# ТЕХНІЧНЕ ЗАВДАННЯ
на створення
авторизованої системи з безпеки
на основі
комплексної системи захисту інформації
для інформаційно-комунікаційних систем

На основі НД ТЗІ 3.7-001-99

17 червня 2026 р.

## 1 Загальні відомості

Повне найменування КСЗІ: Комплексна система захисту інформації і авторизація системи захисту в автоматизованій системі. Умовне позначення: КСЗІ-АСЗ-АС.

Шифр теми: [Вказати шифр].

Найменування підприємств-розробників та замовника: [Вказати реквізити].

Перелік документів, на підставі яких створюється КСЗІ:

- НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»;
- НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем...»;
- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності...»;
- Інші нормативні документи.

Планові терміни початку і закінчення робіт: [Вказати].
Джерела фінансування: [Вказати].
Порядок оформлення результатів: [Вказати].

# 2 Мета і призначення комплексної системи захисту інформації

Метою розробки КСЗІ в АС ERP/1 є забезпечення захисту інформації з обмеженим доступом від несанкціонованого доступу та витоку технічними каналами відповідно до вимог законодавства України та нормативних документів Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України.

Функціональне призначення: Реалізація комплексного захисту в ERP-системі, яка обробляє критичну бізнес-інформацію, фінансові дані, персональні дані тощо.

# 3 Загальна характеристика автоматизованої системи та умов її функціонування

АС ERP/1 призначена для автоматизації бізнес-процесів підприємства (фінанси, логістика, HR тощо).

Структурна схема: Клієнт-серверна архітектура з центральним сервером баз даних, веб-клієнтами, інтеграціями з зовнішніми системами.

Клас АС: Відповідно до НД ТЗІ 2.5-005-99 — [Вказати клас, наприклад 2Б або 1Г].

Характеристики інформації: Обробляється інформація з обмеженим доступом (конфіденційна, комерційна таємниця).

Персонал: [Кількість користувачів, ролі, рівні доступу].

Фізичне середовище: Розміщення в [описати].

Потенційні загрози: Несанкціонований доступ, витік через ПЕМВН, внутрішні загрози тощо.

Функціонуючі засоби захисту: [Описати наявні].

# 4 Вимоги до комплексної системи захисту інформації

## 4.1 Вимоги в частині захисту від несанкціонованого доступу

Функціональний профіль захищеності: [Вказати профіль відповідно до НД ТЗІ 2.5-005-99].

Політика безпеки:

- Об'єкти доступу: Бази даних, файли, модулі ERP.
- Принципи керування доступом: Рольовий доступ (RBAC), мандатний контроль.
- Правила розмежування потоків.

- Аудит та реєстрація подій.

Послуги безпеки (відповідно до НД ТЗІ 2.5-004-99):

1. Конфіденційність — рівень [вказати].
2. Цілісність — рівень [вказати].
3. Доступність — рівень [вказати].
4. Спостереженість — рівень [вказати].

Рівень гарантій: [Вказати, наприклад EAL3 або відповідний].

### 4.2 Вимоги в частині захисту від витоку інформації технічними каналами

Загальні вимоги: Захист від ПЕМВН відповідно до ТР ЕОТ-95 та ТР ПЕМВН-95.

Показники захищеності:

- Нормовані значення співвідношення сигнал/шум.
- Застосування фільтрів, зашумлення, екранування.

Спецперевірки та спецдослідження ЗОТ.

## 5 Вимоги до складу проектної та експлуатаційної документації

- Технічне завдання на КСЗІ в АС.
- Проектна документація (архітектура, специфікації).
- Експлуатаційна документація (інструкції, керівництва).
- Програми та методики випробувань.
- Акти приймання.

## 6 Етапи виконання робіт

1. Попередній етап (аналіз, класифікація).
2. Проектування та розробка КСЗІ.
3. Випробування та введення в експлуатацію.

Календарний план: [Вказати].

## 7 Порядок внесення змін і доповнень

Зміни оформлюються доповненням, погоджуються та затверджуються в установленому порядку.

## 8 Порядок проведення випробувань

Розробка Програми та методики випробувань. Проведення комісією. Використання умовної інформації. Документи завершення: акт, сертифікат, наказ.

# 9 Додатки

## 9.1 Додаток А. Структурна схема ІКС

## 9.2 Додаток Б. Модель загроз

Модель загроз розроблено відповідно до вимог НД ТЗІ 3.7-001-99 (пп. 5.2, 6.3), НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, ТР ЕОТ-95 та ТР ПЕМВН-95.

### 9.2.1 1. Об'єкти захисту

Інформаційні ресурси автоматизованої системи ERP/1, що підлягають захисту:

- Бази даних (фінансові дані, бухгалтерська інформація, персональні дані працівників, комерційна таємниця, дані контрагентів);
- Конфігураційні файли та модулі системи ERP;
- Інтерфейси (веб-портал, API, інтеграції з зовнішніми системами);
- Логи та журнали аудиту;
- Резервні копії даних;
- Дані, що передаються мережевими каналами.

### 9.2.2 2. Модель порушника

Розглядаються такі категорії порушників:

| Категорія | Рівень | Мотивація | Приклади |
|---|---|---|---|
| Зовнішній хакер | Високий | Фінансова вигода, шантаж | APT, ransomware-групи |
| Внутрішній порушник (інсайдер) | Середньо-високий | Помста, особиста вигода, необережність | Співробітник, підрядник |
| Партнер/контрагент | Середній | Комерційна вигода | Через канали інтеграції |
| Технічна розвідка | Високий | Витік конфіденційної інформації | ПЕМВН, закладні пристрої |
| Випадковий порушник | Низький | Нецілеспрямований | Помилки користувачів, шкідливе ПЗ |

Табл. 1: Модель порушника

### 9.2.3 3. Загрози несанкціонованого доступу (НСД)

1. Підбір або викрадення облікових даних (брутфорс, фішинг, кейлогери, credential stuffing).
2. Експлуатація вразливостей програмного забезпечення (SQLi, XSS, RCE тощо).
3. Підвищення привілеїв (Privilege Escalation).

4. Несанкціонований доступ через інсайдера (зловживання правами).
5. Атаки на ланцюг постачання (компрометація оновлень або інтеграцій).
6. Атаки на доступність (DoS/DDoS).

#### 9.2.4 4. Загрози витоку інформації технічними каналами

1. Побічні електромагнітні випромінювання (ПЕМВ) від засобів обчислювальної техніки.
2. Наводки по мережах електроживлення.
3. Витік інформації по лініях зв'язку (LAN, Wi-Fi, зовнішні інтерфейси).
4. Закладні електронні пристрої.
5. Акустичні, вібраційні та оптичні канали витоку.
6. Витік через периферійні пристрої (принтери, USB-накопичувачі).

#### 9.2.5 5. Інші загрози

- Порушення цілісності інформації (несанкціонована модифікація даних).
- Порушення доступності інформації (збої, ransomware).
- Фізичні загрози (несанкціонований доступ до серверних приміщень, крадіжка носіїв).
- Природні та техногенні загрози (пожежа, затоплення, перебої в електропостачанні).

#### 9.2.6 6. Оцінка ризиків

| **Загроза** | **Ймовірність** | **Наслідки** | **Рівень ризику** | **Пріоритет** |
|---|---|---|---|---|
| Викрадення облікових даних | Висока | Високі фінансові втрати | Критичний | 1 |
| Експлуатація вразливостей ПЗ | Висока | Високі | Критичний | 1 |
| Витік через ПЕМВН | Середня | Високі | Високий | 1 |
| Інсайдерська загроза | Середня | Високі | Високий | 2 |
| DDoS-атака | Середня | Середні | Середній | 3 |

Табл. 2: Оцінка ризиків

#### 9.2.7 7. Рекомендації щодо нейтралізації загроз

- Реалізація політики найменших привілеїв (Least Privilege) та рольового доступу (RBAC);
- Багатофакторна автентифікація (MFA);
- Мережеве сегментування та принципи Zero Trust;
- Регулярне проведення спецперевірок та спецдосліджень ЗОТ;
- Використання сертифікованих засобів захисту;
- Постійне навчання персоналу та контроль дотримання політики безпеки.

### 9.3 Додаток В. Матриця розмежування доступу

### 9.4 Додаток Г. Календарний план робіт

## 9.5 Додаток Д. Перелік нормативних документів

НД ТЗІ 1.1-002-99.txt
НД ТЗІ 1.1-003-99.txt
НД ТЗІ 1.4-001-00.txt
НД ТЗІ 1.4-002-08.txt
НД ТЗІ 1.5-001-00.txt
НД ТЗІ 1.5-002-12.txt
НД ТЗІ 1.6-005-13.txt
НД ТЗІ 2.3-001-01.txt
НД ТЗІ 2.3-002-01.txt
НД ТЗІ 2.3-003-01.txt
НД ТЗІ 2.3-004-01.txt
НД ТЗІ 2.3-005-01.txt
НД ТЗІ 2.3-006-01.txt
НД ТЗІ 2.3-025-24-Т1.txt
НД ТЗІ 2.3-025-24-Т2.txt
НД ТЗІ 2.3-025-24-Т3.txt
НД ТЗІ 2.5-004-99.txt
НД ТЗІ 2.5-005-99.txt
НД ТЗІ 2.5-006-99.txt
НД ТЗІ 2.5-008-02.txt
НД ТЗІ 2.5-010-03.txt
НД ТЗІ 2.6-001-11.txt
НД ТЗІ 2.7-002-99.txt
НД ТЗІ 2.7-009-09.txt
НД ТЗІ 2.7-010-09.txt
НД ТЗІ 2.7-011-12.txt
НД ТЗІ 3.6-001-00.txt
НД ТЗІ 3.6-006-24.txt
НД ТЗІ 3.7-001-99.txt
НД ТЗІ 3.7-003-23.txt
НД ТЗІ 4.7-001-01.txt
НАД №409 від 30.06.2025.txt
НАД №419 від 02.07.2025.txt