона визначає здатність держави та організацій не лише протидіяти кібератакам, але й швидко відновлювати функціонування після інцидентів, мінімізуючи їхні наслідки. Для України це також пов'язано з процесом євроінтеграції та необхідністю адаптації до стандартів ЄС у сфері кібербезпеки, зокрема вимог директиви NIS2. Таким чином, дослідження рівня кіберзахисту організацій України та країн ЄС є актуальним як з наукової, так і з практичної точки зору, оскільки дозволяє визначити розриви, виявити слабкі місця та сформувати ефективні напрями їх подолання [3, с. 75].

У сучасних умовах інтенсивної цифрової трансформації економіки та суспільних процесів кібербезпека перетворюється на один із ключових елементів забезпечення стійкого функціонування організацій. Поширення цифрових технологій, хмарних сервісів, віддалених моделей роботи та автоматизованих систем управління супроводжується суттєвим зростанням кіберризиків. Кіберзлочинність стає більш організованою, технологічно складною та орієнтованою на критичну інфраструктуру, бізнес-сектор і державні установи. У таких умовах ефективний кіберзахист виступає не лише технічною необхідністю, а й стратегічною складовою національної та організаційної безпеки [1, с. 48].

Актуальність дослідження посилюється процесами європейської інтеграції України, що передбачають гармонізацію національного законодавства та практик у сфері кібербезпеки з нормативними рамками Європейського Союзу. ЄС сформував комплексну систему кіберзахисту, яка базується на ризик-орієнтованому підході, обов'язкових вимогах до управління кіберінцидентами, стандартах інформаційної безпеки (зокрема ISO/IEC 27001) та новітніх регуляторних актах, таких як NIS2 Directive і GDPR [3, с. 75]. Водночас в Україні система кіберзахисту перебуває у стані активного розвитку, що зумовлює необхідність детального аналізу її ефективності у порівнянні з європейськими практиками.

Аналіз сучасних українських наукових публікацій демонструє, що дослідження у сфері кібербезпеки розвиваються досить інтенсивно, однак залишаються фрагментованими за тематичними напрямами та методологічною глибиною. Умовно їх можна поділити на кілька груп: роботи, присвячені національній безпеці та критичній інфраструктурі, дослідження впливу гібридної війни, нормативно-правові аспекти, а також оглядові праці загального характеру. Більшість досліджень, зокрема праці А.В. Цьоменка [4, с. 370], О.І. Червякова [5, с. 511] розглядають кібербезпеку переважно як елемент національної безпеки держави. Такий підхід є логічним у контексті війни в Україні, однак він часто звужує проблематику до рівня державних структур, залишаючи поза увагою корпоративний сектор та практичні механізми кіберзахисту організацій. У працях З.І. Книш [6, с. 59] та Ю.В. Завгородньої [7, с. 33], що стосуються правового регулювання, основна увага приділяється формуванню законодавчої бази України та її гармонізації з європейськими стандартами.

О. Гоманюк [8, с. 19] розглядає кібербезпеку як складову міжнародної та національної безпеки, підкреслюючи зростання кіберзагроз для державних інституцій та критичної інфраструктури. В.М. Василенко [9, с. 782] фокусується на ролі територіальних громад у забезпеченні цифрової безпеки в умовах гібридних загроз. Сильним аспектом є акцент на взаємодії поліції, держави та місцевого рівня, що відповідає сучасній децентралізованій моделі управління безпекою. С. Храмов та І. Опірський [10, с. 187] аналізували структуру та динаміку кібератак проти України під час повномасштабної війни. Особливу увагу приділено DDoS-атакам, шкідливому ПЗ та інформаційним операціям. Стаття Г.Л. Бондар [11, с. 30] присвячена аналізу кібератак на Україну в контексті початку повномасштабного вторгнення. Розглядаються атаки на державні органи та критичну інфраструктуру. А. Лисеюк, Т. Свінцицька [12,

с. 89] досліджували розвиток міжнародного співробітництва у сфері кібербезпеки та правового регулювання. Автори акцентували увагу на міжнародних механізмах; аналізі правових рамок; визначали актуальність для євроінтеграції України. А. Ільєнко, В. Телющенко, О.Дубчак [13, с. 150] зосереджені на аналізі кіберзагроз критичній інфраструктурі України та інших країн. Автори детально розглядають типи атак (фішинг, соціальна інженерія, шкідливе ПЗ), а також їх вплив на енергетику, транспорт і державні системи. Незважаючи на значну кількість наукових праць, присвячених питанням кібербезпеки, недостатньо дослідженими залишаються аспекти комплексного порівняльного оцінювання рівня кіберзахисту організацій України та країн ЄС на основі єдиних індикаторних підходів. Особливо актуальним є виявлення системних розривів у нормативному, організаційному та технологічному забезпеченні кібербезпеки, а також визначення практичних напрямів їх подолання.

Метою роботи є здійснення порівняльного аналізу рівня кіберзахисту в організаціях України та країн Європейського Союзу на основі системи критеріїв та індикаторів, а також обґрунтування напрямів його вдосконалення з урахуванням міжнародних стандартів і найкращих практик у сфері кібербезпеки.

Для досягнення поставленої мети визначено такі завдання:

– проаналізувати сучасні кіберзагрози та їх вплив на функціонування організаційних систем;

– дослідити міжнародні стандарти та регуляторні фреймворки у сфері кіберзахисту;

– здійснити порівняльний аналіз рівня кіберзахисту організацій України та ЄС;

– оцінити рівень зрілості систем кіберзахисту з використанням індикаторних моделей;

– обґрунтувати напрями вдосконалення кіберзахисту з урахуванням європейського досвіду.

Виклад основного матеріалу дослідження. Кіберзахист організацій — це сукупність організаційних, технічних, правових і управлінських заходів, спрямованих на запобігання, виявлення та нейтралізацію кіберзагроз, а також на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів. У сучасному розумінні кіберзахист охоплює не лише захист інформаційних систем від несанкціонованого доступу, але й комплексне управління ризиками, пов’язаними з використанням цифрових технологій у діяльності організації. Його основними завданнями є [10, с. 187]:

- запобігання кібератакам (превентивний рівень);
- виявлення інцидентів інформаційної безпеки;
- реагування на кіберінциденти;
- відновлення нормального функціонування систем після атак.

Концептуально кіберзахист базується на міжнародних стандартах, зокрема ISO/IEC 27001 та NIST Cybersecurity Framework, які визначають структурований підхід до управління ризиками інформаційної безпеки та побудови систем захисту в організаціях. Кіберстійкість (cyber resilience) — це здатність організації не лише протистояти кіберзагрозам, але й зберігати або швидко відновлювати свою функціональність під час та після кіберінцидентів, мінімізуючи їхній негативний вплив. На відміну від традиційного кіберзахисту, який орієнтований переважно на запобігання атакам, кіберстійкість передбачає [2, с. 235]:

- прийняття факту неминучості кібератак;
- забезпечення безперервності бізнес-процесів;
- швидке відновлення критичних систем;
- адаптацію до нових типів загроз.

Кіберстійкість є більш сучасною концепцією, яка активно використовується в політиках Європейського Союзу, зокрема в межах директиви NIS2, що акцентує увагу на здатності організацій забезпечувати безперервність послуг навіть у разі масштабних кіберінцидентів. Кіберзахист і кіберстійкість є взаємодоповнювальними концепціями. Кіберзахист формує перший рівень оборони — запобігання та реагування на атаки, тоді як кіберстійкість забезпечує здатність організації функціонувати навіть у випадку успішного проникнення в систему. У сучасних умовах цифрової трансформації та зростання складності кібератак ефективна модель безпеки організації передбачає інтеграцію обох підходів у єдину систему управління ризиками кібербезпеки [6, с. 59]. Таким чином, кіберзахист можна розглядати як базовий рівень забезпечення інформаційної безпеки організації, тоді як кіберстійкість виступає стратегічним розвитком цієї концепції, орієнтованим на довгострокову стабільність, адаптивність та безперервність діяльності в умовах постійних кіберзагроз.

Таблиця 1

Основні моделі оцінки кібербезпеки організацій

Критерій	NIST Cybersecurity Framework (CSF)	ISO/IEC 27001	ENISA Maturity Models
Призначення моделі	Управління кіберризиками та побудова системи захисту	Створення системи управління інформаційною безпекою (ISMS)	Оцінка рівня кіберзрілості організації або держави
Основний підхід	Ризик-орієнтований	Процесно-управлінський	Модель зрілості (maturity-based)
Структура	5 функцій: Identify, Protect, Detect, Respond, Recover	PDCA-цикл (Plan–Do–Check–Act) + вимоги контролів	Рівні зрілості (від початкового до оптимізованого)
Кількісна оцінка рівня	Немає чіткої шкали	Частково (через аудит і сертифікацію)	Так (рівні зрілості організації)
Сертифікація	Ні	Так (міжнародна сертифікація ISO)	Ні
Сфера застосування	Переважно США, глобальне використання	Глобальна, універсальна для організацій	ЄС, державні та стратегічні структури
Гнучкість впровадження	Висока	Середня / низька (через стандартизовані вимоги)	Середня
Орієнтація на порівняння (Україна–ЄС)	Обмежена	Обмежена	Висока (основна перевага)
Недоліки	Відсутність сертифікації, нечіткі метрики	Висока складність, дороговартісність	Обмежена стандартизація та деталізація

Джерело: сформовано автором на основі [14-16]

Сучасні підходи до оцінки рівня кібербезпеки організацій базуються на міжнародних стандартизованих моделях, які дозволяють системно аналізувати стан захисту інформаційних систем, рівень управління ризиками та загальну кіберзрілість. Серед найбільш визнаних у світовій практиці є NIST Cybersecurity Framework (CSF), ISO/IEC 27001 та моделі зрілості ENISA, які застосовуються відповідно у США, глобальній практиці та країнах Європейського Союзу. Кожна з цих моделей має власну методологічну основу, ступінь формалізації та сферу застосування, що зумовлює необхідність їх порівняльного аналізу [2, с. 235]. У межах даного дослідження такі моделі розглядаються як взаємодоповнюючі інструменти, що дозволяють оцінити рівень кіберзахисту організацій України та країн ЄС з різних методологічних позицій — від ризик-орієнтованого управління до оцінки зрілості кіберсистем (табл. 1).

Розглянуті моделі кібербезпеки мають різну функціональну спрямованість і не можуть бути взаємозамінними. NIST CSF забезпечує гнучку систему управління кіберризиками, ISO/IEC 27001 формує структуровану систему управління інформаційною безпекою з можливістю сертифікації, а ENISA maturity models дозволяють оцінювати рівень кіберзрілості організацій і здійснювати порівняльний аналіз між країнами та секторами.Найбільш ефективним підходом до оцінки рівня кіберзахисту організацій є комбіноване використання зазначених моделей, що дозволяє поєднати управлінську, нормативну та аналітичну складові. Саме така інтеграція є особливо актуальною в контексті порівняння України та країн Європейського Союзу, де рівень впровадження стандартів кібербезпеки суттєво відрізняється [1, с. 48].

Сучасне кіберсередовище характеризується стрімким зростанням складності та масштабів кіберзагроз, що суттєво впливають як на окремі організації, так і на національні інформаційні системи в цілому. Найбільш небезпечними серед них є цілеспрямовані APT-атаки, програми-вимагачі (ransomware) та атаки на критичну інфраструктуру, які відрізняються високим рівнем організації, технологічною складністю та значними наслідками для безпеки держав і бізнесу [6, с. 59]. У наведеній табл. 2 систематизовано основні типи сучасних

кіберзагроз за їх сутністю, цілями, методами реалізації та потенційними наслідками для організацій. Такий підхід дозволяє комплексно оцінити характер кіберризиків і визначити ключові напрями посилення кіберзахисту в умовах цифрової трансформації та гібридних загроз.

Проведений аналіз основних типів кіберзагроз свідчить про їхню еволюцію від ізольованих технічних атак до складних, багатовекторних кібероперацій, які мають стратегічний характер. APT-атаки, ransomware та атаки на критичну інфраструктуру становлять найбільшу небезпеку для сучасних організацій, оскільки поєднують технічні, фінансові та геополітичні аспекти впливу. Це підтверджує необхідність впровадження комплексних систем кіберзахисту та кіберстійкості в організаціях України та країн ЄС. Ефективна протидія таким загрозам потребує не лише технічних засобів захисту, а й впровадження комплексних моделей кіберзахисту та кіберстійкості, що враховують багаторівневий характер сучасного кіберпростору та специфіку організацій як в Україні, так і в країнах Європейського Союзу [8, с. 19].

Геополітичні фактори сьогодні відіграють визначальну роль у формуванні сучасної архітектури кібербезпеки. Кіберпростір став невід'ємною складовою міжнародного протистояння, де держави використовують цифрові технології як інструмент стратегічного впливу. Особливо це проявляється в контексті російсько-української кібервійни, яка суттєво вплинула на підходи до кіберзахисту як в Україні, так і в країнах Європейського Союзу [11, с. 30]. У табл. 3 систематизовано ключові геополітичні фактори та їхній вплив на стан кібербезпеки України та ЄС. Такий підхід дозволяє порівняти особливості формування кіберполітики в різних умовах, а також визначити спільні тенденції та відмінності у рівні кіберзахисту та кіберстійкості.

Геополітичні фактори є одним із ключових детермінантів розвитку кібербезпеки в сучасному світі. Для України визначальним чинником виступає російсько-українська кібервійна, яка формує необхідність функціонування систем кіберзахисту в умовах постійних атак. Для Європейського Союзу основним драйвером є розвиток нормативно-правової бази та посилення кіберстійкості через впровадження директиви NIS2 [19]. Водночас посилення міжнародної співпраці між Україною, ЄС та НАТО сприяє зближенню підходів до кібербезпеки, однак зберігається асиметрія у ресурсному забезпеченні та рівні кіберзрілості. Це підкреслює необхідність подальшої гармонізації стандартів та розвитку спільних механізмів протидії кіберзагрозам [13, с. 150].

Таблиця 2

Основні загрози сучасного кіберсередовища

Тип загрози	Зміст	Основні цілі атак	Методи реалізації	Наслідки для організацій
APT-атаки (Advanced Persistent Threats)	Тривалі, цілеспрямовані та приховані кібероперації з високим рівнем складності	Державні органи, критична інфраструктура, великі корпорації	Zero-day вразливості, фішинг, шкідливе ПЗ, соціальна інженерія	Викрадення даних, довготривалий несанкціонований доступ, промислове/державне шпигунство
Ransomware (програми-вимагачі)	Шкідливе ПЗ, що блокує або шифрує дані з вимогою викупу	Бізнес-організації, лікарні, освітні заклади, державні установи	Фішингові листи, експлуатація вразливостей, заражені файли	Втрата доступу до даних, фінансові збитки, зупинка бізнес-процесів
Атаки на критичну інфраструктуру	Кібератаки, спрямовані на стратегічно важливі системи держави	Енергетика, транспорт, фінанси, телекомунікації, держреєстри	DDoS-атаки, шкідливе ПЗ, проникнення в SCADA/ICS системи	Порушення роботи державних і соціальних систем, економічні втрати, загроза національній безпеці

Джерело: сформовано автором на основі [1, с. 48; 3, с. 75; 17, с. 344]

Таблиця 3

Вплив геополітичних факторів на кібербезпеку (Україна–ЄС–російська кібервійна)

Геополітичний фактор	Україна	Європейський Союз	Вплив на кібербезпеку
Російсько-українська кібервійна	Постійні масовані кібератаки на держсектор і критичну інфраструктуру; кіберзахист здійснюється в умовах війни	Посилення кіберзагроз через розширення конфлікту; підтримка України	Перехід до режиму кібероборони; зростання ролі кіберстійкості
Гібридна війна як стратегія впливу	Поєднання кібератак, інформаційних операцій та військових дій	Визнання кіберпростору як елементу безпеки НАТО/ЄС	Розширення поняття кібербезпеки до рівня нацбезпеки
Євроінтеграція України	Гармонізація законодавства з NIS2 та стандартами ЄС	Підтримка уніфікації кіберполітик	Підвищення стандартів кіберзахисту в Україні
Регуляторна політика ЄС (NIS2)	Часткова імплементація, нерівномірне впровадження в організаціях	Повноцінне впровадження обов'язкових вимог кіберстійкості	Підвищення вимог до кіберзахисту організацій
Міжнародна кіберкооперація (Україна–ЄС–НАТО)	Отримання технічної та аналітичної підтримки	Розширення програм кібердопомоги та обміну даними	Посилення обміну інформацією про загрози
Економічна та технологічна нерівність	Обмежені ресурси, дефіцит кадрів кібербезпеки	Високий рівень фінансування та технологій	Асиметрія рівня кіберзахисту між регіонами

Джерело: сформовано автором на основі [18-22]

Нормативно-правове регулювання у сфері кібербезпеки є ключовим чинником формування ефективної системи захисту інформаційних ресурсів як на рівні держави, так і на рівні окремих організацій. В умовах стрімкого розвитку цифрових технологій, зростання кібератак та посилення геополітичної напруги законодавство України та Європейського Союзу зазнає активних змін і оновлень [11, с. 30]. У табл. 4 систематизовано найновіші нормативно-правові акти України та ЄС у сфері кібербезпеки, які визначають сучасні підходи до кіберзахисту, управління ризиками, реагування на кіберінциденти та забезпечення кіберстійкості. Такий порівняльний аналіз дозволяє оцінити рівень розвитку законодавчої бази та ступінь її гармонізації між Україною та Європейським Союзом.

Законодавча база Європейського Союзу у сфері кібербезпеки є більш зрілою, системною та орієнтованою на забезпечення кіберстійкості, що підтверджується впровадженням директиви NIS2 та дією GDPR. Вона встановлює чіткі вимоги до організацій щодо управління кіберризиками, реагування на інциденти та відповідальності керівництва [16]. В Україні у 2025–2026 роках спостерігається активний процес оновлення нормативно-правової бази, спрямований на адаптацію до європейських стандартів. Водночас національна система кібербезпеки залишається на етапі трансформації, що проявляється у частковій імплементації принципів NIS2 та поступовому впровадженні сучасних механізмів кіберзахисту. Рівень гармонізації між Україною та ЄС можна визначити як перехідний із чіткою тенденцією до зближення, що є важливим етапом інтеграції України до європейського кіберпростору [12, с. 89].

У статті [29, с. 40] прямо зазначено, що статус кандидата в ЄС вимагає від України термінової гармонізації політики кібербезпеки з acquis ЄС (зокрема NIS2), а імплементація цієї директиви є ключовим напрямом реформ у сфері кіберзахисту. Гармонізація українського законодавства з правовими стандартами Європейського Союзу у сфері кібербезпеки сьогодні набуває стратегічного характеру, оскільки визначає не лише темпи євроінтеграції, а й реальну здатність держави протистояти сучасним кіберзагрозам. У цьому контексті особливо показовими є результати дослідження [29, с. 40], які здійснили комплексний аналіз відповідності української нормативно-правової бази вимогам директиви NIS2. Автори наголошують, що хоча Україна вже сформувала базову інституційну архітектуру кіберзахисту (зокрема через функціонування ДССЗЗІ, CERT-UA та прийняття профільного закону), рівень її інтегрованості в європейську систему залишається фрагментарним і потребує системного доопрацювання.

Таблиця 4

Нормативно-правові акти у сфері кібербезпеки Україна–ЄС

Нормативний акт	Ключовий зміст	Значення для кіберзахисту
Україна		
Стратегія кібербезпеки України (оновлення заходів)	Формування національної системи кіберстійкості, інтеграція з ЄС і НАТО	Визначає стратегічний напрям розвитку кіберзахисту
Порядок оцінювання стану кіберзахисту ІТС	Регламент оцінки рівня захищеності інформаційних систем	Запроваджує контроль і аудит кіберзахисту
Порядок реагування на кіберінциденти	Процедури виявлення та реагування на кібератаки	Підвищує оперативність реагування на загрози
Порядок взаємодії суб'єктів кібербезпеки	Координація між CERT-UA, держорганами та критичною інфраструктурою	Покращує міжвідомчу співпрацю
Стандарти кіберзахисту та криптографії	Оновлення технічних вимог до захисту інформації	Підвищує технічний рівень кіберзахисту
Європейський Союз		
NIS2 Directive	Обов'язкове управління кіберризиками та кіберстійкість критичних секторів	Формує єдину систему кібербезпеки в ЄС
GDPR	Захист персональних даних, контроль обробки інформації	Посилює кіберзахист даних громадян
EU Cybersecurity Strategy	Розвиток кіберстійкості та міжнародної кооперації	Підсилює стратегічний рівень кібербезпеки

Джерело: сформовано автором на основі [20; 23-28]

Адаптація до NIS2 у цьому процесі виступає ключовим вектором реформ, оскільки саме ця директива встановлює уніфіковані підходи до управління ризиками, інцидент-менеджменту, захисту критичної інфраструктури та відповідальності суб'єктів кіберпростору [21]. Дослідження демонструє, що українське законодавство вже частково імплементує окремі елементи NIS2, однак значні прогалини зберігаються у сфері сертифікації ІТ-продуктів, механізмів колективної кіберстійкості та координації між державними органами. Процес гармонізації має виходити за межі формального запозичення норм і передбачати трансформацію всієї системи управління кібербезпекою відповідно до європейської логіки — від централізованих адміністративних моделей до мережевих, інтегрованих та ризик-орієнтованих підходів. Імплементація цієї директиви стає не просто технічним завданням, а фундаментальною реформою, яка визначає подальший розвиток української системи кіберзахисту та її здатність функціонувати як повноцінний елемент європейського цифрового простору [22].

Аналіз динаміки кіберінцидентів у 2023–2025 роках свідчить про те, що кіберсередовище в Україні є значно більш агресивним порівняно з країнами Європейського Союзу. Насамперед це проявляється у масштабах і темпах зростання атак: якщо у 2022 році зафіксовано понад 200 цільових інцидентів, то вже у 2025 році їх кількість перевищила 5900, що означає майже трикратне збільшення. При цьому інтенсивність атак зросла до приблизно 15 інцидентів на добу, що вказує на фактичну відсутність «спокійних періодів» у кіберпросторі (рис. 1).

Додатково варто відзначити, що понад половина атак спрямована на державний сектор та об'єкти критичної інфраструктури, що суттєво відрізняє Україну від більшості країн ЄС, де структура атак є більш диверсифікованою і значна частка інцидентів припадає на приватний сектор. В українському випадку домінують цілеспрямовані атаки, пов'язані з діяльністю державних або проксі-груп, що свідчить про високий рівень організованості та стратегічний характер кіберзагроз [30].

Ключовою особливістю українського кіберсередовища є синхронізація кібератак із фізичними ударами, зокрема по енергетичній та телекомунікаційній інфраструктурі. Це формує принципово нову модель загроз, у якій кіберпростір виступає невід'ємною складовою бойових дій. На відміну від ЄС, де кіберінциденти здебільшого мають кримінальний або економічний характер, в

Україні вони виконують військово-стратегічні функції. Кіберсередовище України характеризується високою інтенсивністю, цілеспрямованістю та безперервністю атак, що дозволяє розглядати його як один із найбільш агресивних кіберпросторів у світі. Це, у свою чергу, визначає необхідність переходу від класичних моделей кіберзахисту до систем кіберстійкості, здатних функціонувати в умовах постійного тиску [32].

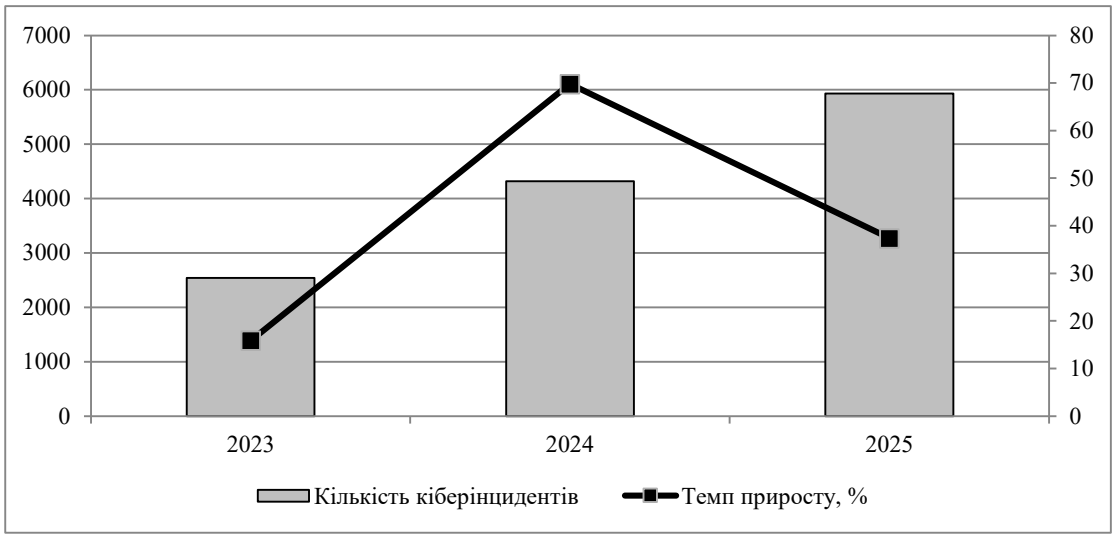

Рис.1. Динаміка кіберінцидентів в Україні за 2023–2025 рр.

Джерело: сформовано автором на основі [30-31]

Таблиця 5

Порівняльний аналіз рівня кіберзахисту організацій

Критерій оцінки	Україна	Країни ЄС
Рівень впровадження стандартів	Часткове впровадження міжнародних стандартів (ISO 27001, NIST), переважно у великих організаціях та державному секторі; відсутня повна уніфікація	Високий рівень стандартизації; обов'язкове застосування NIS2, GDPR, Cybersecurity Act; інтеграція стандартів у всі сектори економіки
Зрілість систем управління кіберризиками	Нерівномірна: високий рівень у державному секторі та критичній інфраструктурі, але недостатній у МСП; обмежена інтеграція risk-based підходів	Системний risk-based підхід; управління кіберризиками є частиною корпоративного управління; широке застосування безперервного моніторингу ризиків
Технічний рівень захисту	Використання базових і середніх технологій (IDS/IPS, SIEM, EDR), але часто фрагментовано; обмежене фінансування та залежність від окремих рішень	Високий рівень інтегрованих технологій (SIEM, SOC, Zero Trust, AI-based security); комплексні багаторівневі системи захисту
Ефективність реагування на інциденти	Наявні CERT-UA та державні механізми реагування, але є проблеми координації та швидкості реагування; відсутність єдиної платформи обміну даними	Висока ефективність завдяки інтегрованим CSIRT/ CERT-мережам, спільним платформам обміну інформацією (TIS), регулярним навчанням і координації
Інституційна та організаційна зрілість	Система формується; існують проблеми з координацією між органами та кадровим забезпеченням	Високий рівень інституційної координації; підхід «whole-of-society» із залученням держави, бізнесу та науки

Джерело: сформовано автором на основі [29, с. 40; 34, с. 60; 35, с. 79]

Порівняльний аналіз рівня кіберзахисту організацій України та країн ЄС доцільно здійснювати через систему ключових індикаторів, які відображають як управлінські, так і технічні аспекти кіберстійкості [33, с. 125]. У сучасних дослідженнях наголошується, що країни ЄС формують комплексні системи кібербезпеки, інтегруючи нормативні вимоги, технології та практики реагування в єдину модель, тоді як Україна перебуває на етапі активного становлення цієї системи та її адаптації до європейських стандартів (табл. 5).

Порівняння демонструє чітку асиметрію у рівні розвитку кіберзахисту організацій. У країнах ЄС сформовано зрілу модель, що базується на інтеграції регуляторних вимог, стандартизованих процесів управління ризиками та сучасних технологій. Така модель дозволяє забезпечити високий рівень кіберстійкості як у державному, так і в приватному секторі, зокрема через використання спільних механізмів реагування та обміну інформацією [34, с. 60].

В Україні, незважаючи на значний прогрес, система кіберзахисту організацій має перехідний характер. Вона характеризується нерівномірністю розвитку: окремі сегменти (критична інфраструктура, державні органи) демонструють достатньо високий рівень зрілості, тоді як бізнес-сектор, особливо малий і середній, залишається вразливим. Дослідження також вказують на системні проблеми, пов’язані з дефіцитом ресурсів, недостатньою координацією та фрагментацією інституційної структури [29, с. 40]. Ключовим завданням для України є перехід від фрагментарної моделі кіберзахисту до комплексної системи, орієнтованої на принципи NIS2: інтегроване управління ризиками, централізований обмін інформацією, підвищення ролі керівництва організацій та розвиток колективної кіберстійкості. Саме ці напрями визначають подальше скорочення розриву між Україною та країнами ЄС у сфері кібербезпеки [21].

Таблиця 6

Напрями вдосконалення кіберзахисту організацій

Напрям вдосконалення	Практична реалізація	Очікуваний ефект
Впровадження стандартів ЄС (NIS2, ISO 27001)	Аудит поточного стану, сертифікація СУІБ, інтеграція risk-based підходу	Підвищення відповідності міжнародним нормам та довіри партнерів
Розвиток систем управління кіберризиками	Формування реєстру ризиків, регулярна оцінка загроз, використання NIST CSF	Зниження ймовірності інцидентів та мінімізація їх наслідків
Модернізація технічної інфраструктури	Використання SIEM, EDR/XDR, Zero Trust Architecture, MFA	Підвищення рівня захищеності інформаційних систем
Захист критичної інфраструктури	Сегментація мереж, резервування, захист ICS/SCADA	Забезпечення безперервності функціонування ключових процесів
Підвищення кіберобізнаності персоналу	Проведення тренінгів, симуляцій фішингових атак, регулярні інструктажі	Зменшення людського фактора як головної причини інцидентів
Оптимізація реагування на інциденти	Створення SOC, впровадження playbooks, інтеграція CERT/CSIRT	Підвищення оперативності та ефективності реагування
Забезпечення безпеки ланцюгів постачання	Проведення аудитів постачальників, впровадження вимог NIS2 щодо supply chain	Зменшення ризиків через сторонні організації
Використання інноваційних технологій	Застосування AI/ML для виявлення загроз, автоматизація процесів безпеки	Підвищення точності виявлення атак та швидкості реагування
Розвиток міжорганізаційної співпраці	Обмін інформацією про загрози, участь у кібернавчаннях, інтеграція в європейські мережі	Підвищення колективної кіберстійкості
Інституційне зміцнення кіберзахисту	Призначення CISO, формування політик governance, інтеграція кібербезпеки в бізнес-процеси	Системність управління кібербезпекою на всіх рівнях

Джерело: авторська розробка

У сучасних умовах стрімкої цифровізації та зростання масштабів кіберзагроз питання вдосконалення кіберзахисту організацій набуває стратегічного значення. Особливої актуальності ця проблема набуває для України, яка функціонує в умовах постійного кібервпливу в рамках гібридної війни, а також одночасно інтегрується у європейський цифровий простір. Це зумовлює необхідність не лише підвищення рівня технічного захисту, а й комплексної трансформації управління кібербезпекою відповідно до сучасних міжнародних стандартів [34, с. 60]. У зв'язку з цим важливо визначити ключові напрями вдосконалення кіберзахисту, які охоплюють організаційні, технологічні та нормативні аспекти, що відображено у наведеній табл. 6.

Результати узагальнення дозволяють зробити висновок, що ефективне підвищення кіберстійкості організацій можливе лише за умови комплексного підходу, який поєднує впровадження міжнародних стандартів, модернізацію технічної інфраструктури, розвиток культури кібербезпеки та активізацію міжсекторної взаємодії. Ключовим вектором розвитку виступає адаптація до вимог ЄС, зокрема NIS2, що формує основу для гармонізації політик та підвищення рівня довіри до організацій на міжнародному рівні [21]. Водночас інтеграція інноваційних технологій і вдосконалення механізмів реагування на інциденти забезпечують здатність системи кіберзахисту оперативно адаптуватися до нових викликів. Сукупність зазначених заходів створює передумови для формування стійкої, гнучкої та ефективної системи кібербезпеки, здатної протидіяти сучасним загрозам [35, с. 79]. Удосконалення кіберзахисту організацій є безперервним процесом, що вимагає системного підходу, інвестицій у технології та людський капітал, а також адаптації до міжнародних стандартів. Реалізація зазначених рекомендацій дозволить підвищити рівень кіберстійкості, зменшити вразливість до сучасних загроз і забезпечити стабільність функціонування організацій у цифровому середовищі.

Висновки. Таким чином, встановлено, що сучасна система кібербезпеки функціонує в умовах суттєвого ускладнення загрозового середовища, що обумовлено як технологічними чинниками, так і геополітичними процесами. Для України визначальним фактором виступає повномасштабна кібервійна, яка трансформує підходи до забезпечення безпеки від реактивних до превентивно-адаптивних. У свою чергу, країни ЄС формують більш стабільну та системну модель кіберзахисту, базовану на уніфікованих стандартах, таких як NIS2, GDPR та ISO/IEC 27001.

Порівняльний аналіз показав, що рівень кіберзрілості організацій у ЄС є значно вищим за ключовими критеріями: ступінь впровадження стандартів, інтеграція систем управління ризиками, технологічна оснащеність та ефективність реагування на інциденти. Водночас в Україні спостерігається нерівномірність розвитку кіберзахисту між секторами, обмеженість ресурсів та дефіцит кваліфікованих кадрів. Gap-аналіз засвідчив найбільші розриви саме у сфері управління ризиками, інцидент-менеджменту та кадрового забезпечення.

Окремо слід підкреслити, що процес гармонізації українського законодавства з нормами ЄС, зокрема імплементація директиви NIS2, виступає ключовим інструментом підвищення рівня кіберзахисту. Водночас ефективність цього процесу залежить не лише від формального впровадження нормативних вимог, а й від їх практичної реалізації в діяльності організацій.

Важливим висновком є те, що кіберстійкість сучасних організацій формується не лише за рахунок технологічних рішень, а й завдяки комплексному поєднанню управлінських, кадрових і нормативних компонентів. Зокрема, критичне значення мають розвиток культури кібербезпеки, впровадження ризик-орієнтованих підходів та інтеграція сучасних технологій (SIEM, EDR, Zero Trust, AI-аналітика).

Таким чином, підвищення рівня кіберзахисту організацій в Україні потребує системних змін, спрямованих на зменшення розриву з країнами ЄС. Це включає масштабне впровадження міжнародних стандартів, розвиток інституційної спроможності, підвищення кваліфікації персоналу та активізацію міжнародної співпраці. Реалізація зазначених напрямів дозволить сформувати адаптивну, стійку та ефективну систему кібербезпеки, здатну протидіяти сучасним викликам і забезпечувати стабільне функціонування організацій в умовах цифрової трансформації.

Література

1. Wróblewski W., Wiśniewski M. Cybersecurity in the context of Hybrid Warfare in Ukraine: Analysis of its impact on the public sector and society in Poland. Central European Journal of Security Studies. 2023 Vol. 1, Issue 1. pp.48-60. DOI: 10.15804/CEJSS.2023105
2. Krawczyk D., et al. "Analysis of Information Security Under the Conditions of Hybrid War in Ukraine: Social Aspects. Management Systems in Production Engineering. 2024. vol. 32, no. 2. pp. 235-243. URL: https://doi.org/10.2478/mspe-2024-0023
3. Kelemen R. The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations. Connections: The Quarterly Journal. 2023. vol. 22, no. 2. Pp. 75-90 URL: https://doi.org/10.11610/Connections.22.2.55
4. Tsomenko A.V. Ensuring cybersecurity as a component of national security: modern challenges and mechanisms for countering threats. Науковий вісник Ужгородського Національного Університету. 2026. Серія ПРАВО. Випуск 93: частина 3. С. 370-374. DOI https://doi.org/10.24144/2307-3322.2026.93.3.51
5. Червяков О.І. Особливості забезпечення кібербезпеки як провідної складової національної безпеки України. Вісник Кримінологічної асоціації України. 2026. № 33(3). С. 511-518. DOI: https://doi.org/10.32631/vca.2024.3.47
6. Книш З. І. Кібербезпека: актуальний стан нормативно-правової бази та перспективи її розвитку. Історико-правовий часопис. 2025. № 24(1). С. 59–65. DOI: https://doi.org/10.32782/2409-4544/2025-1/8
7. Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2021. Випуск 4(52). С.33-38. DOI https://doi.org/10.20535/2308-5053.2021.4(52).248130
8. Гоманюк О. Кіберзагрози та глобальна безпека: від національних стратегій до міжнародної співпраці. Міжнародні відносини, суспільні комунікації та регіональні студії. 2024. №3 (20). С. 19-34. DOI 10.29038/2524-2679-2024-03-19-34
9. Василенко В.М. Роль громад у забезпеченні цифрової безпеки: партнерство з поліцією в умовах гібридних загроз. Вісник Кримінологічної асоціації України. 2026. № 33(3). С. 782-793. DOI: https://doi.org/10.32631/vca.2024.3.74
10. Храмов С., Опірський І. Аналіз поточного стану кібератак в Україні під час війни. Український журнал досліджень інформаційної безпеки. 2024. № 26 (1). С. 187–196. DOI: https://doi.org/10.18372/2410-7840.26.18842
11. Бондар Г.Л. Кібервійна в Україні та виклики національній безпеці: кібератаки на цифрову інфраструктуру (державні органи, критична інфраструктура та організації третього сектору). Державне управління та регіональний розвиток. 2022. №15. С. 30–67. DOI: https://doi.org/10.34132/pard2022.15.02
12. Лисеюк А., Свінцицька Т. Розвиток міжнародного співробітництва у сфері кібербезпеки: нормативно-правові засади та перспективи). Право та інноваційне суспільство. 2024. № 2(23). С. 89–95. URL: https://doi.org/10.37772/2309-9275-2024-2(23)-890
13. Ільєнко А., Телющенко В., Дубчак О. Сучасні кіберзагрози критичної інфраструктури україни та світу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. № 3(27). С. 150–164. DOI: https://doi.org/10.28925/2663-4023.2023.27.719
14. ISO/IEC 27001:2022. URL: https://www.iso.org/standard/27001
15. Ssessment of national cyber capabilities: what is the level of cybersecurity maturity of ukraine according to the enisa methodology? URL: https://understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_1_en.pdf
16. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
17. Живило Є. О. Мілітаризація викликів та загроз в кіберпросторі як операційному середовищі. Державне будівництво. 2024. № 1 (35). С. 344–359. DOI: https://doi.org/10.26565/1992- 2337-2024-1-26
18. Cyber defence. 2024. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence
19. EU cybersecurity: strategy and key policies. URL: https://www.consilium.europa.eu/en/policies/cybersecurity/
20. Directive (EU) 2022/2555 of the european parliament and of the council of 14 December 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
21. NIS2 Directive: securing network and information systems. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
22. ENISA aims to raise cybersecurity awareness and promote behavioural change. URL: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene)
23. Постанова «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури» від 31 грудня 2025 р. № 1799. URL:

https://zakon.rada.gov.ua/laws/show/en/1799-2025-%D0%BF#Text
24. Постанова «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» від 26 листопада 2025 р. № 1533. URL: https://zakon.rada.gov.ua/laws/show/en/1533-2025-%D0%BF#Text
25. Розпорядження «Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України» від 7 березня 2025 р. № 204-р. URL: https://zakon.rada.gov.ua/laws/show/en/204-2025-%D1%80#Text
26. Наказ «Про затвердження Порядку формування програм із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, технічної перевірки проекту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, розсилання, перевірки та перегляду стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, ведення їх каталогу та форм документів» від 16.12.2025 № 832. URL: https://zakon.rada.gov.ua/laws/show/en/z0147-26#Text
27. Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
28. Cybersecurity. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity
29. Krainiuk O., Yevseiev S., DidenkoN., Piksasov M. Transformation of the regulatory and legal framework for cybersecurity in Ukraine: analysis of compliance with the requirements of the nis2 directive and the cybersecurity act. Територія безпеки. 2025. Т.1, №3. С. 40-48. URL: https://doi.org/10.20998/3083-6298.2025.03.05
30. У 2024 році кількість кібератак українського кіберпростору зросла на 70%. 2025. URL: https://skilky-skilky.info/u-2024-rotsi-kilkist-kiberatak-ukrainskoho-kiberprostoru-zrosla-na-70/
31. Торік CERT-UA опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37%. 2026. URL: https://info.poda.gov.ua/news/251006
32. Хакери атакують. Від початку війни Україна пережила понад 200 кібератак — хто зараз у зоні ризику. 2024. URL: https://biz.nv.ua/ukr/markets/200-kiberatak-na-ukrajinski-ustanovi-ta-kompaniji-u-2022-roci-derzhspeczv-yazok-50388782.html
33. Боженко В., Пахненко О., Койбічук В. Досвід ЄС щодо розробки та впровадження національної стратегії кіберстійкості фінансового сектору. Цифрова економіка та економічна безпека : науково-практичний журнал. 2023. №8 (08). С. 125–129. DOI: https://doi.org/10.32782/dees.8-21
34. Котляров О. Ю., Бортнік Л. Л. Порівняльний аналіз сучасних систем захисту віртуальних мереж та їх методології. Сучасний захист інформації. 2024. № 4(60). С. 60-72. DOI: 10.31673/2409-7292.2024.040007
35. Пасічник В., Недошитко А. Інституційні механізми кібербезпеки: порівняльний аналіз практик України та країн НАТО. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2026. №15. С. 79–88. DOI: https://doi.org/10.31470/2786-6246-2026-15-79-88)

References

1. Wróblewski W., Wiśniewski M. Cybersecurity in the context of Hybrid Warfare in Ukraine: Analysis of its impact on the public sector and society in Poland. Central European Journal of Security Studies. 2023 Vol. 1, Issue 1. rr.48-60. DOI: 10.15804/CEJSS.2023105
2. Krawczyk D., et al. "Analysis of Information Security Under the Conditions of Hybrid War in Ukraine: Social Aspects. Management Systems in Production Engineering. 2024. vol. 32, no. 2. pp. 235-243. URL: https://doi.org/10.2478/mspe-2024-0023
3. Kelemen R. The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations. Connections: The Quarterly Journal. 2023. vol. 22, no. 2. Rr. 75-90 URL: https://doi.org/10.11610/Connections.22.2.55
4. Tsomenko A.V. Ensuring cybersecurity as a component of national security: modern challenges and mechanisms for countering threats. Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. 2026. Seriia PRAVO. Vypusk 93: chastyna 3. S. 370-374. DOI https://doi.org/10.24144/2307-3322.2026.93.3.51
5. Cherviakov O.I. Osoblyvosti zabezpechennia kiberbezpeky yak providnoi skladovoi natsionalnoi bezpeky Ukrainy. Visnyk Kryminolohichnoi asotsiatsii Ukrainy. 2026. № 33(3). S. 511-518. DOI: https://doi.org/10.32631/vca.2024.3.47
6. Knysh Z. I. Kiberbezpeka: aktualnyi stan normatyvno-pravovoi bazy ta perspektyvy yii rozvytku. Istoryko-pravovyi chasopys. 2025. № 24(1). S. 59–65. DOI: https://doi.org/10.32782/2409-4544/2025-1/8
7. Zavhorodnia Yu. V. Kiberbezpeka yak innovatsiinyi zakhyst u politychnomu prostori Ukrainy. Visnyk NTUU «KPI». Politolohiia. Sotsiolohiia. Pravo. 2021. Vypusk 4(52). S.33-38. DOI https://doi.org/10.20535/2308-5053.2021.4(52).248130
8. Homaniuk O. Kiberzahrozy ta hlobalna bezpeka: vid natsionalnykh stratehii do mizhnarodnoi spivpratsi. Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii. 2024. №3 (20). S. 19-34. DOI 10.29038/2524-2679-2024-03-19-34

9. Vasylenko V.M. Rol hromad u zabezpechenni tsyfrovoi bezpeky: partnerstvo z politsiieiu v umovakh hibrydnykh zahroz. Visnyk Kryminolohichnoi asotsiatsii Ukrainy. 2026. № 33(3). S. 782-793. DOI: https://doi.org/10.32631/vca.2024.3.74
10. Khramov S., Opirskyi I. Analiz potochnoho stanu kiberatak v Ukraini pid chas viiny. Ukrainskyi zhurnal doslidzhen informatsiinoi bezpeky. 2024. № 26 (1). S. 187–196. DOI: https://doi.org/10.18372/2410-7840.26.18842
11. Bondar H.L. Kiberviina v Ukraini ta vyklyky natsionalnii bezpetsi: kiberataky na tsyfrovu infrastrukturu (derzhavni orhany, krytychna infrastruktura ta orhanizatsii tretoho sektoru). Derzhavne upravlinnia ta rehionalnyi rozvytok. 2022. №15. S. 30–67. DOI: https://doi.org/10.34132/pard2022.15.02
12. Lyseiuk A., Svintsytska T. Rozvytok mizhnarodnoho spivrobitnytstva u sferi kiberbezpeky: normatyvno-pravovi zasady ta perspektyvy). Pravo ta innovatsiine suspilstvo. 2024. № 2(23). S. 89–95. URL: https://doi.org/10.37772/2309-9275-2024-2(23)-890
13. Ilienko A., Teliushchenko V., Dubchak O. Suchasni kiberzahrozy krytychnoi infrastruktury ukrainy ta svitu. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika». 2025. № 3(27). S. 150–164. DOI: https://doi.org/10.28925/2663-4023.2023.27.719
14. ISO/IEC 27001:2022. URL: https://www.iso.org/standard/27001
15. Ssessment of national cyber capabilities: what is the level of cybersecurity maturity of ukraine according to the enisa methodology? URL: https://understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_1_en.pdf
16. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
17. Zhyvylo Ye. O. Militaryzatsiia vyklykiv ta zahroz v kiberprostori yak operatsiinomu seredovyshchi. Derzhavne budivnytstvo. 2024. № 1 (35). S. 344–359. DOI: https://doi.org/10.26565/1992- 2337-2024-1-26
18. Cyber defence. 2024. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence
19. EU cybersecurity: strategy and key policies. URL: https://www.consilium.europa.eu/en/policies/cybersecurity/
20. Directive (EU) 2022/2555 of the european parliament and of the council of 14 December 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
21. NIS2 Directive: securing network and information systems. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
22. ENISA aims to raise cybersecurity awareness and promote behavioural change. URL: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene)
23. Postanova «Pro zatverdzhennia Poriadku otsiniuvannia stanu kiberzakhystu informatsiinykh, elektronnykh komunikatsiinykh ta informatsiino-komunikatsiinykh system, obiektiv krytychnoi infrastruktury, obiektiv krytychnoi informatsiinoi infrastruktury» vid 31 hrudnia 2025 r. № 1799. URL: https://zakon.rada.gov.ua/laws/show/en/1799-2025-%D0%BF#Text
24. Postanova «Deiaki pytannia reahuvannia na kiberintsydenty, kiberataky ta kiberzahrozy» vid 26 lystopada 2025 r. № 1533. URL: https://zakon.rada.gov.ua/laws/show/en/1533-2025-%D0%BF#Text
25. Rozporiadzhennia «Pro zatverdzhennia planu zakhodiv na 2025 rik z realizatsii Stratehii kiberbezpeky Ukrainy» vid 7 bereznia 2025 r. № 204-r. URL: https://zakon.rada.gov.ua/laws/show/en/204-2025-%D1%80#Text
26. Nakaz «Pro zatverdzhennia Poriadku formuvannia prohram iz standartyzatsii kryptohrafichnoho ta tekhnichnoho zakhystu informatsii, kiberzakhystu, protydii tekhnichnym rozvidkam, tekhnichnoi perevirky proektu standartu kryptohrafichnoho ta tekhnichnoho zakhystu informatsii, kiberzakhystu, protydii tekhnichnym rozvidkam, rozsylannia, perevirky ta perehliadu standartiv kryptohrafichnoho ta tekhnichnoho zakhystu informatsii, kiberzakhystu, protydii tekhnichnym rozvidkam, vedennia yikh katalohu ta form dokumentiv» vid 16.12.2025 № 832. URL: https://zakon.rada.gov.ua/laws/show/en/z0147-26#Text
27. Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
28. Cybersecurity. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity
29. Krainiuk O., Yevseiev S., DidenkoN., Piksasov M. Transformation of the regulatory and legal framework for cybersecurity in Ukraine: analysis of compliance with the requirements of the nis2 directive and the cybersecurity act. Terytoriia bezpeky. 2025. T.1, №3. S. 40-48. URL: https://doi.org/10.20998/3083-6298.2025.03.05
30. U 2024 rotsi kilkist kiberatak ukrainskoho kiberprostoru zrosla na 70%. 2025. URL: https://skilky-skilky.info/u-2024-rotsi-kilkist-kiberatak-ukrainskoho-kiberprostoru-zrosla-na-70/
31. Torik CERT-UA opratsiuvala maizhe 6000 kiberintsydentiv: kilkist vorozhykh atak zrosla na 37%. 2026. URL: https://info.poda.gov.ua/news/251006
32. Khakery atakuiut. Vid pochatku viiny Ukraina perezhyla ponad 200 kiberatak — khto zaraz u zoni

ryzyku. 2024. URL: https://biz.nv.ua/ukr/markets/200-kiberatak-na-ukrajinski-ustanovi-ta-kompaniji-u-2022-roci-derzhspeczv-yazok-50388782.html
33. Bozhenko V., Pakhnenko O., Koibichuk V. Dosvid YeS shchodo rozrobky ta vprovadzhennia natsionalnoi stratehii kiberstiikosti finansovoho sektoru. Tsyfrova ekonomika ta ekonomichna bezpeka : naukovo-praktychnyi zhurnal. 2023. №8 (08). S. 125–129. DOI: https://doi.org/10.32782/dees.8-21
34. Kotliarov O. Yu., Bortnik L. L. Porivnialnyi analiz suchasnykh system zakhystu virtualnykh merezh ta yikh metodolohii. Suchasnyi zakhyst informatsii. 2024. № 4(60). S. 60-72. DOI: 10.31673/2409-7292.2024.040007
35. Pasichnyk V., Nedoshytko A. Instytutsiini mekhanizmy kiberbezpeky: porivnialnyi analiz praktyk Ukrainy ta krain NATO. Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia. 2026. №15. S. 79–88. DOI: https://doi.org/10.31470/2786-6246-2026-15-79-88)

Serdiukov K.S., Assessment of the level of cyber protection in organizations of ukraine and eu countries: comparative analysis and directions for improvement

The swift expansion in the volume and intricacy of cyber dangers directly impacts the steadiness of operations for entities across diverse economic spheres. Amidst digital evolution and Ukraine's incorporation into European cyberspace, a comparative assessment of cybersecurity levels with EU nations holds special relevance for pinpointing current deficiencies and frailties. The outcomes of such an examination are crucial for shaping successful governmental and company strategies in cybersecurity and boosting organizational cyber robustness. The goal of this study is to perform a comparative analysis of the cyber defense degree in organizations within Ukraine and European Union member states based on selected metrics and signs, and to support the spheres for its enhancement, considering contemporary global benchmarks and proven methods in the cybersecurity domain. This research employed a set of general scientific and particular methods of cognition that allow for a thorough assessment of the degree of cyber defense within enterprises in Ukraine and EU nations. Specifically, a systematic framework was utilized to view cyber protection as a complete, tiered structure, alongside a contrastive examination to pinpoint shared characteristics and divergences in national cybersecurity frameworks. The content review technique was applied to examine regulatory documents and global benchmarks concerning cyber defense, whilst the metric method enabled gauging the advancement level of organizations' cyber defense mechanisms. Furthermore, aggregation and combination techniques were put to use to construct well-founded findings and determine avenues for enhancing cyber protection. The core of cybersecurity and cyber resilience, contemporary methods for their provision, along with the chief international frameworks for gauging the degree of cyber defense, are examined. Current cyber dangers and their effect on enterprises are investigated. The legal structure of Ukraine and the EU concerning cyber protection is scrutinized, notably NIS2, GDPR, and Ukrainian governing documents, and the extent of their alignment is evaluated. A contrasting examination of the cyber defense standard among organizations in Ukraine and EU nations is performed. The influence of wartime and emergency situations on Ukraine's cybersecurity is estimated. Avenues for boosting the cyber protection of organizations are pinpointed. Actionable guidance is developed for augmenting cyber robustness, employing advanced defense technologies, and aligning with EU norms. The scholarly originality of this research resides in the organization of strategies for the relative evaluation of the cyber protection status of entities in Ukraine and EU member states based on an indicator structure, and in revealing main discrepancies between domestic and European practices.

***Keywords**: digital transformation, cyberspace, cyber threats, cyber defense, organization, regulatory framework, risk management, integration.*

Сердюков Костянтин Сергійович – аспірант кафедри публічного управління, менеджменту та маркетингу Східноукраїнського національного університету імені Володимира Даля, м. Київ
https://orcid.org/0009-0009-7098-3907
serdiukovk@gmail.com

Дата першого надходження статті 31.03.2026.
Дата прийняття статті до друку після рецензування 22.04.2026.
Дата публікації 30.05.2026.