

**ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ**

МАТЕРІАЛИ

**міжнародної науково-практичної конференції
молодих учених**

**«Проблеми та перспективи
забезпечення цивільного захисту»**

Черкаси – 2026

УДК 614.8; 614.84; 614.83; 623.26; 504.05; 504.06; 351.861; 623.45

Проблеми та перспективи забезпечення цивільного захисту: матеріали міжнародної науково-практичної конференції молодих учених. Черкаси: НУЦЗ України, 2026. 611 с. Матеріали опубліковано українською та англійською мовами.

Збірник містить матеріали доповідей учасників міжнародної науково-практичної конференції молодих учених на базі Національного університету цивільного захисту України. Розглянуто аспекти вдосконалення цивільного захисту держави.

У публікаціях висвітлено широкий спектр актуальних питань, що стосуються сучасних стратегій профілактики надзвичайних ситуацій, інноваційних методів гасіння пожеж та оптимізації управління оперативно-рятувальними підрозділами. Значну увагу приділено розробленню та впровадженню безпілотних систем, робототехніки, автоматичних систем безпеки, а також питанням радіаційного, хімічного захисту та протимінної діяльності. Автори аналізують екологічні аспекти техногенної безпеки, психологічні особливості роботи в екстремальних умовах та сучасні підходи до публічного управління у сфері цивільного захисту.

Матеріали призначені для інженерно-технічних працівників Державної служби України з надзвичайних ситуацій, науково-педагогічного складу, ад'юнктів, слухачів, студентів та курсантів закладів вищої освіти України та інших країн світу.

*Рекомендовано до друку засіданням
науково-інноваційного центру
Національного університету цивільного захисту України
(протокол № 30 від 30 березня 2026 року)*

*Дозволяється публікація матеріалів збірника у відкритому
доступі комісією з питань роботи із службовою інформацією
у Національному університеті цивільного захисту України
(протокол № 3 від 18 березня 2026 року)*

УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗГІДНО ЗІ СТАНДАРТАМИ ISO/IEC 27035, ISO/IEC 27002 ТА NIST SP 800-61

Малярова Д.М., здобувач вищої освіти, ХНУРЕ
НК – Маляров М.В., к.т.н., доцент, НУЦЗ України

Стрімкий розвиток інформаційних технологій та цифровізація бізнес-процесів зумовили зростання обсягів даних, що обробляються у мережевому середовищі. За таких умов важливо не лише впроваджувати засоби захисту, а й своєчасно виявляти та належним чином реагувати на інциденти інформаційної безпеки (ІБ), щоб мінімізувати шкоду та скоротити час відновлення.

Міжнародні стандарти визначають багатоступеневий процес реагування на інциденти. ISO/IEC 27035 [1, 2] є процесно-орієнтованим стандартом і задає життєвий цикл: планування і підготовка; виявлення та повідомлення; оцінювання та прийняття рішень; реагування; навчання на досвіді. ISO/IEC 27002 [3] є рекомендаційним кодом практик для контролів ІБ і встановлює вимоги щодо фіксації інцидентів, відповідальності та звітності. NIST SP 800-61 орієнтований на практичну реалізацію та деталізує операційні процедури, включно зі створенням команд реагування, застосуванням технічних засобів і веденням журналів.

У NIST SP 800-61 виділено чотири етапи: підготовка; виявлення та аналіз; стримування, ліквідація та відновлення; діяльність після інциденту. Підготовка охоплює політики, команду реагування, підготовку персоналу та інструменти моніторингу і аналізу журналів. Виявлення та аналіз передбачає збір і аналіз даних із систем моніторингу, журналів подій, мережевих індикаторів та повідомлень користувачів.

Подальші дії включають ізоляцію інциденту, відновлення уражених систем із перевіркою цілісності та документування уроків і оновлення процедур. Виявлення інцидентів є базовим процесом реагування. Згідно зі стандартом ISO/IEC 27035 [1, 2] воно включає аналіз подій із різних джерел: журнали подій, повідомлення користувачів, дані моніторингу, засоби виявлення атак, попередження про вразливості. ISO/IEC 27002 [3] зазначає, що мережі, системи та програми повинні контролюватися для виявлення подій, які можуть вплинути на інформаційну безпеку. Практичні методи й інструменти включають аналіз журналів подій, моніторинг трафіку, зовнішні попередження (CERT тощо), IDS/IPS, SIEM, антивірусні засоби, контроль цілісності та системи управління журналами подій.

У комплексі стандарти формують цілісну методологію: ISO/IEC 27002 визначає систему контролів, ISO/IEC 27035 – процес управління інцидентами, а NIST SP 800-61 – практичні механізми реагування. Таке застосування забезпечує відтворюваний процес управління інцидентами ІБ.

ЛІТЕРАТУРА

1. Information technology. Security techniques. Information security incident management. Part 1: Principles of incident management : ISO/IEC 27035-1:2016
2. Information technology. Security techniques. Information security incident management. Part 2: Guidelines to plan and prepare for incident response : ISO/IEC 27035-2:2016.
3. Information technology. Security techniques. Code of practice for information security controls : ISO/IEC 27002:2013.

Малець О.-С.І., Смотри О.О. Гібридні генеративні моделі та бітове шифрування в латентному просторі нейроаудіостеганографії.....	326
Малярова Д.М., Маляров М.В. Управління інцидентами інформаційної безпеки згідно зі стандартами ISO/IEC 27035, ISO/IEC 27002 та NIST SP 800-61.....	327
Михаленко Є.К., Кальченко Я.Ю. Дослідження пожежної небезпеки трансформаторних підстанцій.....	328
Мірошниченко Д.Ю., Дурсєв В.О. Параметричні дослідження роботи чутливого елемента з однодомених феромагнітних матеріалів теплового пожежного сповіщувача.....	329
Мірошниченко Д.Ю., Парамонова К.О., Дерев'янка О.А. Аналіз технічної тенденції розвитку вибухозахищених пожежних сповіщувачів в Україні та країнах ЄС.....	330
Мірошниченко Д.Ю., Якухін С.С. Виконавчий прилад адаптивної системи протипожежного захисту.....	331
Намазило В.А., Смотри О.О. Розробка системи інтерактивного навчання для підготовки медичних спеціалістів на базі Unity.....	332
Носик А.Ю., Чиж О.В. Геофенсинг (geofencing) як інструмент автоматичного обмеження швидкості електросамокатів у пішохідних зонах.....	333
Павлось К.В., Мельник А.В. Роль систем зв'язку у наданні дистанційної психологічної допомоги постраждалим при надзвичайних ситуаціях.....	334
Пилипенко В.М., Малець І.О. Інформаційна технологія адаптивного моделювання евакуаційних маршрутів для маломобільних груп населення.....	335
Покотілов Б.Р., Крутоус В.С., Зобенко О.О. Основні причини загорянь в електроустановках.....	336
Полов'ян А.В., Демент М.О. Застосування інформаційних технологій в автоматизованих системах пожежної сигналізації.....	337
Полтавський Д.О., Олійник В.В. Застосування широтно-імпульсного управління інерційними об'єктами адаптивних систем безпеки.....	338
Приходько Ю.Ю., Атаманчук В.М. Сучасні системи відеоспостереження та їх характеристика.....	339
Пристацька Ю.О., Шаповалов О.В. Перспективи удосконалення електроживлення систем протипожежного захисту.....	340
Пристацька Ю.О., Шаповалов О.В. Спосіб забезпечення функціонування систем протипожежного захисту в умовах дефіциту електроенергії.....	341
Савченко В.Р., Борсук О.В. Аналіз пожежної небезпеки на автозаправних станціях в умовах застосування резервного живлення.....	342
Савчук Т.Б., Полукаров Ю.О. Інтеграція хмарних технологій в автоматизовані системи оповіщення населення.....	343
Сидоренко С.В., Кравець І.П. Автоматизований моніторинг навантаження електромереж.....	344