DOI: 10.58254/viti.9.2026.14.176

УДК 004.056

канд. техн. наук Мазулевський О. Є. ORCID: 0000-0002-6042-2577 (ВІТІ ім. Героїв Крут)

ОЦІНКА ЗАБЕЗПЕЧЕНОСТІ КІБЕРБЕЗПЕКИ ОБОРОННОГО ВІДОМСТВА З УРАХУВАННЯМ ПЕРЕДОВИХ МІЖНАРОДНИХ ПРАКТИК

Вступ. У сучасних умовах інтенсивного розвитку інформаційних технологій та зростання кількості складних кіберзагроз особливого значення набуває забезпечення належного рівня кібербезпеки інформаційно-комунікаційних систем відомчих структур, особливо у секторі безпеки й оборони. Зростаюча залежність від ІКС обумовлює необхідність формування системних підходів до оцінювання рівня їх захищеності.

Проблематика. Існуючі міжнародні та державні стандарти, зокрема ДСТУ ISO/IEC 27001, а також методології NIST і моделі зрілості типу CMMC, визначають вимоги до забезпечення кібербезпеки, однак не забезпечують достатньо формалізованого, компактного та адаптованого під відомчі структури інструментарію оцінювання рівня її забезпеченості. Відсутність уніфікованого підходу ускладнює проведення порівняльного аналізу між підрозділами та формування узагальненої оцінки на рівні відомства.

Мета. Метою дослідження є розроблення способу оцінювання забезпечення кібербезпеки у відомчих інформаційно-комунікаційних системах, який дозволяє здійснювати кількісну оцінку рівня впровадження заходів безпеки на основі вимог Системи управління інформаційною безпекою за ДСТУ ISO/IEC 27001.

Матеріали й методи. У роботі використано підходи системного аналізу, методи експертного оцінювання та узагальнення державних та міжнародних практик у сфері кібербезпеки. Запропонований спосіб базується на оцінюванні трьох складових: документального забезпечення (наявність та актуальність політик і процедур), змістовної глибини опрацювання питань інформаційної безпеки (чек-листи відповідності ДСТУ ISO/IEC 27001) та технічного забезпечення (наявність і впровадження технічних засобів захисту). Оцінювання здійснюється шляхом застосування рівнозважених коефіцієнтів із подальшим агрегуванням результатів на рівні підрозділів і відомства.

Результати. У результаті дослідження сформовано універсальний спосіб, який дозволяє проводити стандартизоване оцінювання рівня забезпеченості кібербезпеки підрозділів, визначати слабкі місця в організаційних, процесних та технічних компонентах, а також здійснювати порівняльний аналіз між підрозділами. Запропоновано підхід до визначення загального рівня кібербезпеки відомства на основі мінімального значення серед підрозділів, що відповідає принципу "найслабшої ланки". Спосіб узгоджується з концепцією профілів безпеки та може бути інтегрований з інструментами автоматизованого контролю відповідності (SCAP/OpenSCAP).

Висновки. Запропонований спосіб забезпечує підвищення об'єктивності, відтворюваності та формалізації процесу оцінювання забезпечення кібербезпеки у відомчих інформаційно комунікаційних мережах. Його застосування дозволяє підвищити ефективність управління кібербезпекою, забезпечити узгодженість із міжнародними стандартами та створити основу для подальшого розвитку нормативно-методичного забезпечення у сфері кіберзахисту державних інформаційних систем.

Ключові слова: *кібербезпека, СУІБ, ДСТУ ISO/IEC 27001, оцінювання, інформаційно-комунікаційні системи, відомство, профілі безпеки, SCAP, CMMC.*

O. Mazulevskyi. Assessment of cybersecurity of the defense department taking into account best international practices

Introduction. In the context of rapid development of information technologies and the increasing complexity of cyber threats, ensuring an adequate level of cybersecurity for departmental information and communication systems (ICS), especially in the defense sector, becomes critically important. The growing dependence on ICS necessitates systematic approaches to assessing their security level.

Problem statement. Existing state and international standards such as ISO/IEC 27001 (DSTU), as well as NIST methodologies and maturity models like CMMC, define cybersecurity requirements but do not provide a sufficiently formalized, compact, and adaptable assessment framework for departmental structures. The absence of a unified approach complicates comparative analysis between organizational units and the formation of an aggregated departmental-level assessment.

Purpose. The purpose of this study is to develop a method for assessing cybersecurity provision in departmental ICS, enabling quantitative evaluation of implemented security measures based on the Information Security Management System (ISMS) requirements of ISO/IEC 27001.

Materials and methods. The study applies system analysis, expert evaluation methods, and generalization of international cybersecurity practices. The proposed method is based on evaluating three components: documentary support (availability and relevance of policies and procedures), depth of policy content (ISO/IEC 27001-based

checklists), and technical implementation (availability and deployment of security controls). The assessment uses equally weighted coefficients and aggregates results at both unit and departmental levels.

Results. The study proposes a unified method that enables standardized assessment of cybersecurity provision across organizational units, identification of weaknesses in organizational, procedural, and technical domains, and comparative analysis between units. A departmental-level assessment approach based on the minimum unit score is introduced, reflecting the "weakest link" principle. The method is compatible with security profile frameworks and can be integrated with automated compliance assessment tools such as SCAP/OpenSCAP.

Conclusions. The proposed method improves objectivity, repeatability, and formalization of cybersecurity assessment processes in departmental ICS. Its application enhances cybersecurity management effectiveness, ensures alignment with international standards, and provides a foundation for further development of regulatory and methodological frameworks in the protection of state information systems.

Keywords: *cybersecurity, ISMS, ISO/IEC 27001, assessment, information and communication systems, department, security profiles, SCAP, CMMC.*

Постановка проблеми. Стрімка цифровізація, що охоплює всі сфери діяльності людини, включно і військову, зумовлює зростання залежності від інформаційних технологій. У військовому контексті надійність функціонування інформаційно-комунікаційних систем (ІКС) безпосередньо пов'язана з безпекою особового складу та виконанням критичних завдань, що надає кібербезпеці статусу ключової умови стабільності відомства. Забезпечення належного рівня кіберзахисту ускладнюється інтегрованістю більшості ІКС з глобальною мережею Інтернет і широким використанням загальнодоступного програмного забезпечення, що сприяє накопиченню випадкових і непередбачуваних негативних впливів. У такій ситуації Інтернет-орієнтація ІКС розглядається крізь призму необхідності системного захисту ресурсів під час виконання базових технологічних процесів – отримання, зберігання, транспортування, оброблення та відображення інформації. Відповідно, оцінка забезпечення кібербезпеки у відомстві набуває практичної значущості як інструмент управління ризиками, запобігання виникнення кризових ситуацій шляхом оцінки та підвищення кіберстійкості. Оцінка кіберстійкості повинна бути різносторонньою та охоплювати різні аспекти функціонування ІКС. В цій статті матеріал продовжує висвітлювати роботу в галузі оцінки кіберстійкості, але фокусується на оцінці забезпечення кібербезпеки як складової кіберстійкості.

Аналіз досліджень і публікацій. Оцінювання відповідності стандартам і рамкам кібербезпеки у відомчих структурах спирається на три взаємодоповнюючі напрями:

системи управління інформаційною безпекою рівня міжнародного стандарту ISO/IEC 27001 [2] та/або ДСТУ ISO/IEC 27001 [3];

каталоги контролів та формалізовані процедури їх оцінювання (базовий, галузевий та цільовий профілі безпеки, NIST SP 800-53/53A [4; 5], 800-171 [6]);

галузеві (військові) моделі зрілості та сертифікаційні моделі (англ. Cybersecurity Maturity Model Certification, CMMC) [7; 8; 13] разом з автоматизованими технічними перевірками (SCAP/OpenSCAP) [9–11].

Така конвергенція дозволяє поєднати процесний нагляд, доказову перевірку контролів та операційну автоматизацію відповідності.

Міжнародний стандарт ISO/IEC 27001 та/або державний стандарт ДСТУ ISO/IEC 27001:23 визнають вимоги до створення, впровадження та безперервного поліпшення системи управління інформаційною безпекою (СУІБ, англ. Information Security Management System, ISMS), уніфікуючи політики, ролі, оцінювання ризиків і контрольні заходи на рівні організації, в якій він впроваджується. Актуальна редакція стандарту ISO/IEC 27001 – 2022 рік (ДСТУ ISO/IEC 27001 – 2023 рік) закріплює його як базовий орієнтир для відомчих та оборонних структур, незалежно від масштабу, і передбачає узгодження процесів СУІБ із ризик-менеджментом і суміжними рамками контролів (зокрема NIST).

Вивчення досвіду США показує, що через національні регулюючі документи затверджено "Каталоги контролів і процедури їх оцінювання". Ці каталоги містяться в [4] та надають інформацію:

повний перелік контролів безпеки та приватності;

адаптовані під ризик-менеджмент і різні технологічні домени;

проведено формалізацію методики та процедур оцінювання визначених контролів із вимогами до доказів і критеріїв прийняття.

Для середовищ, де обробляється CUI (Controlled Unclassified Information, укр. аналог – державні інформаційні ресурси, ДІР) поза федеральними системами NIST SP 800-171 Rev. 3 [6] встановлює вимоги та прямо відсилає до оцінювальних процедур SP 800-171A/53A [5; 12]. У сукупності ці документи задають перевірочні критерії відповідності для державного сектору та оборонно-промислової галузі.

Програма визначення зрілості і сертифікації кібербезпеки для оборонної сфери (CMMC) інституційно визначає рівні зрілості захисту FCI/CUI (FCI – Federal Contracting Information, CUI – Controlled Unclassified Information) у підрядників Міноборони США і вводить обов’язкові само-оцінювання або третьо-сторонні оцінювання залежно від рівня. Фінальне правило 32-CFR:2024 [7] закріплює вимоги, а CAP v2.0 [8] детально описує процес оцінювання на рівні ролей, фаз, артефактів та прийняття рішень для C3PAO/CCA (Certified Third-Party Assessor Organization / Cybersecurity Maturity Model Certification, укр. – сертифікованих організацій оцінювачів третьої сторони / військової моделі визначення зрілості кібербезпеки), що критично для відомчих перевірок і взаємного визнання практик.

Довідково: FCI та CUI – це два типи конфіденційної інформації, що обробляється під час роботи з федеральним урядом. FCI – це будь-яка інформація, що не призначена для публічного розповсюдження, а CUI – це більш чутливий тип даних, що вимагає суворіших заходів безпеки для захисту від несанкціонованого доступу.

Автоматизація відповідності (SCAP/OpenSCAP) [9–11]. Для технічних конфігураційних перевірок застосовують набір взаємодіючих специфікацій SCAP, який уніфікує машинозчитуваний контент, сканування та звітування; ініціативи NIST підтримують валідацію продуктів. Проєкт OpenSCAP надає інструментарій і профілі відповідності, що дозволяє інтегрувати контрольні перевірки з процесами аудиту та звітністю.

Довідково: SCAP (Security Content Automation Protocol) – це набір взаємопов’язаних специфікацій для машиночитних перевірок безпеки: опису політик, виявлення вразливостей/невідповідностей і уніфікованої звітності. OpenSCAP – відкритий інструментарій, що реалізує SCAP-перевірки (CLI oscap, профілі відповідності, генерація ARF/HTML-звітів, можливості ремедіації). На офіційному порталі – огляд, політики, довідники та набір утиліт (у т. ч. для парку систем).

Моделі процесної зрілості ISO/IEC 21827 [14], Systems Security Engineering – Capability Maturity Model (SSE-CMM). SSE-CMM описує характеристику процесів інженерії безпеки як стандартну метрику зрілості, що застосовується на всіх етапах життєвого циклу та рівнях організації, її використовують для оцінки зрілості та планування розвитку спроможностей. Для відомчих структур це корисний “надпроцесний” шар, сумісний із СУІБ та контрольними каталогами.

У НАТО та ЄС наголошується на формалізованому оцінюванні спроможностей і узгодженні з технічними керівництвами. Документи НАТО з кібероборони й доктрина AJP-3.20 [15] підкреслюють потребу у взаємосумісних заходах і процедурах. ENISA [16] пропонує технічні настанови та цілі безпеки – EECC/NIS (англ. European Electronic Communication Code / Network and Information Security), які можуть слугувати базисом для відомчих оцінювань в європейських організаціях.

В Україні формується трирівнева модель профілів безпеки для ІКС:

базовий (державний рівень, затверджує Державна служба спеціального зв’язку та захисту інформації України (далі – Держспецзв’язку);

галузевий (рівень відомства);

цільовий (для конкретної ІКС).

Кабінет Міністрів України у 2025 році затвердив порядок розробки профілів безпеки та порядок авторизації з безпеки. Держспецзв’язку оприлюднила базові профілі безпеки та методичні рекомендації розробки цільових профілів, а також порядок моніторингу й оцінки дотримання.

Під час перевірки власник ІКС має надати докази реалізації заходів, визначених у відповідному профілі.

Ключові норми нормативних вимог й оголошень містяться у наступних документах:

постанова КМУ № 627 від 30.05.2024 як початок експериментального проєкту з декларування відповідності КСЗІ на основі профілів (базових і цільових) [17];

наказ Адміністрації ДССЗЗІ № 317 від 24.06.2024 визначає Базовий профіль безпеки інформації (структура вимог) [18];

методичні рекомендації щодо формування ЦПБ (протокол від 14.03.2025 № 09-2025) визначає, як розробляти цільовий профіль безпеки для цільової ІКС [19];

постанова КМУ № 712 від 18.06.2025 визначає системний Порядок розроблення та затвердження профілів і Порядок авторизації з безпеки (експеримент замінили постійною процедурою) [20];

порядок моніторингу (реєстр, аналіз звітів) – наказ АДССЗЗІ/Мін’юст, березень 2025 – акцент на аналізі повноти, об’єктивності та достатності доказів за ЦПБ [21];

повідомлення ДССЗЗІ про затвердження базових профілів (08.07.2025) – підкреслюють призначення базового профілю та подальше формування ЦПБ на його основі [22].

У статті [1] було показано частину оцінки, яку засновано на динаміці зміни кількості зафіксованих кіберінцидентів.

Метою статті є розробка моделі для формалізації оцінювання забезпечення інформаційної безпеки на рівні підрозділів з опорою на Систему управління інформаційною безпекою оборонного відомства з урахуванням профілів безпеки для ІКС.

Виклад основного матеріалу дослідження. Розглянуті в попередньому аналізі джерел та публікацій підходи оцінки застосовано в закордонних системах, які логічно поєднуються із сучасними вимогами профілів безпеки, із побудовою СУІБ, перевіркою відповідності CMMC та із можливістю використання автоматизації періодичного підтвердження відповідності SCAP/OpenSCAP. Далі розглянемо можливість такої реалізації.

Структура профілів безпеки наближена до “policy baseline” у СУІБ:

базовий профіль – це державний мінімум;

галузевий профіль безпеки забезпечує уточнення з урахуванням ризиків і задач оборонного відомства;

цільовий профіль безпеки являє собою конкретизацію під ІКС. У СУІБ це відповідає ієрархії політик/процедур і “Statement of Applicability”.

Для зберігання доказів варто організувати “реєстр доказів” (evidence register), де будуть пов’язані “Вимога профілю” – “контроль/процедура” – “доказ” (політика, журнал, налаштування, протокол проведення тесту). Методично перетинаються з підходом NIST 800-53A/800-171A [5; 12] і процесом CMMC CAP (опитування, огляд доказів, технічні тести) [8].

Технічна перевірка – для конфігурацій/вразливостей слід додати процедуру SCAP/OpenSCAP:

XCCDF/OVAL-профілі;

регулярні сканування oscap;

ARF/HTML-звіти як формалізовані докази виконання відповідних пунктів профілю.

Довідково: XCCDF і OVAL – це стандартизовані формати для машиночитних перевірок безпеки. XCCDF (Extensible Configuration Checklist Description Format) описує чек-лист/бенчмарк: правила; профілі; параметри; важливість; посилання.

Open Vulnerability and Assessment Language (OVAL) описує тести поточного стану системи, що саме і як перевірити на кінцевому пристрої (реєстр/файл/пакет/сервіс тощо).

Згідно зі статтею 8 Закону України “Про основні засади забезпечення кібербезпеки України” [23] Міністерство оборони України є одним із основних суб’єктів національної системи кібербезпеки і відповідно до компетенції здійснює заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі. Також Міністерством оборони України пройшло сертифікацію системи управління інформаційною безпекою на відповідність стандарту ISO/IEC [24], що підтверджує побудову СУІБ та її ефективне використання.

Виходячи із вищезазначеного, слід реалізувати можливість оцінити стан кіберстійкості ІКС оборонного відомства для прийняття зважених управлінських рішень в мирний час та під час функціонування в особливий період (військовий стан). Розгляд цього питання піднімався в статті [1], де запропоновано розробити Метод прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних, та представлено один із його складових – підхід оцінювання поточного стану кіберстійкості оборонного відомства з урахуванням ситуації у кіберпросторі на основі статистичного аналізу зафіксованих кіберінцидентів.

У цій статті буде представлено ще один етап оцінювання кіберстійкості, а саме спосіб оцінювання забезпечення інформаційної безпеки оборонного відомства на рівні підрозділів. Спосіб забезпечує:

відтворюваність і прозорість оцінювання;

порівнюваність між підрозділами;

можливість агрегування результатів на рівень відомства та включення їх у цикл планування заходів СУІБ.

За допомогою способу, описаного в цій статті, можливо буде оцінювати структурні підрозділи відомства, що експлуатують ІКС, для яких визначені вимоги цільового профілю безпеки (ЦПБ) і встановлено межі СУІБ оборонного відомства. Спосіб не замінює проведення аудиту відповідності, а надає регулярний вимір рівня забезпечення та дотримання вимог за трьома взаємодоповнювальними векторами.

Логічна модель оцінювання та вектори забезпечення – оцінювання здійснюється за принципом “мінімально достатнього” набору контрольних пунктів (чек-листів), згрупованих у три рівноважні вектори:

1. Документальне забезпечення – наявність і актуальність ключових документів СУІБ (політики, методики, Декларація про застосовність (англ. Statement of Applicability, SoA), ролі/відповідальності, процедури інцидент-менеджменту, планування безперебійності в роботі та відновлення після збоїв тощо).

2. Глибина опрацювання регламентуючих документів – ступінь розкриття обов’язкових питань СУІБ:

контекст і зацікавлені сторони; критерії прийняття ризиків;

трасування SoA – Додаток А стандартів [2; 3] – докази;

навчання;

життєвий цикл доступів;

логування/моніторинг;

управління вразливостями;

бекапи;

інтеграції безпеки на кожному етапі розробки програмного забезпечення (DevSecOps);

робота з постачальниками;

фізична безпека;

метрики СУІБ.

3. Технічне забезпечення СУІБ – наявність мінімального набору технологічних контролів відповідно до Додатоку А стандартів [2; 3] та обраних цілей безпеки (багатофакторна автентифікація, захист кінцевих пристроїв та антивірусний захист, централізоване логування, резервування, управління оновленнями програмним

забезпеченням, поштовий/вебзахист, сегментація мережі, шифрування, сканування вразливостей, за можливості – автоматизовані перевірки за прикладом SCAP/OpenSCAP).

Кожний вектор оцінювання відбиває різні шари спроможностей СУІБ:

управлінський – через документи;

змістовий/процесний – через глибину вмісту політик;

технологічний – через реалізацію технічних контролів.

Рівнозваженість відображає принцип системності – жоден шар сам по собі не гарантує достатню кіберстійкість.

Шкали вимірювання та обчислення інтегральних показників. При оцінюванні контрольних пунктів чек-листа застосовується трирівнева шкала з урахуванням доказів:

1,0 – виконано повністю (наявний і впроваджений елемент; подані підтверджувальні артефакти);

0,5 – виконано частково (елемент існує, але є прогалини, а саме неповний обсяг, або неактуальність, або відсутність частини доказів);

0,0 – не виконано.

Позначення "Н/З" (не застосовується) вилучає пункт із розрахунку (див. знаменник у формулах нижче).

Показники векторів. Нехай s_i – бал за i-й пункт у відповідному векторі v, а n_v – кількість релевантних (без "Н/З") пунктів у цьому векторі. Тоді середній бал вектору буде визначатися за формулою:

$$S_v = \frac{\sum_{i=1}^{n_v} s_i}{n_v}.$$

Інтегральний показник підрозділу. З огляду на рівнозваженість векторів, інтегральний бал підрозділу визначається як середнє арифметичне:

$$S_{\text{підр}} = \frac{S_{\text{док}} + S_{\text{контент}} + S_{\text{тех}}}{3}.$$

За потреби вводиться коефіцієнт достовірності доказів ($C \in [0{,}8 \ldots 1{,}0]$), що модулює ступінь довіри до наданих артефактів (1,0 – повний комплект артефактів, включно з технічними звітами; 0,9 – без технічних; 0,8 – переважно декларації). Тоді скоригований інтегральний бал буде визначатися за формулою:

$$S`_{\text{підр}} = S_{\text{підр}} * C.$$

Для висвітлення стану та визначення необхідності прийняття управлінських рішень пропонуються такі порогові значення:

0,85–1,00 – Високий рівень: СУІБ стабільно функціонує, підтверджена наявними доказами;

0,70–0,84 – Достатній рівень: поодинокі прогалини, необхідні планові поліпшення;

0,50–0,69 – Базовий рівень: суттєві ризики, потрібен план покращення/відновлення;

0,00–0,49 – Низький рівень: відсутні ключові елементи СУІБ.

Далі розглянемо можливі мінімальні переліки (чек-листи) перевірок за векторами.

Документальне забезпечення (зразок мінімуму):

політика інформаційної безпеки (схвалена керівництвом, актуальна версія).

сфера СУІБ (опис меж і виключень);

методика й звіт з оцінювання ризиків, реєстр ризиків;

декларація про застосовність Statement of Applicability – (SoA) із обґрунтуванням включень/виключень контролів Додатку А стандартів [2; 3];

ролі та відповідальності (власники процесів/активів);

політика управління активами (класифікація, власники);

політика контролю доступу (принципи, багатофакторна автентифікація, найменші привілеї);

політика криптографії (використання, керування ключами);

безперервність функціонування та відновлення після збоїв (визначення цільової точки відновлення, цільового часу відновлення, тести);

інцидент-менеджмент (ролі, ескалації, журнал);

політика постачальників (оцінка, вимоги ІБ у договорах);

план внутрішніх аудитів СУІБ та звіти з виявлення, аналізу та усунення причин невідповідностей;

управління змінами (процедури, протоколи).

Примітка. Кожен пункт має бути закріплений до відповідної вимоги цільового профілю безпеки та/або Додатку А стандартів [2; 3] для забезпечення спостережності (tracing) у звіті.

Глибина опрацювання політик (ключові питання):

визначені контекст і зацікавлені сторони, що періодично оновлюються;

формалізовані критерії прийняття ризиків; наявний план обробки ризиків;

трасування SoA – Додатку А стандартів [2; 3] – докази (матриця відповідності);

навчання та обізнаність (план, % покриття, перевірка знань) персоналу;

життєвий цикл управління доступом (надання/позбавлення/перевірка);

політика логування та моніторингу (перелік подій, зберігання, захист журналів);

управління вразливостями (періодичність сканування, рівень обслуговування/ покращення/відновлення);

резервне копіювання (частота, шифрування, тести відновлення);

безпечна розробка/DevSecOps (за наявності);

оцінювання постачальників (анкети/аудити, вимоги до повідомлень про інциденти).

фізична безпека (периметр, серверні кімнати, журнали доступів);

метрики СУІБ (наприклад, середній час на відновлення після інцидентів, % виконаних тестів аналізу та усунення причин невідповідностей).

Технічне забезпечення СУІБ (мінімальний набір):

а) Організаційні/кадрові/фізичні (Додаток А стандартів [2; 3], пункти А.5–А.7):

розмежування обов'язків;

реалізація принципу найменших привілеїв;

багатофакторна автентифікація для адміністраторів;

навчання;

договір про нерозголошення;

контроль фізичного доступу (бейджі, журнали, ключі).

б) Технологічні (Додаток А стандартів [2; 3], пункт А.8):

ідентифікація та автентифікація: багатофакторна автентифікація, централізована система автентифікації, політика паролів;

антивірус/EDR на кінцевих точках;

політики реагування;

в) Логування і кореляція:

централізований збір (впровадження SIEM/лог-сховище),

зберігання не менше 90 днів.

г) резервні копії:

офлайн-сайт/ізоляція,

шифрування,

перевірочні відновлення.

д) Управління оновленнями ПЗ:

швидкість встановлення оновлень (критичних не більше 14 днів),

інвентаризація активів.

е) Захист пошти/веб:

реалізація механізмів захисту вебсервісів та поштових сервісів;

фільтрація вкладень/URL.

ж) Мережеві засоби:

сегментація мережі (VLAN/VRF);

впровадження міжмережевих екранів;

VPN сучасних протоколів;

системи виявлення/протидії вторгнень (щонайменше на периметрі).

з) Шифрування даних:

у транзиті (TLS сучасних версій);

у спокої (за потреби).

і) Управління вразливостями:

регулярне сканування;

реєстр вразливостей;

сканування за пріоритетами.

к) Регулярна автоматична перевірка контролів профілів безпеки (за можливості):

XCCDF/OVAL-профілі;

регулярне сканування на підвищення привілеїв;

наявність ARF/HTML-звітів як формалізованих доказів.

Далі розглянемо процедуру проведення оцінювання підрозділу:

Етап 1: Підготовка.

Визначаються підрозділи, власники ІКС, переліки артефактів; погоджуються пункти, до яких вимоги не застосовуються.

Формується реєстр доказів: вимога профілю – елемент профілю – доказ реалізації вимоги.

Етап 2: Збір даних і виставлення балів.

Двоє незалежних оцінювачів перевіряють артефакти/налаштування, опитують відповідальних, виставляють оцінки за пунктами чек-листів.

Етап 3: Вирівнювання та верифікація.

Розбіжності узгоджуються консенсусом; фіксується коефіцієнт C (коефіцієнт достовірності доказів). У разі оцінки технічних пунктів – перевага надається автоматизованим звітам (наприклад, ARF/HTML з OpenSCAP).

Етап 4: Агрегація та звітування.

Розраховуються $S_{док}$, $S_{контент}$, $S_{тех}$, $S_{\text{підр}}$ та $S'_{\text{підр}}$. Формуються:

зведена таблиця по підрозділах;

“теплова карта” виконання пунктів;

огляд трьох векторів;

рейтинг підрозділів.

Етап 5: Планування покращення.

Для кожного пункту з балом від 0 до 0,5 визначаються власник, дія, термін, метрика завершення (наприклад, % зменшення високих відхилень у SCAP-скануваннях, збільшення періоду зберігання журналів тощо).

Приклад фрагмента матриці оцінювання підрозділу наведено в таблиці 1.

Автоматизований шаблон розрахунку може виключати “Н/З” з підрахунку (n_v) і підсвічувати “вузькі місця” (пункти з оцінкою 0 або 0,5), формуючи вхідну чергу для покращення/відновлення.

Спосіб передбачає пряму перевірку пунктів чек-листів до вимог цільового профілю безпеки, який, у свою чергу, наслідує вимоги галузевого та базового профілів безпеки. В аналітичному додатку до звіту доцільно навести таблицю відповідностей: Вимога профілю – пункт чек-листа – контроль Додатку А стандартів [2; 3] – тип доказу – періодичність перевірки – власник. Такий підхід полегшує як внутрішні перевірки, так і зовнішні інспекції/аудити.

Для технічних пунктів рекомендовано, де це можливо, застосовувати SCAP/OpenSCAP як джерело машинозчитуваних доказів (доказів, які сформовані при автоматичній перевірці і записані в форматі, який здатен прочитати комп’ютер). У випадках, коли відомство орієнтується на сумісність із практиками CMMC/NIST (для взаємодії з міжнародними партнерами), матриця оцінювання може включати додаткові колонки “Сімейство вимог NIST 800-171/контроль 800-53” [4; 12] та “процедура оцінювання (800-53A)” [5], що підвищує взаємну сумісність доказової бази.

Таблиця 1

Приклад фрагмента матриці оцінювання підрозділу

Вектор	**Пункт**	**Бал**	**Доказ реалізації**
Документи	Політика ІБ затверджена та актуальна	1,0	Наказ №…, PDF від 2025-09-12
Документи	SoA із обґрунтуванням виключень	0,5	SoA v1.2; немає пояснення щодо A.8.23
Контент	Критерії прийняття ризиків	1,0	Методика ризиків, розд. 4
Технічні	MFA для адміністраторів	1,0	Скріни IdP + журнал подій
Технічні	Централізоване логування (≥90 днів)	0,5	SIEM: 60 днів
Технічні	OpenSCAP щоквартально	0,0	Немає профілів/звітів

Контроль якості оцінювання та управління упередженнями. Щоб знизити суб’єктивність, пропонується:

використовувати подвійне оцінювання (два оцінювачі на підрозділ);

фіксувати розбіжності та процедуру їх розв’язання;

застосовувати коефіцієнт достовірності C;

зберігати артефакти у централізованому “реєстрі доказів” із контрольними сумами/версіями.

Додатково для пунктів, що покладаються на процесні артефакти (накази, протоколи), періодично проводити перевірочні спостереження. Наприклад, тестове відновлення з резервних копій, перевірка вибірки заявок на доступ, контроль наявності слідів аудиту в журналах SIEM тощо.

Розглянутий спосіб оцінки забезпеченості кібербезпеки оборонного відомства із урахуванням передових міжнародних практик навмисно використовує мінімальний набір пунктів для забезпечення керованості в умовах великої кількості підрозділів. Це обмеження може призводити до втрати частини “глибини” оцінки. Шляхами вдосконалення може бути:

розширити чек-листи для специфічних підрозділів і галузей;

інтегрувати показники результативності;

автоматизувати збирання технічних доказів;

апробувати вагові коефіцієнти замість рівноважного усереднення там, де це виправдано ризиком.

Визначивши оцінки забезпечення кібербезпеки по підрозділах, можливо зробити загальну оцінку забезпечення кібербезпеки за оборонне відомство. Для оцінювання усього відомства варто висвітлювати наступні значення для узагальнення оцінок підрозділів:

1. Індикатор ризику – найнижче значення $S'_{підр}$.
2. Середнє значення, тобто типове значення по підрозділах.

3. 10-й перцентиль (визначає значення найгірших) – "хвіст ризику".

4. Покриття $Coverage_{\tau}$ – відсоткова частка підрозділів, що має оцінку більше цільового порогу (наприклад, $S' \geq 0{,}70$, $\tau = 0{,}7$).

Форми реагування (управлінських рішень) при отриманні загальної оцінки:

якщо $S'_{min} < 0{,}50$ – "червоний статус" оборонного відомства, негайна реалізація плану відновлення/покращення для підрозділу-аутсайдера, щотижневий моніторинг;

якщо $S'_{min} \geq 0{,}50$, але $S_{10\,\%} < 0{,}70$ або $Coverage_{0{,}7} < 80\,\%$ – "жовтий статус", реалізація програми вирівнювання, варто звернути увагу на аутсайдерів;

якщо $S'_{min} \geq 0{,}70$ і $Coverage_{0{,}70} \geq 95\,\%$ – "зелений статус", фокус діяльності на підвищенні медіани/технічній глибині.

Висновки. Запропонований спосіб оцінки забезпеченості кібербезпеки оборонного відомства із урахуванням передових міжнародних практик надає оборонному відомству уніфікований спосіб вимірювання забезпечення кібербезпеки на рівні підрозділів із опорою на СУІБ (ДСТУ ISO/IEC 27001:2023), профілі безпеки для ІКС та кращі міжнародні практики. Розподіл на три рівноважні вектори дозволяє балансувати управлінські, процесні та технологічні аспекти. Також використання чек-листів і прозорих формул гарантує відтворюваність результатів, а включення машинозчитуваних доказів (SCAP/OpenSCAP) зменшує суб'єктивність і підвищує доказову силу результатів. Спосіб масштабується на рівень відомства і дає основу для планування покращення/відновлення та підвищення кіберстійкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мазулевський О. Є., Жолобович Н. В. Оцінка поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі // Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 3 (51). С. 34–40. DOI: 10.33099/2311-7249/2024-51-3-34-40.

2. ISO/IEC 27001:2022. Information security management systems – Requirements. Женева: ISO/IEC, 2022. URL: https://www.iso.org/standard/27001 (дата звернення: 03.11.2025).

3. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. [Чинний від 2023-08-22]. Вид. офіц. К.: ДП "УкрНДНЦ", 2023.

4. Joint Task Force. NIST SP 800-53, Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2020. 492 p. DOI: 10.6028/NIST.SP.800-53r5. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (дата звернення: 06.11.2025).

5. Force J. T., Quinn S., Nadeau E. et al. NIST SP 800-53A Rev.5. Assessing Security and Privacy Controls in Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2022. 689 p. DOI: 10.6028/NIST.SP.800-53Ar5.

6. Ross R., Pillitteri V. NIST SP 800-171, Rev. 3. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2024. 120 p. DOI: 10.6028/NIST.SP.800-171r3.

7. Department of Defense. Office of the Secretary. Cybersecurity Maturity Model Certification (CMMC) Program: Final rule // Federal Register. 2024. Vol. 89, No. 199. P. 83092–83237. (32 CFR Part 170; Doc. No. 2024-22905; ефективно з 16.12.2024). URL: https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program; офіц. PDF на GovInfo. (дата звернення: 06.11.2025).

8. CMMC Assessment Process (CAP), v2.0. The Cyber AB, 16.12.2024. URL: https://cyberab.org/Portals/0/CMMC%20Assessment%20Process%20v2.0.pdf (дата звернення: 03.11.2025).

9. Security Content Automation Protocol (SCAP): Project Overview. NIST CSRC. URL: https://csrc.nist.gov/projects/security-content-automation-protocol (дата звернення: 03.11.2025).

10. SCAP Validated Products and Modules. NIST CSRC. URL: https://csrc.nist.gov/projects/scap-validation-program/validated-products-and-modules (дата звернення: 03.11.2025).

11. OpenSCAP Portal. URL: https://www.open-scap.org/ (дата звернення: 03.11.2025).

12. Ross R., Pillitteri V. NIST SP 800-171A Rev.3. Assessing Security Requirements for Controlled Unclassified Information. Gaithersburg, MD: National Institute of Standards and Technology, 2024. 106 p. DOI: 10.6028/NIST.SP.800-171Ar3. URL: https://csrc.nist.gov/pubs/sp/800/171/a/r3/final (дата звернення: 06.11.2025).

13. Code of Federal Regulations. Title 32–National Defense. Part 170 – Cybersecurity Maturity Model Certification (CMMC) Program. Electronic Code of Federal Regulations (eCFR), поточна редакція. URL: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170 (розд. 32 CFR Part 170) (дата звернення: 06.11.2025).

14. ISO/IEC 21827:2008. Systems Security Engineering – Capability Maturity Model (SSE-CMM). Женева: ISO/IEC, 2008. URL: https://www.iso.org/standard/44716.html (дата звернення: 03.11.2025).

15. NATO. Allied Joint Doctrine for Cyberspace Operations (AJP-3.20). 2020. URL: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (дата звернення: 03.11.2025).

16. ENISA. Guideline on Security Measures under the EECC (4th ed.). 2021. URL: https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc (дата звернення: 03.11.2025).

17. Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації: постанова Каб. Міністрів України від 30.05.2024 № 627. URL: https://zakon.rada.gov.ua/laws/show/627-2024-%D0%BF#Text (дата звернення: 03.11.2025).

18. Про визначення Базового профілю безпеки інформації: наказ Адміністрації ДССЗЗІ від 24.06.2024 № 317. URL: https://zakon.rada.gov.ua/rada/show/v0317519-24#Text (дата звернення: 03.11.2025).

19. Методичні рекомендації з формування цільового профілю безпеки інформації: схвал. рішенням ЕР з питань державної експертизи в сфері ТЗІ (протокол від 14.03.2025 № 09-2025). URL: https://www.cip.gov.ua/ua/docs/metodichni-rekomendaciyi-z-formuvannya-cilovogo-profilyu-bezpeki-informaciyi-skhvaleni-rishennyam-er-z-pitan-derzhavnoyi-ekspertizi-v-sferi-tzi-protokol-vid-14-03-2025-09-2025 (дата звернення: 03.11.2025).

20. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем: постанова Каб. міністрів України від 18.06.2025 № 712. URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text (дата звернення: 03.11.2025).

21. Про затвердження Порядку здійснення моніторингу систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням базових та цільових профілів безпеки інформації: наказ Адміністрації ДССЗЗІ від 10.03.2025 № 160. (Зареєстровано в Міністерстві юстиції України 20 березня 2025 року за № 448/43854.) URL: https://zakon.rada.gov.ua/laws/show/z0448-25#Text (дата звернення: 03.11.2025).

22. Повідомлення ДССЗЗІ про затвердження базових профілів (08.07.2025). URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-zatverdila-bazovi-profili-bezpeki-modernizuyuchi-pidkhodi-do-kiberzakhistu-derzhavnikh-sistem (дата звернення: 03.11.2025).

23. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 03.11.2025).

24. Повідомлення на офіційному сайті Міністерства оборони України. Міністерство оборони пройшло сертифікацію системи управління інформаційною безпекою на відповідність стандарту ISO/IEC. (24.04.2025) URL: https://mod.gov.ua/news/ministerstvo-oboroni-projshlo-sertifikacziyu-sistemi-upravlinnya-informaczijnoyu-bezpekoyu-na-vidpovidnist-standartu-iso-iec (дата звернення: 03.11.2025).

Надійшла до редколегії 12.02.2026.
Схвалена до друку 22.05.2026.
Дата публікації 29.05.2026.