



Силабус дисципліни «Інформаційна культура»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ · БАКАЛАВР

ОП: Організація захисту інформації в інформаційно-комунікаційних системах

90

Годин загальний обсяг дисципліни

3

Кредити ЄКТС відповідно до
стандарту

3

Змістовних модулів курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Інформаційна культура

Спеціальність: 123 Комп'ютерна інженерія

Ступінь: Бакалавр

ОП: Організація захисту інформації в ІКС

Обсяг: 90 годин / 3 кредити ЄКТС

Модулів: 3 змістовних блоки курсу

Мета дисципліни

Дисципліна «Інформаційна культура» формує у студентів спеціальності «Комп'ютерна інженерія» освітньої програми «Організація захисту інформації в інформаційно-комунікаційних системах» систему знань, умінь і навичок щодо ефективної роботи з інформацією в цифровому середовищі. Курс спрямований на розвиток критичного мислення, медіаграмотності, навичок пошуку, оцінювання та безпечного використання інформаційних ресурсів, а також формування відповідального ставлення до інформаційної діяльності в контексті захисту інформації.

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 інформації в цифровому та інформаційному середовищі: виявлення достовірних джерел, порівняння альтернативних інтерпретацій, формування обґрунтованих висновків і висловлення власної позиції. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час опрацювання інформаційних ресурсів, підготовки рефератів та аналітичних матеріалів.

Здатність до усної та письмової професійної комунікації в інформаційному середовищі: чітко пояснювати поняття інформаційної культури та безпеки, аргументовано відповідати на запитання, оформлювати звіти та аналітичні матеріали. Відповідальність та готовність дотримуватися норм інформаційної етики у власній та командній роботі.

- Аналізувати навчальну, наукову та цифрову інформацію
- Виділяти головне та узагальнювати результати досліджень
- Планувати власну діяльність і дотримуватися дедлайнів
- Коректно комунікувати в цифровому та академічному середовищі
- Брати участь у командній роботі та розподіляти обов'язки

Фахові компетентності

Розуміння сутності та закономірностей інформаційної культури особистості й суспільства, її місця в системі захисту інформації в інформаційно-комунікаційних системах. Знання ключових понять, принципів і моделей інформаційної культури, вміння застосовувати їх в контексті комп'ютерної інженерії та кібербезпеки.

Здатність застосовувати методи критичного аналізу інформаційних ресурсів, розуміти механізми інформаційних загроз, дезінформації та маніпуляцій, а також формувати стійкі навички безпечної поведінки в цифровому просторі, зокрема в контексті захисту інформаційно-комунікаційних систем.

- Характеризувати основні компоненти інформаційної культури
- Аналізувати інформаційні потреби та стратегії пошуку
- Оцінювати достовірність і якість інформаційних джерел
- Орієнтуватися в правових та етичних нормах інформаційної діяльності
- Застосовувати навички інформаційної гігієни та безпеки

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових категорій та явищ: інформаційна культура, медіаграмотність, інформаційна гігієна, цифрова компетентність, захист інформації, інформаційна безпека, дезінформація, пропаганда. Характеризувати основні компоненти інформаційної культури особистості в контексті фахової діяльності інженера з комп'ютерних систем.

2

Аналіз та оцінювання

Аналізувати причини та наслідки низького рівня інформаційної культури, виявляти закономірності розвитку інформаційного суспільства. Оцінювати якість і достовірність інформаційних джерел, розпізнавати маніпуляції, фейки та дезінформацію в цифровому просторі.

3

Застосування знань

Застосовувати методи та інструменти інформаційного пошуку для вирішення фахових завдань у сфері захисту інформації. Використовувати нормативні, наукові та цифрові джерела для підготовки обґрунтованих висновків та аналітичних матеріалів із питань інформаційної безпеки.

4

Комунікація та рефлексія

Аргументовано викладати власну позицію щодо дискусійних питань інформаційної культури та безпеки. Формувати відповідальне ставлення до власної інформаційної поведінки та дотримуватися норм інформаційної етики в професійній діяльності.

Модуль 1. Основи інформаційної культури та інформаційне суспільство

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Інформаційна культура як наукова категорія. Поняття, сутність та структура інформаційної культури. Інформаційна культура особистості, суспільства, організації. Історія розвитку концепції інформаційної культури. Взаємозв'язок інформаційної культури з інформаційною безпекою. Місце дисципліни в системі підготовки фахівців з комп'ютерної інженерії.

Тема 1.2

Інформаційне суспільство та цифрова трансформація. Етапи становлення інформаційного суспільства. Цифрова економіка та е-урядування в Україні. Цифрова нерівність та шляхи її подолання. Роль інформаційно-комунікаційних систем у розвитку суспільства. Виклики інформаційного суспільства для сфери захисту інформації.

Тема 1.3

Інформаційні потреби та поведінка користувача. Поняття інформаційної потреби, запиту та пошуку. Моделі інформаційної поведінки особистості. Стратегії пошуку інформації в цифровому середовищі. Особливості роботи з науковими, технічними та нормативно-правовими джерелами у сфері захисту інформації. Когнітивні упередження в процесі сприйняття інформації.

Тема 1.4

Правові та етичні норми інформаційної діяльності. Законодавство України у сфері інформації та захисту персональних даних. Авторське право та ліцензування в цифровому середовищі. Етика інформаційної діяльності. Норми академічної доброчесності. Відповідальність за порушення в інформаційній сфері.

Модуль 2. Медіаграмотність та безпека в інформаційному просторі

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Медіаграмотність та критичне мислення. Поняття медіаграмотності та медіакультури. Моделі та рівні медіаграмотності. Критичне сприйняття медіаконтенту. Перевірка фактів та методи верифікації інформації. Розпізнавання маніпулятивних технологій у медіа. Цифрові інструменти для перевірки достовірності інформації.

Тема 2.2

Дезінформація, фейки та інформаційні загрози. Типи та механізми поширення дезінформації. Пропаганда, маніпуляція та інформаційна війна. Технології deepfake та синтетичний контент. Інформаційні операції в контексті збройних конфліктів. Захист від інформаційно-психологічних впливів. Роль фахівця з IT у протидії інформаційним загрозам.

Тема 2.3

Інформаційна гігієна та цифровий добробут. Поняття інформаційної гігієни та цифрового благополуччя. Інформаційне перевантаження та методи його подолання. Управління увагою в цифровому середовищі. Цифровий детокс та технологічна грамотність. Безпечна поведінка в соціальних мережах. Захист персональних даних у повсякденній практиці.

Модуль 3. Інформаційні ресурси та цифрові компетентності фахівця

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Наукова та фахова комунікація в цифровому середовищі. Системи наукової комунікації та академічні бази даних. Наукометрія та бібліометричні показники. Відкритий доступ (Open Access) до наукових публікацій. Оформлення наукових робіт і цитування джерел. Академічна доброчесність та плагіат. Інструменти для роботи з науковою літературою у сфері інформаційної безпеки.

Тема 3.2

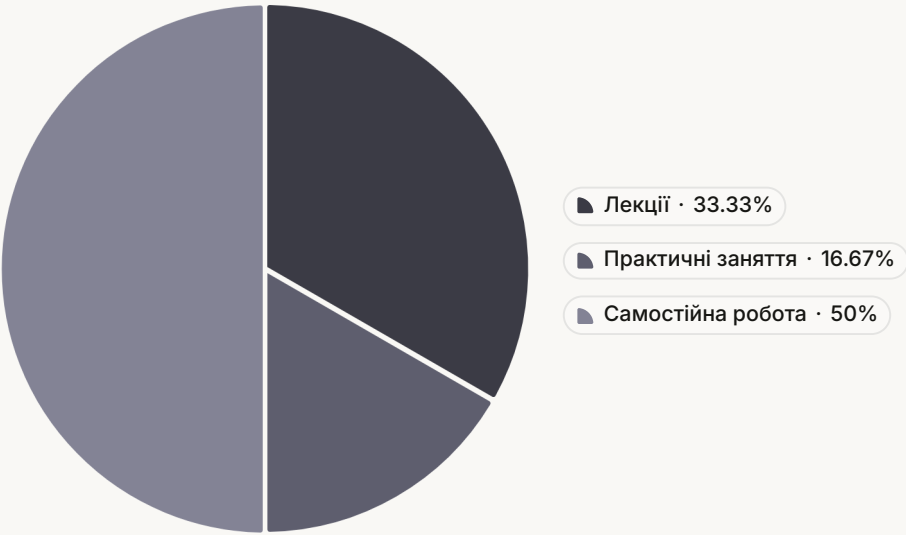
Цифрові інструменти та управління інформацією. Класифікація та характеристика цифрових інформаційних ресурсів. Системи управління знаннями та документами. Хмарні сервіси та їхній вплив на інформаційну безпеку. Інструменти організації і структурування інформації. Нотатки, системи PKM (Personal Knowledge Management). Автоматизація роботи з інформацією засобами ШІ.

Тема 3.3

Цифрова компетентність фахівця з захисту інформації. Цифрова компетентність: моделі та стандарти (DigComp). Цифровий слід та управління онлайн-репутацією. Кібергігієна: базові правила та інструменти. Захист інформаційних активів користувача. Безпечна робота з конфіденційною інформацією в ІКС. Перспективи розвитку інформаційної культури фахівця з комп'ютерної інженерії.

Розподіл навчального часу — 90 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Інформаційна культура як наукова категорія	4	2	6
	Тема 1.2 — Інформаційне суспільство та цифрова трансформація	4	2	6
	Тема 1.3 — Інформаційні потреби та поведінка користувача	2	1	4
	Тема 1.4 — Правові та етичні норми інформаційної діяльності	2	2	5
Модуль 2	Тема 2.1 — Медіаграмотність та критичне мислення	4	2	6
	Тема 2.2 — Дезінформація, фейки та інформаційні загрози	4	2	6
	Тема 2.3 — Інформаційна гігієна та цифровий добробут	4	2	6
Модуль 3	Тема 3.1 — Наукова та фахова комунікація в цифровому середовищі	4	1	5
	Тема 3.2 — Цифрові інструменти та управління інформацією	4	2	6
	Тема 3.3 — Цифрова компетентність фахівця з захисту інформації	2	1	5
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 джерел, дискусії
- **Самостійна робота (45 год. — 50%)**: поглиблене вивчення, підготовка завдань

📖 Самостійна робота становить **50% обсягу дисципліни** — студенти навчаються самостійно працювати з інформаційними ресурсами та розвивати цифрові компетентності.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з інформаційної культури, медіаграмотності та цифрових компетентностей, науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння підходів різних авторів до концепцій інформаційної культури та безпеки.	Індивідуальні завдання Виконання аналітичних завдань щодо оцінювання інформаційних джерел, верифікації фактів, аналізу прикладів дезінформації та маніпуляцій. Підготовка есе, аналітичних записок, міні-досліджень з актуальних питань інформаційної безпеки та цифрового суспільства. Застосування теорії на практиці та обґрунтування висновків.
Робота з інформаційними ресурсами Опрацювання офіційних сайтів: Верховна Рада (zakon.rada.gov.ua), Держспецзв'язок (cip.gov.ua), CERT-UA (cert.gov.ua). Аналіз нормативних документів у сфері захисту інформації, статистичних даних, пошук актуальної фахової інформації.	Підготовка до занять Підготовка до практичних занять шляхом опрацювання першоджерел, повторення теоретичного матеріалу; підготовка до тестувань через вивчення ключових термінів і визначень; систематизація знань перед контрольними роботами та модульними підсумковими завданнями.

Методи викладання

- **Лекції**
Системне подання теоретичного матеріалу з використанням наочних схем, інфографіки, реальних прикладів інформаційних загроз; студенти ведуть конспекти та задають уточнювальні запитання.
- **Кейс-стаді**
Аналіз реальних ситуацій, пов'язаних із дезінформацією, витоками даних та порушеннями інформаційної безпеки; студенти виявляють проблему та пропонують обґрунтовані рішення.
- **Дискусії**
Обговорення дискусійних питань цифрового суспільства, інформаційної безпеки та медіаграмотності; розвиток критичного мислення, аргументації та вміння відстоювати власну позицію.
- **Верифікація джерел**
Практичне опрацювання методів перевірки достовірності інформації, фактчекінгу та розпізнавання маніпуляцій; формування навичок критичного аналізу цифрового контенту.
- **Самостійне дослідження**
Підготовка аналітичних записок, рефератів і презентацій за обраною темою в галузі інформаційної культури та кібербезпеки; розвиток навичок самостійного пошуку та систематизації інформації.

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, практичні завдання з верифікації інформації, аналізу цифрових джерел та участь у дискусіях.

2

Проміжний контроль

Самостійна робота — комплексне ситуаційне завдання або реферат, які охоплюють теми змістовного модуля (теоретичні питання, аналіз інформаційних ресурсів, оцінювання достовірності джерел). Оцінюються повнота відповіді, правильність аналізу та обґрунтованість висновків. Проводиться після кожного змістовного 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 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 інформаційно-комунікаційних системах» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Баранов О. А. Правові основи захисту персональних даних в інформаційних системах: навч. посіб. — Київ : Видавничий дім «Академія», 2022. — 320 с.
2. Бурячок В. Л., Толюпа С. В., Воробієнко П. П. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. — Київ : ДУТ, 2022. — 411 с.
3. Горова С. В. Медіаграмотність і цифрова культура: навч. посіб. — Київ : Національна бібліотека України ім. В. І. Вернадського, 2023. — 224 с.
4. Гриценко В. І., Фурс М. В. Інформаційне суспільство та цифрова трансформація: навч. посіб. — Київ : Академперіодика, 2023. — 288 с.
5. Євсєєв С. П., Мілов О. В., Остапов С. Е. Кібербезпека: основи кодування та криптографії. — Харків : Новий Світ-2000, 2023. — 657 с.
6. Литвиненко О. В. Інформаційні операції та суспільна свідомість: монографія. — Київ : Смолоскип, 2022. — 256 с.
7. Титова Н. М., Рідей Н. М., Настрадін В. П. Інформаційна безпека та кібербезпека держави: навч. посіб. — Київ : Юрінком Інтер, 2024. — 348 с.
8. Тімченко О. В., Скопенко Н. С. Цифрова компетентність фахівця: теорія і практика: навч. посіб. — Київ : КНЕУ, 2023. — 198 с.
9. Шевчук Б. В., Яшанов С. М. Цифрові технології: навч.-метод. посіб. — Київ : Вид-во УДУ імені Михайла Драгоманова, 2023. — 359 с.
10. Яненко Я. В. Медіакультура та інформаційна гігієна в цифрову епоху: навч. посіб. — Суми : СумДУ, 2024. — 210 с.

Офіційні інтернет-ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. — URL: <https://cip.gov.ua/>
2. CERT-UA — Урядова команда реагування на комп'ютерні надзвичайні події. — URL: <https://cert.gov.ua/>
3. Офіційний сайт Верховної Ради України. — URL: <https://zakon.rada.gov.ua/>
4. Національна бібліотека України ім. В. І. Вернадського. — URL: <https://nbuv.gov.ua/>
5. Інститут інформаційного суспільства. — URL: <https://iis.org.ua/>
6. Офіційний сайт Кабінету Міністрів України. — URL: <https://www.kmu.gov.ua/>
7. StopFake — платформа верифікації фактів. — URL: <https://www.stopfake.org/uk/>
8. VoxCheck — проєкт фактчекінгу. — URL: <https://voxukraine.org/voxcheck/>



Рекомендована література охоплює видання **2022–2024 років** українських авторів відповідно до вимог актуальності навчально-методичного забезпечення дисципліни.