Робоча програма дисципліни «Економіка захисту інформації»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

120

Годин

Загальний обсяг дисципліни

4

Кредити ЄКТС

Відповідно до стандарту

4

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Економіка захисту інформації

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 120 годин / 4 кредити ЄКТС

Модулів: 4 змістовних блоки

Призначення дисципліни

Дисципліна «Економіка захисту інформації» формує у студентів системне розуміння економічних засад захисту інформації: методів оцінювання вартості інформаційних активів, аналізу витрат на заходи безпеки, економічного обґрунтування управлінських рішень у сфері захисту інформаційно-комунікаційних систем та мінімізації економічних збитків від кіберінцидентів.

Дисципліна є обов'язковою для підготовки бакалаврів за освітньою програмою «Організація захисту інформації в інформаційно-комунікаційних системах» і забезпечує формування фахових компетентностей, передбачених освітньо-професійною програмою спеціальності 123.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання економічної інформації у сфері захисту: виявлення загроз, економічне оцінювання ризиків, порівняння варіантів захисту інформаційних активів з урахуванням їх вартості та ефективності.

Комунікація

Здатність до усної та письмової комунікації у сфері економіки інформаційної безпеки: чітко викладати техніко-економічні аспекти захисту, оформлювати бізнес-кейси, аналітичні записки, звіти про витрати та ефективність заходів ЗІ.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання практичних і самостійних завдань у визначені строки, зокрема під час підготовки економічних обґрунтувань систем захисту інформації.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді під час групового аналізу економічних наслідків кіберінцидентів, розробки бюджетів захисту ІКС та спільного вирішення техніко-економічних задач.

Студент повинен вміти: аналізувати економічну, нормативну та технічну інформацію у сфері ЗІ; виявляти загрози й оцінювати їх економічні наслідки; планувати власну діяльність і дотримуватися строків; коректно взаємодіяти з викладачами та одногрупниками; брати участь у командній роботі та розподіляти обов'язки.

Фахові компетентності

Економіка інформаційних активів

Розуміння сутності інформації як економічного ресурсу, методів оцінювання вартості інформаційних активів підприємства, класифікації інформаційних ресурсів за економічною значущістю та підходів до визначення збитків від їх компрометації.

Економічний аналіз ризиків ЗІ

Здатність проводити економічний аналіз ризиків інформаційної безпеки, кількісне та якісне оцінювання очікуваних збитків (ALE, SLE, ARO), порівнювати витрати на захист із потенційними втратами та обґрунтовувати доцільність заходів ЗІ.

Бюджетування та ефективність ЗІ

Знання методів формування бюджету на заходи захисту інформації, розрахунку ROI (Return on Security Investment), оцінювання ефективності реалізованих заходів, планування витрат на ліцензування, сертифікацію та аудит ІБ.

Правове та страхове регулювання

Орієнтування в нормативно-правовій базі у сфері економічних аспектів захисту інформації; розуміння механізмів страхування кіберризиків, відповідальності за витоки даних та економічних наслідків порушення вимог стандартів ISO/IEC 27001.

Результати навчання

01

Пояснення ключових категорій

Пояснювати сутність ключових понять і явищ: інформаційний актив, вартість інформації, кіберризик, очікувані збитки (ALE/SLE), витрати на захист, ROSI, TCO систем ЗІ, страхування кіберризиків, економічна ефективність заходів безпеки.

02

Кількісне оцінювання ризиків

Застосовувати методи кількісного та якісного оцінювання економічних ризиків інформаційної безпеки: розраховувати SLE, ARO, ALE; будувати матрицю ризиків; порівнювати варіанти захисту з урахуванням витрат і потенційних збитків.

03

Обґрунтування інвестицій у ЗІ

Розробляти техніко-економічне обґрунтування заходів захисту інформації: розраховувати ROSI, TCO, порівнювати альтернативні варіанти захисту, формувати бюджет на ІБ, аргументувати рішення керівництву організації.

04

Аналіз збитків та страхування

Аналізувати економічні наслідки кіберінцидентів та витоків даних для організацій; орієнтуватися у механізмах кіберстрахування, визначати страхові суми та умови покриття, розробляти заходи зменшення фінансових втрат від інцидентів ІБ.

МОДУЛЬ 1

Економічні засади захисту інформації

1 — Тема 1.1

Інформація як економічний ресурс. Вартість інформаційних активів: поняття, класифікація, підходи до оцінювання

2 — Тема 1.2

Економічна природа загроз інформаційній безпеці. Класифікація збитків від кіберінцидентів та витоків даних

3 — Тема 1.3

Методи кількісного оцінювання ризиків ІБ: SLE, ARO, ALE. Матриця ризиків та її застосування в економічному аналізі

4 — Тема 1.4

Нормативно-правова та стандартизаційна база економічних аспектів ЗІ. Відповідальність за порушення вимог захисту інформації

МОДУЛЬ 1 · ТЕМА 1.1

Інформація як економічний ресурс та оцінювання активів

Лекційний матеріал (2 год.)

Лекція 1: Поняття інформаційного активу в економічному вимірі. Інформація як стратегічний ресурс підприємства та об'єкт захисту. Класифікація інформаційних активів за рівнем конфіденційності та економічною цінністю. Методи оцінювання вартості інформаційних активів: витратний, дохідний, порівняльний підходи. Поняття матеріального та репутаційного збитку від втрати інформаційних активів.

Концептуальна основа: Взаємозв'язок між цінністю інформаційних активів і рівнем необхідного захисту. Принцип співмірності витрат на ЗІ та вартості захищуваних активів. Класифікація інформаційних ресурсів підприємства відповідно до НД ТЗІ та стандарту ISO/IEC 27001.

Ключові питання лекції

- Інформація як економічний ресурс та нематеріальний актив
- Методи оцінювання вартості інформаційних активів
- Класифікація інформаційних активів за цінністю та чутливістю
- Взаємозв'язок вартості активу і витрат на захист
- Реєстр інформаційних активів: призначення та структура

Практичне заняття (2 год.)

Завдання 1. Складання реєстру інформаційних активів умовного підприємства: ідентифікація, класифікація за рівнем конфіденційності та критичності, первинна оцінка вартості кожного активу.

Завдання 2. Кейс: порівняльний аналіз підходів до оцінювання вартості інформаційних активів. Групова робота та обговорення результатів.

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

Самостійна робота (7 год.)

- Опрацювання: Євсєєв С. П. та ін. «Кібербезпека: основи кодування та криптографії» (2023) — розділ «Інформаційні активи»
- Підготовка реферату: «Методи оцінювання вартості інформаційних активів: вітчизняний та зарубіжний досвід»
- Складання порівняльної таблиці підходів до класифікації інформаційних активів за ISO/IEC 27001 та НД ТЗІ

Очікуваний результат: студент вміє ідентифікувати інформаційні активи підприємства, класифікувати їх за рівнем цінності та застосовувати методи оцінювання їх вартості.

МОДУЛЬ 1 · ТЕМА 1.2

Економічна природа загроз та збитки від кіберінцидентів

1

Прямі фінансові збитки

Витрати на ліквідацію наслідків: відновлення даних, систем, розслідування інциденту, виплата штрафів.

2

Непрямі збитки

Репутаційні втрати, відтік клієнтів, зниження ринкової вартості, судові витрати, компенсації постраждалим.

3

Операційні збитки

Простій бізнес-процесів, недоотриманий прибуток, витрати на тимчасові рішення, зниження продуктивності.

4

Регуляторні санкції

Штрафи за порушення GDPR, Закону «Про захист персональних даних», відкликання ліцензій, приписи регуляторів.

Лекційний матеріал (2 год.)

Економічна природа загроз інформаційній безпеці. Класифікація збитків від кіберінцидентів: прямі та непрямі, матеріальні та репутаційні. Методика оцінювання збитків від витоку персональних даних, розкриття комерційної таємниці, порушення доступності ІКС. Аналіз реальних кейсів: економічні наслідки кіберінцидентів в Україні та світі за 2022–2024 рр.

Практичне заняття (2 год.) та СРС (7 год.)

Практичне: Аналіз економічних наслідків реальних кіберінцидентів в Україні (за відкритими джерелами); розробка моделі збитків для умовної організації з урахуванням типів загроз та категорій втрат.

СРС: Опрацювання: Єршова О. О., Гончаренко І. М. «Сучасні підходи до управління кіберризиками в умовах воєнного стану» (Журнал стратегічних досліджень, 2023); підготовка аналітичної записки «Економічні збитки від кіберінцидентів в Україні: 2022–2024 рр.».

МОДУЛЬ 1 · ТЕМИ 1.3–1.4

Кількісне оцінювання ризиків ІБ та нормативна база

Тема 1.3 — Методи кількісного оцінювання ризиків (Лекція 3, 2 год.)

Методологія кількісного оцінювання ризиків ІБ. Ключові показники: SLE (Single Loss Expectancy) — одиничний очікуваний збиток; ARO (Annualized Rate of Occurrence) — частота виникнення; ALE (Annualized Loss Expectancy) — річний очікуваний збиток. Побудова матриці ризиків «ймовірність × вплив». Порівняння якісного та кількісного підходів. Методологія CRAMM, COBIT for Risk, OCTAVE в контексті економічного аналізу.

Практичне (2 год.): Розрахунок SLE, ARO, ALE для типових загроз ІБ умовного підприємства; побудова матриці ризиків; порівняння рівня ризику із вартістю контрзаходів; оцінка доцільності впровадження захисних заходів.

СРС (7 год.): Опрацювання стандарту ISO/IEC 27005:2022; Єршова О. О., Гончаренко І. М. «Сучасні підходи до управління кіберризиками» (2023) — методологічний аспект; підготовка звіту «Порівняльний аналіз методик кількісного оцінювання ризиків ІБ».

Тема 1.4 — Нормативно-правова база (Лекція 4, 2 год.)

Нормативно-правова та стандартизаційна база економічних аспектів ЗІ. Закон «Про захист персональних даних» (ред. 2022): штрафні санкції. Закон «Про інформацію»: відповідальність за порушення. Регламент GDPR та його економічні наслідки для українських організацій. Стандарт ISO/IEC 27001:2022: витрати на впровадження та сертифікацію. НД ТЗІ: ліцензування діяльності у сфері ЗІ та його вартість. Страхування кіберризиків: регуляторне середовище в Україні.

Практичне (2 год.): Аналіз санкцій за порушення вимог захисту інформації та персональних даних; розрахунок потенційних штрафів для умовної організації; порівняння вартості відповідності вимогам із вартістю можливих санкцій.

СРС (7 год.): Підготовка аналітичної записки «Економічна відповідальність за порушення вимог захисту персональних даних: GDPR vs. законодавство України»; вивчення актуального законодавства України у сфері ЗІ.

МОДУЛЬ 2

Витрати на захист інформації та економічне обґрунтування рішень

Тема 2.1

Класифікація витрат на захист інформації. Сукупна вартість володіння (ТСО) системою ЗІ: структура, методи розрахунку.

Тема 2.2

Повернення інвестицій у безпеку (ROSI). Методи обґрунтування інвестицій у заходи захисту інформації.

Тема 2.3

Бюджетування інформаційної безпеки організації. Планування та оптимізація витрат на ЗІ в держсекторі та бізнесі.

Тема 2.4

Економічні аспекти ліцензування та сертифікації у сфері технічного захисту інформації. Вартість аудиту ІБ.

МОДУЛЬ 2 · ТЕМА 2.1

Класифікація витрат та ТСО системи захисту інформації

Лекційний матеріал (2 год.)

Класифікація витрат на захист інформації: капітальні (CAPEX) та операційні (OPEX) витрати. Складові ТСО (Total Cost of Ownership) системи ЗІ: витрати на придбання, впровадження, навчання персоналу, технічне обслуговування, оновлення, аудит. Порівняння ТСО різних підходів до захисту: власна інфраструктура vs. аутсорсинг ІБ vs. хмарні рішення. Приховані витрати на ЗІ: вплив на продуктивність, адміністративне навантаження.

Ключові питання

- CAPEX та OPEX у сфері захисту інформації
- Структура ТСО системи ЗІ організації
- Порівняння моделей: власна ІБ vs. аутсорсинг vs. MSSP
- Приховані витрати на захист інформації
- Вплив масштабу організації на ТСО системи ЗІ

Практичне заняття (2 год.)

Завдання 1. Розрахунок ТСО системи захисту інформації для умовного підприємства: визначення складу витрат, збір даних, обчислення за трирічний горизонт планування, порівняння альтернативних моделей захисту.

Завдання 2. Кейс: порівняння ТСО власної SOC-команди та послуги MSSP (Managed Security Service Provider) для середнього підприємства. Аргументоване обґрунтування рекомендацій.

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

Самостійна робота (7 год.)

- Опрацювання: Остроухов В. В. та ін. «Інформаційна безпека» (Ліра-К, 2022) — розділ «Організація та економіка ЗІ»
- Підготовка реферату: «ТСО систем захисту інформації: методика розрахунку та оптимізація витрат»
- Аналіз відповідних методичних рекомендацій Держспецзв'язку щодо побудови КСЗІ

Очікуваний результат: студент вміє розраховувати ТСО системи ЗІ, класифікувати витрати та порівнювати економічну доцільність альтернативних моделей захисту.

МОДУЛЬ 2 · ТЕМА 2.2

Повернення інвестицій у безпеку (ROSI)

Визначення ALE до

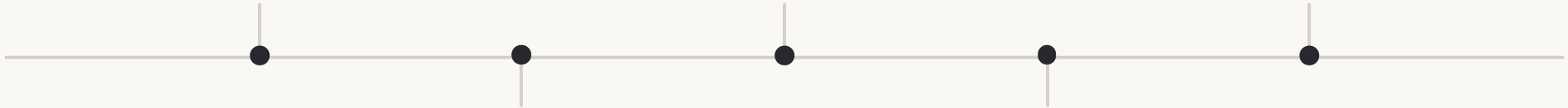
Розрахунок очікуваних річних збитків до впровадження заходу захисту (ALE_before).

Вартість захисту

Визначення річних витрат на заходи захисту (ACS — Annual Cost of Safeguard).

Прийняття рішення

Порівняння ROSI альтернативних заходів. Вибір оптимального варіанта захисту. Документування обґрунтування.



Визначення ALE після

Розрахунок очікуваних річних збитків після впровадження заходу захисту (ALE_after).

Розрахунок ROSI

ROSI = (ALE_before − ALE_after − ACS) / ACS × 100%. Інтерпретація результату.

Лекційний матеріал (2 год.)

Поняття ROSI (Return on Security Investment). Методологія розрахунку: від ALE до обґрунтування інвестиційного рішення. Формула ROSI та її інтерпретація. Обмеження та критика методу ROSI. Альтернативні підходи: NPV, IRR, аналіз беззбитковості у сфері ІБ. Практика обґрунтування інвестицій у ІБ для керівництва організацій. Фактори невизначеності при оцінюванні ROSI.

Практичне (2 год.) та СРС (7 год.)

Практичне: Розрахунок ROSI для типових заходів захисту (антивірусний захист, SIEM-система, навчання персоналу з ІБ, впровадження MFA); порівняльний аналіз варіантів; підготовка обґрунтування для умовного керівника організації.

СРС: Опрацювання: Гриценко В. С. «Кібербезпека: сучасні виклики та технології» (Київ: Юрінком Інтер, 2022) — розділ «Економічне обґрунтування ІБ»; підготовка аналітичної записки «Методологія ROSI: застосування в українських організаціях».

МОДУЛЬ 2 · ТЕМИ 2.3–2.4

Бюджетування ІБ та економіка ліцензування і сертифікації

Тема 2.3 — Бюджетування інформаційної безпеки (Лекція 7, 2 год.)

Принципи формування бюджету на інформаційну безпеку організації. Типові статті бюджету ІБ: персонал, технічні засоби, ліцензії, навчання, аудит, страхування. Методи визначення розміру бюджету ІБ: відсоток від ІТ-бюджету, ризикорієнтований підхід, бенчмаркінг з галузевими показниками. Особливості бюджетування ІБ в органах державної влади: бюджетний кодекс, публічні закупівлі (Prozorro). Оптимізація бюджету ІБ в умовах ресурсних обмежень.

Практичне (2 год.): Розробка бюджету на інформаційну безпеку для умовної організації: визначення статей, обґрунтування розміру витрат, пріоритизація заходів при обмеженому бюджеті, підготовка презентації бюджету для керівництва.

СРС (7 год.): Опрацювання: Корченко О. Г. та ін. «Захист інформації в інформаційно-телекомунікаційних системах» (НАУ, 2022) — розділ «Управління ресурсами ЗІ»; підготовка звіту «Бюджетування ІБ в українських організаціях: типові помилки та кращі практики».

Тема 2.4 — Економіка ліцензування та сертифікації ЗІ (Лекція 8, 2 год.)

Економічні аспекти ліцензування діяльності у сфері ТЗІ: вартість отримання ліцензій, обов'язкові умови, терміни. Сертифікація засобів захисту інформації в Україні: державна система сертифікації, вартість та терміни. КСЗІ: вартість проектування, побудови та атестації. Сертифікація за ISO/IEC 27001: витрати на підготовку, проведення аудиту, підтримання сертифіката. Порівняльний аналіз витрат на вітчизняну та міжнародну сертифікацію. Економічна доцільність сертифікації для організацій різних секторів.

Практичне (2 год.): Розрахунок витрат на отримання ліцензії Держспецзв'язку та побудову КСЗІ для умовного об'єкта ІТ-інфраструктури; порівняння витрат на НД ТЗІ-атестацію vs. ISO/IEC 27001-сертифікацію.

СРС (7 год.): Підготовка аналітичної записки «Економічні аспекти сертифікації КСЗІ в Україні: витрати, терміни та результати»; аналіз порядку ліцензування за відповідними НД ТЗІ та постановами КМУ.

МОДУЛЬ 3

Страхування кіберризиків та економіка управління інцидентами

Тема 3.1

Кіберстрахування: сутність, ринок, продукти. Страхування ризиків ІБ як інструмент управління фінансовими наслідками кіберінцидентів.

Тема 3.2

Економіка управління кіберінцидентами. Вартість реагування на інцидент, відновлення систем та даних. Витрати на цифрову криміналістику.

Тема 3.3

Економіка захисту персональних даних. Фінансові санкції за порушення GDPR та Закону «Про захист персональних даних». Вартість відповідності.

Тема 3.4

Економічні аспекти аутсорсингу функцій інформаційної безпеки. Оцінка ефективності MSSP, SOC-as-a-Service, хмарних рішень безпеки.

МОДУЛЬ 3 · ТЕМА 3.1

Кіберстрахування: ринок, продукти та механізми

Лекційний матеріал (2 год.)

Поняття кіберстрахування (cyber insurance) та його місце в системі управління ризиками ІБ. Ринок кіберстрахування: світові тенденції та стан в Україні. Типові страхові продукти у сфері кіберризиків: перше- та третьосторонні покриття. Страхові суми та франшизи. Умови виключення зі страхового покриття. Вплив кіберстрахування на стимули до інвестування в заходи ІІ. Законодавче регулювання кіберстрахування в Україні та ЄС.

Ключові питання

- Сутність та класифікація кіберстрахових продуктів
- Методологія оцінювання кіберризику страховиком
- Умови виключення та обмеження покриття
- Ринок кіберстрахування в Україні: стан та перспективи
- Кіберстрахування як стимул до підвищення рівня ІІ

Практичне заняття (2 год.)

Завдання 1. Аналіз типових умов кіберстрахових полісів: визначення обсягу покриття, виключень, вимог до андеррайтингу. Оцінка страхової суми для умовної організації.

Завдання 2. Кейс: порівняння вартості кіберстрахового полісу та прямих витрат на ліквідацію наслідків гіпотетичного кіберінциденту. Аргументація доцільності страхування.

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

Самостійна робота (7 год.)

- Опрацювання: Єршова О. О., Гончаренко І. М. «Сучасні підходи до управління кіберризиками в умовах воєнного стану» (2023) — аспект страхування
- Підготовка реферату: «Ринок кіберстрахування в Україні: поточний стан та перспективи розвитку»
- Аналіз зарубіжного досвіду кіберстрахування: США, ЄС, практика провідних страховиків

Очікуваний результат: студент вміє характеризувати ринок кіберстрахування, аналізувати умови страхових продуктів та обґрунтовувати доцільність страхування кіберризиків.

МОДУЛЬ 3 · ТЕМА 3.2

Економіка управління кіберінцидентами та відновлення

Лекційний матеріал (2 год.)

Економічна складова управління кіберінцидентами: вартість кожного етапу циклу реагування (NIST SP 800-61). Витрати на цифрову криміналістику (digital forensics). Вартість відновлення даних та систем. Економічні наслідки простою (downtime cost): методологія розрахунку. RTO (Recovery Time Objective) та RPO (Recovery Point Objective) в економічному вимірі. Вартість ransomware-атак: аналіз реальних випадків в Україні та світі за 2022–2024 рр.

Практичне (2 год.) та СРС (7 год.)

Практичне: Розрахунок вартості реагування на умовний кіберінцидент (ransomware-атака): витрати на кожному етапі циклу реагування; оцінка вартості простою; порівняння витрат на реагування з витратами на превентивний захист.

СРС: Опрацювання: Сілін Є. С., Кадубовський О. А. «Основи кібербезпеки» (КНУ ім. Тараса Шевченка, 2023) — розділ «Реагування на інциденти»; підготовка аналітичної записки «Вартість кіберінцидентів в Україні у 2022–2024 рр.: аналіз відкритих даних».

Очікуваний результат: студент вміє розраховувати вартість реагування на кіберінцидент та обґрунтовувати економічну доцільність превентивних заходів захисту.

МОДУЛЬ 3 · ТЕМА 3.3

Економіка захисту персональних даних та відповідність вимогам

Інвентаризація даних

Визначення категорій персональних даних, що обробляються. Вартість проведення DPO-аудиту та картографування потоків даних.

Витрати на відповідність

Вартість заходів для відповідності GDPR та Закону «Про захист персональних даних»: технічні та організаційні витрати.

Санкції та збитки

Розмір штрафів за GDPR (до 4% річного обороту або 20 млн євро). Збитки від судових позовів суб'єктів даних.

Лекційний матеріал (2 год.)

Економічна складова захисту персональних даних. Вартість відповідності вимогам GDPR та українського законодавства. Штрафні санкції: розмір, порядок накладення, практика застосування в ЄС. Вартість витоку персональних даних: прямі збитки, витрати на повідомлення, репутаційні наслідки. Роль DPO (Data Protection Officer): вартість посади та функції. Порівняння витрат на відповідність із потенційними санкціями.

Практичне (2 год.) та СРС (7 год.)

Практичне: Розрахунок потенційних штрафів за GDPR та Законом «Про захист персональних даних» для умовної організації; оцінка витрат на відповідність; підготовка звіту-обґрунтування для керівництва.

СРС: Опрацювання: Григоренко О. Ю. «Захист персональних даних в умовах цифровізації» (НЮУ ім. Ярослава Мудрого, 2023); підготовка аналітичної записки «Порівняльний аналіз санкцій за порушення захисту персональних даних: Україна та ЄС».

МОДУЛЬ 3 · ТЕМА 3.4

Економіка аутсорсингу функцій інформаційної безпеки

Лекційний матеріал (2 год.)

Аутсорсинг функцій ІБ: моделі (MSSP, SOC-as-a-Service, хмарна безпека). Порівняльний аналіз витрат: власний підрозділ ІБ vs. зовнішній провайдер. Ризики та переваги аутсорсингу з економічної точки зору. Критерії вибору MSSP: SLA, вартість, компетентності. Особливості аутсорсингу ІБ для держсектору: вимоги законодавства щодо обробки інформації з обмеженим доступом. Тенденції ринку послуг кіберзахисту в Україні.

Ключові питання

- Моделі аутсорсингу функцій ІБ та їх економічні характеристики
- Порівняльний TCO: власний підрозділ ІБ vs. MSSP
- SLA у договорах аутсорсингу ІБ: економічний вимір
- Обмеження аутсорсингу для держорганів України
- Ринок MSSP в Україні: гравці, тенденції, вартість послуг

Практичне заняття (2 год.)

Завдання 1. Порівняльний аналіз TCO власного підрозділу ІБ та послуги MSSP для умовної організації (середній бізнес, 200 співробітників): розрахунок витрат, визначення точки беззбитковості, рекомендації.

Завдання 2. Аналіз типового SLA на послуги кіберзахисту: оцінка фінансових умов, штрафних санкцій за недотримання SLA, рівнів покриття.

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

Самостійна робота (7 год.)

- Опрацювання: Живило Є. О. «Захист інформації та кібербезпека в електронних комунікаційних мережах» (ПНТУ, 2023) — розділ «Хмарні сервіси безпеки»
- Підготовка аналітичної записки «Аутсорсинг функцій ІБ в Україні: можливості, обмеження та економічна ефективність»
- Аналіз ринку MSSP в Україні: провідні гравці, типові послуги, цінові моделі

Очікуваний результат: студент вміє порівнювати моделі організації ІБ за критерієм економічної ефективності та обґрунтовувати вибір оптимальної моделі для конкретної організації.

МОДУЛЬ 4

Економічне управління інформаційною безпекою та стратегічне планування

Тема 4.1

Економічне обґрунтування впровадження СУІБ. Вартість сертифікації за ISO/IEC 27001 та ROI від її впровадження в організації.

Тема 4.2

Стратегічне планування витрат на ІБ. Довгострокові інвестиційні програми у сфері інформаційної безпеки організацій та держави.

Тема 4.3

Економіка людського фактора у сфері ІБ. Вартість навчання персоналу, підбір і утримання фахівців з кібербезпеки, наслідки інсайдерських загроз.

Тема 4.4

Макроекономічні аспекти кіберзахисту. Економіка кібербезпеки на рівні держави. Вплив кіберзагроз на ВВП та критичну інфраструктуру.

МОДУЛЬ 4 · ТЕМА 4.1

Економічне обґрунтування впровадження СУІБ та ISO/IEC 27001

Лекційний матеріал (2 год.)

Економічне обґрунтування впровадження системи управління інформаційною безпекою (СУІБ). Вартість проекту з впровадження ISO/IEC 27001:2022: етапи, ресурси, типові витрати. ROSI від сертифікації: зниження ризиків, зменшення страхових премій, конкурентні переваги, вихід на нові ринки. Бізнес-кейс для керівництва: як обґрунтувати інвестиції у СУІБ. Типові помилки при бюджетуванні проекту ISO/IEC 27001. Відповідність вимогам NIS2 ЄС та її економічна складова.

Ключові питання

- Етапи та вартість впровадження ISO/IEC 27001
- Кількісна оцінка переваг від сертифікації СУІБ
- Розробка бізнес-кейсу впровадження СУІБ для керівництва
- ROI від ISO/IEC 27001: методологія розрахунку
- Економічні вимоги директиви NIS2 для українських організацій

Практичне заняття (2 год.)

Завдання 1. Розробка бізнес-кейсу впровадження СУІБ на основі ISO/IEC 27001:2022 для умовної IT-компанії: розрахунок витрат на всіх етапах, оцінка вигод, розрахунок ROSI, підготовка презентації для керівництва.

Завдання 2. Порівняльний аналіз: впровадження СУІБ власними силами vs. із залученням зовнішнього консультанта — економічна доцільність кожного підходу.

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

Самостійна робота (7 год.)

- Опрацювання: Остроухов В. В. та ін. «Інформаційна безпека» (Ліра-К, 2022) — розділ «Управління ІБ та стандартизація»
- Підготовка реферату: «ROI від впровадження ISO/IEC 27001: міжнародний досвід та оцінки»
- Аналіз вимог директиви NIS2 та їх економічних наслідків для українського бізнесу

Очікуваний результат: студент вміє розробляти бізнес-кейс впровадження СУІБ, розраховувати ROI від сертифікації та обґрунтовувати інвестиції перед керівництвом.

МОДУЛЬ 4 · ТЕМА 4.2

Стратегічне планування витрат на захист інформації

Аналіз стану

Оцінювання поточного рівня зрілості ІБ. Gap-аналіз відповідно до цільової моделі (ISO/IEC 27001, NIST CSF).

1

Визначення цілей

Формулювання цілей ІБ, пов'язаних з бізнес-стратегією. Визначення пріоритетних напрямків інвестування.

2

Формування програми

Розробка багаторічної інвестиційної програми ЗІ. Розподіл бюджету між напрямками за ризикорієнтованим підходом.

3

Моніторинг та KPI

Визначення ключових показників ефективності (KPI) програми ЗІ. Механізми контролю витрат та коригування планів.

4

Лекційний матеріал (2 год.)

Стратегічне планування інвестицій у сферу інформаційної безпеки. Зв'язок стратегії ІБ з бізнес-стратегією організації. Багаторічне бюджетування програм ЗІ. Ризикорієнтований розподіл бюджету ІБ. KPI та метрики ефективності програми ІБ. Державні стратегії фінансування кібербезпеки: досвід України та країн ЄС. Вплив воєнного стану на стратегічне планування ЗІ в Україні 2022–2024 рр.

Практичне (2 год.) та СРС (7 год.)

Практичне: Розробка трирічної інвестиційної програми ЗІ для умовної організації: gap-аналіз, пріоритизація заходів, розподіл бюджету по роках, визначення KPI ефективності програми.

СРС: Опрацювання: Кулініч О. О. «Організаційно-правові основи захисту інформації з обмеженим доступом в органах державної влади» (Алерта, 2023) — аспект стратегічного планування; підготовка аналітичної записки «Стратегічне планування ІБ в умовах воєнного стану: адаптація пріоритетів».

МОДУЛЬ 4 · ТЕМА 4.3

Економіка людського фактора у сфері захисту інформації

Лекційний матеріал (2 год.)

Людський фактор в економіці ІБ: роль персоналу як найбільш уразливої ланки. Ринок праці у сфері кібербезпеки в Україні: дефіцит фахівців, рівень заробітних плат, тенденції 2022–2024 рр. Вартість підбору, навчання та утримання фахівців з ІБ. Програми підвищення обізнаності (Security Awareness Training): методологія оцінювання ефективності та ROI. Економічні наслідки інсайдерських загроз: збитки та витрати на протидію. Соціальна інженерія як джерело економічних збитків: статистика та методи зниження ризиків.

Ключові питання

- Ринок праці у сфері кібербезпеки в Україні: стан та тенденції
- Вартість програм підвищення обізнаності персоналу з ІБ
- ROI від навчання персоналу: методологія оцінювання
- Економічні збитки від інсайдерських загроз
- Соціальна інженерія як джерело фінансових втрат організації

Практичне заняття (2 год.)

Завдання 1. Розробка та економічне обґрунтування програми підвищення обізнаності персоналу з питань ІБ для умовної організації: бюджет, KPI, методологія оцінювання ефективності, розрахунок ROI.

Завдання 2. Кейс: аналіз фінансових наслідків успішної фішингової атаки (соціальна інженерія); розробка економічно обґрунтованих заходів протидії.

Завдання 3. Дискусія: «Інвестиції в навчання персоналу vs. технічні засоби захисту: що ефективніше?»

Самостійна робота (7 год.)

- Опрацювання: Довгань О. Д., Ткачук Т. Ю. «Інформаційна безпека держави в умовах гібридної агресії» (ДНДІ МВС України, 2022) — розділ «Людський фактор»
- Підготовка аналітичної записки «Ринок праці у сфері кібербезпеки в Україні: дефіцит кадрів та економічні наслідки»
- Аналіз звітів (ISC)², ENISA щодо глобального дефіциту фахівців з кібербезпеки та його економічних наслідків

Очікуваний результат: студент вміє розробляти економічно обґрунтовані програми навчання персоналу з ІБ та оцінювати фінансові наслідки людського фактора у сфері ІБ.

МОДУЛЬ 4 · ТЕМА 4.4

Макроекономічні аспекти кіберзахисту: рівень держави

Лекційний матеріал (2 год.)

Економіка кібербезпеки на державному рівні. Вплив кіберзагроз на ВВП та економічну стабільність країни. Витрати держави на забезпечення кібербезпеки: державний бюджет, програми фінансування. Економічні наслідки атак на критичну інфраструктуру: енергетику, фінанси, транспорт. Досвід України 2022–2024 рр.: масштаби економічних збитків від кіберскладової гібридної агресії. Міжнародне фінансування кіберзахисту України: НАТО, ЄС, двосторонні програми. Державні інвестиції в кіберекосистему: освіта, R&D, стартапи у сфері кіберзахисту.

Ключові питання

- Макроекономічні наслідки кібератак на рівні держави
- Бюджетне фінансування кібербезпеки в Україні
- Економічні збитки від атак на критичну інфраструктуру
- Міжнародна фінансова підтримка кіберзахисту України
- Державні інвестиції у розвиток кіберекосистеми

Практичне заняття (2 год.)

Завдання 1. Аналіз економічних збитків від масштабних кібератак на критичну інфраструктуру України 2022–2024 рр.: атрибуція, оцінка прямих та непрямих збитків, джерела фінансування відновлення.

Завдання 2. Дискусія: «Скільки держава має витрачати на кібербезпеку?» Аналіз відповідних показників країн НАТО та ЄС, обґрунтування рекомендацій для України.

Завдання 3. Підготовка та презентація міні-проекту: «Економічне обґрунтування державної програми фінансування кіберзахисту конкретного сектору критичної інфраструктури».

Самостійна робота (7 год.)

- Опрацювання: Довгань О. Д., Ткачук Т. Ю. «Інформаційна безпека держави в умовах гібридної агресії» (ДНДІ МВС України, 2022)
- Підготовка аналітичної записки «Макроекономічні збитки від кіберагресії Росії проти України: оцінки та методологія»
- Аналіз звітів Microsoft MSTIC, Cybersecurity Ventures щодо глобальних економічних збитків від кіберзлочинності

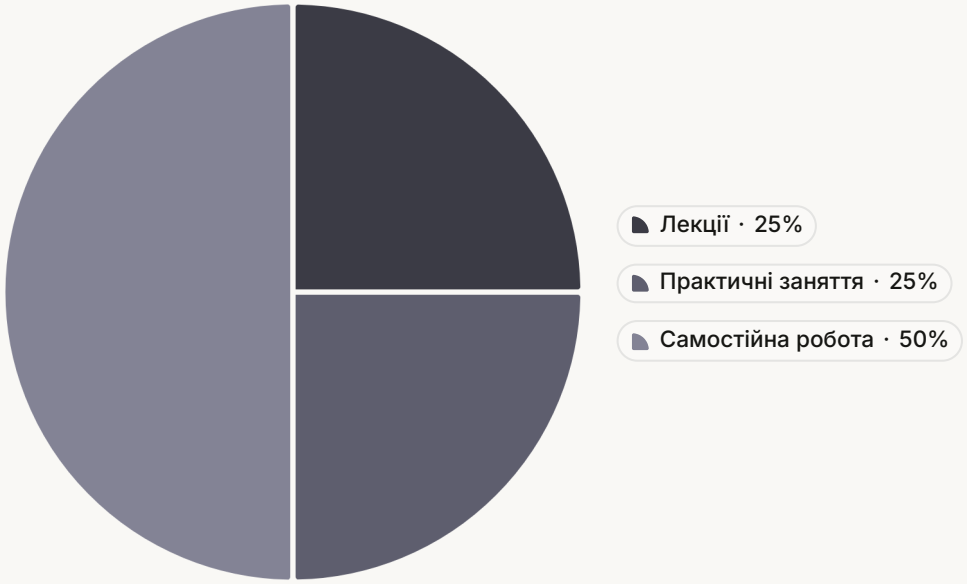
Очікуваний результат: студент вміє аналізувати макроекономічні наслідки кіберзагроз, оцінювати ефективність державних інвестицій у кіберзахист та формулювати рекомендації щодо стратегічного фінансування ІБ.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Інформація як економічний ресурс	2	2	7
	Тема 1.2 — Збитки від кіберінцидентів	2	2	7
	Тема 1.3 — Методи кількісного оцінювання ризиків	2	2	7
	Тема 1.4 — Нормативно-правова база ЗІ	2	2	7
Модуль 2	Тема 2.1 — ТСО системи захисту інформації	2	2	7
	Тема 2.2 — ROSI: повернення інвестицій у безпеку	2	2	7
	Тема 2.3 — Бюджетування інформаційної безпеки	2	2	7
	Тема 2.4 — Ліцензування та сертифікація ЗІ	2	2	7
Модуль 3	Тема 3.1 — Кіберстрахування	2	2	7
	Тема 3.2 — Економіка управління інцидентами	2	2	7
	Тема 3.3 — Економіка захисту персональних даних	2	2	7
	Тема 3.4 — Аутсорсинг функцій інформаційної безпеки	2	2	7
Модуль 4	Тема 4.1 — Економіка СУІБ та ISO/IEC 27001	2	2	7
	Тема 4.2 — Стратегічне планування витрат на ЗІ	2	2	7
	Тема 4.3 — Економіка людського фактора в ЗІ	2	2	7
	Тема 4.4 — Макроекономічні аспекти кіберзахисту	2	2	7
Разом	**16 тем**	**30**	**30**	**60**

Загальний обсяг: 120 годин = 4 кредити ЄКТС. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **120 годин (4 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теорією та практикою.

Лекції — 30 год. (25%)

Системне подання ключового теоретичного матеріалу з використанням наочних схем, таблиць і прикладів із вітчизняної та міжнародної практики економіки захисту інформації та управління кіберризиками.

Практичні заняття — 30 год. (25%)

Відпрацювання практичних навичок: розрахунок ALE, ROSI, TCO; розробка бюджетів ІІ; аналіз кіберінцидентів; обґрунтування інвестицій. Рівна частка з лекціями підкреслює практичну спрямованість курсу.

Самостійна робота — 60 год. (50%)

Поглиблене вивчення, підготовка аналітичних завдань, 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 економіки ІІ (Остроухов, Євсєєв, Гриценко, Корченко, Григоренко та ін.), нормативно-правовими актами, стандартами ISO/IEC 27001/27005, науковими статтями у фахових виданнях. Студент конспектує ключові положення та порівнює економічні підходи різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань (розрахунок ALE/ROSI/TCO, аналіз кіберінцидентів, порівняльний аналіз варіантів захисту); творчих завдань — аналітичні записки, звіти, бізнес-кейси з техніко-економічного обґрунтування заходів ІІ.

Робота з інформаційними ресурсами

Опрацювання офіційних ресурсів: Держспецзв'язку (**cip.gov.ua**), CERT-UA (**cert.gov.ua**), Верховної Ради (**zakon.rada.gov.ua**), ENISA, звітів Cybersecurity Ventures, IBM Cost of a Data Breach. Аналіз статистичних даних та актуальних аналітичних матеріалів.

Підготовка до занять

Підготовка до практичних занять (вивчення методологій оцінювання ризиків, розрахункових формул, стандартів); підготовка до тестувань (ключові терміни, визначення); підготовка до контрольних робіт за кожним модулем (систематизація знань, типові задачі розрахунку).

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 усного захисту практичної роботи.	Самостійна робота — комплексне розрахункове або ситуаційне завдання, яке охоплює теми змістовних модулів (теоретичні питання, розрахунки ALE/ROSI/TCO, аналіз кіберінцидентів, розробка бюджету ЗІ). Оцінюються повнота відповіді, правильність розрахунків та обґрунтованість висновків. Проводиться після завершення кожного змістовного модуля.	Іспит відповідно до навчального плану. Форма проведення — тестування та письмові розрахункові задачі. 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 «Економіка захисту інформації» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок техніко-економічного обґрунтування рішень у сфері захисту інформаційно-комунікаційних систем.

Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, таблиць і реальних прикладів економічних наслідків кіберінцидентів; студенти ведуть конспекти та задають уточнювальні запитання.

Розрахункові задачі

Розв'язання задач на розрахунок ALE, SLE, ARO, ROSI, TCO; побудова матриць ризиків; формування бюджету ІІ; формування навичок кількісного обґрунтування рішень.

Кейс-стаді

Аналіз реальних кіберінцидентів та їх економічних наслідків; оцінювання збитків організацій; аналіз рішень щодо страхування, бюджетування та аутсорсингу ІБ.

Дискусії

Обговорення дискусійних питань: скільки витрачати на ІІ, куди інвестувати обмежений бюджет, де межа між достатнім захистом та економічною доцільністю; розвиток аналітичного мислення.

Практичний практикум

Практична робота з методологіями оцінювання ризиків ІБ, розрахунок економічних показників захисту, побудова реєстрів ризиків та реєстрів активів, аналіз варіантів бюджетування ІІ.

Проектна робота

Підготовка бізнес-кейсів, техніко-економічних обґрунтувань, аналітичних записок та міні-проектів з економіки захисту ІКС; розвиток навичок самостійного аналізу та синтезу.

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. Остроухов В. В. та ін.
Інформаційна безпека: підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. — Київ : Ліра-К, 2022. — 412 с.

2. 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.

3. Гриценко В. С.
Кібербезпека: сучасні виклики та технології : навч. посіб. — Київ : Юрінком Інтер, 2022. — 310 с.

4. Корченко О. Г. та ін.
Захист інформації в інформаційно-телекомунікаційних системах : навч. посіб. — Київ : НАУ, 2022. — 328 с.

5. Григоренко О. Ю.
Захист персональних даних в умовах цифровізації : монографія. — Харків : НЮУ ім. Ярослава Мудрого, 2023. — 224 с.

6. Сілін Є. С., Кадубовський О. А.
Основи кібербезпеки : навчальний посібник. — Київ : КНУ ім. Тараса Шевченка, 2023. — 210 с.

7. Живило Є. О.
Захист інформації та кібербезпека в електронних комунікаційних мережах : навч. посіб. — Полтава : ПНТУ «Полтавська політехніка ім. Юрія Кондратюка», 2023. — 188 с.

8. Yevseiev S. et al.
Models of socio-cyber-physical systems security : monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. — Kharkiv : PC TECHNOLOGY CENTER, 2023. — 168 p.

Додаткова література та наукові статті

9. 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 модулів 1, 3 (кількісне оцінювання ризиків, страхування).*

10. 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 1.4, 4.1–4.2.*

11. Довгань О. Д., Ткачук Т. Ю.

Інформаційна безпека держави в умовах гібридної агресії: правові та організаційні засади : монографія. — Київ : ДНДІ МВС України, 2022. — 244 с. *Рекомендується для тем 1.2, 4.3–4.4.*

12. Бурячок В. Л. та ін.

Кібербезпека і управління інформаційними ресурсами : навч. посіб. — Київ : КУБГу, 2022. — 288 с. *Рекомендується для модулів 2–3 (бюджетування, аутсорсинг ІБ).*

Нормативно-правова база

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

  Визначає засади функціонування системи кібербезпеки України. **zakon.rada.gov.ua**

- Закон «Про захист персональних даних» від 01.06.2010 № 2297-VI (ред. 2022)

  Правові засади захисту персональних даних; санкції за порушення. **zakon.rada.gov.ua**

- Закон «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 (ред. 2022)

  Регулює відносини у сфері захисту інформації в ІТС; відповідальність за порушення. **zakon.rada.gov.ua**

- Регламент ЄС GDPR (2016/679) та його імплементація в законодавстві України

  Вимоги до захисту персональних даних; штрафні санкції до 4% річного обороту або 20 млн євро. **zakon.rada.gov.ua**

- Стандарт ISO/IEC 27001:2022 «Системи управління інформаційною безпекою — Вимоги»

  Міжнародний стандарт СУІБ; основа для економічного обґрунтування витрат на ЗІ та сертифікації.

Офіційні ресурси та фахові видання

Держспецзв'язку України

cip.gov.ua — офіційні матеріали, НД ТЗІ, нормативна база, реєстр сертифікованих засобів захисту інформації, відомості про ліцензування.

CERT-UA (урядова команда реагування)

cert.gov.ua — щотижневі звіти про кіберінциденти, технічні рекомендації, статистика атак — основа для аналізу економічних наслідків.

Верховна Рада України

zakon.rada.gov.ua — нормативно-правова база у сферах ІБ, кібербезпеки, захисту персональних даних та економічної відповідальності.

Національна бібліотека України ім. В. І. Вернадського

nbuv.gov.ua — електронні ресурси, наукові статті, монографії з інформаційної безпеки, кібербезпеки та економіки ЗІ.

ENISA (Агенція ЄС з кібербезпеки)

enisa.europa.eu — щорічні звіти про кіберзагрози та їх економічні наслідки, методичні матеріали з оцінювання ризиків та кіберстрахування.

IBM Security — Cost of a Data Breach Report

ibm.com — щорічний звіт про вартість витоку даних у світі; ключове джерело для модулів 1 та 3.

Журнал «Захист інформації» (НАУ)

НАУ — провідне фахове видання з технічного захисту інформації та кібербезпеки; публікує статті з економічних аспектів ЗІ.

Міністерство освіти і науки України

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

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

Чому «Економіка захисту інформації» для інженерів?

Дисципліна є невід'ємною складовою підготовки бакалаврів за ОП «Організація захисту інформації в ІКС». Розуміння економічних засад ЗІ формує у майбутніх інженерів здатність проектувати та впроваджувати захищені ІКС не лише технічно грамотно, але й економічно обґрунтовано — відповідно до реальних бюджетних обмежень і пріоритетів організацій.

Сучасний фахівець у сфері захисту інформації повинен вміти «говорити мовою цифр» з керівництвом: обґрунтовувати необхідність інвестицій у ЗІ, розраховувати ROSI та TCO, аргументувати вибір між технічними рішеннями з урахуванням їх вартості та ефективності.

Практичне значення для майбутньої кар'єри

- Навички техніко-економічного обґрунтування заходів ЗІ для будь-якого роботодавця
- Розуміння методів ROSI та TCO для роботи в сфері кібербезпеки та IT-менеджменту
- Знання кіберстрахування для роботи в галузі ризик-менеджменту та ІБ
- Навички бюджетування ІБ для роботи CISO, SOC-аналітика, консультанта з ЗІ
- Компетентності для роботи в органах кібербезпеки, Держспецзв'язку, страхових компаніях
- Готовність до економічного аналізу рішень у сфері захисту критичної інфраструктури

Ключові компетентності курсу — Підсумок

Курс охоплює всі ключові аспекти економіки захисту інформації — від оцінювання вартості активів і кількісного аналізу ризиків до стратегічного бюджетування та макроекономічного виміру кіберзахисту — і формує у студентів цілісне розуміння механізмів економічно обґрунтованого захисту інформаційно-комунікаційних систем.

Бажаємо успіхів у вивченні «Економіки захисту інформації»!

120

Годин

Загальний обсяг дисципліни

4

Кредити ЄКТС

Відповідно до стандарту

16

Тем

У 4 змістовних модулях

12

Джерел

Рекомендованої літератури 2022–2024 рр.

> «Хто вміє рахувати вартість захисту — той вміє захищати ефективно.»

Спеціальність 123 · Комп'ютерна інженерія · ОП: Організація захисту інформації в ІКС · Бакалавр · 4 кредити ЄКТС