

АТЕСТАЦІЯ ТА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ КСЗІ ПОРІВНЯЛЬНИЙ АНАЛІЗ УКРАЇНСЬКИХ І МІЖНАРОДНИХ ПІДХОДІВ

Вінницький національний технічний університет

Анотація

У роботі розглянуто особливості атестації та оцінювання ефективності комплексних систем захисту інформації (КСЗІ) в інформаційно-телекомунікаційних системах. Проаналізовано нормативно-правову базу України у сфері технічного захисту інформації та визначено основні етапи створення і атестації КСЗІ. Розглянуто міжнародні підходи до оцінювання ефективності систем захисту інформації. Проведено порівняльний аналіз національного та міжнародного підходів до оцінювання ефективності систем інформаційної безпеки. Визначено основні відмінності між процедурою атестації КСЗІ та ризик-орієнтованими моделями управління інформаційною безпекою. Обґрунтовано доцільність інтеграції міжнародних підходів до оцінювання ефективності систем захисту інформації з національною системою атестації КСЗІ.

Ключові слова: комплексна система захисту інформації, КСЗІ, атестація, інформаційна безпека, технічний захист інформації, оцінювання ефективності, управління ризиками, інформаційно-телекомунікаційні системи.

Abstract

The paper examines the features of certification and effectiveness evaluation of comprehensive information protection systems (CIPS) in information and telecommunication systems. The regulatory framework of Ukraine in the field of technical information protection is analyzed, and the main stages of development and certification of CIPS are identified. International approaches to evaluating the effectiveness of information security systems are considered. A comparative analysis of national and international approaches to assessing the effectiveness of information security systems is conducted. The main differences between the CIPS certification procedure and risk-based information security management models are identified. The feasibility of integrating international approaches to evaluating the effectiveness of information protection systems with the national CIPS certification framework is substantiated.

Keywords: comprehensive information protection system, CIPS, certification, information security, technical information protection, effectiveness evaluation, risk management, information and telecommunication systems.

Вступ

Забезпечення захисту інформації в інформаційно-телекомунікаційних системах є обов'язковою складовою діяльності органів державної влади, підприємств та організацій, які обробляють інформацію з обмеженим доступом. В Україні основним інструментом реалізації вимог щодо захисту такої інформації є створення та впровадження комплексних систем захисту інформації (КСЗІ), порядок розроблення, впровадження та введення в експлуатацію яких регламентується нормативними документами системи технічного захисту інформації (НД ТЗІ).

У міжнародній практиці питання оцінювання ефективності систем захисту інформації розглядається в межах систем управління інформаційною безпекою (ISMS), що ґрунтуються на ризик-орієнтованому підході та принципі безперервного вдосконалення. Міжнародні стандарти серії ISO/IEC 27000 визначають вимоги до оцінювання результативності заходів захисту, внутрішніх аудитів та управління ризиками, однак не передбачають атестації у класичному для української системи розумінні.

Наявність відмінностей між українськими та міжнародними підходами до атестації та оцінювання ефективності КСЗІ зумовлює актуальність їх порівняльного аналізу. Особливо це важливо в умовах поступової гармонізації національної системи технічного захисту інформації з міжнародними стандартами у сфері інформаційної безпеки. Метою даних тез є проведення порівняльного аналізу підходів до атестації та оцінювання ефективності КСЗІ відповідно до українських нормативних

документів і міжнародних стандартів з метою визначення їх спільних та відмінних рис, а також можливостей інтеграції кращих практик у національну систему захисту інформації.

Результати дослідження

В Україні створення та функціонування комплексних систем захисту інформації регулюється законодавством у сфері технічного та криптографічного захисту інформації. Основним нормативно-правовим актом, що визначає загальні принципи захисту інформації в інформаційно-телекомунікаційних системах, є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». У цьому законі встановлено вимогу щодо забезпечення захисту інформації під час її оброблення в інформаційних системах, а також визначено необхідність створення систем захисту інформації, які повинні відповідати встановленим вимогам та підтверджувати свою відповідність установленому порядку [1].

Реалізація вимог законодавства щодо захисту інформації здійснюється через впровадження комплексних систем захисту інформації, створення яких регламентується нормативними документами системи технічного захисту інформації. Одним із ключових документів у цій сфері є НД ТЗІ 3.7-003-2005 «Порядок створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Цей документ визначає основні етапи створення КСЗІ, зокрема проведення обстеження інформаційної системи, розроблення технічного завдання, проектування системи захисту, впровадження організаційних та технічних заходів безпеки, а також проведення випробувань і підготовку до атестації [2].

У межах національної моделі захисту інформації атестація КСЗІ розглядається як завершальний етап створення системи захисту. Основною метою цієї процедури є підтвердження відповідності реалізованих заходів захисту встановленим нормативним вимогам та прийняття рішення щодо можливості експлуатації інформаційно-телекомунікаційної системи для оброблення інформації з обмеженим доступом. Атестація передбачає перевірку організаційних, технічних та програмних заходів безпеки, а також оцінювання документації, що описує функціонування системи захисту [2].

Важливим елементом оцінювання ефективності захисту інформації є визначення рівня захищеності системи від несанкціонованого доступу. Для цього застосовується НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Документ встановлює систему критеріїв і вимог до механізмів захисту, які повинні бути реалізовані в інформаційній системі, включаючи механізми ідентифікації та автентифікації користувачів, розмежування доступу, реєстрацію подій безпеки та контроль цілісності інформації [3].

Таким чином, український підхід до атестації КСЗІ базується на нормативно визначеній процедурі перевірки відповідності системи захисту встановленим вимогам. Основна увага приділяється правильності реалізації організаційних і технічних заходів захисту, а також наявності необхідної документації. Така модель забезпечує стандартизацію процесів створення та експлуатації КСЗІ, однак водночас орієнтується переважно на формальну відповідність вимогам, що відрізняє її від підходів, які застосовуються у міжнародних стандартах інформаційної безпеки [2].

У міжнародній практиці забезпечення інформаційної безпеки оцінювання ефективності систем захисту інформації розглядається як складова комплексної системи управління інформаційною безпекою організації. Однією з найбільш поширених міжнародних моделей є система стандартів сімейства ISO/IEC 27000, яка визначає підходи до побудови, впровадження та постійного вдосконалення систем управління інформаційною безпекою. Ці стандарти встановлюють загальні принципи захисту інформації, термінологію та базові концепції управління інформаційною безпекою [4].

Ключовим стандартом у межах цієї серії є ISO/IEC 27001, який визначає вимоги до створення та функціонування системи управління інформаційною безпекою (ISMS). У стандарті наголошується на необхідності застосування процесного та ризик-орієнтованого підходу до управління безпекою інформації. Зокрема, організації повинні регулярно оцінювати ефективність впроваджених заходів захисту, проводити внутрішні аудити та забезпечувати постійне вдосконалення системи управління інформаційною безпекою відповідно до циклу PDCA (Plan–Do–Check–Act) [5].

Значний вплив на розвиток міжнародних підходів до оцінювання ефективності систем інформаційної безпеки мають також рекомендації Національного інституту стандартів і технологій США (NIST). Зокрема, документ NIST SP 800-37 описує рамкову модель управління ризиками (Risk

Management Framework), яка визначає етапи інтеграції заходів безпеки в життєвий цикл інформаційної системи. У цій моделі оцінювання ефективності системи безпеки здійснюється на регулярній основі шляхом проведення перевірок, аудитів та аналізу реалізації контрольних заходів [6].

Проведемо порівняльний аналіз національної процедури атестації комплексних систем захисту інформації та міжнародних практик управління інформаційною безпекою з метою більш наочного визначення особливостей підходів до оцінювання ефективності систем захисту інформації. Розглянемо детальне порівняння підходів, наведене у таблиці 1.

Таблиця 1 – Порівняльна характеристика національного та міжнародного підходів до оцінювання ефективності систем захисту інформації

Критерій	Український підхід (КСЗІ)	Міжнародний підхід (ISO / NIST)
Основна концепція	Атестація системи захисту інформації перед введенням системи в експлуатацію	Управління інформаційною безпекою на основі ризиків
Нормативна база	НД ТЗІ, законодавство України у сфері технічного захисту інформації	Міжнародні стандарти ISO/IEC 27000, рекомендації NIST
Основна мета оцінювання	Підтвердження відповідності системи встановленим вимогам	Оцінювання ефективності контролів безпеки та управління ризиками
Періодичність оцінювання	Переважно під час атестації та переатестації системи	Постійний моніторинг, регулярні аудити
Підхід до загроз	Орієнтація на нормативно визначені механізми захисту	Орієнтація на актуальні ризики та загрози
Управління безпекою	Переважно технічний і процедурний підхід	Комплексна система управління інформаційною безпекою

Порівняльний аналіз свідчить про суттєві відмінності між національною системою атестації комплексних систем захисту інформації та міжнародними підходами до оцінювання ефективності інформаційної безпеки.

Українська модель базується на процедурі атестації, яка передбачає перевірку відповідності реалізованих заходів захисту встановленим нормативним вимогам перед введенням інформаційної системи в експлуатацію. Основна увага приділяється правильності реалізації технічних і організаційних механізмів захисту, визначених нормативними документами системи технічного захисту інформації [2].

Міжнародні стандарти, зокрема серія стандартів ISO/IEC 27000 та рекомендації NIST, орієнтуються на ризик-орієнтований підхід до управління інформаційною безпекою. У межах цього підходу оцінювання ефективності системи захисту здійснюється на постійній основі шляхом аналізу ризиків, аудиту системи управління інформаційною безпекою, а також безперервного моніторингу стану інформаційної системи. Така модель дозволяє оперативно адаптувати систему безпеки до нових кіберзагроз та змін у середовищі функціонування інформаційних систем [5].

Таким чином, результати порівняння демонструють, що міжнародні підходи до оцінювання ефективності систем захисту інформації мають більш гнучкий та адаптивний характер. Водночас українська система атестації забезпечує чітку регламентацію процедур перевірки відповідності систем захисту нормативним вимогам. Поєднання цих підходів може сприяти підвищенню ефективності функціонування комплексних систем захисту інформації та гармонізації національної системи інформаційної безпеки з міжнародними стандартами.

Висновки

У результаті проведеного дослідження було розглянуто підходи до атестації та оцінювання ефективності комплексних систем захисту інформації, а також проаналізовано нормативно-правову базу України у цій сфері. Встановлено, що створення та функціонування КСЗІ в Україні регламентується законодавством у сфері технічного захисту інформації та відповідними нормативними документами, які визначають порядок розроблення, впровадження та атестації систем захисту інформації в інформаційно-телекомунікаційних системах.

Проведений аналіз показав, що національна модель оцінювання ефективності КСЗІ ґрунтується на процедурі атестації, яка передбачає перевірку відповідності реалізованих організаційних та технічних заходів захисту встановленим вимогам нормативних документів системи технічного захисту інформації. Основна увага в межах цього підходу приділяється перевірці механізмів захисту, правильності оформлення документації та результатам випробувань інформаційної системи перед введенням її в експлуатацію.

Водночас аналіз міжнародних підходів до оцінювання ефективності систем захисту інформації показав, що сучасні стандарти інформаційної безпеки орієнтуються на ризик-орієнтовану модель управління безпекою. Зокрема, стандарти серії ISO/IEC 27000 передбачають впровадження системи управління інформаційною безпекою, яка базується на постійному аналізі ризиків, аудиті системи безпеки та безперервному вдосконаленні механізмів захисту інформації.

Отже, результати дослідження свідчать про наявність суттєвих відмінностей між національною системою атестації КСЗІ та міжнародними підходами до оцінювання ефективності інформаційної безпеки. Українська модель має більш регламентований процедурний характер, тоді як міжнародні стандарти орієнтовані на безперервне управління інформаційною безпекою на основі аналізу ризиків.

Перспективним напрямом розвитку системи оцінювання ефективності КСЗІ в Україні є поступова інтеграція ризик-орієнтованих підходів до управління інформаційною безпекою, що застосовуються у міжнародних стандартах. Це сприятиме підвищенню ефективності функціонування систем захисту інформації, їхній адаптації до сучасних кіберзагроз та гармонізації національної системи інформаційної безпеки з міжнародними практиками.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про захист інформації в інформаційно-комунікаційних системах. Офіційний вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> (дата звернення: 07.03.2026).
2. ТЗІ – інформаційна безпека та захист інформації. URL: <https://tzi.com.ua/downloads/3.7-003-2005.pdf> (дата звернення: 07.03.2026).
3. ТЗІ – інформаційна безпека та захист інформації - Інформаційна безпека та захист інформації. URL: <https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf> (дата звернення: 07.03.2026).
4. ISO/IEC 27000:2018. ISO. URL: <https://www.iso.org/standard/73906.html> (дата звернення: 07.03.2026).
5. ISO/IEC 27001:2022. ISO. URL: <https://www.iso.org/standard/27001> (дата звернення: 08.03.2026).
6. SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy | CSRC. NIST Computer Security Resource Center | CSRC. URL: <https://csrc.nist.gov/pubs/sp/800/37/r2/final> (дата звернення: 08.03.2026).

Пінчук Дар'я Олександрівна – студентка групи 1KITC-226, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Науковий керівник: **Павловський Павло Валерійович** – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: prepod@vntu.edu.ua

Pinchuk Daria O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Supervisor: **Pavlovsky Pavlo V.** – assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: prepod@vntu.edu.ua