УДК 004.056.5:351.746.1(477)
DOI: 10.31673/2409-7292.2025.041214

Нужний С.М., Костяк М.Ю., Пархуць Л.Т.

АНАЛІЗ ПРОЦЕСУ РЕКОНФІГУРАЦІЇ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Генеральна лінія розвитку України полягає в її вступі в ЄС, що вимагає гармонізації законодавчої та нормативно-правової бази України до вимог ЄС. В сфері захисту інформації ці процеси почались більше 20-и років тому, однак їх пік відбувається безпосередньо зараз. Керівництвом держави, в рамках підготовки України до вступу до ЄС, поставлене завдання по оновленню всієї нормативно-правової бази з максимальним врахуванням вимог NIS 2 та NIST. Однак, дія вказаних нормативних документів не розповсюджується на структуру та алгоритми дії систем безпеки щодо інформації з обмеженим доступом, особливо такої, що мітить державну таємницю. В роботі проведено порівняльний аналіз діючої в Україні нормативно-правової бази з вимогами NIS 2, NIST, NIST-SP-800 та відповідними документами НАТО. Результати дослідження показали значну нерівномірність по об'ємам робіт щодо реконфігурації нормативно-правової бази України. Так, в питаннях забезпечення захисту інформації на об'єктах інформаційної діяльності критичної інфраструктури головним питанням є підвищення рівня теоретичної підготовки працівників нижньої ланки. Практичні навички, в більшості випадків, у цих працівників знаходяться на високому рівні. При цьому головне питання реконфігурації полягає в зменшенні рівня формалістики в їх роботі – колосальна кількість звітів, актів, протоколів та інше, що забирають більшість робочого часу. З іншого боку, в сфері кіберзахисту, Україна має значні проблеми в нормативно-правовому забезпеченні. Це багато в чому, пов'язане з неможливістю формалізувати звітність по виконаних роботах і небажанням молодих фахівців, що в більшості випадків мають високі теоретичні і практичні навички, до роботи з таким рівнем формалізації звітності. Ці проблеми, багато в чому, вже вирішені в Регламентах ЄС та США щодо побудови систем кібербезпеки. Тим більше, що питання побудови систем захисту інформації від загроз кібербезпеці, в більшості випадків, є інваріантним до інформації, що потребує захисту.

Ключові слова: системи захисту інформації, НД ТЗІ, NIS 2, NIST, NIST-SP-800, CIS, STANAG.

Вступ

В 2019 році Верховна Рада України прийняла зміни до Конституції України, що юридично закріплюють стратегічний курс країни на ЄС та НАТО. Внесені положення про європейську ідентичність України та незворотність цього курсу [1]. Однією з умов вступу є гармонізація законодавчої та нормативно-правової бази України [2, 3]. До переліку напрямків, що потребують змін, включено й питання вдосконалення та гармонізації нормативно-правової бази систем захисту інформації [4-6].

Для вирішення задач, пов'язаних захистом інформації та врахуванням досвіду протидії кіберзагрозам останнього десятиліття, Рада ЄС затверджує оновлений регламент NIS 2 [6]. Хоча Рішення Ради ЄС, щодо кібербезпеки, безпосередньо не накладає зобов'язань на Україну, воно має стратегічне значення для нашої країни. Воно визначає напрямки розвитку кібербезпеки в ЄС, до яких Україні необхідно адаптувати своє законодавство та практики для забезпечення відповідності європейським стандартам. Це включає розвиток національної кіберстратегії, вдосконалення механізмів реагування на кіберінциденти та інтеграцію в європейські структури обміну інформацією та співпраці в сфері кібербезпеки.

Одночасно з цим, необхідно відмітити, що регламент NIS 2 встановлює нормативні вимоги до систем захисту інформації, в тому числі й до систем кібербезпеки. Однак, більшість авторів, що досліджують дану тему, не звертають увагу на важливий факт – в NIS2 «маркування (категорування) інформації» розглядається дещо інакше, ніж у NATO чи НД ТЗІ. В ньому немає жорстких рівнів «COSMIC TOP SECRET» / «SECRET» / «CONFIDENTIAL» / «RESTRICTED», а використовується ризик-орієнтований підхід, де маркування прив'язане до категоризації впливу на інформацію. За основу прийнято так званий FLIPS 199 [7], який визначає три базових рівня, в залежності від комбінації загроз – Low (невелика шкода), Moderate (помірна шкода) та High (серйозна шкода).

Для вирішення вказаної проблеми в [6] та інших джерелах рекомендовано використання американського стандарту NIST [7], який є набором рекомендацій щодо побудови системи

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115.
https://doi.org/10.31673/2409-7292.2025.041214

кібербезпеки мінімального рівня захищеності інформації, в залежності від структурного рівня об'єкту, як для окремо взятої організації/фірми, так і держави в цілому. Однак далі рекомендації не встановлюють нормативні вимоги до рівня безпеки інформації і, фактично, обмежені питаннями кібербезпеки. Це призводить до того, що в них не регламентовано розподіл інформації по вимогам до її захисту і не розглядається питання структурування систем безпеки для обробки інформації з обмеженим доступом. Більш того, безпосередньо в NIST питання захисту держаної таємниці не розглядаються, а підпорядковані NIST SP-800-53 та NIST SP-800-171 [8,9]. Враховуючи те, що в цих документах за основ взято FLIPS 199, [8] «маркування» в NIST ґрунтується на зв'язку інформації з категорією впливу, що використовується для управління доступом, зберігання та передачі, та не враховує безпосередньо «критичність (значимість)» самої інформації.

Таким чином, як видно з огляду, пряме запозичення [6-9] Україною вказаних документів, в умовах військового стану та постійного збільшення інцидентів в наслідок дії порушників, є недоречним та може призвести до критичних порушень в системах безпеки інформації.

Враховуючи поточний військовий стан в Україні та особливості роботи систем захисту інформації в умовах російсько-української війни, є сенс розглянути підходи до побудови систем захисту інформації, що засновані на нормативних документах НАТО.

Основними документами, що регламентують розробку та функціонування систем захисту інформації в НАТО є [10-16]. Аналіз вказаних документів показує що системи захисту інформації в НАТО мають чітку структурованість і маркування (категорування) інформації, що підлягає захисту. Більш того, саме інформація (її маркер) є відправною точкою в розробці системи захисту інформації.

Нормативно-правова база України свій початок веде з отримання Україною незалежності, однак має значний вплив радянської епохи – значний відсоток нормативних документів, які офіційно були відмінені, продовжував діяти, особливо таких, що нормували проведення робіт на об'єктах де циркулює державна таємниця [17]. Це не було «ЗРАДОЮ», а лише показувало на те, що документи спирались на закони фізики та/або нормували процедури розробки звітних документів про стан системи захисту інформації, або її частини, на об'єкті. Однак, історичне відставання СРСР від світового рівня розвитку технологій захисту інформації на 5-10 років та намагання максимально формалізувати звітність про виконану роботу призвели до формування власного підходу до розробки та експлуатації систем захисту інформації. Вагомий вплив на нормативну базу СРСР мали й зовнішні умови (стан «холодної війни») і підходів та технологій у головних конкурентів – США та НАТО. СРСР мав значне відставання в наукових дослідженнях і ще більше в підготовці кадрів для розробки та експлуатації систем безпеки. Так, в США попередня підготовка фахівця для виконання таких задач йшла протягом декількох років та в багатьох випадках опиралась на попередню освіту (коледж) здобувача (курсанта). В СРСР, крім вимушених випадків що вимагали посади офіцера, підхід був простий – в кращому випадку короткострокові курси (6 місяців) без врахування рівня освіти і здобувач направлявся в частину, для виконання поставлених задач. Враховуючи недоліки теоретичної підготовки, а в певних випадках і обмеження в їх вивченні, головним завданням стало набуття здобувачами практичних, механічних навичок роботи з конкретними системами та пристроями (це впливало й на майбутній розподіл по місцям служби) в штатних та позаштатних випадках. А для контролю за роботою фахівця та системи захисту інформації був використаний метод максимально формалізованої звітності (формуляри, акти, протоколи та інше). Це дозволяло під час перевірок встановити стан системи захисту і, якщо були, причини відмов. Одна, з часом, це та інші негативні процеси в радянському суспільстві призвело до зниження рівня теоретичної підготовки і самих перевіряльників. Нові розробки (власні та запозичені) навої техніки та дослідження проводились в НДІ і вимагали постійного підвищення фахових теоретичних та практичних навиків користувачів, а враховуючи недоліки в їх підготовці, ще більше підвищувало статус

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

формалізованої звітності. Технологічне відставання та особливості структури радянського суспільства постійно призводили до виникнення інцидентів, пов'язаних з недооцінкою певних напрямків розвитку технологій. Так, не зважаючи на активну діяльність інституту кібернетики [18] та інших, в СРСР фактично на рівні керівництва державою був пропущеним процес розвитку інтернет середовища, і, відповідно, необхідність розробки систем безпеки для користувачів. Біль того, постійний розвиток цього не вкладається в рамки формалізованої звітності. В США та ЄС для побудови систем захисту та оцінки рівня захищеності інформації перейшли на «ризиковий» підхід [6-8], який вимагає розуміння причин виникнення ризиків та методів їх локалізації, а це в свою чергу потребує високої теоретичної підготовки та практичних навиків.

Постановка проблеми

В Україні та й в Світі виникла ситуація, що характеризується наявністю двох методологій.

– Маркування ризиків в залежності від збитків, які виникають в наслідок інциденту, та розбудова систем безпеки спрямованих на запобіганню виникнення інцидентів (зменшення збитків). Щодо інформації, яку повинна захистити система безпеки, то її важливість враховується на рівні величини збитків в наслідок втрати її конфіденційності та/цілісності та/або доступності. Біль того, NTS 2 та NIST взагалі не призначені для розробки систем безпеки для захисту інформації що містить держану таємницю (методика розрахунку величини збитків не розрахована для таких випадків). Наявність в інформації, що потребує захисту, держаної таємниці розглядається в NIST SP-800, однак ці документи рекомендують як побудувати систему безпеки, мають рекомендаційний характер і не встановлюють певних (законодавчих) вимог до рівнів захисту безпосередньо самої інформації. На цій методології засновані нормативно-правові бази США, ЄС та інших.

– Маркування інформації в залежності від її важливості (наприклад наявності в ній державної таємниці) та розбудова систем безпеки спрямованих на її захист. Величина збитків (витрати на розбудову системи, її супровід, збитки від інциденту та інше) є додатковим фактором, який враховується шляхом підвищення окремих вимог (гарантій, критеріїв, та інше) в порівнянні з типовим рівнем і фактично може не впливати на структуру системи безпеки (витрати на розбудову системи та її експлуатацію можуть значно перевищувати величину збитків від інциденту). На цій методології засновані нормативно-правові бази НАТО, України та інших;

Таким чином, гармонізація нормативно-правової бази України з розробки та функціонування систем захисту інформації з базою ЄС потребує розуміння мети та шляхів такої гармонізації.

Метою проведеного дослідження є визначення шляхів узгодження діючої в Україні нормативно-правової бази розробки та експлуатації систем безпеки інформації з базами США та ЄС.

Для досягнення поставленої мети в роботі виконані задачі:

1. Проведено порівняльний аналіз базового нормативного документу (регламенту) ЄС, стандартів США, нормативних документів НАТО та діючих в Україні НД ТЗІ;

2. Розроблено рекомендації, щодо вдосконалення нормативної бази НД ТЗІ / окремих вимог, з метою її гармонізація з вимогами NIS2/NIST та НАТО.

Порівняльний аналіз

Аналіз та порівняння NTS 2 [6] та NIST [8]

Врахуємо, що порівняння NIS2 та NIST вимагає врахування контексту, бо це два різні підходи до кібербезпеки:

– NIS2 – європейська директива (законодавча вимога).

– NIST – американська організація, яка публікує стандарти та рамки (не обов'язкові, але широко прийняті).

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

Порівняння виконуємо за наступними критеріями:
- загальне порівняння (табл.1);
- структура та підхід(табл.2);
- сфера застосування(табл.3);
- сумісність та інтеграція(табл.4);
- захист інформації що містить державну таємницю (табл.5).

Таблиця 1

Загальне порівняння

Критерій	**NIS2**	**NIST**
Походження	ЄС (Директива Європейського Союзу)	США (Національний інститут стандартів і технологій)
Тип	Законодавчий акт (обов’язковий для країн ЄС)	Стандарти та рекомендації (добровільні, але часто використовуються)
Мета	Підвищити кіберстійкість критичної інфраструктури в ЄС	Допомогти організаціям керувати ризиками кібербезпеки
Застосування	Обов'язкове для певних секторів (критична інфраструктура, великі компанії тощо)	Добровільне, але широко використовується у державному та приватному секторі
Фокус	Регулювання та відповідальність	Практичні інструменти та фреймворки

Таблиця 2

Структура та підхід

Критерій	**NIS2**	**NIST (CSF 2.0)**
Підхід	Top-down (встановлення вимог згори)	Bottom-up (гнучкий підхід для адаптації)
Обов’язки	Визначено конкретні обов'язки керівництва, аудит, оцінка ризиків, інцидент-менеджмент	Рекомендовано впровадження заходів за принципом «Ідентифікуй, Захищай, Виявляй, Реагуй, Відновлюй»
Оцінка ризиків	Обов’язкова	Гнучка, адаптується до бізнесу
Вимоги до звітності	Суворі (повідомлення про інциденти у 24 години)	Рекомендовані, але не юридично зобов'язуючі

Таблиця 3

Сфера застосування

Критерій	**NIS2**	**NIST**
Обов'язковість	Так, для компаній, які підпадають під директиву	Ні, але часто використовується як best practice (найкраща практика)
Цільова аудиторія	Критичні та важливі сектори (енергетика, транспорт, фінанси, охорона здоров’я, IT тощо)	Будь-яка організація (приватна чи державна)
Санкції за недотримання	Так (штрафи, відповідальність керівництва)	Ні, але може впливати на сертифікації, страхування тощо

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

Таблиця 4

Сумісність та інтеграція

Критерій	NIS2	NIST
Можливість інтеграції з іншими стандартами	Так, може поєднуватись із NIST, ISO 27001	Так, гнучкий фреймворк, інтегрується з ISO, COBIT тощо
Технічна деталізація	Високорівневі вимоги	Більш детальні технічні рекомендації

Перш ніж порівнювати вказані документи щодо захисту інформації, що містить державну таємницю, визначимо термін «державна таємниця».

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [19,20].

Таблиця 5

Захист інформації що містить державну таємницю

Аспект	Що може вимагати держава щодо секретної інформації	Як NIS2 справляється	Як NIST справляється / кращий підхід
Класифікація, маркування	Обов'язкова класифікація (напр. «таємно», «секретно», «особливо секретно»), чітке маркування документів і записів	Не задає класифікацій інформації – лише загальні вимоги до захисту інформації	Не обов'язково задає політики класифікації держтаємниці, але в федеральних системах можливі внутрішні політики; контрольні заходи SP 800-53 можна використовувати у середовищах зі суворими вимогами
Криптографічний захист	Використання сертифікованих алгоритмів, шифрування «з і до», захищені канали зв'язку	Вимагає шифрування, але не деталізує конкретні алгоритми чи сертифікати	У своїх керівництвах, особливо для систем високого рівня захисту визначає конкретні криптографічні стандарти або посилання на федеральні стандарти (FIPS, Suite B, шифри, ключі)
Контроль доступу та привілеїв	Розмежування доступу, найменші привілеї (least privilege), суворі процедури затвердження доступу	Стимулює контроль доступу, багатофакторну автентифікацію	Детально описує механізми контролю доступу, управління правами, відстеження змін у доступах
Моніторинг, аудит, журналювання	Обов'язковий аудит всіх операцій з секретною інформацією, збереження логів, форензика	Включає вимоги до моніторингу, виявлення інцидентів, звітування	Забезпечує детальні практики аудиту, моніторингу, відповіді на інциденти і аналіз (intrusion detection, continuous monitoring)
Реагування на інциденти / управління інцидентами	Спеціальні процедури повідомлення, класифікація інцидентів, внутрішнє розслідування, захист доказів	Вимагає планів реагування, повідомлення відповідним органам у чіткі строки	Містить глибокі керівництва з інцидент-менеджменту, відновлення, аналізу після інциденту

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

Аспект	Що може вимагати держава щодо секретної інформації	Як NIS2 справляється	Як NIST справляється / кращий підхід
Управління ризиками	Постійна оцінка ризиків, аналіз загроз, сценарії “worst case”, планування захисту	Чітко вимагає управління ризиками	Пропонує структуровані процеси управління ризиками (оцінка, реагування, моніторинг)
Життєвий цикл секретної інформації	Сувора політика зберігання, транспортировки, копіювання, знищення секретної інформації	Не деталізує повністю процедури життєвого циклу секретної інформації	Глибоко охоплює політики резервного копіювання, знищення, контроль копій і носіїв
Вимоги до персоналу / допусків / безпеки людини	Перевірка персоналу й допуски, обмежений доступ, підготовка, нерозголошення	Говорить про ролі, відповідальність, надходження до процесів безпеки	Може враховувати такі вимоги як політики управління людським фактором, але не забезпечує національні допуски
Юридичні санкції	Жорстке законодавство, кримінальна відповідальність за витік, заборона пересилання секретної інформації	Передбачає штрафи, санкції, відповідальність	Не має юридичної сили сам по собі – його застосовують через політики державних органів або контрактів

В США, поняття та класифікація (маркування) державної таємниці відбувається згідно зі стандарту «Classified National Security Information» [21], та державними нормативами.

Таким чином, державна таємниця – це високо захищена інформація, яка часто має власні правові, процедурні й технічні вимоги на рівні національного законодавства. При порівнянні NIS2 та NIST треба враховувати, що жоден із цих стандартів чи директив прямо не призначений для «державної таємниці» (тобто «classified / секретної інформації») – вони здебільшого орієнтовані на кібербезпеку загалом, захист інформації середнього чи високого рівня, але не класифікованих державних документів з особливою секретністю. Тим не менше, можна подивитися, які вимоги NIS2 і NIST (особливо деякі їхні підмножини, такі як NIST SP 800 53 [8] або SP 800 171 [9]) можуть бути застосовані чи порівняні у контексті захисту дуже чутливої інформації, і де вони не задовольняють вимог до захисту державної таємниці.

Таким чином:

– NIS2 – це директива на рівні ЄС із загальними обов’язками з кібербезпеки, яка не покриває всі вимоги, які притаманні режиму державної таємниці (класифікація, допуски, дуже жорсткі криптографічні стандарти, контроль над носіями, процедури фізичної безпеки тощо);

– NIST, особливо через свої керівництва як SP 800 53 або інші, пропонує набагато більше деталізації й може бути ближчим до рівня потреб секретної інформації. Але він не гарантує виконання всіх національних (державних) вимог для секретності; він має бути доповнений національними стандартами з держтаємниці;

– Для захисту державної таємниці потрібно застосовувати національні нормативи безпеки інформації та захист інформації з режимом таємності, а NIS2 / NIST можуть бути базою або доповненням до цих норм.

Аналіз та порівняння стандартів з захисту інформації, що містить державну таємницю, в Україні та НАТО

Основними напрямками регламентації, за якими розробляються стандарти та директиви НАТО є:

1. Політика та базові директиви [15,23] – визначають політику управління інформацією, в тому числі й таємною: обробка, класифікація, зберігання, передача, знищення;

2. Маркування електронних даних за рівнями секретності та їх цілісності [10,11,23] – встановлюють вимоги до маркування даних за рівнем секретності, правила (регламенти) для

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

програмного забезпечення для роботи з мітками, в тому числі по обробці цих міток при обміні інформацією, її коригування;

3. Директиви безпеки для захисту інформації [12-14] – встановлюють вимоги щодо захисту інформації від побічних електромагнітних випромінювань (TEMPEST), правил проведення випробувань на відповідність, акредитацію та захист систем, які обробляють інформацію НАТО;

Таблиця 6

Порівняння НД ТЗІ та стандартів НАТО щодо захисту таємної інформації

Аспект	**НД ТЗІ (Україна)**	**Стандарти НАТО**	**Рекомендовані кроки для України**
Система класифікації	4 рівні секретності: «Особливо важлива», «Цілком таємно», «Таємно», «Для службового користування» (ДСК)	4 рівні секретності: Cosmic top Secret (CTS), Nato Secret / Secret (NS/S), Confidential (C), Restricted (R)	Розширити систему рівнів секретності для сумісності з НАТО, адаптувати маркування документів
Принцип доступу	«Need-to-know», обмеження термінів зберігання	«Need-to-know», чіткі процедури доступу та передачі інформації	Впровадити стандартизовані процедури доступу та обмеження доступу до секретної інформації
Атестація та перевірка персоналу	Дозвіл видається державними органами після перевірки на благонадійність	Національна перевірка + NATO Security Clearance	Запровадити перевірки персоналу відповідно до стандартів NATO, включно з міжнародною атестацією для співпраці
Відповідальність за витік	Адміністративна та кримінальна	Серйозна кримінальна та дисциплінарна відповідальність, включаючи санкції альянсу	Уточнити кримінальну та адміністративну відповідальність за витік інформації НАТО, адаптувати внутрішні санкції
Захист технічних засобів та ІС	Фізичний захист, криптозахист, контроль доступу, моніторинг	Використання сертифікованих криптозасобів, стандарти NATO INFOSEC/STANAG	Сертифікувати інформаційні системи та криптозасоби відповідно до стандартів НАТО, впровадити регулярний аудит
Передача та обмін інформацією	Тільки захищені канали, маркування документів	Захищені канали, COMSEC, маркування відповідно до рівня секретності	Впровадити стандартизовані процедури обміну інформацією з союзниками НАТО, включно із захищеними каналами
Контроль та аудит	Перевірки державними органами	Регулярні аудитні перевірки НАТО, інспекції, документування інцидентів	Розробити систему регулярного аудиту та контролю за дотриманням стандартів НАТО в органах влади та оборони
Гармонізація для інтеграції	Необхідно адаптувати класифікацію та сертифікацію, розробити стандартизовані процедури інцидентів	Встановлені чіткі стандарти для міжнародного обміну та сертифікації	Створити дорожню карту гармонізації НД ТЗІ з NATO INFOSEC та STANAG, включаючи навчання персоналу та модернізацію систем

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

4. Вимоги до персоналу та фізичного захисту [24, 25] – визначають процедуру надання доступу до секретної інформації та норми фізичного контролю доступу до приміщень, сховищ, архівів з інформацією НАТО;

5. Окремі інструкції щодо маркування, передавання, копіювання, знищення документів з позначкою NS/C/R та процедури обов'язкової звітності у випадку втрати чи компрометації класифікованої інформації [26].

Як показав аналіз, НД ТЗІ та стандарти НАТО мають багато спільного, що зумовлене основою в побудові систем безпеки – інформацією, яку потрібно захистити. Наявність розбіжностей, в більшості випадків, зумовлена тим, що стандарти НАТО розраховані на об'єднання країн. Тобто вони визначають як спільні дії так і взаємодію цих країн, в тому числі й при використанні інформації що містить державну таємницю (як для однієї з країн, так і для декількох чи всіх разом).

Порівняння NATO, НД ТЗІ (Україна) та NIST / NIS2 (США / ЄС)

Розглянемо результати порівняння (компактна, практична таблиця 7) та мапа процедур по роботі з інформацією з обмеженим доступом, з конкретними відмінностями в рівнях, маркуванні, процедурах життєвого циклу, атестації й вимогах до персоналу.

Таблиця 7

Порівняльна таблиця вимог NATO, НД ТЗІ (Україна) та NIST / NIS2 (США / ЄС) по роботі з інформацією з обмеженим доступом

Аспект	**NATO**	**НД ТЗІ (Україна)**	**NIST (SP-800) / NIS2 (EU)**
Рівні / класифікація	Позначення й чіткі наслідки компрометації → CTS, NS/S, NC/C, NR/R	Українська модель: державна таємниця → ОС, ЦТ, Т + ДСК (ІзОД) з категоризацією об'єктів/інформації; НД ТЗІ містять деталі категорування.	NIST не дає «натівських» рівнів – використовує категоризацію за ризиком (FIPS199 → Low/Moderate/High) та контрольні сімейства (SP-800-53). NIS2 вимагає ідентифікації критичних систем та їх захисту на національному рівні на основі FIPS199.
Маркування / метадані	Стандарти STANAG/IS забезпечують маркування та обробку міток (STANAG 4774–4779). Документи і електронні дані повинні бути чітко позначені.	НД ТЗІ визначають вимоги до позначення, обігу та зберігання матеріалів ІзОД; є вимоги до обліку і журналів.	NIST рекомендує маркування/категоризацію інформації відповідно до визначеного рівня впливу; NIS2 вимагає прозорих політик і обліку інцидентів.
Життєвий цикл (handling)	Життєвий цикл: створення → класифікація → зберігання → передача (контрольована) → архівація/знищення; існують IHNCI (instructions) для практики.	НД ТЗІ деталізують етапи: проектування комплексу ТЗІ, впровадження, випробування та атестація, експлуатація й підтримка.	NIST дає технічні контрольні механізми (IAM, шифрування, аудит, моніторинг), NIS2 – обов'язкові процеси управління ризиками та реагування на інциденти.
Технічні вимоги (TEMPEST, CIS)	[13,14] (TEMPEST), [12] (захист CIC) – вимоги до ЕМЗ/витоків та акредитації CIS.	НД ТЗІ включають вимоги до технічних засобів, периметрів захисту, криптографії та тестування/атестації (протоколи випробувань).	NIST: криптографічні стандарти, контроль доступу, логування, тестування – докладні контролі [8]. NIS2: вимоги до мінімального набору заходів кібербезпеки.

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

Аспект	NATO	НД ТЗІ (Україна)	NIST (SP-800) / NIS2 (EU)
Персонал / допуски	директиви по перевірці персоналу: Personnel Security Clearance, background checks, need-to-know	НД ТЗІ + національні акти регулюють допуски, доступ до ІзОД та процедури категорування працівників.	NIST описує ролі та відповідальності (security roles); NIS2 підкреслює управління кадрами в рамках корпоративної відповідальності.
Атестація / аудит / звітність	Акредитація систем, аудит, обов'язкове звітування про інциденти згідно процедур НАТО; існують детальні інструкції для обміну та звітності.	Обов'язкові випробування та атестація комплексу ТЗІ; оформлення протоколів випробувань, акти випробувань.	NIST: планові оцінки контролів, незалежні аудити; NIS2: обов'язкова звітність та нагляд з потенційними санкціями для non-compliance.

Практична мапа процедур (що робити на практиці – уніфікований алгоритм)

1. Категоризація інформації:

– NATO: застосовувати рівні (CTS / NS / NC / NR) і маркувати.

– НД ТЗІ: застосувати національні категорії ІзОД згідно НД (пункти по категоруванню ОІД).

– NIST: провести FIPS199-категоризацію (Low/Moderate/High) як технічну базу для вибору контролів.

2. Проектування захисту (архітектура + політики):

– Маркування документу/файлу, контроль доступу (least-privilege), фізичний захист, криптозахист, сегментація. (NATO STANAG / NIST controls / НД ТЗІ (технічні засоби).

3. Впровадження технічних заходів

– IAM, MFA, шифрування даних у спокої/при передачі, HSM/КЕП, журналювання подій, захист від витоків (TEMPEST/SDIP-27).

4. Випробування та атестація

– Провести пен-тести, функціональні випробування ТЗІ згідно НД; TEMPEST-випробування за SDIP-28 якщо потрібно; оформити протоколи/акти.

5. Експлуатація та супровід

– Моніторинг, регулярні аудити, оновлення політик; процес звітності про інциденти (NATO/NIS2 мають суворі правила звітності).

6. Знищення / архівація

– Процедури безпечного знищення матеріалів згідно маркування; архівація з контролем доступу. (всі три підходи).

2.3.3 Головна різниця (практично)

– NATO дає чітку ієрархію рівнів та операційні інструкції (маркування, обмін, TEMPEST, персональні допуски) й очікує акредитацію та суворе дотримання процедур під час міжнародного обміну.

– НД ТЗІ – деталізує український процес створення, випробувань і атестації комплексу ТЗІ (формати, протоколи, методики) – «як формально зробити» ТЗІ.

– NIST / NIS2 – дають рамки ризик-орієнтованого вибору контролів (NIST – технічні контролі; NIS2 – організаційні обов'язки та звітність для ЄС). Використовуються як чек-лист технічного налаштування та управління ризиками.

Recommendations for harmonizing the ND TZI framework with NIS2, NIST, and NATO requirements

Отримані результати дослідження, щодо роботи з інформацією з обмеженням доступу, в тому числі й такої, що містить державну таємницю, представимо у вигляді матриці відповідності, що розділена на 10 напрямків. Такий підхід дозволяє структурувати та формалізувати вимоги.

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

Сама матриця є 3D-структурою, в якій вісь Z відповідає напрямами гармонізації; вісь Y – країна (об'єднання) та/або назва її нормативно-правової бази із захисту інформації (назва базового документу/групи документів); вісь X – відповідає за стан нормативно-правової бази із захисту інформації з обмеженим доступом, в тому числі й таку що містить державну таємницю, і ділиться на групи («поточний стан», «обмеження», «рекомендації по вдосконаленню») та підгрупи (за необхідності). В кожній комірці матриці можлива додаткова внутрішня структура, яка розкриває її призначення, механізми, принципи взаємодії з іншими задачами та інше.

В групі «рекомендації по вдосконаленню», по кожному напрямку, запропоновано рекомендації, щодо вдосконалення нормативної бази НД ТЗІ / окремих вимог, з метою її гармонізація до вимог NIS2/NIST та НАТО.

Оскільки представлена такої структури в статті має технічні обмеження, наводимо лінеарізований витяг, розділений по напрямкам. До кожного з напрямків додається рекомендація по вдосконаленню (гармонізації) нормативно-правової бази України (НД ТЗІ).

Лінеарізована матриця відповідності (витяг):

1. Класифікація рівнів та маркування інформації.

– NATO: CTS / NS / NC / NR; метадані конфіденційності –конфіденційні мітки й binding згідно [10,11].

– НД ТЗІ: документи по категоруванню об'єктів і обігу ІзОД згідно [27] та оформлення маркування; загальні вимоги до позначення та обліку ІзОД.

– NIST (контролі): MP – (Media Protection) – маркування, захист носіїв (MP-1…MP-8); PL – (System and Services Planning) для політик категоризації; PM – (Program Management) для управління інформацією.

Рекомендації: впровадити механізм прив'язки метаданих до файлу/документу (label binding) і політику «marking + handling» згідно [14]; в НД ТЗІ – оформити локальні правила маркування та обліку.

2. Життєвий цикл інформації (handling / lifecycle).

– NATO: в [22] та інш. – визначають життєвий цикл (create → classify → store → transmit → archive → destroy).

– НД ТЗІ: [28]та інш. – порядок проведення робіт по створенню комплексу ТЗІ.

– NIST

• Контролі для збереження слідів життєвого циклу: MP (media handling), CP (Contingency Planning), AU (Audit and Accountability),

• Контролі для коректності обробки: SI (System and Information Integrity).

Рекомендації: документи повинні містити інструкції по обробці кожного рівня секретності, процедури архівації та безпечного знищення; журналювання всіх операцій з документами.

3. Контроль доступу та управління привілеями (IAM).

– NATO: політики need-to-know, personnel access rules, контроль фізичних і логічних доступів ([22] + директиви з безпеки).

– НД ТЗІ: регламенти доступу до ІзОД, процедурні вимоги до оформлення доступу (категоризація, журнали доступу). ([27] та інші).

– NIST (контролі): AC – (Access Control) сімейство (AC-1 … AC-22), IA – (Identification and Authentication) сімейство (IA-1…IA-8), PM – та PS – (Personnel Security) для процедур перевірки персоналу.

Рекомендації: впроваджувати MFA, least-privilege, ролі/перевірки привілеїв, аудит змін привілеїв.

4. Аудит/логування та моніторинг (Audit & Accountability).

– NATO: вимоги до журналювання доступу, обміну і інцидентів згідно [22]

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

– НД ТЗІ: ведення журналів обліку документів, доступу, акти випробувань; процедурні вимоги до звітності.

– NIST (контролі): AU – (Audit and Accountability) сімейство (AU-2, AU-6 тощо), SI-4 (monitoring).

Рекомендації: зберігання логів згідно політик (retention), централізований збір, інструменти SIEM, регулярні перевірки.

5. Обмін/передача секретної інформації (Cross-Domain / Label handling).

– NATO: використання [10,11] для метаданих конфіденційності; директиви передачі між націями/партнерами.

– НД ТЗІ: правила передачі інформації ІзОД, облікові процедури, протоколи передачі (паперові і електронні) [30].

– NIST (контролі): SC – (System and Communications Protection) сімейство (SC-8, SC-12, SC-13), MP – (media protection), AC – (controls on sharing).

Рекомендації: забезпечити binding мітки → шифрування при передачі → автентифікований канал; контроль копій/реплікацій.

6. Захист від побічних випромінювань (TEMPEST / EMSEC).

– NATO: TEMPEST – поділ на класи (A/B/C) та вимоги до обладнання і його випробувань згідно [13,14].

– НД ТЗІ: вимоги до захисту технічними засобами від витоків інформації по неінформаційних каналах (ЕЕМ/АК) – процедурні і технічні пункти у НД (включаючи вимоги до приміщень) згідно [28-30].

– NIST (контролі): PE – (Physical and Environmental Protection) для фізичного розміщення й контролю приміщень; SC – контролі частково покривають захист каналів; додатково – спеціалізовані стандарти, однак [8] рекомендує застосовувати фізичний захист і аналіз витоків.

Рекомендації: якщо потрібні TEMPEST-вимоги, то необхідно застосовувати [13] для процес сертифікації обладнання; в НД ТЗІ необхідно передбачити вимоги до екранування та випробувань.

7. Акредитація/атестація інформаційних систем (System Accreditation).

– NATO: акредитація CIS / CIC під [12] та національні процедури; регулярні перевірки.

– НД ТЗІ: формалізована процедура випробувань/атестації комплексу ТЗІ (протоколи випробувань, акти). В [28] детально описує етапи створення і випробувань.

– NIST (контролі): CA – (Security Assessment and Authorization) сімейство (CA-2, CA-5) – оцінка та авторизація систем; PM – (program governance).

Рекомендації: поєднати національну атестацію [28] з вимогами SDIP/натівської акредитації при обміні інформацією.

8. Персональна безпека і допуски (Personnel Security).

– NATO: Personnel Security Clearances — background checks, need-to-know, процедури позбавлення доступу.

– НД ТЗІ: процедури оформлення допусків до ІзОД, регламенти щодо відповідальності персоналу і ведення обліку [29].

– NIST (контролі): PS – (Personnel Security) сімейство (PS-2, PS-3), та AT – (Awareness and Training) для навчання та розуміння ролей.

Рекомендації: впровадити процес перевірок, контракти/угоди про нерозголошення, регулярні перевірки прав доступу.

9. Реагування на інциденти і звітність (Incident Response & Reporting).

– NATO: процедури повідомлення та розслідування інцидентів, вимоги до повідомлення при компрометації класифікованої інформації (NIMP/внутрішні інструкції).

– НД ТЗІ: ведення актів, протоколів випадків порушень, заходи локалізації/відновлення згідно процедур [31].

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

– NIST (контролі): IR – (Incident Response) сімейство (IR-1…IR-8); AU – /SI – для розслідування, CP – для відновлення.

Рекомендації: NIS2 додає зобов'язання щодо термінів звітності (для ЄС) – варто уніфікувати локальні процедури з міжнародними вимогами.

10. Фізичний захист приміщень і документів (Physical Security).

– NATO: директиви з фізичної безпеки, контроль доступу до сховищ, серверних, архівів.

– НД ТЗІ: вимоги до фізичного захисту об'єкта інформаційної діяльності (периметр, сейфи, контроль доступу, відео), прописані в НД.

– NIST (контролі): PE – (Physical and Environmental Protection) сімейство (PE-1…PE-20) та MP – для медіа.

Рекомендації: синхронізувати вимоги доступу (badge, escort, visitor logs) із контролями доступу в інформаційних системах.

Висновки

1. Проведено порівняльний аналіз нормативно-правового забезпечення з розробки та експлуатації систем захисту інформації США (NIST, NIST SP800), ЄС (NIS 2), НАТО та України, що дозволило визначити основні розбіжності в підходах до формування принципів побудови систем безпеки.

В США та ЄС використовується «ризико-збитковий» підхід, що дає змогу побудувати системи захисту інформації з мінімізацією збитків від інцидентів. Однак при цьому не враховується суть самої інформації, не проводиться її маркування, а отже не враховується статус інформації, проти якої стався інцидент.

В НАТО і Україні побудова систем безпеки ведеться на основі маркування інформації, що забезпечує побудову ієрархічних систем захисту, спрямованих на оптимізацію структури системи захисту інформації, їх спрямованість на захист інформаційного ресурсу. Недоліком таких систем є не врахування збитків на побудову та експлуатацію системи захисту та збитків від інциденту.

2. У межах дослідження розроблено рекомендації щодо вдосконалення нормативно-правової бази НД ТЗІ та окремих вимог з метою її гармонізації з міжнародними стандартами NIS2, NIST та НАТО.

Розроблення здійснено методом системного аналізу та структурного моделювання, з використанням тривимірної матриці відповідності, яка охоплює напрями гармонізації, країни (або організації) та стан нормативно-правових актів. Такий підхід дав змогу формалізувати взаємозв'язки між вимогами різних систем безпеки та визначити конкретні напрями вдосконалення.

У результаті створено універсальну методологічну основу для оцінки, порівняння та модернізації нормативно-методичних документів у сфері технічного захисту інформації з обмеженим доступом, в тому числі й таку, що містить державну таємницю, що забезпечує узгодження української нормативної бази з міжнародними практиками та підвищує ефективність управління інформаційною безпекою на національному рівні.

Перелік посилань

1. Верховна Рада України. (2019, 7 лютого). Закон України «Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору)» № 2680-VIII.

2. European Council. (1993, June 21–22). Conclusions of the Copenhagen European Council. Copenhagen, Denmark

3. European Union, & Ukraine. (2014). Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. Official Journal of the European Union, L 161, 3–2137.

4. Кабінет Міністрів України. (2025). Звіт про виконання Угоди про асоціацію між Україною та Європейським Союзом за 2024 рік. Офіційний вебсайт Кабінету Міністрів України.

5. Європейська Комісія. (2025). Звіт щодо виконання Угоди про асоціацію між Україною та ЄС за 2023-2024 роки.

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214

6. Рада Європейського Союзу. (2022). Рішення Ради Європейського Союзу щодо кібербезпеки.
7. National Institute of Standards and Technology. (2004). Standards for security categorization of federal information and information systems (FIPS PUB 199).
8. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5).
9. National Institute of Standards and Technology. (2020). Protecting controlled unclassified information in nonfederal systems and organizations (NIST Special Publication 800-171, Revision 2).
10. NATO. (2017, December 20). Confidentiality Metadata Label Syntax (STANAG 4774 Ed 1; ADatP-4774 Ed A Ver 1). NATO.
11. NATO. (2018, October 26). Metadata Binding Mechanism (ADatP-4778 Ed A Ver 1; STANAG 4778 Ed 1). NATO.
12. NATO (SECAN). (2009, August). TEMPEST Product Qualification and Control (SDIP-55).
13. NATO (SECAN). (n.d.). Emission Security / Compromising Emanations Standard (SDIP-27).
14. NATO (SECAN). (n.d.). Zoning Procedures for Emission Security (SDIP-28).
15. NATO. (2002, 17 червня). Security Within the North Atlantic Treaty Organization (Document C-M(2002)49).
16. NATO. (2002, July 11). The Management of Non-Classified NATO Information (Document C-M(2002)60).
17. НІКС. (2024). Перелік нормативно-методичних документів в галузі захисту інформації.
18. Інститут кібернетики імені В. М. Глушкова НАН України. (2025). Історія.
19. Верховна Рада України. (1994). Закон України «Про державну таємницю» (№ 3855-XII). Офіційний вісник України.
20. Служба безпеки України. (2020, 23 грудня). Наказ «Про затвердження Зводу відомостей, що становлять державну таємницю» (№ 383).
21. The White House. (2009, December 29). Executive Order 13526: Classified National Security Information (Vol. 75, No. 2). Federal Register.
22. North Atlantic Council. (2007, December 11). The NATO Information Management Policy (NIMP) (C-M(2007)0118)
23. North Atlantic Treaty Organization. (рік). STANAG 4779: Confidentiality Metadata Binding. NATO Standardization Office.
24. North Atlantic Treaty Organization. (2020). Directive on personnel security (AC/35-D/2000-REV8). NATO Security Committee.
25. North Atlantic Treaty Organization. (2020). Directive on physical security (AC/35-D/2001-REV3). NATO Security Committee.
26. North Atlantic Treaty Organization. (n.d.). NATO Security Incident Reporting Procedures [Internal document]. NATO Communications and Information Agency.
27. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2013, 15 квітня). Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці: НД ТЗІ 1.6-005-2013 (Наказ № 215).
28. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2016). НД ТЗІ 3.6-003-2016: Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації (Наказ № 41/дск).
29. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2024). НД ТЗІ 2.3-025-24: Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (Наказ № 45/дск).
30. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2023). НД ТЗІ 3.7-003-2023: Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі (Наказ № 924).
31. Державна служба спеціального зв'язку та захисту інформації України. (2003). НД ТЗІ 2.5-010-2003: Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. Київ: Держспецзв'язку України. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

Надійшла 20.10.2025

© Нужний С.М., Костяк М.Ю., Пархуць Л.Т. (2025) Аналіз процесу реконфігурації нормативно-правового забезпечення інформаційної безпеки України. Сучасний захист інформації, 4(64), 103–115. https://doi.org/10.31673/2409-7292.2025.041214