Робоча програма дисципліни «Управління інноваціями»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

150

Годин

Загальний обсяг дисципліни

5

Кредити ЄКТС

Відповідно до стандарту

5

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Управління інноваціями

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 150 годин / 5 кредитів ЄКТС

Модулів: 5 змістовних блоки

Лекції: 45 год. | **Практичні:** 30 год. | **СРС:** 75 год.

Призначення дисципліни

Дисципліна «Управління інноваціями» формує у студентів системне розуміння концептуальних засад інноваційної діяльності, методів управління інноваційними процесами та проектами в сфері інформаційних технологій та кібербезпеки. Курс охоплює теоретичні основи інноватики, організаційно-економічні методи управління інноваціями, сучасні підходи до цифрової трансформації та захисту об'єктів інтелектуальної власності у ІТ-галузі.

Дисципліна є обов'язковою для підготовки бакалаврів за ОП «Організація захисту інформації в інформаційно-комунікаційних системах» та забезпечує формування фахових компетентностей, пов'язаних з інноваційним розвитком у сфері комп'ютерної інженерії та захисту інформації.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання інформації у сфері інноваційного менеджменту: виявлення інноваційних можливостей, оцінювання ризиків інноваційних проектів у галузі IT та кібербезпеки.

Комунікація

Здатність до усної та письмової комунікації у сфері управління інноваціями: чітко викладати концепції інноваційних рішень, оформлювати бізнес-плани, аналітичні записки та проектну документацію.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання практичних і самостійних завдань у визначені строки, зокрема під час розробки інноваційних проектів у сфері захисту інформації.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді під час групових проектів з розробки та впровадження інноваційних рішень у сфері IT та кібербезпеки.

Студент повинен вміти: аналізувати нормативну, технічну та аналітичну інформацію у сфері інноваційного менеджменту; виявляти інноваційні можливості й оцінювати ризики; планувати власну діяльність і дотримуватися строків; коректно взаємодіяти з викладачами та одногрупниками; брати участь у командній роботі над інноваційними проектами.

Фахові компетентності

Основи інноваційного менеджменту

Розуміння сутності та закономірностей інноваційної діяльності, місця інновацій у системі розвитку IT-галузі та кібербезпеки. Знання ключових понять, видів інновацій, інноваційного процесу та циклу, вміння їх аналізувати в контексті сучасних технологічних викликів.

Управління інноваційними проектами

Здатність планувати та управляти інноваційними проектами у сфері IT, застосовувати методи Agile, Scrum, Lean Startup; оцінювати ефективність інноваційних рішень та управляти ризиками проектів у галузі захисту інформації.

Цифрова трансформація та інновації

Знання концепцій цифрової трансформації організацій, принципів Industry 4.0 та їх застосування у сфері кібербезпеки; розуміння ролі штучного інтелекту, великих даних та хмарних технологій як драйверів інноваційного розвитку.

Інтелектуальна власність та комерціалізація

Орієнтування у нормативно-правовій базі у сфері інтелектуальної власності в IT; знання методів комерціалізації інновацій, трансферу технологій, стартап-екосистем та венчурного фінансування у технологічній сфері.

Результати навчання

01

Пояснення ключових категорій

Пояснювати сутність ключових понять і явищ: інновація, інноваційний процес, інноваційний цикл, технологічний уклад, дифузія інновацій, інноваційна система, цифрова трансформація, стартап, інтелектуальна власність у сфері ІТ.

02

Характеристика методів управління

Характеризувати основні методи та інструменти управління інноваційною діяльністю, застосовувати методи аналізу інноваційного потенціалу, оцінювання ризиків та ефективності інноваційних проектів у сфері ІТ та кібербезпеки.

03

Аналіз інноваційних процесів

Аналізувати реальні інноваційні процеси в ІТ-галузі для виявлення тенденцій, можливостей та методів управління інноваційним розвитком на рівні підприємства та держави.

04

Розробка інноваційних проектів

Розробляти інноваційні проекти у сфері захисту інформації та кібербезпеки: формулювати ідею, обґрунтовувати інноваційне рішення, оцінювати ефективність та управляти ризиками проекту.

05

Робота з нормативною базою

Орієнтуватися у нормативно-правовій базі інноваційної діяльності та інтелектуальної власності в Україні; використовувати законодавчі акти та стандарти для вирішення практичних завдань управління інноваціями в ІТ-сфері.

МОДУЛЬ 1

Теоретичні засади управління інноваціями

1 — Тема 1.1

Сутність та концепція інновацій. Класифікація інновацій. Інноваційний процес та його закономірності

2 — Тема 1.2

Технологічні уклади та довгі хвилі Кондратьєва. Сучасний технологічний уклад в ІТ-галузі

3 — Тема 1.3

Національна та регіональна інноваційна система України. Державна політика стимулювання інновацій

МОДУЛЬ 1 · ТЕМА 1.1

Сутність та концепція інновацій

Лекційний матеріал (3 год.)

Лекція 1: Поняття «інновація»: генезис, сутність, зміст. Відмінність інновації від винаходу та раціоналізаторської пропозиції. Класифікація інновацій: продуктові, процесні, організаційні, маркетингові. Інновації в IT-галузі та сфері кібербезпеки: специфіка та приклади.

Лекція 2: Інноваційний процес: поняття, стадії, учасники. Моделі інноваційного процесу (лінійна, інтерактивна, відкрита). Дифузія інновацій. Концепція відкритих інновацій (Open Innovation). Інноваційний цикл у розробці програмного забезпечення та систем захисту.

Ключові питання лекції

- Поняття інновації та її відмінність від нововведення
- Класифікація інновацій за різними ознаками
- Стадії інноваційного процесу в IT-галузі
- Концепція відкритих інновацій та її застосування
- Дифузія інновацій: теорія Е. Роджерса

Практичне заняття (2 год.)

Завдання 1. Аналіз класифікації інновацій у сфері кібербезпеки: виявлення продуктових, процесних та організаційних інновацій на прикладі реальних IT-компаній України.

Завдання 2. Кейс: побудова моделі інноваційного процесу для умовної IT-компанії у сфері захисту інформації. Групова робота та обговорення результатів.

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

Самостійна робота (8 год.)

- Опрацювання: Захарченко В. І. та ін. «Інноваційний менеджмент: теорія і практика» — розділ «Теоретичні засади інноватики»
- Підготовка реферату: «Інновації у сфері кібербезпеки: сучасні тенденції та перспективи»
- Складання порівняльної таблиці «Моделі інноваційного процесу: переваги та обмеження»

Очікуваний результат: студент вміє пояснювати концептуальні засади інноватики, класифікувати інновації та описувати стадії інноваційного процесу.

МОДУЛЬ 1 · ТЕМИ 1.2–1.3

Технологічні уклади та інноваційна система України

Тема 1.2 — Технологічні уклади (Лекція 3, 3 год.)

Концепція технологічних укладів (Кондратьєв, Шумпетер). Характеристика технологічних укладів I–VI. Сучасний VI технологічний уклад: штучний інтелект, квантові обчислення, кібербезпека, великі дані. Industry 4.0 та Industry 5.0: відмінності та вплив на IT-галузь. Позиція України в глобальному інноваційному просторі.

Практичне (2 год.): Аналіз технологічного укладу IT-галузі України: визначення ключових технологій, лідерів, бар'єрів розвитку; побудова карти технологічних можливостей у сфері кібербезпеки.

СРС (8 год.): Опрацювання: Гук О. В., Шендерівська Л. П., Мохонько Г. А. «Інвестування інноваційної діяльності» (КПІ ім. Ігоря Сікорського, 2022); підготовка аналітичної записки «Перспективи VI технологічного укладу в Україні: IT та кібербезпека».

Тема 1.3 — Інноваційна система України (Лекція 4, 3 год.)

Поняття національної інноваційної системи (НІС). Суб'єкти НІС України: університети, наукові установи, бізнес, держава. Законодавча база: Закон України «Про інноваційну діяльність», Стратегія інноваційного розвитку. Державна підтримка IT-стартапів: Дія.City, UNIT.City, Ukrainian Startup Fund. Інноваційна інфраструктура: технопарки, бізнес-інкубатори, кластери.

Практичне (2 год.): Дослідження структури НІС України; аналіз Закону «Про інноваційну діяльність»; складання схеми взаємодії суб'єктів інноваційної екосистеми у сфері IT та кібербезпеки.

СРС (8 год.): Опрацювання: Захарченко В. І. та ін. «Інноваційний менеджмент: теорія і практика» (2022); підготовка аналітичної записки «Інноваційна екосистема України у сфері IT: стан та виклики».

МОДУЛЬ 2

Організація та управління інноваційною діяльністю

Тема 2.1

Організаційні форми інноваційної діяльності. Інноваційні підприємства, стартапи та технологічні компанії у сфері кібербезпеки.

Тема 2.2

Інноваційний потенціал організації та методи його оцінювання. Управління інноваційним розвитком IT-підприємства.

Тема 2.3

Фінансування інноваційної діяльності. Венчурний капітал, краудфандинг, гранти та державна підтримка IT-інновацій в Україні.

МОДУЛЬ 2 · ТЕМА 2.1

Організаційні форми інноваційної діяльності

Лекційний матеріал (3 год.)

Організаційні форми інноваційної діяльності: внутрішньофірмові (R&D відділи, центри компетенцій, корпоративні акселератори) та зовнішні (спін-оффи, венчурні підрозділи). Стартап як інноваційна організаційна форма: визначення, стадії, відмінності від традиційного бізнесу. Технологічні компанії у сфері кібербезпеки: бізнес-моделі та організаційні структури. Інноваційні кластери та технопарки.

Ключові питання

- Класифікація організаційних форм інноваційної діяльності
- Стартап: поняття, стадії розвитку, екосистема
- Організаційні структури IT-компаній у сфері кібербезпеки
- Технопарки та інноваційні кластери в Україні
- Корпоративні інновації vs. стартапи: переваги та ризики

Практичне заняття (2 год.)

Завдання 1. Аналіз організаційної структури провідних IT-компаній України у сфері кібербезпеки: визначення інноваційних підрозділів, їх функцій та взаємодії з основним бізнесом.

Завдання 2. Кейс: розробка організаційної моделі стартапу у сфері захисту інформації — визначення команди, функцій, інноваційного продукту та ринку збуту.

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

Самостійна робота (8 год.)

- Опрацювання: Захарченко В. І. та ін. «Інноваційний менеджмент: теорія і практика» (2022) — розділ «Організаційні форми»
- Підготовка реферату: «Стартап-екосистема України у сфері кібербезпеки: гравці та можливості»
- Аналіз діяльності Дія.City як інноваційного майданчика для IT-компаній

Очікуваний результат: студент вміє характеризувати організаційні форми інноваційної діяльності, описувати структуру стартапів та визначати особливості інноваційних IT-компаній.

МОДУЛЬ 2 · ТЕМА 2.2

Інноваційний потенціал організації

Ресурсний складник

Людські, фінансові, технологічні, інформаційні ресурси. Компетенції команди R&D.

Технологічний складник

Технологічна база, патенти, ноу-хау, R&D-інфраструктура підприємства.

Оцінювання потенціалу

SWOT, VRIO, технологічний аудит. KPI інноваційної активності IT-компанії.

Організаційний складник

Культура інновацій, управлінські процеси, системи мотивації до інновацій.

Ринковий складник

Конкурентні переваги, ринкові позиції, партнерська мережа та канали збуту.

Лекційний матеріал (3 год.)

Поняття та складники інноваційного потенціалу організації. Методи оцінювання інноваційного потенціалу: SWOT-аналіз, VRIO-аналіз, технологічний аудит. Управління інноваційним розвитком IT-підприємства: стратегії, цілі, KPI. Організаційна культура інновацій. Бар'єри інноваційного розвитку в IT-компаніях.

Практичне (2 год.) та СРС (8 год.)

Практичне: Проведення оцінювання інноваційного потенціалу умовної IT-компанії у сфері захисту інформації; побудова матриці SWOT та VRIO; формування рекомендацій щодо підвищення інноваційного потенціалу.

СРС: Опрацювання: Защепкіна Н.М., Дорожинська Г.В. «Організація науково-інноваційної діяльності» (КПІ ім. Ігоря Сікорського, 2022); підготовка аналітичної записки «Інноваційний потенціал провідних IT-компаній України».

МОДУЛЬ 2 · ТЕМА 2.3

Фінансування інноваційної діяльності в IT-сфері

Лекційний матеріал (3 год.)

Джерела фінансування інноваційної діяльності: власні кошти, банківські кредити, венчурний капітал, бізнес-ангели, краудфандинг, гранти. Стадії венчурного фінансування: pre-seed, seed, Series A–C. Державна підтримка IT-інновацій в Україні: Ukrainian Startup Fund, Дія.City, гранти ЄС (Horizon Europe). Міжнародні фонди підтримки IT-стартапів. Оцінювання вартості інноваційного IT-стартапу.

Ключові питання

- Класифікація джерел фінансування інновацій
- Стадії венчурного фінансування IT-стартапів
- Ukrainian Startup Fund: умови та результати
- Гранти ЄС для українських IT-компаній
- Оцінювання вартості IT-стартапу: методи та підходи

Практичне заняття (2 год.)

Завдання 1. Аналіз механізмів державної підтримки інноваційних IT-компаній в Україні (Ukrainian Startup Fund, Дія.City): умови участі, вимоги, результати.

Завдання 2. Кейс: розробка стратегії фінансування інноваційного стартапу у сфері кібербезпеки — визначення джерел, обгрунтування вибору, оцінювання ризиків.

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

Самостійна робота (8 год.)

- Опрацювання: Гук О. В., Шендерівська Л. П., Мохонько Г. А. «Інвестування інноваційної діяльності» (КПІ ім. Ігоря Сікорського, 2022) — розділ «Венчурне фінансування»
- Підготовка аналітичної записки «Фінансування кібербезпекових стартапів в Україні: можливості та бар'єри»
- Аналіз умов участі в програмах Ukrainian Startup Fund та Horizon Europe

Очікуваний результат: студент вміє характеризувати джерела фінансування інноваційної діяльності та розробляти стратегію фінансування для IT-стартапу.

МОДУЛЬ 3

Управління інноваційними проектами в IT

Тема 3.1

Методологія управління інноваційними проектами. Agile, Scrum, Kanban у розробці інноваційних IT-рішень.

Тема 3.2

Оцінювання ефективності інноваційних проектів. NPV, IRR, ROI для IT-проектів у сфері захисту інформації.

Тема 3.3

Управління ризиками інноваційних проектів. Методи ідентифікації та мінімізації ризиків у IT-інноваціях.

МОДУЛЬ 3 · ТЕМА 3.1

Методологія управління інноваційними проектами

Лекційний матеріал (3 год.)

Поняття інноваційного проекту: ознаки, відмінності від традиційного проекту. Методологія управління проектами: PMBoK, PRINCE2. Гнучкі методології (Agile): Scrum, Kanban, SAFe. Методологія Lean Startup (E. Pic): цикл Build-Measure-Learn. Design Thinking як інструмент інноваційного проектування. Застосування методологій у розробці інноваційних рішень з кібербезпеки.

Ключові питання

- Відмінності управління інноваційним та традиційним проектом
- Agile-методології у інноваційних IT-проектах
- Lean Startup: цикл Build-Measure-Learn
- Design Thinking: етапи та застосування в кібербезпеці
- Вибір методології залежно від типу інновації

Практичне заняття (2 год.)

Завдання 1. Розробка структури інноваційного проекту у сфері захисту інформації за методологією Scrum: формування бек-логу продукту, визначення спринтів та критеріїв успіху.

Завдання 2. Застосування циклу Lean Startup для валідації інноваційної ідеї у сфері кібербезпеки: побудова MVP (мінімально життєздатного продукту).

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

Самостійна робота (8 год.)

- Опрацювання: Захарченко В. І. та ін. «Інноваційний менеджмент: теорія і практика» (2022) — розділ «Управління інноваційними проектами»
- Підготовка реферату: «Agile-методології у розробці інноваційних рішень з кібербезпеки»
- Аналіз кейсу успішного IT-стартапу у сфері захисту інформації

Очікуваний результат: студент вміє характеризувати методології управління інноваційними проектами та застосовувати Agile і Lean Startup для розробки інноваційних рішень у сфері IT.

МОДУЛЬ 3 · ТЕМИ 3.2–3.3

Ефективність та ризики інноваційних проектів

Тема 3.2 — Оцінювання ефективності (Лекція 9, 3 год.)

Критерії оцінювання ефективності інноваційних проектів: економічні (NPV, IRR, PP, ROI) та неекономічні. Специфіка оцінювання IT-проектів у сфері захисту інформації. Методи прогнозування доходів від інновацій. Аналіз «витрати-вигоди» (Cost-Benefit Analysis). Оцінювання соціального ефекту інновацій. Практика оцінювання кібербезпекових рішень.

Практичне (2 год.): Розрахунок NPV, IRR та ROI для умовного інноваційного проекту у сфері захисту інформаційних систем; порівняльний аналіз двох інноваційних рішень та обґрунтування вибору оптимального варіанту.

СРС (8 год.): Опрацювання: Гук О. В., Шендерівська Л. П., Мохонько Г. А. «Інвестування інноваційної діяльності» (2022) — розділ «Оцінювання ефективності»; підготовка звіту «Методи оцінювання ефективності інноваційних IT-проектів».

Тема 3.3 — Управління ризиками (Лекція 10, 3 год.)

Поняття ризику в інноваційному проекті. Класифікація ризиків: технологічні, ринкові, фінансові, управлінські, правові. Специфіка ризиків IT-інновацій та кібербезпекових проектів. Методи ідентифікації ризиків: мозковий штурм, метод Делфі, FMEA. Якісний та кількісний аналіз ризиків. Методи мінімізації ризиків. Реєстр ризиків проекту.

Практичне (2 год.): Ідентифікація та оцінювання ризиків інноваційного проекту у сфері кібербезпеки; побудова реєстру ризиків та матриці ймовірність × вплив; розробка плану реагування на ризики.

СРС (8 год.): Опрацювання: Захарченко В. І. та ін. «Інноваційний менеджмент: теорія і практика» (2022); підготовка аналітичної записки «Управління ризиками у кібербезпекових стартапах: методологія та практика».

МОДУЛЬ 4

Цифрові інновації та трансформація в ІКС

Тема 4.1

Цифрова трансформація організацій. Концепції Industry 4.0 та Smart Enterprise. Цифрові технології як драйвери інновацій у захисті інформації.

Тема 4.2

Інновації у сфері штучного інтелекту та великих даних. Застосування AI/ML у кібербезпеці. Управління ШІ-інноваціями.

Тема 4.3

Хмарні та IoT-інновації в ІКС. Управління інноваційними рішеннями у хмарній безпеці та захисті Інтернету речей.

МОДУЛЬ 4 · ТЕМА 4.1

Цифрова трансформація та інновації

Лекційний матеріал (3 год.)

Поняття цифрової трансформації (Digital Transformation): сутність, рівні, відмінність від цифровізації. Концепція Industry 4.0: кіберфізичні системи, IoT, AI, Big Data, хмарні технології. Цифрові платформи та екосистеми. Цифрова трансформація у сфері захисту інформації та кібербезпеки. Цифрова трансформація держсектору України: «Дія», е-уряд, відкриті дані. Бар'єри та чинники успіху цифрової трансформації.

Ключові питання

- Рівні цифрової трансформації організації
- Industry 4.0: ключові технології та їх вплив на ІКС
- Цифрові платформи та їх роль в інноваційному розвитку
- Цифрова трансформація у сфері кібербезпеки
- Е-урядування як інноваційний процес

Практичне заняття (2 год.)

Завдання 1. Розробка дорожньої карти цифрової трансформації умовної організації у сфері захисту інформації: визначення цілей, технологій, дій та KPI трансформації.

Завдання 2. Кейс: аналіз досвіду цифрової трансформації державного сектору України («Дія», e-Services) — виявлення інноваційних рішень, ризиків та результатів.

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

Самостійна робота (8 год.)

- Опрацювання: Защепкіна Н.М., Дорожинська Г.В. «Організація науково-інноваційної діяльності» (КПІ, 2022) — розділ «Цифрова трансформація»
- Підготовка реферату: «Цифрова трансформація системи кібербезпеки: технологічні рішення та управлінські виклики»
- Аналіз Концепції розвитку цифрової економіки та суспільства України

Очікуваний результат: студент вміє характеризувати концепцію цифрової трансформації, визначати її роль у розвитку систем захисту інформації та розробляти дорожні карти інноваційного розвитку.

МОДУЛЬ 4 · ТЕМИ 4.2–4.3

AI/ML-інновації та хмарна безпека

Тема 4.2 — Інновації AI/ML у кібербезпеці (Лекція 13, 3 год.)

Штучний інтелект та машинне навчання як інноваційні технології кібербезпеки: виявлення аномалій, поведінковий аналіз, автоматизоване реагування. Великі дані (Big Data) у захисті ІКС: збір, обробка, аналіз інцидентів. Генеративний ШІ як нова загроза та інструмент захисту. Управління інноваційними AI-проектами у сфері кібербезпеки. Ринок AI-кібербезпекових рішень в Україні та у світі.

Практичне (2 год.): Аналіз AI-інструментів у сфері кібербезпеки; розробка концепції інноваційного AI-рішення для захисту ІКС; оцінювання потенційного ринку та конкурентів.

СРС (8 год.): Опрацювання: Єршова О. О., Гончаренко І. М. «Сучасні підходи до управління кіберризиками в умовах воєнного стану» (2023); підготовка аналітичної записки «AI-рішення у кібербезпеці: інноваційний потенціал та ринкові перспективи».

Тема 4.3 — Хмарні та IoT-інновації (Лекція 14, 3 год.)

Хмарні обчислення як інноваційна платформа для ІКС: моделі IaaS, PaaS, SaaS з точки зору інноваційного управління. Інноваційні хмарні рішення у сфері кібербезпеки (Security-as-a-Service, SASE). IoT як інноваційна технологія та нові виклики безпеки. Управління інноваційними проектами у сфері хмарних та IoT-рішень. Вимоги до хмарних інновацій у держсекторі України.

Практичне (2 год.): Розробка концепції інноваційного хмарного рішення для захисту інформаційних систем держорганів: визначення моделі, ключових функцій, ринкових переваг та ризиків впровадження.

СРС (8 год.): Опрацювання: Захарченко В. І. та ін. «Інноваційний менеджмент: теорія і практика» (2022) — розділ «Цифрові платформи»; підготовка аналітичної записки «Хмарні інновації у сфері кібербезпеки: бізнес-моделі та управлінські рішення».

МОДУЛЬ 5

Інтелектуальна власність та стратегічне управління інноваціями

Тема 5.1

Інтелектуальна власність в IT-галузі. Правовий захист інновацій: патенти, авторське право, комерційна таємниця в ІКС.

Тема 5.2

Стратегічне управління інноваційним розвитком IT-підприємства. Інноваційна стратегія та конкурентні переваги.

Тема 5.3

Комерціалізація інновацій та трансфер технологій у сфері IT. Бізнес-моделі кібербезпекових компаній.

МОДУЛЬ 5 · ТЕМА 5.1

Інтелектуальна власність в IT-галузі

Лекційний матеріал (3 год.)

Поняття інтелектуальної власності (ІВ) та її значення в IT-інноваціях. Об'єкти права ІВ у сфері IT: програмне забезпечення, бази даних, алгоритми, технічні рішення. Засоби правового захисту: патент, авторське право, торговельна марка, комерційна таємниця. Захист ноу-хау та конфіденційної інформації у IT-компаніях. Законодавча база: Цивільний кодекс, Закон «Про авторське право». Міжнародні аспекти охорони ІВ в IT.

Ключові питання

- Об'єкти права інтелектуальної власності у сфері IT
- Патентний захист програмного забезпечення: можливості та обмеження
- Авторське право на ПЗ та бази даних
- Комерційна таємниця в IT-компаніях: захист та ризики
- Нормативно-правова база охорони ІВ в Україні

Практичне заняття (2 год.)

Завдання 1. Аналіз патентного портфеля провідних IT-компаній у сфері кібербезпеки: виявлення ключових патентів, їх захисних функцій та стратегічного значення для конкурентоспроможності.

Завдання 2. Розробка стратегії захисту інтелектуальної власності для умовної компанії у сфері захисту інформації — вибір засобів правового захисту, обґрунтування рішень.

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

Самостійна робота (9 год.)

- Опрацювання: Кулініч О. О. «Організаційно-правові основи захисту інформації з обмеженим доступом» (Київ: Алерта, 2023) — розділ «Охорона ІВ»
- Підготовка реферату: «Патентний захист інновацій у сфері кібербезпеки: практика та перспективи»
- Аналіз Закону України «Про авторське право та суміжні права» (нова редакція 2022 р.)

Очікуваний результат: студент вміє характеризувати об'єкти і засоби правового захисту ІВ в IT-галузі та розробляти стратегію захисту інновацій.

МОДУЛЬ 5 · ТЕМИ 5.2–5.3

Стратегічне управління інноваціями та комерціалізація

Тема 5.2 — Інноваційна стратегія (Лекція 17, 3 год.)

Поняття інноваційної стратегії підприємства та її місце в загальній стратегії. Типи інноваційних стратегій: наступальна, захисна, імітаційна, ніш. Стратегічне управління інноваційним розвитком IT-компанії. Конкурентні переваги на основі інновацій у сфері кібербезпеки. Аналіз конкурентного середовища (Porter's Five Forces) для IT-ринку. Цифрові інноваційні стратегії компаній-лідерів ринку кібербезпеки.

Практичне (2 год.): Розробка інноваційної стратегії для умовної IT-компанії у сфері захисту інформації: аналіз конкурентів, вибір типу стратегії, визначення ключових інноваційних ініціатив та KPI.

СРС (9 год.): Опрацювання: Захарченко В. І. та ін. «Інноваційний менеджмент: теорія і практика» (2022) — розділ «Стратегічне управління інноваціями»; підготовка аналітичної записки «Інноваційна стратегія провідних кібербезпекових компаній: порівняльний аналіз».

Тема 5.3 — Комерціалізація інновацій (Лекція 18, 3 год.)

Поняття комерціалізації інновацій. Канали комерціалізації: ліцензування, спін-офф, продаж патентів, партнерство, власне виведення на ринок. Трансфер технологій: механізми, учасники, особливості в IT-галузі. Бізнес-моделі компаній у сфері кібербезпеки: SaaS, ліцензування, консалтинг, MSP. Формування ціннісної пропозиції для інноваційного IT-продукту. Вихід на міжнародні ринки.

Практичне (2 год.): Розробка бізнес-моделі Canvas для інноваційного продукту у сфері захисту інформації: визначення ціннісної пропозиції, сегментів клієнтів, каналів збуту, ключових ресурсів та джерел доходів.

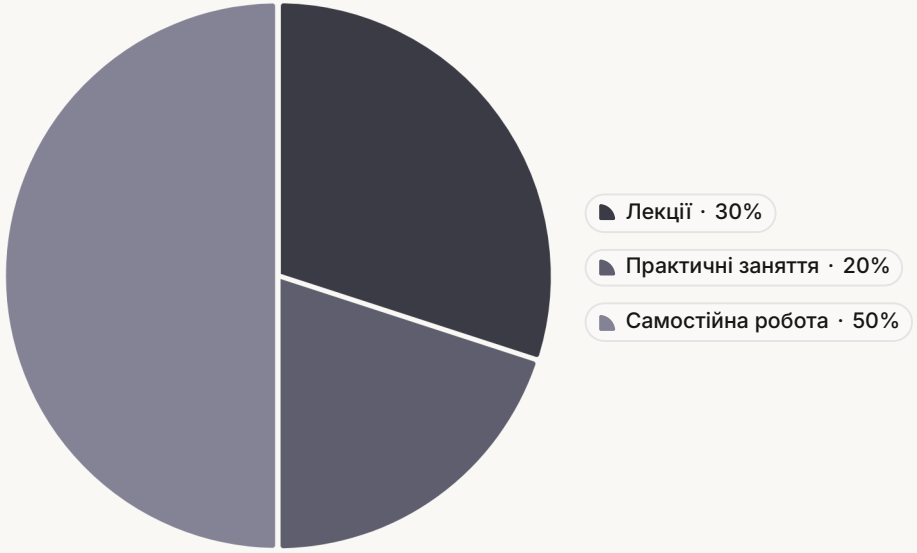
СРС (9 год.): Підготовка підсумкового інноваційного проекту: «Інноваційний IT-продукт у сфері захисту інформаційних систем — від ідеї до бізнес-моделі»; аналіз досвіду українських IT-компаній у комерціалізації кібербезпекових рішень.

Розподіл навчального часу — 150 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Концепція інновацій	3	2	8
	Тема 1.2 — Технологічні уклади	3	2	8
	Тема 1.3 — Інноваційна система України	3	2	8
Модуль 2	Тема 2.1 — Організаційні форми	3	2	8
	Тема 2.2 — Інноваційний потенціал	3	2	8
	Тема 2.3 — Фінансування інновацій	3	2	8
Модуль 3	Тема 3.1 — Методологія проектів	3	2	8
	Тема 3.2 — Оцінювання ефективності	3	2	8
	Тема 3.3 — Управління ризиками	3	2	8
Модуль 4	Тема 4.1 — Цифрова трансформація	3	2	8
	Тема 4.2 — AI/ML-інновації у КБ	3	2	8
	Тема 4.3 — Хмарні та IoT-інновації	3	2	8
Модуль 5	Тема 5.1 — Інтелектуальна власність	3	2	9
	Тема 5.2 — Інноваційна стратегія	3	2	9
	Тема 5.3 — Комерціалізація інновацій	3	2	9
Разом	**15 тем**	**45**	**30**	**75**

Загальний обсяг: 150 годин = 5 кредитів ЄКТС. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **150 годин (5 кредитів ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теорією та практикою.

Лекції — 45 год. (30%)

Системне подання ключового теоретичного матеріалу з використанням наочних схем, таблиць і прикладів із вітчизняної та міжнародної практики управління інноваціями в IT-галузі.

Практичні заняття — 30 год. (20%)

Відпрацювання практичних навичок: розробка інноваційних проектів, оцінювання ефективності, управління ризиками, побудова бізнес-моделей та стратегій у сфері захисту інформації.

Самостійна робота — 75 год. (50%)

Поглиблене вивчення, підготовка аналітичних завдань і проектів, робота з нормативними актами та науковою літературою. Самостійна робота становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками та посібниками з управління інноваціями (Захарченко, Гук, Защепкіна та ін.), нормативно-правовими актами, стандартами, науковими статтями у фахових виданнях. Студент конспектує ключові положення та порівнює підходи різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань (оцінювання інноваційного потенціалу, розробка бізнес-моделей, аналіз ринку кібербезпекових інновацій); творчих завдань — аналітичні записки, звіти, міні-дослідження з актуальних питань управління IT-інноваціями.

Робота з інформаційними ресурсами

Опрацювання офіційних ресурсів: Ukrainian Startup Fund (**usf.com.ua**), Дія.City (**city.diia.gov.ua**), Верховної Ради (**zakon.rada.gov.ua**), UNIT.City, звітів міжнародних організацій (WIPO, Horizon Europe). Аналіз наукових статей та пошук актуальної інформації.

Підготовка до занять

Підготовка до практичних занять (вивчення методологій, стандартів, нормативних актів); підготовка до тестувань (ключові терміни, визначення); підготовка до контрольних робіт за кожним модулем; розробка підсумкового інноваційного проекту.

Форми контролю знань

1	2	3
Поточний контроль	**Проміжний контроль**	**Підсумковий контроль**
Завдання: аналітичні та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання завдань, якість звітів з практичних робіт і рівень засвоєння матеріалу. Проводиться після кожної теми у формі тестування (10–15 питань) або захисту практичної роботи.	Самостійна робота — комплексне ситуаційне завдання або аналітична записка, які охоплюють теми змістовних модулів (теоретичні питання, аналіз інноваційного потенціалу, розробка проектних рішень). Оцінюються повнота відповіді, аргументованість та практична обґрунтованість висновків. Проводиться після завершення кожного змістовного модуля.	Іспит відповідно до навчального плану. Форма проведення — тестування та письмові відповіді / практичні задачі, захист підсумкового інноваційного проекту. 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 «Управління інноваціями» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок управління інноваційними проектами у сфері захисту інформації, необхідних для майбутньої інженерної діяльності.

Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, таблиць і реальних прикладів інноваційної діяльності в IT-галузі; студенти ведуть конспекти та задають уточнювальні запитання.

Робота з документами

Опрацювання нормативних документів (Закон «Про інноваційну діяльність», стандарти управління проектами PMBoK, Agile Manifesto); формування навичок критичного аналізу нормативної бази.

Кейс-стаді

Аналіз реальних кейсів успішних та провалених інновацій у сфері IT та кібербезпеки; студенти виявляють чинники успіху, управлінські рішення та уроки для майбутньої практики.

Дискусії

Обговорення дискусійних питань інноваційного розвитку: роль держави у стимулюванні інновацій, баланс між захистом ІВ та відкритим доступом; розвиток критичного мислення.

Практичний практикум

Розробка інноваційних проектів за методологіями Agile та Lean Startup, побудова бізнес-моделей Canvas, оцінювання ефективності та ризиків інноваційних рішень у сфері кібербезпеки.

Проектна робота

Підготовка підсумкового інноваційного проекту «Інноваційний IT-продукт у сфері захисту інформації»; розвиток навичок самостійного аналізу, синтезу та систематизації інформації.

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. Захарченко В. І. та ін.

Інноваційний менеджмент: теорія і практика : навч. посіб. / В. І. Захарченко, Н. М. Корсікова, М. М. Меркулов. — Київ : Центр учбової літератури, 2022. — 448 с.

2. Гук О. В., Шендерівська Л. П., Мохонько Г. А.

Інвестування інноваційної діяльності : навч. посіб. для здобувачів ступеня магістра за спеціальністю 073 «Менеджмент». — Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2022. — 186 с.

3. Защепкіна Н. М., Дорожинська Г. В.

Організація науково-інноваційної діяльності : навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 84 с. URL: **ela.kpi.ua**

4. Пермінова С. О.

Інноваційний менеджмент : навч. наочний посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 186 с. URL: **ela.kpi.ua**

5. Кулініч О. О.

Організаційно-правові основи захисту інформації з обмеженим доступом в органах державної влади України : монографія. — Київ : Алерта, 2023. — 196 с. *Рекомендується для тем 5.1–5.2.*

6. Єршова О. О., Гончаренко І. М.

Сучасні підходи до управління кіберризиками в умовах воєнного стану. Журнал стратегічних досліджень. — 2023. — № 3(9). — С. 45–56. *Рекомендується для теми 4.2, 3.3.*

7. Євсєєв С. П. та ін.

Кібербезпека: основи кодування та криптографії / С. П. Євсєєв, О. В. Мілов, С. Е. Остапов, О. В. Сєвєрінов. — Харків : Новий Світ-2000, 2023. — 296 с. *Рекомендується для тем 4.2–4.3.*

8. Живило Є. О.

Захист інформації та кібербезпека в електронних комунікаційних мережах : навч. посіб. — Полтава : ПНТУ «Полтавська політехніка ім. Юрія Кондратюка», 2023. — 188 с. *Рекомендується для тем 4.3.*

Нормативно-правова база

- Закон «Про інноваційну діяльність» від 04.07.2002 № 40-IV (зі змінами)

  Визначає засади державної інноваційної політики, об'єкти та суб'єкти інноваційної діяльності в Україні. **zakon.rada.gov.ua**

- Закон «Про авторське право і суміжні права» від 01.12.2022 № 2811-IX

  Нова редакція законодавства про охорону авторського права на програмне забезпечення та бази даних. **zakon.rada.gov.ua**

- Закон «Про стимулювання розвитку цифрової економіки в Україні» від 15.07.2021 № 1667-IX

  Засади функціонування Дія.City та державної підтримки IT-інновацій. **zakon.rada.gov.ua**

- Концепція розвитку цифрової економіки та суспільства України на 2021–2030 рр.

  Стратегічний документ щодо цифрової трансформації та інноваційного розвитку IT-галузі. **zakon.rada.gov.ua**

- Закон «Про охорону прав на винаходи і корисні моделі» від 15.12.1993 № 3687-XII (ред. 2023)

  Засади патентного захисту технологічних рішень та інновацій у сфері IT. **zakon.rada.gov.ua**

Офіційні ресурси та фахові видання

Ukrainian Startup Fund

usf.com.ua — офіційні умови грантових програм, портфоліо проінвестованих стартапів, методичні матеріали для засновників IT-компаній.

Дія.City

city.diia.gov.ua — умови вступу до спеціального правового режиму для IT-компаній, нормативна база, перелік учасників.

Верховна Рада України

zakon.rada.gov.ua — нормативно-правова база у сферах інноваційної діяльності, інтелектуальної власності, цифрової економіки.

Національна бібліотека України ім. В. І. Вернадського

nbuv.gov.ua — електронні ресурси, наукові статті, монографії з інноваційного менеджменту та управління IT-проектами.

Журнал «Проблеми науки»

problems.org.ua — фахове видання з питань науково-технічного прогресу, інноваційної діяльності та управління R&D.

WIPO (Всесвітня організація ІВ)

wipo.int — міжнародні стандарти охорони інтелектуальної власності, патентні бази даних, методичні матеріали.

Міністерство освіти і науки України

mon.gov.ua — освітні стандарти, навчальні програми, методичні матеріали для спеціальності 123 «Комп'ютерна інженерія».

Horizon Europe (ЄС)

eic.ec.europa.eu — програми грантового фінансування інноваційних проектів ЄС, доступних для українських IT-компаній та дослідників.

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

Чому «Управління інноваціями» для інженерів з захисту інформації?

Дисципліна є невід'ємною складовою підготовки бакалаврів за ОП «Організація захисту інформації в ІКС». Розуміння інноваційних процесів та управлінських підходів формує у майбутніх інженерів здатність не лише впроваджувати захищені ІКС, але й генерувати та управляти інноваційними рішеннями у сфері кібербезпеки.

Сучасний фахівець з захисту інформації працює в середовищі постійних технологічних змін, де управління інноваціями стає обов'язковою умовою ефективної професійної діяльності та конкурентоспроможності на ринку праці.

Практичне значення для майбутньої кар'єри

- Здатність генерувати та реалізовувати інноваційні рішення у сфері захисту інформації
- Навички управління інноваційними проектами (Agile, Lean Startup) в IT-компаніях
- Розуміння механізмів фінансування IT-стартапів та оцінювання їхньої ефективності
- Знання засобів правового захисту ІВ у сфері IT для роботи в технологічних компаніях
- Компетентності для роботи в інноваційних підрозділах IT-компаній, стартапах, кіберцентрах
- Готовність до розробки та комерціалізації інноваційних продуктів у галузі кібербезпеки

Бажаємо успіхів у вивченні «Управління інноваціями»!

150

Годин

Загальний обсяг дисципліни

5

Кредити ЄКТС

Відповідно до стандарту

15

Тем

У 5 змістовних модулях

8

Джерел

Рекомендованої літератури 2022–2024 рр.

> «Інновації — це не випадковість, а результат системного управління ідеями, ресурсами та людьми.»

Спеціальність 123 · Комп'ютерна інженерія · ОП: Організація захисту інформації в ІКС · Бакалавр · 5 кредитів ЄКТС