Робоча програма дисципліни «Стратегічне управління»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

ОП: Організація захисту інформації в інформаційно-комунікаційних системах

150

Годин

Загальний обсяг дисципліни

5

Кредити ЄКТС

Відповідно до стандарту

5

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Стратегічне управління

Спеціальність: 123 Комп'ютерна інженерія

Ступінь: Бакалавр

Обсяг: 150 годин / 5 кредитів ЄКТС

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

Модулів: 5 змістовних блоки

ОП: Організація захисту інформації в ІКС

Призначення дисципліни

Дисципліна «Стратегічне управління» формує у студентів системне розуміння методології та інструментарію стратегічного планування й управління організаціями в умовах цифровізації та інформаційних викликів. Курс охоплює ключові концепції, методи стратегічного аналізу, розробку та реалізацію стратегій захисту інформації в інформаційно-комунікаційних системах.

Дисципліна є обов'язковою для підготовки бакалаврів зі спеціальності 123 «Комп'ютерна інженерія» (ОП «Організація захисту інформації в ІКС») та забезпечує формування загальних і фахових компетентностей, передбачених освітньо-професійною програмою.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання управлінської й безпекової інформації: виявлення причинно-наслідкових зв'язків, порівняння стратегічних альтернатив, формування обґрунтованих управлінських рішень.

Комунікація

Здатність до усної та письмової комунікації: чітко пояснювати стратегічні концепції та управлінські рішення, аргументовано презентувати результати аналізу, оформлювати аналітичні записки та звіти.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки стратегічних аналізів, кейсів та дослідницьких проектів.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді під час групового розроблення стратегій, аналізу кейсів та захисту стратегічних проектів у сфері інформаційної безпеки.

Студент повинен вміти: аналізувати навчальну, статистичну та аналітичну інформацію; виділяти головне та узагальнювати результати; планувати власну діяльність і дотримуватися дедлайнів; коректно спілкуватися з викладачами та одногрупниками; брати участь у командній роботі та розподіляти обов'язки.

Фахові компетентності

Стратегічне мислення у сфері ІБ

Розуміння сутності та закономірностей стратегічного управління організаціями, що здійснюють захист інформації в ІКС. Знання ключових концепцій, методів і моделей стратегічного менеджменту та вміння застосовувати їх у контексті інформаційної безпеки.

Стратегічний аналіз середовища

Здатність проводити стратегічний аналіз зовнішнього та внутрішнього середовища організацій: застосовувати SWOT, PESTEL, модель п'яти сил Портера для виявлення загроз і можливостей у сфері захисту інформаційно-комунікаційних систем.

Розробка та реалізація стратегій

Знання методів формування стратегій захисту інформації, корпоративних і функціональних стратегій в ІКС-середовищі. Уміння розробляти стратегічні плани та обирати оптимальні стратегічні альтернативи на основі аналізу ризиків і ресурсів.

Нормативно-правова база

Орієнтування в нормативно-правовій базі у сфері стратегічного управління інформаційною безпекою; використання законодавчих актів, стандартів і наукових джерел для обґрунтування стратегічних рішень у сфері захисту інформації.

Результати навчання

01

Пояснення стратегічних категорій

Пояснювати сутність ключових понять і явищ: стратегія, місія, візія, стратегічний потенціал, конкурентна перевага, стратегічна безпека, ризик, стратегічне планування, SWOT-аналіз, збалансована система показників.

02

Характеристика процесів стратегічного управління

Характеризувати основні процеси та етапи стратегічного управління організаціями у сфері захисту інформації в ІКС; застосовувати методи стратегічного та ситуаційного аналізу, визначати тенденції та формулювати висновки.

03

Розробка стратегічних рішень

Розробляти стратегічні рішення щодо організації захисту інформації в ІКС, оцінювати їх ефективність та обґрунтовувати вибір стратегічних альтернатив на основі аналізу зовнішнього і внутрішнього середовища.

04

Робота з науковими джерелами

Орієнтуватися в науковій та нормативній базі зі стратегічного управління та інформаційної безпеки; використовувати наукові та інформаційні ресурси для підготовки обґрунтованих аналітичних матеріалів.

МОДУЛЬ 1

Концептуальні засади стратегічного управління

1 — Тема 1.1

Сутність, предмет і завдання стратегічного управління. Еволюція стратегічного менеджменту

2 — Тема 1.2

Місія, цілі та стратегічне бачення організації. Ієрархія стратегій

3 — Тема 1.3

Стратегічне управління в організаціях сфери захисту інформації в ІКС

МОДУЛЬ 1 · ТЕМА 1.1

Сутність та еволюція стратегічного управління

Лекційний матеріал (3 год.)

Лекція 1: Поняття «стратегічне управління» і «стратегічний менеджмент»: зміст, структура, відмінності. Еволюція стратегічного управління: від бюджетування до стратегічного мислення. Школи стратегій (Мінцберг). Стратегічне управління як цілісна система: об'єкт, суб'єкт, принципи.

Лекція 2: Стратегічне управління в IT-організаціях та підрозділах захисту інформації. Специфіка стратегічного менеджменту у сфері інформаційної безпеки. Сучасні підходи до стратегічного управління в умовах цифровізації та кіберзагроз.

Ключові питання лекції

- Сутність і структура стратегічного управління
- Відмінність стратегічного від оперативного управління
- Еволюція концепцій стратегічного менеджменту
- Специфіка стратегічного управління в сфері ІБ
- Сучасні виклики для стратегічного управління ІКС

Практичне заняття (2 год.)

Завдання 1. Складання порівняльної таблиці «Еволюція підходів до стратегічного управління»: характеристика за критеріями (часовий горизонт, акцент, методи, обмеження).

Завдання 2. Кейс: аналіз стратегічних підходів до управління підрозділом інформаційної безпеки. Обговорення дискусійних питань.

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

Самостійна робота (9 год.)

- Опрацювання: Ігнатьєва І. А. «Стратегічний менеджмент» — розділ «Концептуальні засади». Київ: Каравела, 2023
- Підготовка реферату: «Стратегічне управління в цифрову епоху: виклики та можливості»
- Складання схеми «Еволюція стратегічного управління від 1950-х до сьогодні»

Очікуваний результат: студент вміє характеризувати сутність стратегічного управління, пояснювати еволюцію підходів та визначати специфіку для сфери ІКС.

МОДУЛЬ 1 · ТЕМИ 1.2–1.3

Місія, цілі та стратегічне управління в ІКС-організаціях

Тема 1.2 — Місія та ієрархія стратегій (Лекція 3, 3 год.)

Місія, візія та стратегічні цілі організації: поняття, вимоги, взаємозв'язок. Ієрархія стратегій: корпоративна, бізнес-стратегія, функціональна. Стратегічний потенціал організації. Збалансована система показників (BSC) як інструмент управління стратегією. Стратегічні карти.

Практика (2 год.): Розробка місії та стратегічних цілей для умовного підрозділу захисту інформації; побудова ієрархії стратегій; дискусія «Як місія впливає на стратегічні рішення в ІБ?».

СРС (9 год.): Опрацювання: Деміхов О. І., Дегтярьова І. О. «Стратегічне управління та управління змінами: конспект лекцій». Київ: ННІМП УМО, 2023; підготовка аналітичної записки «Місія та цілі організації у сфері кіберзахисту».

Тема 1.3 — Стратег. управління в ІКС (Лекція 4, 3 год.)

Особливості стратегічного управління організаціями, що здійснюють захист інформації в ІКС. Стратегічна безпека як ключова категорія. Зв'язок між корпоративною стратегією та стратегією інформаційної безпеки. Стратегічне управління ризиками в ІКС. Модель зрілості кіберзахисту як стратегічний орієнтир.

Практика (2 год.): Аналіз взаємозв'язку корпоративної стратегії та стратегії захисту інформації; кейс «Розробка стратегічних цілей у сфері ІБ для підприємства».

СРС (9 год.): Опрацювання: Білоус С., Трохименко А., Камінський В. «Стратегічне управління розвитком підприємства в умовах кризи та військових викликів». Економіка та суспільство, 2024, № 68; підготовка реферату «Стратегічне управління ризиками в ІКС».

МОДУЛЬ 2

Стратегічний аналіз середовища організації

Тема 2.1

Аналіз зовнішнього середовища: PESTEL-аналіз, модель п'яти конкурентних сил М. Портера. Кіберзагрози як стратегічний фактор.

Тема 2.2

Аналіз внутрішнього середовища організації: ресурсний підхід, ланцюжок цінностей, аналіз стратегічного потенціалу в сфері ІБ.

Тема 2.3

SWOT-аналіз та його застосування для стратегічного управління захистом інформації в ІКС. Матричні методи стратегічного аналізу.

МОДУЛЬ 2 · ТЕМА 2.1

Аналіз зовнішнього середовища організації

Лекційний матеріал (3 год.)

Зовнішнє середовище організації: макро- та мікрооточення. PESTEL-аналіз: політичні, економічні, соціальні, технологічні, екологічні та правові фактори в контексті ІКС. Модель п'яти конкурентних сил М. Портера. Аналіз галузі та конкурентного середовища. Кіберзагрози та кібератаки як стратегічні фактори зовнішнього середовища. Державна стратегія кібербезпеки України як стратегічний контекст.

Ключові питання

- Структура зовнішнього середовища організації
- Методологія PESTEL для ІКС-організацій
- Конкурентні сили у сфері кіберзахисту
- Кіберзагрози як ключовий фактор зовнішнього середовища
- Вплив державної стратегії кібербезпеки на організаційну стратегію

Практичне заняття (2 год.)

Завдання 1. Проведення PESTEL-аналізу для підприємства, що здійснює захист інформації в ІКС: виявлення ключових факторів впливу та їх оцінка.

Завдання 2. Кейс: «Застосування моделі п'яти сил Портера для аналізу ринку кіберзахисту в Україні». Групова робота та презентація висновків.

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

Самостійна робота (9 год.)

- Опрацювання: Ігнатьєва І. А. «Стратегічний менеджмент». Київ: Каравела, 2023 — розділ «Стратегічний аналіз зовнішнього середовища»
- Підготовка реферату: «PESTEL-аналіз галузі захисту інформації в Україні: сучасний стан та тенденції»
- Аналіз Стратегії кібербезпеки України як зовнішнього стратегічного фактора

Очікуваний результат: студент вміє проводити PESTEL-аналіз та застосовувати модель п'яти сил Портера до організацій сфери захисту інформації.

МОДУЛЬ 2 · ТЕМИ 2.2–2.3

Аналіз внутрішнього середовища та SWOT-аналіз

Тема 2.2 — Внутрішнє середовище (Лекція 6, 3 год.)

Аналіз внутрішнього середовища організації: ресурси, здатності, компетентності. Ресурсний підхід у стратегічному управлінні. Ланцюжок цінностей М. Портера та його застосування для ІКС-організацій. Стратегічний потенціал організації у сфері захисту інформації: технологічний, кадровий, організаційний, фінансовий виміри. Ключові компетентності в кіберзахисті.

Практика (2 год.): Аналіз ланцюжка цінностей підрозділу захисту інформації; оцінка стратегічного потенціалу за ресурсними групами; кейс «Ключові компетентності ІТ-компанії у сфері ІБ».

СРС (9 год.): Опрацювання: Буднік М. М., Невертій Г. С., Курилова Н. М. «Стратегічне управління: навчальний посібник». Київ: Кондор, 2020; підготовка аналітичної записки «Стратегічний потенціал організації захисту інформації в ІКС».

Тема 2.3 — SWOT-аналіз (Лекція 7, 3 год.)

SWOT-аналіз: методологія, структура, застосування у стратегічному управлінні ІКС. Матриця SWOT для прийняття стратегічних рішень у сфері захисту інформації. Матричні методи стратегічного аналізу: матриця BCG, матриця McKinsey/GE, матриця Ансоффа. Стратегічний баланс: поєднання зовнішнього та внутрішнього аналізу для вибору стратегії ІБ.

Практика (2 год.): Проведення комплексного SWOT-аналізу для організації у сфері захисту ІКС; побудова стратегічної матриці та формулювання стратегічних альтернатив.

СРС (9 год.): Опрацювання: Деміхов О. І., Дегтярьова І. О. «Стратегічне управління та управління змінами». Київ: ННІМП УМО, 2023; підготовка реферату «SWOT-аналіз сфери кіберзахисту в Україні: виклики та можливості».

МОДУЛЬ 3

Формування та вибір стратегій

Тема 3.1

Базові конкурентні стратегії М. Портера. Стратегії лідерства за витратами, диференціації та фокусування у сфері ІБ.

Тема 3.2

Корпоративні стратегії: зростання, стабілізації, скорочення. Стратегії диверсифікації та їх застосування для ІКС-організацій.

Тема 3.3

Функціональні стратегії: стратегія інформаційної безпеки як складова загальної стратегії організації. Стратегії управління ризиками.

МОДУЛЬ 3 · ТЕМА 3.1

Базові конкурентні стратегії та їх застосування

Лекційний матеріал (3 год.)

Базові конкурентні стратегії М. Портера: лідерство за витратами, диференціація, фокусування. Умови та ризики застосування кожної стратегії. Конкурентні переваги в контексті захисту інформації в ІКС. Стратегії «блакитного океану» як альтернативний підхід. Сучасні підходи до формування стратегій в умовах цифрових трансформацій та кіберзагроз. Стратегічне позиціонування організацій з ІБ на ринку.

Ключові питання

- Три базові конкурентні стратегії М. Портера
- Умови вибору стратегії диференціації для ІБ-організацій
- Конкурентні переваги у сфері захисту інформації
- Стратегія «блакитного океану» в кіберзахисті
- Стратегічне позиціонування на ринку ІБ-послуг

Практичне заняття (2 год.)

Завдання 1. Аналіз застосування конкурентних стратегій провідними ІТ-компаніями у сфері кіберзахисту: порівняльна характеристика підходів.

Завдання 2. Кейс: «Вибір конкурентної стратегії для стартапу у сфері захисту інформації: аналіз умов та обґрунтування рішення».

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

Самостійна робота (9 год.)

- Опрацювання: Ігнатьєва І. А. «Стратегічний менеджмент». Київ: Каравела, 2023 — розділ «Конкурентні стратегії»
- Підготовка реферату: «Конкурентні стратегії українських ІТ-компаній у сфері кіберзахисту»
- Складання порівняльної таблиці «Умови і ризики базових конкурентних стратегій для ІБ-організацій»

Очікуваний результат: студент вміє характеризувати базові конкурентні стратегії та обґрунтовувати їх вибір для організацій у сфері захисту інформації.

МОДУЛЬ 3 · ТЕМИ 3.2–3.3

Корпоративні та функціональні стратегії в ІКС

Тема 3.2 — Корпоративні стратегії (Лекція 10, 3 год.)

Корпоративні стратегії: зростання (концентрація, інтеграція, диверсифікація), стабілізації, скорочення. Стратегії злиття та поглинання в ІТ-сфері. Матриця Ансоффа «товар/ринок». Корпоративний портфельний аналіз. Стратегії аутсорсингу ІБ-функцій та їх стратегічні наслідки для організацій, що захищають інформацію в ІКС.

Практика (2 год.): Аналіз корпоративних стратегій провідних ІТ-компаній сфери кіберзахисту; дискусія «Аутсорсинг ІБ vs власний підрозділ: стратегічний вибір»; кейс за матрицею Ансоффа.

СРС (9 год.): Опрацювання: Буднік М. М., Невертій Г. С., Курилова Н. М. «Стратегічне управління». Київ: Кондор, 2020 — розділ «Корпоративні стратегії»; підготовка аналітичної записки «Стратегії розвитку ІТ-компаній в умовах воєнного стану».

Тема 3.3 — Функціональні стратегії (Лекція 11, 3 год.)

Функціональні стратегії як складові загальної стратегії організації. Стратегія інформаційної безпеки: компоненти, розробка, впровадження. Стратегія управління ризиками ІБ. Стратегія управління персоналом у сфері кіберзахисту. Стратегія технологічного розвитку підрозділу ІБ. Узгодженість функціональних стратегій із загальною стратегією організації.

Практика (2 год.): Розробка функціональної стратегії інформаційної безпеки для умовної організації; аналіз узгодженості стратегій різних рівнів; кейс «Стратегія управління ризиками ІБ».

СРС (9 год.): Опрацювання: Деміхов О. І., Дегтярьова І. О. «Стратегічне управління та управління змінами». Київ: ННІМП УМО, 2023; підготовка реферату «Стратегія інформаційної безпеки організації: методологія та практика».

МОДУЛЬ 4

Реалізація та контроль стратегій в організаціях захисту інформації

Тема 4.1

Процес реалізації стратегії: організаційні структури, ресурсне забезпечення, управління змінами у сфері ІБ.

Тема 4.2

Стратегічний контроль та оцінка ефективності реалізації стратегії. Система збалансованих показників (BSC) для ІКС-організацій.

Тема 4.3

Стратегічне управління змінами в умовах кіберзагроз. Адаптація стратегії до нових загроз і технологій. Антикризове стратегічне управління.

МОДУЛЬ 4 · ТЕМА 4.1

Реалізація стратегії: організація та ресурси

Лекційний матеріал (3 год.)

Процес реалізації стратегії: ключові елементи та умови успіху. Організаційні структури, що підтримують стратегію захисту інформації в ІКС. Ресурсне забезпечення реалізації стратегії: фінансові, кадрові, технологічні ресурси. Управління змінами при впровадженні стратегії ІБ: моделі Коттера та Льюіна. Стратегічна культура та її роль у захисті інформації. Лідерство у впровадженні стратегічних змін.

Ключові питання

- Ключові елементи успішної реалізації стратегії
- Організаційні структури управління ІБ: переваги та обмеження
- Управління змінами при впровадженні стратегії ІБ
- Стратегічна культура безпеки
- Ресурсне забезпечення стратегії захисту ІКС

Практичне заняття (2 год.)

Завдання 1. Аналіз організаційних структур підрозділів ІБ провідних організацій: ефективність для реалізації стратегії.

Завдання 2. Кейс: «Управління змінами при переході до нової стратегії захисту інформації — аналіз бар'єрів та методів їх подолання».

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

Самостійна робота (9 год.)

- Опрацювання: Ігнатьєва І. А. «Стратегічний менеджмент». Київ: Каравела, 2023 — розділ «Реалізація стратегії»
- Підготовка реферату: «Управління змінами при впровадженні стратегії кіберзахисту в організації»
- Аналіз організаційних структур управління ІБ в сучасних організаціях (на основі відкритих джерел)

Очікуваний результат: студент вміє характеризувати процес реалізації стратегії, обирати організаційні структури та методи управління змінами для впровадження стратегій захисту ІКС.

МОДУЛЬ 4 · ТЕМИ 4.2–4.3

Стратегічний контроль та управління змінами

Тема 4.2 — Стратегічний контроль (Лекція 14, 3 год.)

Стратегічний контроль: сутність, принципи, система показників. Збалансована система показників (BSC) Нортона і Каплана: чотири перспективи (фінанси, клієнти, внутрішні процеси, навчання та розвиток). Застосування BSC для організацій захисту інформації в ІКС. Ключові показники ефективності (KPI) у сфері ІБ. Аудит стратегії інформаційної безпеки. Стратегічне бенчмаркінгування в ІБ.

Практика (2 год.): Розробка BSC для підрозділу захисту інформації; визначення KPI у сфері ІБ; дискусія «Як виміряти ефективність стратегії кіберзахисту?».

СРС (9 год.): Опрацювання: Буднік М. М. та ін. «Стратегічне управління». Київ: Кондор, 2020 — розділ «Стратегічний контроль»; підготовка аналітичної записки «KPI у сфері захисту інформації: методика формування та оцінювання».

Тема 4.3 — Управління змінами (Лекція 15, 3 год.)

Стратегічне управління змінами в умовах динамічних кіберзагроз. Адаптація стратегії до нових загроз і технологій: цикл PDCA у стратегічному управлінні ІБ. Антикризове стратегічне управління: реагування на кіберінциденти стратегічного рівня. Управління стратегічними ризиками в умовах воєнного стану та гібридних загроз. Резильєнтність організацій у контексті кіберзахисту.

Практика (2 год.): Кейс «Антикризовий стратегічний план організації після масштабної кібератаки»; аналіз практик адаптації стратегії ІБ до нових загроз.

СРС (9 год.): Опрацювання: Білоус С., Трохименко А., Камінський В. «Стратегічне управління в умовах кризи та військових викликів». Економіка та суспільство, 2024, № 68; підготовка реферату «Стратегічна резильєнтність організації в умовах гібридних кіберзагроз».

МОДУЛЬ 5

Стратегічне управління ІБ: сучасні виклики та практика

Тема 5.1

Стратегічне управління інформаційною безпекою в умовах цифровізації та хмарних технологій. Zero Trust як стратегічна парадигма.

Тема 5.2

Стратегія кібербезпеки України: нормативна база, пріоритети, механізми реалізації. Євроінтеграційний вимір стратегічного управління ІБ.

Тема 5.3

Стратегічне планування розвитку фахівця з захисту інформації. Кар'єрні стратегії та компетентнісний профіль спеціаліста 123.

МОДУЛЬ 5 · ТЕМА 5.1

Стратегічне управління ІБ в умовах цифровізації

Лекційний матеріал (3 год.)

Стратегічне управління ІБ в умовах цифрової трансформації: виклики та можливості. Хмарні технології та їх вплив на стратегію захисту інформації в ІКС. Концепція Zero Trust як нова стратегічна парадигма кіберзахисту. Штучний інтелект у стратегічному управлінні ІБ: автоматизація, виявлення загроз, аналіз ризиків. Стратегії цифрової трансформації підрозділів захисту інформації.

Ключові питання

- Вплив цифровізації на стратегію захисту інформації в ІКС
- Zero Trust: принципи та стратегічні переваги
- Хмарна безпека як стратегічний пріоритет
- Роль ШІ у стратегічному управлінні кіберзахистом
- Стратегії цифрової трансформації підрозділів ІБ

Практичне заняття (2 год.)

Завдання 1. Аналіз стратегій провідних організацій щодо впровадження концепції Zero Trust: ключові компоненти та результати реалізації.

Завдання 2. Кейс: «Розробка стратегії переходу на хмарну інфраструктуру з урахуванням вимог захисту інформації».

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

Самостійна робота (9 год.)

- Опрацювання: Ігнатьєва І. А. «Стратегічний менеджмент». Київ: Каравела, 2023 — розділ «Стратегічне управління в умовах цифровізації»
- Підготовка реферату: «Zero Trust як стратегія захисту інформації в ІКС: теорія та практика»
- Аналіз стратегій цифрової трансформації в українських ІТ-компаніях

Очікуваний результат: студент вміє характеризувати стратегічне управління ІБ в умовах цифровізації, обґрунтовувати вибір стратегічних підходів (Zero Trust, хмарна безпека, ШІ) для захисту ІКС.

МОДУЛЬ 5 · ТЕМИ 5.2–5.3

Стратегія кібербезпеки України та розвиток фахівця

Тема 5.2 — Стратегія кібербезпеки України (Лекція 17, 3 год.)

Стратегія кібербезпеки України: нормативна база, пріоритети, механізми реалізації. Закон України «Про основні засади забезпечення кібербезпеки України». Доктрина інформаційної безпеки. Євроінтеграційний вимір стратегічного управління ІБ: вимоги NIS2, GDPR. Координація між державою та приватним сектором у забезпеченні стратегічної кібербезпеки.

Практика (2 год.): Аналіз Стратегії кібербезпеки України; порівняння з аналогічними стратегіями країн ЄС; дискусія «Євроінтеграційний курс і стратегія кіберзахисту».

СРС (9 год.): Опрацювання нормативно-правових документів (Закон «Про кібербезпеку», Стратегія кібербезпеки України на 2021–2025 рр.); підготовка аналітичної записки «Євроінтеграція і стратегія інформаційної безпеки України».

Тема 5.3 — Стратегічне планування кар'єри (Лекція 18, 3 год.)

Стратегічне планування розвитку фахівця у сфері захисту інформації. Компетентнісний профіль спеціаліста 123 «Комп'ютерна інженерія» (ОП «Організація захисту інформації в ІКС»). Кар'єрні стратегії: вертикальна, горизонтальна, підприємницька. Безперервний розвиток у сфері ІБ: сертифікації (CISSP, CEH, CompTIA Security+), фахові спільноти, наукова діяльність. Особиста стратегічна карта фахівця.

Практика (2 год.): Розробка особистої стратегічної карти розвитку фахівця з ІБ; аналіз вимог до сертифікацій у сфері кіберзахисту; захист індивідуального стратегічного плану кар'єри.

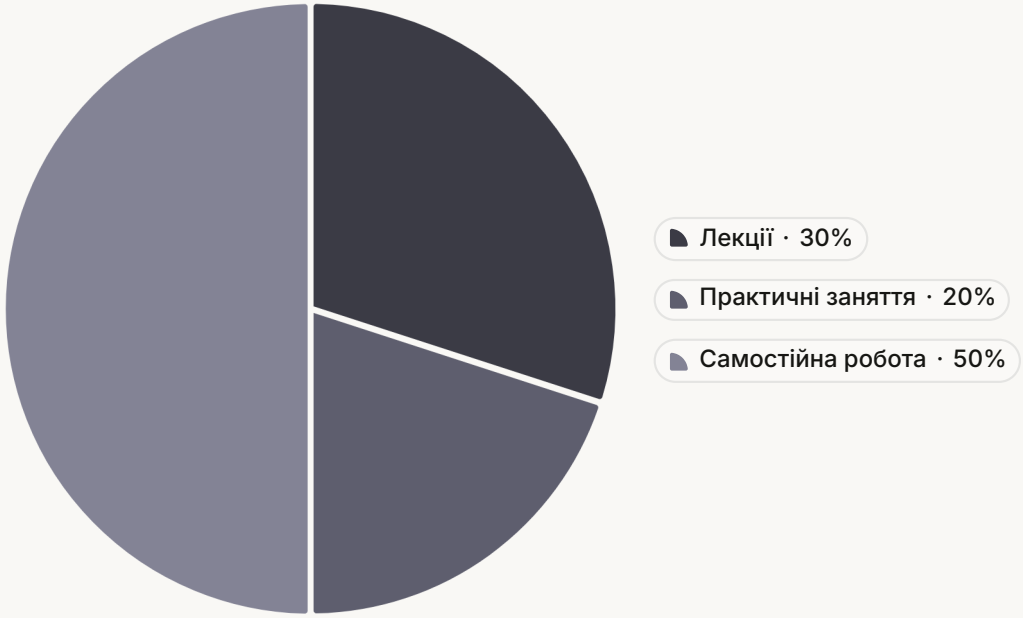
СРС (9 год.): Опрацювання: Білоус С. та ін. «Стратегічне управління в умовах кризи». Економіка та суспільство, 2024, № 68; підготовка стратегічного плану особистого розвитку як фахівця зі спеціальності 123 (ОП «Організація захисту інформації в ІКС»).

Розподіл навчального часу — 150 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Сутність та еволюція СУ	3	2	9
	Тема 1.2 — Місія та ієрархія стратегій	3	2	9
	Тема 1.3 — СУ в ІКС-організаціях	3	2	9
Модуль 2	Тема 2.1 — Аналіз зовнішнього середовища	3	2	9
	Тема 2.2 — Аналіз внутрішнього середовища	3	2	9
	Тема 2.3 — SWOT-аналіз та матричні методи	3	2	9
Модуль 3	Тема 3.1 — Базові конкурентні стратегії	3	2	9
	Тема 3.2 — Корпоративні стратегії	3	2	9
	Тема 3.3 — Функціональні стратегії	3	2	9
Модуль 4	Тема 4.1 — Реалізація стратегії	3	2	9
	Тема 4.2 — Стратегічний контроль (BSC)	3	2	9
	Тема 4.3 — Управління змінами	3	2	9
Модуль 5	Тема 5.1 — СУ ІБ в умовах цифровізації	3	2	9
	Тема 5.2 — Стратегія кібербезпеки України	3	4	9
	Тема 5.3 — Стратегічне планування кар'єри	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 зі стратегічного управління з використанням наочних схем, таблиць і прикладів із практики захисту інформації в ІКС.

Практичні — 30 год. (20%)

Відпрацювання навичок стратегічного аналізу, розгляд кейсів, дискусії та захист стратегічних проектів. Акцент на практичному застосуванні методів стратегічного управління у сфері ІБ.

Самостійна робота — 75 год. (50%)

Поглиблене вивчення, підготовка завдань, робота з джерелами та науковою літературою. Самостійна робота становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками зі стратегічного управління (Ігнатьєва, Буднік, Деміхов та ін.), нормативно-правовими актами у сфері кібербезпеки, науковими статтями у фахових виданнях. Студент конспектує ключові положення, виділяє головні поняття та порівнює підходи різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань (SWOT-аналіз, PESTEL, BSC для організацій захисту ІКС); творчих завдань — реферати, аналітичні записки, стратегічні плани; підготовка міні-проектів зі стратегічного управління у сфері кіберзахисту.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: Держспецзв'язку (**cip.gov.ua**), Верховної Ради (**zakon.rada.gov.ua**), CERT-UA (**cert.gov.ua**), Національної бібліотеки (**nbuv.gov.ua**). Аналіз наукових статей, пошук актуальної інформації про стратегії кібербезпеки.

Підготовка до занять

Підготовка до практичних занять (опрацювання кейсів, повторення теорії стратегічного аналізу); підготовка до тестувань (ключові терміни, моделі, методи); підготовка до контрольних робіт за кожним модулем (систематизація знань).

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 стратегічного аналізу, рівень засвоєння методів і моделей стратегічного управління. Поточний контроль формує накопичувальну оцінку протягом семестру. Проводиться після кожної теми у формі тестування (10–15 питань) або усного опитування.	Самостійна робота — комплексне ситуаційне завдання або реферат, які охоплюють теми змістовних модулів (теоретичні питання, стратегічний аналіз, розробка стратегій захисту ІКС). Оцінюються повнота відповіді, аргументованість та обґрунтованість стратегічних рішень. Проводиться після завершення кожного змістовного модуля.	Іспит відповідно до навчального плану. Форма проведення — тестування та письмові відповіді на питання зі стратегічного управління в контексті захисту інформації в ІКС. 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 «Стратегічне управління» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок стратегічного мислення, необхідних для майбутньої професійної діяльності у сфері захисту інформації в ІКС.

Лекції

Системне подання теоретичного матеріалу зі стратегічного управління з використанням схем, матриць, діаграм і прикладів із практики організацій захисту ІКС; студенти ведуть конспекти та задають уточнювальні запитання.

Стратегічний аналіз

Застосування інструментів SWOT, PESTEL, BSC, матриці Ансоффа до реальних кейсів організацій сфери захисту інформації; формування навичок обґрунтованого вибору стратегії.

Кейс-стаді

Аналіз реальних стратегічних ситуацій у сфері захисту ІКС; студенти виявляють проблему, застосовують методи стратегічного аналізу та обґрунтовують стратегічні рішення.

Дискусії

Обговорення актуальних стратегічних проблем кіберзахисту, євроінтеграційного курсу, антикризових стратегій; розвиток критичного мислення та аргументації стратегічних рішень.

Стратегічне проектування

Підготовка та захист стратегічних проектів (стратегія ІБ, стратегічний план кар'єри, BSC для підрозділу кіберзахисту); розвиток навичок самостійного стратегічного мислення.

Бізнес-симуляції

Рольові ігри та симуляції прийняття стратегічних рішень в умовах невизначеності та кіберзагроз; формування навичок командної розробки та захисту стратегій.

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

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

1. Ігнатьєва І. А.

Стратегічний менеджмент: навч. посіб. — 2-ге вид., перероб. та доп. — Київ: Каравела, 2023. — 480 с. *Рекомендовано МОН України.*

2. Деміхов О. І., Дегтярьова І. О.

Стратегічне управління та управління змінами: конспект лекцій. — Київ: ННІМП УМО, 2023. — 128 с. *Рекомендується для всіх модулів курсу.*

3. Буднік М. М., Невертій Г. С., Курилова Н. М.

Стратегічне управління: навчальний посібник. — Київ: Видавничий дім «Кондор», 2020. — 292 с. *Рекомендується для модулів 2–4.*

4. Білоус С., Трохименко А., Камінський В.

Стратегічне управління розвитком підприємства в умовах кризи та військових викликів. — Економіка та суспільство. — 2024. — № 68. *Рекомендується для модулів 4–5.*

5. Гогуля В. І.

Стратегічне управління: навчальний посібник. — Київ: НУБіП України, 2021. — 340 с. *Рекомендується для модуля 3.*

6. Єршова О. О., Гончаренко І. М.

Сучасні моделі управління розвитком бізнесу в умовах воєнного стану. Журнал стратегічних економічних досліджень. — 2022. — № 2(7). — С. 75–84. *Рекомендується для тем 4.3–5.2.*

7. Снітко Є. О., Завгородня Є. Є.

Стратегічне управління: навч.-метод. посібник для самостійної роботи. — Старобільськ: ДЗ «ЛНУ імені Тараса Шевченка», 2021. — 129 с. *Рекомендується для СРС.*

8. Артеменко Л. П.

Стратегічне управління: конспект лекцій. — Київ: КПІ ім. Ігоря Сікорського, 2021. — 198 с. *Рекомендується для модулів 1–2.*

Додаткова література та наукові статті

9. Довгань Л. Є., Каракай Ю. В., Артеменко Л. П.

Стратегічне управління: навч. посіб. — 2-ге вид. — Київ: Центр учбової літератури, 2011. — 440 с. *Класичний посібник, що залишається актуальним для базових модулів курсу.*

10. Кіндрацька Г. І.

Стратегічний менеджмент: навчальний посібник. — Київ: Знання, 2006. — 365 с. *Рекомендується для поглибленого вивчення стратегічного аналізу (модуль 2).*

11. Грайворонський М. В., Новіков О. М.

Безпека інформаційно-комунікаційних систем. — Київ: Видавнича група BHV, 2009. — 608 с. *Рекомендується для розуміння специфіки ІКС (модулі 1, 5).*

12. Бутко М. П. (ред.)

Стратегічний менеджмент: навчальний посібник. — Чернігів: ЧНТУ, 2017. — 320 с. *Рекомендується для модулів 3–4.*

Нормативно-правова база

- Конституція України

  Прийнята 28 червня 1996 р. Основний Закон держави, що визначає засади інформаційного суверенітету. **zakon.rada.gov.ua**

- Закон «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII

  Визначає правові та організаційні засади забезпечення кібербезпеки України. **zakon.rada.gov.ua**

- Стратегія кібербезпеки України на 2021–2025 роки

  Затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021. Ключовий стратегічний документ у сфері ІБ. **zakon.rada.gov.ua**

- Закон «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

  Базовий закон у сфері захисту інформації в ІКС. **zakon.rada.gov.ua**

- Закон «Про освіту» від 05.09.2017 № 2145-VIII

  Визначає засади освітньої діяльності в Україні. **zakon.rada.gov.ua**

Офіційні ресурси та фахові видання

Держспецзв'язку України

cip.gov.ua — нормативно-методичні документи у сфері технічного захисту інформації та кіберзахисту.

CERT-UA (Урядова команда реагування)

cert.gov.ua — аналітика кіберзагроз, звіти про інциденти, рекомендації щодо стратегічного захисту ІКС.

Верховна Рада України

zakon.rada.gov.ua — нормативно-правова база, законодавчі акти у сфері кібербезпеки та захисту інформації.

Національна бібліотека України ім. В. І. Вернадського

nbuv.gov.ua — електронні ресурси, наукові статті, монографії зі стратегічного управління.

Журнал «Проблеми інформатизації та управління»

piu.nau.edu.ua — фахове видання з питань управління в інформаційній сфері.

Журнал «Безпека інформації»

jrnl.nau.edu.ua — фахове видання з питань захисту інформації та кібербезпеки.

Міністерство цифрової трансформації

thedigital.gov.ua — стратегії цифрової трансформації, нормативні документи у сфері ІКС.

Міністерство освіти і науки України

mon.gov.ua — освітні стандарти, навчальні програми для спеціальності 123.

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

Чому «Стратегічне управління» для захисту ІКС?

Дисципліна «Стратегічне управління» є невід'ємною складовою підготовки бакалаврів зі спеціальністю 123 «Комп'ютерна інженерія» (ОП «Організація захисту інформації в ІКС»). Розуміння стратегічного управління формує у майбутніх фахівців здатність приймати виважені рішення щодо захисту інформаційних систем у довгостроковій перспективі.

Сучасний фахівець у сфері захисту ІКС працює в умовах постійно мінливих кіберзагроз, де стратегічне мислення, планування та управління ресурсами є ключовою конкурентною перевагою.

Практичне значення для майбутньої кар'єри

- Розробка та реалізація стратегій захисту інформації в ІКС організації
- Стратегічне управління ризиками інформаційної безпеки
- Обґрунтування стратегічних рішень щодо інвестицій у кіберзахист
- Управління командою фахівців із захисту інформації
- Аналіз та адаптація до стратегічних змін у сфері кіберзагроз
- Взаємодія з державними органами у сфері кібербезпеки України

Ключові компетентності курсу — Підсумок

Курс охоплює всі ключові аспекти стратегічного управління у сфері захисту інформації в ІКС — від концептуальних засад і стратегічного аналізу до формування, реалізації та контролю стратегій — і формує у студентів цілісне стратегічне мислення, необхідне для ефективної фахової діяльності.

Бажаємо успіхів у вивченні Стратегічного управління!

150

Годин

Загальний обсяг дисципліни

5

Кредити ЄКТС

Відповідно до стандарту

15

Тем

У 5 змістовних модулях

8

Джерел

Рекомендованої літератури 2021–2024 рр.

> «Стратегія без тактики — це найповільніший шлях до перемоги. Тактика без стратегії — це просто метушня перед поразкою.» — Сунь-цзи

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