# Особливості застосування нормативних документів щодо побудови КСЗІ та ISO/IEC 27001

**Владислав Боднар,** студент[1], ORCID: 0009-0000-9807-6422,
**Шабала Євгенія,** канд. техн. наук, доц.[1] ORCID: 0000-0002-0428-9273

[1]*Київський національний університет будівництва і архітектури, Київ, Україна*

АНОТАЦІЯ

У роботі розглянуто теоретичні основи комплексної системи захисту інформації (КСЗІ) та міжнародного стандарту ISO/IEC 27001. Проведено аналіз об'єктів, суб'єктів та структури КСЗІ, а також ключових положень стандарту ISO/IEC 27001, що ґрунтується на циклі постійного вдосконалення PDCA. Визначено відмінності між підходами. Обґрунтовано доцільність поєднання обох підходів для побудови інтегрованої системи управління інформаційною безпекою. Стаття може бути використана при створенні та вдосконаленні політик безпеки організацій, що прагнуть підвищити рівень захисту інформаційних ресурсів та зміцнити довіру партнерів.

*Ключові слова: КСЗІ, ISO/IEC 27001, структура, порівняння, цикл PDCA, забезпечення безпеки.*

## 1. ВСТУП

У сучасних умовах стрімкого розвитку інформаційних технологій питання інформаційної безпеки набуває стратегічного значення для будь-якої організації. Зростання обсягів обробки даних, покращення старих або поява нових кіберзагроз та необхідність дотримання законодавчих вимог зумовлюють потребу у створенні ефективних систем захисту інформації. В Україні таку роль виконував комплекс системи захисту інформації (КСЗІ).Водночас міжнародний досвід пропонує інші підходи, серед яких ключове місце займає стандарт ISO/IEC 27001. Порівняння та можливе поєднання цих двох підходів дозволяє знайти оптимальні рішення для забезпечення належного рівня захисту інформаційних ресурсів, особливо у випадках, коли організація одночасно орієнтується на внутрішній та міжнародний ринки..

## 2. ТЕОРЕТИЧНІ ОСНОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ(КСЗІ)

Комплексна система захисту інформації (КСЗІ) - це сукупність організаційних, технічних та програмно-технічних заходів, спрямованих на забезпечення захисту інформації в автоматизованих системах (інформаційних, телекомунікаційних, інформаційно-телекомунікаційних), яка обробляє інформацію з обмеженим доступом.

### *2.1. Об'єкти та суб'єкти КСЗІ*

Об'єктами захисту КСЗІ є:[2]

- інформація з обмеженим доступом (конфіденційна, службова, комерційна та ін.);
- засоби обробки інформації (сервери, ПК, мережеве обладнання);
- канали передавання інформації;
- програмне забезпечення, яке забезпечує обробку та збереження цієї інформації.

У створенні та функціонуванні КСЗІ беруть участь кілька ключових суб'єктів:

- Замовник — організація, для якої створюється КСЗІ. Визначає вимоги до системи та фінансує її створення.
- Виконавець — організація, яка безпосередньо розробляє, впроваджує та налаштовує КСЗІ.
- Контролюючий орган — Адміністрація Держспецзв'язку, яка здійснює державну політику в галузі технічного захисту інформації, видає дозвільні документи та контролює відповідність КСЗІ вимогам законодавства.
- Організатор експертизи — організація, уповноважена на проведення державної експертизи КСЗІ.
- Підрядник — організація, що може бути залучена на окремі етапи виконання робіт зі створення КСЗІ за рішенням замовника або виконавця.

### *2.2. Структура КСЗІ*

КСЗІ має багаторівневу структуру, в якій поєднуються організаційні, технічні, програмні та криптографічні заходи. Така структура забезпечує всебічний захист інформації на всіх етапах її обробки та зберігання в інформаційно-телекомунікаційній системі.

Організаційна складова включає всі дії, пов'язані з розробкою внутрішніх нормативних документів, які регламентують правила доступу до інформації, обов'язки персоналу, порядок обробки конфіденційних даних, ведення журналів подій безпеки тощо. Важливим елементом цієї складової є визначення ролей користувачів системи, розподіл повноважень, а також призначення відповідальних за інформаційну безпеку осіб.

Технічна складова охоплює фізичні та апаратні засоби, призначені для контролю доступу до інформації та її носіїв. Сюди входять, наприклад, системи контролю і управління доступом (СКУД), відеоспостереження, сейфи та серверні кімнати з обмеженим доступом. Також до технічного захисту належить захист від витоків інформації технічними каналами — наприклад, шляхом екранування, заземлення або застосування спеціальних фільтрів.

Програмно-технічна складова пов'язана з впровадженням засобів захисту на рівні програмного забезпечення. Вона включає антивірусний захист, міжмережеві екрани (фаєрволи), системи виявлення вторгнень, механізми автентифікації користувачів, а також обмеження прав доступу до ресурсів системи. Усі ці елементи мають бути інтегрованими між собою та підтримувати єдину політику безпеки.

Криптографічна складова передбачає застосування сертифікованих засобів криптографічного захисту інформації. Це може бути шифрування даних на рівні файлів, каналів зв'язку або баз даних, а також електронний цифровий підпис (ЕЦП), що забезпечує цілісність і

автентичність інформації. Застосування криптографічних засобів є обов'язковим у випадках, передбачених законодавством, наприклад, при обробці персональних даних.

Контрольна складова включає заходи з перевірки ефективності впроваджених механізмів захисту. Це можуть бути як внутрішні аудити безпеки, так і зовнішня державна експертиза. Регулярна перевірка дозволяє виявляти вразливості, проводити оцінку ризиків та вдосконалювати систему захисту. Контрольна функція також забезпечує підтримку актуального стану документації з безпеки та ведення журналів подій.

## 3. ТЕОРЕТИЧНІ ОСНОВИ СТАНДАРТУ ISO 27001

ISO/IEC 27001 — це міжнародний стандарт, який встановлює вимоги до створення, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення системи управління інформаційною безпекою (СУІБ, англ. ISMS — Information Security Management System).

Цей стандарт є частиною сімейства стандартів ISO/IEC 27000, які розроблені з метою забезпечення системного підходу до захисту інформації в організаціях будь-якого типу — державних, приватних, комерційних чи неурядових.

ISO/IEC 27001 базується на циклі PDCA (Plan–Do–Check–Act), що відображає підхід до постійного вдосконалення:[3]

- Plan (Плануй): встановлення політики безпеки, аналіз ризиків, визначення контролів, розробка плану впровадження;
- Do (Виконуй): реалізація запланованих заходів, впровадження контролів;
- Check (Перевіряй): моніторинг та вимірювання ефективності СУІБ, проведення аудитів;
- Act (Дій): коригувальні дії, вдосконалення політики та процесів захисту.

Стандарт ISO/IEC 27001 має структуру високого рівня (High-Level Structure), яка узгоджується з іншими стандартами ISO (наприклад, ISO 9001 або ISO 14001). Основні розділи включають:

- Контекст організації: аналіз зовнішнього та внутрішнього середовища, зацікавлені сторони.
- Лідерство: зобов'язання керівництва, політика безпеки, розподіл ролей.
- Планування: оцінка ризиків, встановлення цілей, вибір контролів.
- Підтримка: управління ресурсами, компетентність персоналу, обізнаність, комунікації, управління документацією.
- Операційна діяльність: впровадження заходів безпеки, реагування на інциденти.
- Оцінка ефективності: внутрішній аудит, аналіз керівництва, вимірювання результатів.
- Вдосконалення: коригувальні дії, постійне поліпшення СУІБ.

## 4. ДОЦІЛЬНІСТЬ ЗАСТОСУВАННЯ НОРМАТИВІВ КСЗІ ТА ISO 27001

Одна з можливих точок зору полягає у тому, що використання лише нормативної бази КСЗІ є доцільним у контексті дотримання вимог українського законодавства, особливо для організацій, які працюють з персональними даними, державною або службовою інформацією. Проте КСЗІ, за своєю суттю, є більш регуляторно-орієнтованим підходом, що фокусується на забезпеченні базових вимог безпеки в ІТ-системах.

Натомість стандарт ISO/IEC 27001 пропонує більш гнучку, сучасну та ризик-орієнтовану модель, яка дозволяє будувати дійсно ефективну систему управління інформаційною безпекою, орієнтовану на постійне вдосконалення. Саме ця риса робить ISO/IEC 27001 незамінним інструментом для компаній, які прагнуть до міжнародного рівня безпеки та взаємодіють з іноземними партнерами.

У зв'язку з цим найбільш ефективним рішенням вважається поєднання підходів КСЗІ та ISO 27001. Таке поєднання дозволяє:

- забезпечити відповідність законодавчим вимогам України (через КСЗІ);
- інтегрувати найкращі міжнародні практики управління ризиками та процесами безпеки (через ISO/IEC 27001);
- побудувати єдину уніфіковану систему інформаційної безпеки, яка одночасно відповідає обом підходам.

## 5. ВИСНОВОК

КСЗІ та ISO/IEC 27001 відображають два взаємодоповнюючі підходи до організації інформаційної безпеки. КСЗІ забезпечує дотримання вимог українського законодавства та гарантує виконання базових норм захисту інформації в автоматизованих системах. Натомість ISO/IEC 27001 орієнтований на управління ризиками, постійне вдосконалення та відповідність міжнародним стандартам. Найбільш ефективним рішенням для організацій, які прагнуть досягти високого рівня захищеності та міжнародної конкурентоспроможності, є інтеграція обох підходів. Це дозволяє побудувати єдину систему управління інформаційною безпекою, яка одночасно відповідає вимогам національного законодавства та враховує кращі світові практики.

**Список літератури**

[1]Постанова Верховно Ради України https://zakon.rada.gov.ua/laws/show/4336-20#Text

[2] «Що таке комплексна система захисту інформації (КСЗІ)» URL: https://zahyst-ua.com/korisna-informaciya/shho-take-kompleksna-sistema-zahistu-informacii-kszi/

[3] «Що таке модель PDCA ISO 27001?».2025. URL: https://jeep.mercy.cx.ua/ukraincyam/shho-take-model-pdca-iso-27001.html