

Робоча програма дисципліни «Цивільний захист»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

90

Годин

Загальний обсяг дисципліни

3

Кредити ЄКТС

Відповідно до стандарту

3

Модулі

Змістовних блоки курсу



Загальна інформація про дисципліну

Ідентифікація

Назва: Цивільний захист

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 90 годин / 3 кредити ЄКТС

Модулів: 3 змістовних блоки

Призначення дисципліни

Дисципліна «Цивільний захист» формує у студентів системне розуміння принципів і методів захисту населення, матеріальних цінностей та інформаційної інфраструктури в умовах надзвичайних ситуацій природного, техногенного та воєнного характеру.

Курс є обов'язковим для підготовки бакалаврів зі спеціальності 123 «Комп'ютерна інженерія» за ОП «Організація захисту інформації в інформаційно-комунікаційних системах» та забезпечує формування загальних і фахових компетентностей у сфері безпеки.

Загальні компетентності

Безпекова культура

Здатність до аналізу, оцінювання та управління ризиками в умовах надзвичайних ситуацій; виявлення потенційних небезпек, формування обґрунтованих рішень щодо захисту персоналу та інфраструктури.

Комунікація

Здатність до усної та письмової комунікації у сфері цивільного захисту: чітко інформувати про загрози, складати плани реагування, оформлювати звіти та аналітичні записки за результатами оцінки небезпек.

Самоорганізація

Уміння самостійно навчатися, планувати превентивні заходи та організовувати дії в умовах надзвичайних ситуацій; здатність дотримуватися нормативів та регламентів цивільного захисту.

Командна робота

Відповідальність, ініціативність та готовність діяти в команді під час ліквідації наслідків надзвичайних ситуацій, розподіляти функції та координувати заходи захисту на об'єктах інформаційної інфраструктури.

Студент повинен вміти: аналізувати небезпеки та ризики; приймати рішення в умовах обмеженого часу; планувати власну діяльність у надзвичайних ситуаціях; коректно взаємодіяти з рятувальними службами та колегами; брати участь у командних діях із захисту об'єктів IT-інфраструктури.

Фахові компетентності

Правова база цивільного захисту

Розуміння нормативно-правових засад цивільного захисту в Україні: Кодекс цивільного захисту, закони про критичну інфраструктуру, ДСНС. Знання прав та обов'язків громадян і організацій у сфері цивільного захисту.

Оцінка загроз та ризиків

Здатність ідентифікувати та класифікувати надзвичайні ситуації природного, техногенного та воєнного характеру; оцінювати ризики для об'єктів інформаційно-комунікаційних систем; прогнозувати наслідки аварій і катастроф.

Захист критичної інфраструктури

Знання методів захисту об'єктів критичної інформаційної інфраструктури від впливу надзвичайних ситуацій; вміння розробляти плани евакуації, резервування даних та забезпечення безперервності роботи IT-систем в умовах НС.

Реагування та ліквідація НС

Орієнтування в системі органів управління цивільним захистом; вміння організовувати першу допомогу, дотримуватися алгоритмів дій під час хімічних, радіаційних, пожежних та воєнних небезпек.

Результати навчання

01

Пояснення ключових понять

Пояснювати сутність ключових понять: надзвичайна ситуація, цивільний захист, евакуація, небезпечні фактори, критична інфраструктура, ЄДСЦЗ, радіаційна безпека, техногенна катастрофа, воєнна загроза.

03

Захист в умовах НС

Застосовувати засоби індивідуального та колективного захисту; організовувати евакуацію персоналу та резервування критичних даних; надавати першу допомогу постраждалим при різних видах НС.

02

Класифікація та оцінка НС

Класифікувати надзвичайні ситуації за походженням та масштабом; застосовувати методи оцінки радіаційної, хімічної та вибухової обстановки; прогнозувати зони ураження та розраховувати необхідні захисні заходи.

04

Робота з нормативною базою

Орієнтуватися в нормативно-правовій базі цивільного захисту; використовувати офіційні ресурси ДСНС, МОН та НКЦК для підготовки обґрунтованих планів захисту об'єктів ІТ-інфраструктури.

Правові засади та організаційна структура цивільного захисту

- 
- 1 — Тема 1.1
Правові та організаційні основи цивільного захисту в Україні. Кодекс цивільного захисту.
 - 2 — Тема 1.2
Єдина державна система цивільного захисту (ЄДСЦЗ): структура, органи управління, сили та засоби.
 - 3 — Тема 1.3
Класифікація надзвичайних ситуацій. Моніторинг, прогнозування та оцінка ризиків НС.
 - 4 — Тема 1.4
Планування заходів цивільного захисту на об'єктах. Захист критичної інфраструктури від НС.

Правові та організаційні основи цивільного захисту

Лекційний матеріал (4 год.)

Лекція 1–2: Поняття «цивільний захист», його мета, завдання та принципи. Кодекс цивільного захисту України (2012): структура, ключові положення. Права та обов'язки громадян, підприємств та організацій у сфері ЦЗ. Повноваження ДСНС України. Міжнародне співробітництво у сфері ЦЗ. Зв'язок цивільного захисту з кібербезпекою та захистом інформації в ІКС.

Ключові питання лекції

- Сутність та принципи цивільного захисту
- Кодекс цивільного захисту: структура та зміст
- Права та обов'язки в системі ЦЗ
- Повноваження ДСНС та інших органів
- Зв'язок ЦЗ та безпеки інформаційної інфраструктури

Практичне заняття (2 год.)

Завдання 1. Аналіз Кодексу цивільного захисту України: структура, основні поняття, розмежування відповідальності між органами державної влади та суб'єктами господарювання в ІТ-секторі.

Завдання 2. Кейс: «Обов'язки ІТ-компанії у сфері цивільного захисту під час повномасштабного вторгнення». Групова робота та презентація висновків.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Ткачук А. І., Пуляк О. В. «Цивільний захист України» — розділ «Правові основи» (2023)
- Підготовка реферату: «Роль ДСНС у захисті критичної інформаційної інфраструктури»
- Складання схеми «Система органів управління ЦЗ в Україні»



Очікуваний результат: студент знає нормативно-правову базу ЦЗ, розуміє структуру органів управління та їх роль у захисті об'єктів ІТ-інфраструктури.

Єдина державна система цивільного захисту (ЄДСЦЗ)

1

Центральний рівень

Кабінет Міністрів, ДСНС — стратегічне управління та координація.

2

Регіональний рівень

Обласні військові адміністрації, регіональні підрозділи ДСНС.

3

Місцевий рівень

Органи місцевого самоврядування, комунальні аварійно-рятувальні служби.

4

Об'єктовий рівень

Суб'єкти господарювання, ІТ-підприємства, університети — плани ЦЗ об'єкта.

Лекційний матеріал (2 год.)

Структура ЄДСЦЗ: рівні управління, функціональні та територіальні підсистеми. Режими функціонування системи ЦЗ. Сили та засоби ЦЗ: аварійно-рятувальні служби, формування ЦЗ на підприємствах. Завдання ЦЗ в умовах воєнного стану. Оповіщення та інформування населення — роль ІКС у системі сповіщення.

Практика (1 год.) та СРС (8 год.)

Практика: Аналіз структури ЄДСЦЗ; складання схеми взаємодії органів управління ЦЗ для ІТ-підприємства; визначення режиму функціонування та заходів при різних рівнях загрози.

СРС: Опрацювання: Левченко О. Г. та ін. «Охорона праці та цивільний захист» (вид. КПІ ім. Ігоря Сікорського, 2022); підготовка аналітичної записки «Роль систем оповіщення ЦЗ в забезпеченні безпеки персоналу ІТ-компаній».

Класифікація НС та захист критичної інфраструктури

Тема 1.3 — Класифікація та оцінка НС (Лекція 3, 2 год.)

Класифікація надзвичайних ситуацій: природні (геологічні, метеорологічні, гідрологічні), техногенні (аварії на АЕС, хімічно небезпечних об'єктах, транспорт), соціальні та воєнні. Рівні НС (державний, регіональний, місцевий, об'єктовий). Критерії класифікації. Моніторинг і прогнозування НС: методи, технічні засоби. Особливості НС в умовах воєнного стану 2022–2024 рр.

Практика (1 год.): Класифікація НС за ситуаційними картками; оцінка ризиків для конкретного об'єкта ІКС; складання картки небезпек.

СРС (7 год.): Опрацювання: Ткачук А. І., Пуляк О. В. «Цивільний захист України» (2023); підготовка реферату «Техногенні НС на об'єктах критичної інфраструктури: аналіз та уроки».

Тема 1.4 — Захист критичної інфраструктури (Лекція 4, 2 год.)

Поняття критичної інфраструктури та критичної інформаційної інфраструктури. Законодавство України про захист критичної інфраструктури. Категорії об'єктів критичної інфраструктури (енергетика, зв'язок, ІКС, транспорт). Загрози для ІКС з боку НС: пожежа, затоплення, відключення живлення, кібератаки, воєнні дії. Плани захисту, безперервності роботи та відновлення (BCP/DRP) в умовах НС.

Практика (1 год.): Розробка фрагменту плану захисту об'єкта ІКС від НС; аналіз прикладів порушення роботи ІТ-інфраструктури внаслідок НС в Україні 2022–2024 рр.

СРС (7 год.): Опрацювання постанови КМУ № 1109 «Про критичну інфраструктуру» (2023); підготовка аналітичної записки «Захист ІКС-об'єктів в умовах надзвичайної ситуації».

Захист населення та об'єктів від уражаючих факторів НС

Тема 2.1

Засоби індивідуального та колективного захисту населення.
Сховища, укриття, засоби захисту органів дихання.

Тема 2.2

Евакуація населення та персоналу. Організація евакуаційних заходів на підприємствах, у тому числі в ІТ-секторі.

Тема 2.3

Дії в умовах радіаційної та хімічної небезпеки. Оцінка обстановки. Захист персоналу ІТ-інфраструктури.

Тема 2.4

Дії в умовах пожежної небезпеки та вибухів. Пожежна безпека в центрах обробки даних та серверних приміщеннях.

Засоби захисту населення

Лекційний матеріал (2 год.)

Засоби індивідуального захисту (ЗІЗ): класифікація, вимоги, правила використання. Засоби захисту органів дихання: фільтрувальні та ізолювальні протигази, респіратори, ватно-марлеві пов'язки. Засоби захисту шкіри. Медичні засоби захисту. Колективні засоби захисту: захисні споруди, сховища ЦЗ, укриття протирадіаційні. Вимоги до обладнання сховищ для об'єктів із серверними приміщеннями.

Ключові питання

- Класифікація та призначення ЗІЗ
- Правила підбору та використання засобів захисту органів дихання
- Вимоги до захисних споруд та сховищ
- Особливості захисту устаткування ЦОД та серверних кімнат
- Нормативні вимоги до оснащення об'єктів ЦЗ

Практичне заняття (2 год.)

Завдання 1. Практичне відпрацювання одягання та зняття засобів індивідуального захисту; оцінка захисних властивостей різних типів ЗІЗ.

Завдання 2. Кейс: «Вибір та обладнання укриття для персоналу ІТ-підприємства — критерії та практика». Групова робота.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

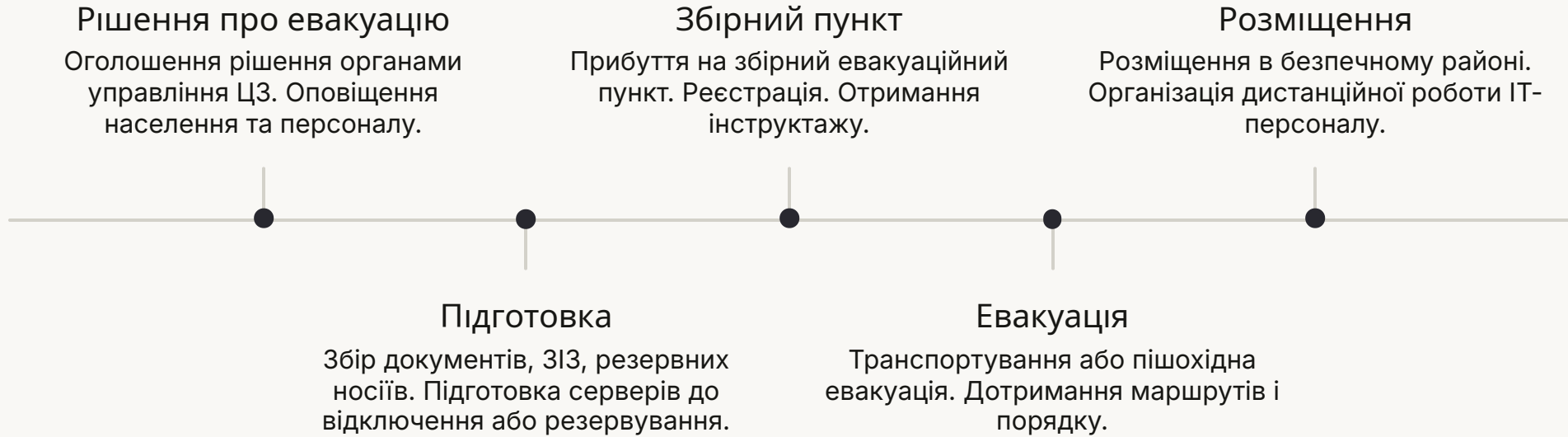
Самостійна робота (7 год.)

- Опрацювання: Запорожець О. І. та ін. «Цивільний захист» — розділ «Засоби захисту» (вид. перероб., 2022)
- Підготовка реферату: «Вимоги до захисних споруд для об'єктів критичної ІТ-інфраструктури»
- Складання порівняльної таблиці засобів захисту органів дихання



Очікуваний результат: студент вміє підбирати та застосовувати засоби індивідуального і колективного захисту, знає вимоги до захисних споруд.

Евакуація населення та персоналу підприємств



Лекційний матеріал (2 год.)

Поняття евакуації, її види: обов'язкова, завчасна, екстрена. Організація евакуаційних заходів: збірні евакуаційні пункти, маршрути евакуації, транспортне забезпечення. Евакуація персоналу ІТ-підприємств: особливості збереження та вивезення серверного устаткування, резервних носіїв, документації з грифом таємності. Реевакуація та повернення. Досвід евакуації в умовах воєнного стану в Україні 2022–2024 рр.

Практика (1 год.) та СРС (8 год.)

Практика: Розробка плану евакуації для навчального корпусу або офісного приміщення ІТ-компанії; відпрацювання алгоритму дій персоналу при сигналі «Повітряна тривога».

СРС: Опрацювання: Дубінін В. А. та ін. «Актуальні питання цивільного захисту» (НУК, 2022) — розділ «Евакуація»; підготовка плану евакуації для реального або модельного ІТ-об'єкта.

Радіаційна, хімічна та пожежна небезпека

Тема 2.3 — Радіаційна та хімічна небезпека (Лекція 7, 2 год.)

Радіаційна небезпека: іонізуюче випромінювання, одиниці вимірювання, допустимі рівні опромінення. Аварії на атомних електростанціях: уроки Чорнобиля та Запорізької АЕС. Хімічна небезпека: класифікація небезпечних хімічних речовин (СДОР), зони хімічного зараження, прогнозування обстановки. Методи дозиметричного та хімічного контролю. Дії персоналу ІТ-об'єктів при радіаційній та хімічній тривозі.

Практика (1 год.): Робота з дозиметричними приладами; розрахунок зони хімічного зараження; складання алгоритму дій при хімічній аварії поблизу ІТ-об'єкта.

СРС (7 год.): Опрацювання: Левченко О. Г. та ін. «Охорона праці та цивільний захист» (КПІ ім. Ігоря Сікорського, 2022) — теми радіаційної та хімічної небезпеки; підготовка аналітичної записки «Запорізька АЕС в умовах воєнного конфлікту: ризики та захист».

Тема 2.4 — Пожежна небезпека та вибухи (Лекція 8, 2 год.)

Основи пожежної безпеки: горіння, класи пожеж, вогнегасні речовини та засоби. Особливості пожежної безпеки в центрах обробки даних (ЦОД), серверних приміщеннях та кабельних трасах. Автоматичні системи пожежогасіння для ІТ-обладнання (газове, аерозольне). Вибухонебезпечні об'єкти поблизу ІТ-інфраструктури. Організація евакуації при пожежі. Перша допомога при опіках та отруєнні продуктами горіння. Воєнні аспекти пожежної безпеки.

Практика (1 год.): Практичне відпрацювання правил користування вогнегасниками; аналіз систем пожежогасіння для ЦОД; складання плану пожежної безпеки серверного приміщення.

СРС (7 год.): Підготовка аналітичної записки «Вимоги до пожежної безпеки центрів обробки даних: стандарти та практика»; опрацювання ДСТУ та будівельних норм для ЦОД.

Медична підготовка та захист в умовах воєнного стану

Тема 3.1

Перша домедична допомога. Алгоритми надання допомоги при різних видах ураження: поранення, опіки, ураження СДОР та РР.

Тема 3.2

Психологічна безпека та стресостійкість в умовах НС та воєнного стану. Психологічна перша допомога.

Тема 3.3

Захист інформаційної інфраструктури в умовах воєнних дій. Забезпечення безперервності роботи ІКС під час НС.

Перша домедична допомога

Лекційний матеріал (2 год.)

Правова база надання першої допомоги в Україні. Алгоритм ABCDE при оцінці постраждалого. Зупинка кровотечі: методи та засоби (джгут, турнікет). Серцево-легенева реанімація (СЛР). Допомога при переломах, вивихах, травмах хребта. Допомога при отруєннях хімічними речовинами та чадним газом. Допомога при опіках, електротравмах. Допомога при мінно-вибуховій травмі (MBT). Сорткування постраждалих за системою START.

Ключові питання

- Алгоритм дій при виявленні постраждалого
- Зупинка зовнішньої кровотечі: турнікет, джгут, пов'язка
- Серцево-легенева реанімація: техніка та показання
- Допомога при хімічному ураженні та отруєнні продуктами горіння
- Принципи медичного сортування в осередку масового ураження

Практичне заняття (2 год.)

Завдання 1. Практичне відпрацювання алгоритму ABCDE: огляд постраждалого, визначення пріоритетів допомоги. Накладання турнікета та джгута.

Завдання 2. Відпрацювання серцево-легеневої реанімації на манекені; надання допомоги при опіках та хімічних ураженнях.

Завдання 3. Тестування за ключовими термінами та алгоритмами (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Гур'єв С. О., Волянський П. Б. «Медицина надзвичайних ситуацій» — навч. посіб. (2023)
- Підготовка інструкції «Дії персоналу IT-підрозділу при виявленні постраждалого»
- Складання алгоритму медичної сортування для осередку ураження



Очікуваний результат: студент вміє надавати першу допомогу при основних видах ураження, застосовувати алгоритм ABCDE та засоби зупинки кровотечі.

Психологічна безпека та стресостійкість в умовах НС

Лекційний матеріал (2 год.)

Психологічні реакції людини на НС та війнні події: шок, паніка, ПТСР. Фактори психологічної стійкості. Психологічна перша допомога (ППД): принципи, методи, алгоритм. Управління стресом в умовах тривалої НС та воєнного стану. Психологічна безпека ІТ-персоналу, що працює з критичними системами в умовах надзвичайних обставин. Ресурси психологічної підтримки в Україні.

Практика (1 год.) та СРС (8 год.)

Практика: Відпрацювання навичок психологічної першої допомоги; аналіз кейсів психологічних реакцій ІТ-спеціалістів в умовах воєнного стану; техніки саморегуляції та зниження стресу.

СРС: Опрацювання методичних рекомендацій МОЗ України «Психологічна перша допомога» (2022); підготовка аналітичної записки «Психологічна безпека ІТ-персоналу в умовах воєнного стану: виклики та рішення».

 **Очікуваний результат:** студент знає принципи психологічної першої допомоги, вміє застосовувати техніки стресостійкості та підтримки колег у кризових ситуаціях.

Захист ІКС та забезпечення безперервності в умовах воєнних дій



Оцінка загроз

Ідентифікація фізичних та кібернетичних загроз для ІКС в умовах воєнного стану. Аналіз вразливостей об'єкта.



Резервування та захист даних

Організація резервного копіювання критичних даних. Хмарні рішення для забезпечення безперервності. Географічне розосередження ресурсів.



Плани відновлення

Розробка та тестування BCP/DRP-планів для ІКС. Процедури аварійного переключення та відновлення після НС.

Лекційний матеріал (4 год.)

Загрози для ІКС в умовах воєнних дій: фізичне руйнування, відключення живлення, кібератаки. Законодавство про захист критичної інформаційної інфраструктури (КІІ). Стандарти безперервності бізнесу (ISO 22301) та їх адаптація до умов НС. Плани забезпечення безперервності роботи (BCP) та відновлення після катастрофи (DRP). Досвід українських ІТ-компаній під час воєнного стану 2022–2024 рр.: хмарна міграція, резервування, дистанційна робота. Координація ЦЗ та кіберзахисту.

Практика (2 год.) та СРС (7 год.)

Практика: Розробка фрагменту BCP/DRP для модельного ІТ-підприємства з урахуванням загроз НС; аналіз реальних кейсів відновлення ІКС після кібератак та фізичних пошкоджень в Україні.

СРС: Опрацювання Закону України «Про критичну інфраструктуру» (2021) та постанови КМУ № 1109 (2023); підготовка міні-проекту «Комплексний план захисту ІКС-об'єкта в умовах НС та воєнного стану».



Очікуваний результат: студент вміє розробляти плани захисту ІКС від НС, організовувати резервування та відновлення критичних даних, застосовувати стандарти безперервності.

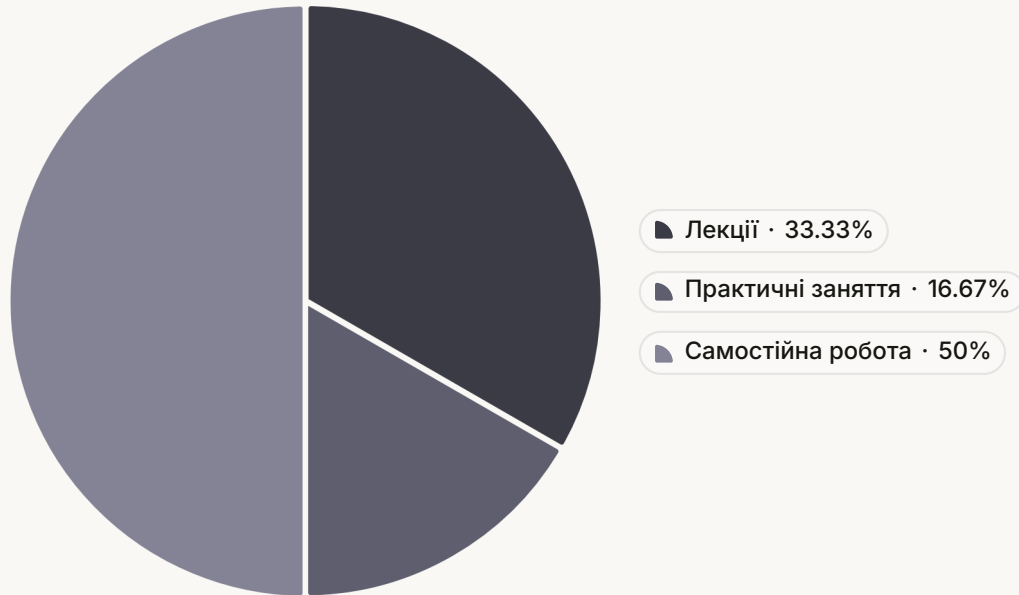
Розподіл навчального часу — 90 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Правові основи ЦЗ	4	2	7
	Тема 1.2 — ЄДСЦЗ	2	1	8
	Тема 1.3 — Класифікація НС	2	1	7
	Тема 1.4 — Захист критичної інфраструктури	2	1	7
Модуль 2	Тема 2.1 — Засоби захисту	2	2	7
	Тема 2.2 — Евакуація	2	1	8
	Тема 2.3 — Радіаційна та хімічна небезпека	2	1	7
	Тема 2.4 — Пожежна небезпека та вибухи	2	1	7
Модуль 3	Тема 3.1 — Перша домедична допомога	2	2	7
	Тема 3.2 — Психологічна безпека	2	1	8
	Тема 3.3 — Захист ІКС в умовах воєнних дій	4	2	7
Разом	11 тем	28	15	47



Загальний обсяг: 90 годин = 3 кредити ЄКТС. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу. Лекцій — 30 год., практичних — 15 год., СРС — 45 год.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **90 годин (3 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теорією та практикою безпеки.

Лекції — 30 год. (33%)

Системне подання теоретичного матеріалу з нормативно-правової бази ЦЗ, класифікації НС, методів захисту та дій персоналу ІКС в умовах надзвичайних ситуацій.

Практичні — 15 год. (17%)

Практичне відпрацювання навичок: ЗІЗ, перша допомога, аналіз кейсів, розробка планів захисту ІКС, складання BCP/DRP-документів.

Самостійна робота — 45 год. (50%)

Поглиблене вивчення, підготовка завдань, робота з нормативною базою та науковою літературою. СРС становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис



Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками та посібниками з цивільного захисту (Запорожець, Михайлюк, Левченко, Ткачук та ін.), нормативно-правовими актами (Кодекс ЦЗ, закони про КИ). Студент конспектує ключові положення, виділяє поняття та порівнює підходи різних авторів.



Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: ДСНС України (dsns.gov.ua), НКЦК (ncsc.gov.ua), Верховної Ради (zakon.rada.gov.ua), МОН (mon.gov.ua). Аналіз нормативних актів і публікацій для навчальних завдань.



Індивідуальні завдання

Виконання аналітичних завдань (оцінка ризиків об'єктів, розробка планів ЦЗ); творчих завдань — реферати, аналітичні записки, міні-проекти з актуальних питань захисту ІКС в умовах НС та воєнного стану.



Підготовка до занять

Підготовка до практичних занять (вивчення алгоритмів дій, повторення теорії); підготовка до тестувань (ключові терміни, нормативи, порядки); підготовка до контрольних робіт за кожним модулем.

Форми контролю знань

1

Поточний контроль

Завдання: аналітичні та тестові вправи за темами змістовного модуля.

Оцінюються регулярність виконання завдань, якість відповідей та рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру.

Проводиться після кожної теми у формі тестування (10–15 питань) або усного опитування.

2

Проміжний контроль

Самостійна робота — комплексне ситуаційне завдання або розробка плану заходів ЦЗ, що охоплює теми змістовних модулів (теоретичні питання, оцінка ризиків, практичні рекомендації). Оцінюються повнота відповіді, аргументованість та обґрунтованість висновків.

Проводиться після завершення кожного модуля.

3

Підсумковий контроль

Залік відповідно до навчального плану. Форма проведення — тестування та письмові відповіді на питання.

Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали: **100-бальна система** з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Методи викладання

Викладання дисципліни «Цивільний захист» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише теоретичної бази, а й практичних навичок безпечної поведінки, необхідних для майбутньої фахової діяльності у сфері захисту інформації в ІКС.



Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, нормативних таблиць і прикладів з практики ЦЗ та захисту ІКС в умовах НС.



Робота з нормативними актами

Опрацювання Кодексу ЦЗ, законів та постанов; формування навичок критичного аналізу правової бази та її застосування до конкретних об'єктів ІКС.



Кейс-стаді

Аналіз реальних надзвичайних ситуацій в Україні та їх наслідків для об'єктів ІКС; вироблення практичних рекомендацій щодо захисту.



Практичні тренування

Відпрацювання навичок першої допомоги, застосування ЗІЗ, складання планів евакуації та ВСП/DRP — ключових компетенцій фахівця з захисту інформації.



Самостійне дослідження

Підготовка аналітичних записок і міні-проектів; розвиток навичок самостійного аналізу ризиків та розробки заходів безпеки для ІКС-об'єктів.



Проектна робота

Розробка комплексного плану захисту модельного об'єкта ІКС від НС природного, техногенного та воєнного характеру — підсумковий проект курсу.



Усі методи спрямовані на формування компетентностей, передбачених ОП «Організація захисту інформації в ІКС» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література — Підручники та посібники (2022–2024 рр.)

1. Ткачук А. І., Пуляк О. В.

Цивільний захист України : навч. посіб. для студентів ЗВО. — Кропивницький : РВВ ЦДУ ім. В. Винниченка, 2023. — 284 с.

2. Левченко О. Г. та ін.

Охорона праці та цивільний захист : підручник / О. Г. Левченко, О. І. Полукаров, В. В. Зацарний та ін. ; за ред. О. Г. Левченка. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 414 с.

3. Дубінін В. А. та ін.

Актуальні питання цивільного захисту : навч. посіб. / В. А. Дубінін, В. І. Ізотов, В. В. Ляшенко та ін. — 2-ге вид., доопр. — Миколаїв : Видавництво «НУК», 2022. — 464 с.

4. Гур'єв С. О., Волянський П. Б.

Медицина надзвичайних ситуацій та медична служба цивільного захисту : навч. посіб. — Київ : Медицина, 2023. — 320 с.

5. Запорожець О. І. та ін.

Цивільний захист : підручник / О. І. Запорожець, В. О. Михайлюк, Б. Д. Халмурадов, А. В. Русаловський, Н. В. Кулалаєва. — 2-ге вид., перероб. — Київ : Центр учбової літератури, 2022. — 264 с.

6. Васійчук В. О. та ін.

Основи цивільного захисту : навч. посіб. / В. О. Васійчук, В. Є. Гончарук, С. І. Качан, С. М. Мохняк. — 3-тє вид., доповн. — Львів : Видавництво Львівської політехніки, 2023. — 384 с.

7. Євдін О. М. та ін.

Захист населення і територій від надзвичайних ситуацій : навч. посіб. / О. М. Євдін, В. В. Могильниченко та ін. — Вид. доопр. — Київ : КІМ, 2022. — 312 с.

8. Сусло С. Т. та ін.

Цивільний захист : навч. посіб. / С. Т. Сусло, В. М. Заплатинський, Г. М. Харамда. — 4-те вид., перероб. — Київ : Академія, 2023. — 264 с.

Додаткова література та наукові статті

9. Михайлюк В. О., Халмурадов Б. Д.

Цивільна безпека : навч. посіб. — 3-тє вид., перероб. та доп. — Київ : Центр учбової літератури, 2022. — 160 с. *Рекомендується для тем 1.1–1.2 (основи ЦЗ).*

11. Тимошенко О. І., Гаврилюк О. В.

Кібербезпека та штучний інтелект у контексті забезпечення безпеки підприємництва у воєнний час // Матеріали IX Міжнар. наук.-практ. конф. «Актуальні питання кібербезпеки та захисту інформації». — Київ : Європейський університет, 2023. — С. 18–22. *Рекомендується для теми 3.3.*

10. Бикова О. В. та ін.

Основи цивільного захисту : посіб. для студентів ЗВО / за заг. ред. М. В. Болотських. — 2-ге вид., доопр. — Київ : ДСНС України, 2023. — 248 с. *Рекомендується для модулів 1–2.*

12. Осипенко С. І., Іванов А. В.

Організація функціонального навчання у сфері цивільного захисту : навч. посіб. — 2-ге вид., оновл. — Київ : ДСНС України, 2022. — 288 с. *Рекомендується для всіх модулів.*

Нормативно-правова база

- Кодекс цивільного захисту України від 02.10.2012 № 5403-VI
Основний законодавчий акт у сфері ЦЗ. Чинний зі змінами. zakon.rada.gov.ua
- Закон «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX
Визначає засади захисту об'єктів критичної інфраструктури, у т. ч. інформаційно-комунікаційних систем. zakon.rada.gov.ua
- Закон «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII
Регулює відносини у сфері кібербезпеки та захисту критичної інформаційної інфраструктури. zakon.rada.gov.ua
- Постанова КМУ № 1109 від 09.10.2023 «Про критичну інфраструктуру»
Визначає порядок формування переліку об'єктів критичної інфраструктури та їх захисту. zakon.rada.gov.ua
- Закон «Про захист населення і територій від надзвичайних ситуацій» від 08.06.2000 № 1809-III
zakon.rada.gov.ua

Офіційні ресурси та фахові видання

ДСНС України

dsns.gov.ua — офіційна інформація про надзвичайні ситуації, нормативні документи, методичні матеріали з ЦЗ.

Верховна Рада України

zakon.rada.gov.ua — нормативно-правова база ЦЗ, кодекси, закони, постанови уряду з питань безпеки та ЦЗ.

НКЦК (Національний координаційний центр кібербезпеки)

ncsc.gov.ua — матеріали із захисту критичної інформаційної інфраструктури, кіберінциденти, рекомендації.

МОН України — ЦЗ та БЖД

mon.gov.ua — освітні стандарти, методичні матеріали з цивільного захисту та безпеки у ЗВО.

Навчально-методичний центр ЦЗ та БЖД

nmc.dsns.gov.ua — навчальні посібники, методичні матеріали, програми підготовки з ЦЗ.

Журнал «Надзвичайна ситуація»

Фахове видання ДСНС України — аналітичні матеріали, огляди нормативної бази, практичний досвід у сфері ЦЗ.

Держспецзв'язку (ДЦКЗ)

cip.gov.ua — матеріали з кіберзахисту об'єктів КІІ, рекомендації, звіти про кіберінциденти в Україні.

Університет цивільного захисту України

nuczu.edu.ua — наукові публікації, монографії та матеріали конференцій у сфері ЦЗ.

Зв'язок дисципліни зі спеціальністю 123 «Комп'ютерна інженерія»

Чому «Цивільний захист» для фахівців із захисту інформації?

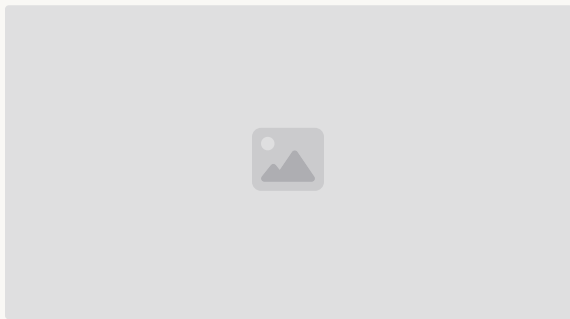
Дисципліна «Цивільний захист» є невід'ємною складовою підготовки бакалаврів за ОП «Організація захисту інформації в ІКС». Фахівець із захисту інформації повинен уміти не лише протидіяти кіберзагрозам, а й забезпечувати фізичну безпеку ІКС-інфраструктури в умовах НС та воєнних дій.

В умовах повномасштабної агресії Росії проти України забезпечення безперервності роботи ІКС, евакуація серверного обладнання та захист даних стали реальними щоденними завданнями ІТ-фахівців.

Практичне значення для майбутньої кар'єри

- Розробка та впровадження BCP/DRP-планів для ІКС-підприємств
- Забезпечення фізичної безпеки центрів обробки даних і серверних приміщень
- Організація захисту персоналу та обладнання в умовах НС
- Взаємодія зі службами ЦЗ та ДСНС при ліквідації наслідків НС на ІКС-об'єктах
- Відповідність вимогам законодавства про захист критичної інформаційної інфраструктури
- Комплексний підхід до безпеки: поєднання кіберзахисту та фізичного ЦЗ

Ключові компетентності курсу — Підсумок



Курс охоплює всі ключові аспекти цивільного захисту — від нормативно-правової бази до практичних навичок рятування та захисту ІКС-інфраструктури — і формує у студентів комплексне розуміння безпеки в сучасних умовах воєнного стану та надзвичайних ситуацій.

Бажаємо успіхів у вивченні Цивільного захисту!

90

Годин

Загальний обсяг дисципліни

3

Кредити ЄКТС

Відповідно до стандарту

11

Тем

У 3 змістовних модулях

8

Джерел

Рекомендованої літератури 2022–2024 рр.

«Безпека — це не просто відсутність небезпеки, це готовність до дії.» — принцип цивільного захисту

Спеціальність 123 · Комп'ютерна інженерія · ОП «Організація захисту інформації в ІКС» · Бакалавр · 3 кредити ЄКТС