



Силабус дисципліни «Цивільний захист»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ · БАКАЛАВР · ОП
«ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІКС»

90

Годин загальний обсяг дисципліни

3

Кредити ЄКТС відповідно до
стандарту

3

Змістовних модулів 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 курсу

Мета дисципліни

Дисципліна «Цивільний захист» формує у студентів спеціальності «Комп'ютерна інженерія» систему знань, умінь і навичок у сфері цивільного захисту населення, захисту критичної інформаційної інфраструктури та забезпечення безпеки в умовах надзвичайних ситуацій. Курс спрямований на опанування нормативно-правової бази, принципів організації єдиної державної системи цивільного захисту, порядку дій при загрозах різного характеру, а також особливостей захисту інформаційно-комунікаційних систем в умовах надзвичайних ситуацій та воєнного стану.

Форми навчання

- Лекції — 30 годин
- Практичні заняття — 15 годин
- Самостійна робота — 45 годин

Компетентності та результати навчання

Загальні компетентності

Здатність до аналізу, синтезу та критичного оцінювання нормативно-правової й технічної інформації у сфері цивільного захисту та безпеки: виявлення суттєвих загроз, порівняння нормативних підходів, формування обґрунтованих висновків щодо організації захисту населення та об'єктів. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки планів реагування та алгоритмів дій у надзвичайних ситуаціях.

Здатність до усної та письмової фахової комунікації: чітко пояснювати вимоги нормативних документів, аргументовано обґрунтовувати рішення щодо захисту в умовах НС. Відповідальність, ініціативність, дисциплінованість та готовність працювати в команді.

- Аналізувати нормативно-правові акти у сфері цивільного захисту та безпеки ІКС
- Планувати власну діяльність і дотримуватися дедлайнів
- Коректно спілкуватися з викладачами та одногрупниками
- Брати участь у командній роботі та розподіляти обов'язки

Фахові компетентності

Розуміння сутності та закономірностей організації цивільного захисту, його місця у системі забезпечення безпеки інформаційно-комунікаційних систем і критичної інфраструктури. Знання ключових понять, нормативних вимог і процедур реагування на надзвичайні ситуації різного характеру, вміння застосовувати їх у практичній діяльності фахівця з інформаційної безпеки.

Здатність застосовувати заходи цивільного захисту для забезпечення сталого функціонування ІКС в умовах надзвичайних ситуацій, кризових явищ та воєнного часу.

- Характеризувати нормативно-правову базу цивільного захисту України
- Організовувати захист персоналу та об'єктів ІКС при НС
- Застосовувати засоби індивідуального та колективного захисту
- Розробляти плани реагування на НС для об'єктів критичної інфраструктури
- Проводити оцінку ризиків та моніторинг загроз у сфері ЦЗ

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять цивільного захисту: надзвичайна ситуація, режим надзвичайного стану, воєнний стан, критична інфраструктура, цивільний захист, евакуація, укриття, засоби індивідуального захисту, радіаційна та хімічна безпека. Характеризувати нормативно-правову базу, що регламентує організацію цивільного захисту в Україні, в тому числі в умовах воєнного стану.

2

Аналіз та оцінювання

Аналізувати загрози надзвичайних ситуацій техногенного, природного та воєнного характеру з точки зору їхнього впливу на функціонування ІКС. Оцінювати відповідність заходів цивільного захисту об'єктів вимогам чинного законодавства та нормативних актів. Виявляти вразливості критичної інфраструктури та інформаційних систем у контексті можливих НС.

3

Застосування знань

Застосовувати методи та засоби цивільного захисту при організації безпеки об'єктів ІКС у надзвичайних ситуаціях. Розробляти плани реагування на НС, інструкції з евакуації, схеми оповіщення та процедури забезпечення безперервності функціонування ІКС в умовах кризових ситуацій.

4

Комунікація та рефлексія

Аргументовано викладати власну позицію щодо організації цивільного захисту об'єктів ІКС у конкретних умовах загроз. Формувати професійну відповідальність і розуміння важливості дотримання вимог безпеки та цивільного захисту у фаховій діяльності фахівця з інформаційної безпеки.

Модуль 1. Правові та організаційні основи цивільного захисту

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Поняття, завдання та принципи цивільного захисту.

Місце цивільного захисту в системі національної безпеки України. Основні терміни та визначення: надзвичайна ситуація, цивільний захист, захист населення, цивільна оборона. Класифікація надзвичайних ситуацій. Принципи організації цивільного захисту. Роль ЦЗ у забезпеченні безпеки об'єктів ІКС.

Тема 1.2

Нормативно-правова база цивільного захисту. Кодекс цивільного захисту України. Закони України «Про правовий режим надзвичайного стану», «Про правовий режим воєнного стану», «Про критичну інфраструктуру». Підзаконні нормативні акти ДСНС. Міжнародні стандарти ISO серії 22301 щодо безперервності бізнесу в умовах надзвичайних ситуацій.

Тема 1.3

Єдина державна система цивільного захисту (ЄДСЦЗ). Структура та завдання ЄДСЦЗ. Органи управління, сили та засоби ЦЗ. Режими функціонування ЄДСЦЗ. Взаємодія органів державної влади, місцевого самоврядування та суб'єктів господарювання. Місце об'єктів ІКС у системі ЦЗ.

Тема 1.4

Організація цивільного захисту на об'єкті господарювання. Обов'язки та завдання керівника з ЦЗ на підприємстві/в установі. Розроблення планів цивільного захисту об'єктів. Організація навчання персоналу. Особливості ЦЗ на об'єктах критичної інфраструктури та в установах, що обробляють інформацію з обмеженим доступом.

Модуль 2. Надзвичайні ситуації та захист населення і територій

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Надзвичайні ситуації техногенного та природного характеру. Класифікація та характеристика техногенних НС: аварії на підприємствах, пожежі, вибухи, викиди СДОР. Надзвичайні ситуації природного характеру. Вражаючі чинники НС. Методи прогнозування та оцінки обстановки. Вплив НС техногенного характеру на функціонування ІКС та центрів обробки даних.

Тема 2.2

Надзвичайні ситуації воєнного характеру та кіберзагрози.

Особливості НС воєнного часу. Захист населення в умовах воєнного стану. Поняття критичної інформаційної інфраструктури (КІІ). Взаємозв'язок фізичних НС і кіберзагроз. Захист ІКС та КІІ від комбінованих загроз. Вимоги до резервування та безперервності функціонування ІКС.

Тема 2.3

Засоби та способи захисту населення. Засоби колективного захисту: сховища, укриття, захисні споруди. Засоби індивідуального захисту органів дихання та шкіри. Евакуаційні заходи: організація та порядок проведення. Медичний захист та домедична допомога. Особливості захисту персоналу об'єктів ІКС при НС різного характеру.

Модуль 3. Захист критичної інфраструктури та ліквідація наслідків НС

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Захист критичної інформаційної інфраструктури в умовах НС. Поняття та класифікація об'єктів КІІ. Категоризація об'єктів критичної інфраструктури. Вимоги до забезпечення безперервності функціонування ІКС при НС. Плани забезпечення безперервності (BCP) та відновлення після катастроф (DRP) в контексті вимог ЦЗ. Міжнародний досвід захисту КІІ.

Тема 3.2

Моніторинг, прогнозування та реагування на НС. Організація моніторингу та прогнозування НС. Системи раннього оповіщення. Порядок дій при загрозі та виникненні НС. Алгоритми реагування персоналу об'єктів ІКС на НС різного характеру. Координація дій з органами ДСНС та іншими службами. Документування інцидентів.

Тема 3.3

Ліквідація наслідків НС та відновлення функціонування ІКС. Організація аварійно-рятувальних та інших невідкладних робіт. Порядок відновлення функціонування ІКС після НС. Розслідування та облік НС. Актуальні зміни нормативно-правового регулювання ЦЗ в умовах воєнного стану. Міжнародна гуманітарна допомога та взаємодія з міжнародними організаціями.

Розподіл навчального часу — 90 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Поняття, завдання та принципи цивільного захисту	2	1	4
	Тема 1.2 — Нормативно-правова база ЦЗ	2	1	4
	Тема 1.3 — Єдина державна система цивільного захисту	2	1	4
	Тема 1.4 — Організація ЦЗ на об'єкті господарювання	2	2	4
Модуль 2	Тема 2.1 — НС техногенного та природного характеру	4	2	5
	Тема 2.2 — НС воєнного характеру та кіберзагрози	4	2	5
	Тема 2.3 — Засоби та способи захисту населення	4	2	5
Модуль 3	Тема 3.1 — Захист критичної інформаційної інфраструктури	4	2	6
	Тема 3.2 — Моніторинг, прогнозування та реагування на НС	4	1	6
	Тема 3.3 — Ліквідація наслідків НС та відновлення ІКС	2	1	6
Разом		30	15	45



Структура навчального часу

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

- **Лекції (30 год. — 33%):** подача ключового теоретичного матеріалу
- **Практичні (15 год. — 17%):** відпрацювання навичок, аналіз нормативних документів, вирішення кейсів
- **Самостійна робота (45 год. — 50%):** поглиблене вивчення, підготовка завдань



Самостійна робота становить **50% обсягу дисципліни** — студенти навчаються працювати з нормативними документами та джерелами самостійно.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з цивільного захисту та безпеки ІКС, нормативно-правовими актами, науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння підходів різних авторів до організації ЦЗ об'єктів критичної інфраструктури.

Індивідуальні завдання

Виконання аналітичних завдань щодо оцінки ризиків НС для об'єктів ІКС, підготовка планів реагування на НС, схем евакуації, аналітичних записок з актуальних питань захисту критичної інформаційної інфраструктури в умовах надзвичайних ситуацій та воєнного стану.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: ДСНС України (dsns.gov.ua), Верховна Рада (zakon.rada.gov.ua), Держспецзв'язку (cip.gov.ua). Аналіз нормативних актів, методичних рекомендацій, стандартів у сфері цивільного захисту та безпеки КІІ.

Підготовка до занять

Підготовка до практичних занять шляхом опрацювання нормативних документів, повторення теоретичного матеріалу; підготовка до тестувань через вивчення ключових термінів та визначень; систематизація знань перед контрольними роботами.

Методи викладання

→ Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, таблиць і прикладів з нормативних актів; студенти ведуть конспекти та задають уточнювальні запитання.

→ Кейс-стаді

Аналіз реальних ситуацій надзвичайних ситуацій та їх впливу на функціонування об'єктів ІКС; студенти виявляють проблему, пропонують рішення та обґрунтовують висновки щодо захисту критичної інфраструктури.

→ Практичні вправи

Розроблення планів реагування на НС, алгоритмів евакуації персоналу, схем оповіщення; відпрацювання навичок надання домедичної допомоги та дій при різних видах НС.

→ Робота з нормативними документами

Опрацювання законів, підзаконних актів, стандартів з питань ЦЗ та безпеки КІІ; формування навичок аналізу нормативно-правового середовища та їх застосування у практичній діяльності.

→ Самостійне дослідження

Підготовка аналітичних записок, рефератів і презентацій за обраною темою; розвиток навичок самостійного пошуку та систематизації нормативної й наукової інформації з питань цивільного захисту.

Форми контролю знань

1

Поточний контроль

Завдання: аналітичні та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання завдань, якість відповідей і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, письмові відповіді на запитання, розбір нормативних актів та участь у вирішенні кейсів із захисту об'єктів ІКС в умовах НС.

2

Проміжний контроль

Самостійна робота — комплексне практичне завдання або реферат, які охоплюють теми змістовних модулів (теоретичні питання, аналіз нормативної бази, розробка плану реагування на НС або схеми захисту об'єкта ІКС). Оцінюються повнота відповіді, правильність аналізу та обґрунтованість висновків. Проводиться після кожного змістовного модуля.

3

Підсумковий контроль

Іспит відповідно до навчального плану. Форма проведення — тестування та письмові відповіді на питання з усіх трьох модулів курсу. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали оцінювання: 100-бальна система з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

- ❏ Усі методи контролю спрямовані на формування компетентностей, передбачених освітньо-професійною програмою «Організація захисту інформації в ІКС» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Беліков А. С., Коротаєв В. С., Шаломов В. А., Подкопаєв С. В. та ін. Цивільний захист: підручник / за заг. ред. А. С. Белікова. — Дніпро : Журфонд, 2024. — 516 с.
2. Васійчук В. О., Гончарук В. Є., Качан С. І., Мохняк С. М. Основи цивільного захисту: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 384 с.
3. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: підручник. — Житомир : ЖНАЕУ, 2023. — 636 с.
4. Дудикевич В. Б., Хорошко В. О. Захист інформації в інформаційно-комунікаційних системах: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 312 с.
5. Євдін О. М., Могильниченко В. В., Михайлюк В. О. Захист населення і територій від надзвичайних ситуацій: навч. посіб. — Київ : КІМ, 2022. — 428 с.
6. Корченко О. Г., Архипов О. Є. Системи захисту інформації: стандарти та нормативна база: підручник. — Київ : НАУ, 2022. — 398 с.
7. Кудрявицька А. М., Ракоїд О. О., Боголюбов В. М. Цивільний захист: навч. посіб. — Київ : НУБіП України, 2024. — 310 с.
8. Романченко І. С., Стрільчук В. Ф. Організація цивільного захисту критичної інфраструктури: навч. посіб. — Київ : НУОУ, 2023. — 296 с.
9. Сідак В. С., Франчук В. І. Правові основи цивільного захисту та безпеки об'єктів критичної інфраструктури: навч. посіб. — Київ : Університет «Україна», 2023. — 264 с.
10. Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки: підручник. — Київ : ДУІКТ, 2022. — 476 с.

Офіційні інтернет-ресурси

1. Державна служба України з надзвичайних ситуацій (ДСНС). — URL: <https://dsns.gov.ua/>
2. Офіційний сайт Верховної Ради України. — URL: <https://zakon.rada.gov.ua/>
3. Державна служба спеціального зв'язку та захисту інформації України. — URL: <https://cip.gov.ua/>
4. Офіційний сайт Кабінету Міністрів України. — URL: <https://www.kmu.gov.ua/>
5. Національний університет цивільного захисту України. — URL: <https://nuczu.edu.ua/>
6. Міністерство цифрової трансформації України. — URL: <https://thedigital.gov.ua/>
7. Науково-технічний журнал «Кібербезпека: освіта, наука, техніка». — URL: <https://csecurity.kubg.edu.ua/>
8. Національна бібліотека України ім. В. І. Вернадського. — URL: <https://nbuv.gov.ua/>



Рекомендована література охоплює видання **2022–2024 років** українських авторів відповідно до вимог актуальності навчально-методичного забезпечення ОП «Організація захисту інформації в ІКС».