Силабус дисципліни «Економіка захисту інформації»

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

120

Годин загальний обсяг дисципліни

4

Кредити ЄКТС відповідно до стандарту

4

Змістовних модулі 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 курсу

Мета дисципліни

Дисципліна «Економіка захисту інформації» формує у студентів спеціальності «Комп'ютерна інженерія» систему знань, умінь і навичок у сфері економічного обґрунтування рішень із захисту інформації в інформаційно-комунікаційних системах. Курс спрямований на опанування методів оцінки вартості інформаційних активів, аналізу та управління ризиками ІБ, розрахунку економічної ефективності заходів захисту, бюджетування та інвестиційного обґрунтування систем захисту інформації.

Форми навчання

- Лекції — 30 годин
- Практичні заняття — 30 годин
- Самостійна робота — 60 годин

Компетентності та результати навчання

Загальні компетентності

Здатність до аналізу, синтезу та критичного оцінювання економічної та нормативно-технічної інформації у сфері захисту інформації: виявлення суттєвих факторів витрат, порівняння підходів до обґрунтування інвестицій у безпеку, формування обґрунтованих висновків щодо економічної доцільності заходів захисту. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки фінансово-аналітичних матеріалів і бізнес-кейсів з інформаційної безпеки.

Здатність до усної та письмової фахової комунікації: чітко пояснювати економічні обґрунтування рішень із захисту інформації, аргументовано доводити доцільність інвестицій у безпеку перед зацікавленими сторонами. Відповідальність, ініціативність та готовність працювати в команді під час виконання практичних завдань.

- Аналізувати економічні аспекти рішень у сфері інформаційної безпеки
- Планувати власну діяльність і дотримуватися дедлайнів
- Чітко комунікувати результати економічного аналізу
- Брати участь у командній роботі під час вирішення кейсів

Фахові компетентності

Розуміння економічної природи інформації як ресурсу та активу, закономірностей формування витрат на захист інформації в інформаційно-комунікаційних системах. Знання методів вартісної оцінки інформаційних активів, кількісного та якісного аналізу ризиків ІБ, розрахунку показників ефективності систем захисту.

Здатність застосовувати економічні інструменти для обґрунтування управлінських рішень у сфері захисту інформації: TCO, ROI, ROSI, NPV, аналіз вигід і витрат, методи оцінки збитків від інцидентів ІБ.

- Оцінювати вартість інформаційних активів організації
- Проводити кількісний та якісний аналіз ризиків ІБ
- Розраховувати економічну ефективність заходів захисту (ROSI)
- Формувати бюджет на інформаційну безпеку
- Обґрунтовувати інвестиції в системи захисту інформації

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять економіки захисту інформації: інформаційний актив, вартість інформації, ризик ІБ, очікувані втрати, ТСО системи захисту, ROSI, бюджет безпеки. Характеризувати нормативно-правову та методологічну базу, що регламентує економічне обґрунтування заходів захисту інформації в Україні.

2

Аналіз та оцінювання

Аналізувати структуру витрат на захист інформації в організації, виявляти економічно невиправдані або недостатні заходи безпеки. Оцінювати ризики ІБ у кількісному вираженні, розраховувати очікувані річні втрати (ALE) та обґрунтовувати оптимальний рівень витрат на захист.

3

Застосування знань

Застосовувати методи та інструменти економічного аналізу (ROI, ROSI, NPV, TCO) для обґрунтування рішень у сфері захисту інформації в ІКС. Розробляти бюджети на інформаційну безпеку, бізнес-кейси для інвестицій у засоби захисту та плани страхування кіберризиків.

4

Комунікація та рефлексія

Аргументовано представляти результати економічного аналізу систем захисту інформації перед керівництвом організації та зацікавленими сторонами. Формувати професійну відповідальність за економічно обґрунтоване управління ресурсами інформаційної безпеки.

Модуль 1. Економічні основи інформаційної безпеки

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Інформація як економічний ресурс та актив. Сутність і особливості інформації як економічного ресурсу. Класифікація інформаційних активів. Вартість інформації: підходи до визначення та оцінки. Економічна цінність конфіденційності, цілісності та доступності інформації. Поняття інформаційного збитку та його складові.

Тема 1.2

Ринок засобів і послуг захисту інформації. Структура та тенденції ринку кібербезпеки в Україні та світі. Класифікація продуктів і послуг захисту інформації. Провідні постачальники засобів захисту. Особливості ціноутворення на ринку ІБ. Нормативно-правові вимоги як чинник ринкового попиту на засоби захисту.

Тема 1.3

Збитки від порушень інформаційної безпеки. Класифікація збитків від інцидентів ІБ: прямі та непрямі, матеріальні та нематеріальні. Методи розрахунку збитків від витоку інформації, НСД, відмов систем. Репутаційні та юридичні наслідки інцидентів. Статистика збитків від кіберінцидентів в Україні та в світі.

Тема 1.4

Нормативно-правові та стандартизаційні основи економіки ЗІ. Законодавство України щодо захисту інформації та відповідальності за інциденти ІБ. Стандарти ISO/IEC серії 27000 як основа управління ризиками і витратами на ЗІ. ДСТУ в сфері оцінки ризиків. Вимоги регуляторів до витрат на безпеку (НБУ, ДССЗЗІ, НКЦК).

Модуль 2. Оцінка та управління ризиками інформаційної безпеки

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Концепція ризику в економіці інформаційної безпеки. Поняття ризику ІБ та його складові: загроза, вразливість, актив, ймовірність, вплив. Класифікація ризиків ІБ. Кількісний та якісний підходи до оцінки ризиків. Показники ALE (Annual Loss Expectancy), SLE, ARO. Стандарт ISO/IEC 27005 та NIST SP 800-30: методологія оцінки ризиків.

Тема 2.2

Методи кількісного аналізу ризиків. Методологія CRAMM, OCTAVE, FAIR. Побудова моделі загроз та матриці ризиків. Розрахунок очікуваних річних втрат. Аналіз чутливості та сценарний аналіз ризиків. Інструментальні засоби для кількісної оцінки ризиків ІБ. Вибір стратегії реагування на ризик: прийняття, уникнення, передача, зниження.

Тема 2.3

Страхування кіберризиків як інструмент управління. Сутність та особливості кіберстрахування. Ринок кіберстрахування в Україні та світі. Типові страхові продукти у сфері ІБ. Процес андерайтингу кіберризиків. Оцінка страхової премії. Взаємодія страхування та технічних заходів захисту. Обмеження та перспективи кіберстрахування.

Модуль 3. Економічне обґрунтування витрат на захист інформації

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Структура витрат на інформаційну безпеку. Класифікація витрат на ІІ: капітальні та операційні, прямі та непрямі. Модель сукупної вартості володіння (TCO) системи захисту. Витрати на попередження інцидентів, виявлення та усунення наслідків. Бенчмаркінг витрат на ІБ: галузеві орієнтири та рекомендації. Вплив зрілості СУІБ на структуру витрат.

Тема 3.2

Показники ефективності інвестицій у захист інформації. Концепція повернення інвестицій (ROI) та її адаптація до сфери ІБ. Показник ROSI (Return on Security Investment): методика розрахунку та обмеження. Аналіз вигід і витрат (CBA) для проектів ІБ. Дисконтовані показники: NPV, IRR, термін окупності інвестицій у безпеку. Якісні показники ефективності заходів захисту.

Тема 3.3

Бюджетування інформаційної безпеки. Підходи до формування бюджету на ІБ: від ризиків, від галузевих нормативів, від бізнес-цілей. Статті бюджету ІБ: персонал, технічні засоби, послуги, навчання, аудит. Обґрунтування бюджету ІБ перед керівництвом (бізнес-кейс). Оптимізація бюджету ІБ в умовах обмежених ресурсів. Моніторинг та контроль виконання бюджету ІБ.

Модуль 4. Економіка кіберінцидентів та стратегічне планування ІБ

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

Економічний аналіз кіберінцидентів. Методи розрахунку збитків від конкретних типів інцидентів: витік даних, ransomware, DDoS, інсайдерські загрози. Прямі та непрямі втрати від інцидентів ІБ. Вартість реагування та відновлення. Аналіз вартості витоку даних (Cost of a Data Breach). Досвід оцінки збитків від кіберінцидентів в Україні в умовах воєнного стану.

Тема 4.2

Економіка хмарної та розподіленої безпеки. Економічні аспекти переходу на хмарні технології з позицій ІБ. Моделі хмарних сервісів безпеки (SECaaS): вартість та ефективність. Порівняльний аналіз витрат: власна ІБ-інфраструктура vs. хмарні рішення. Аутсорсинг функцій ІБ (MSSP): економічне обґрунтування. Управління витратами в гібридних середовищах.

Тема 4.3

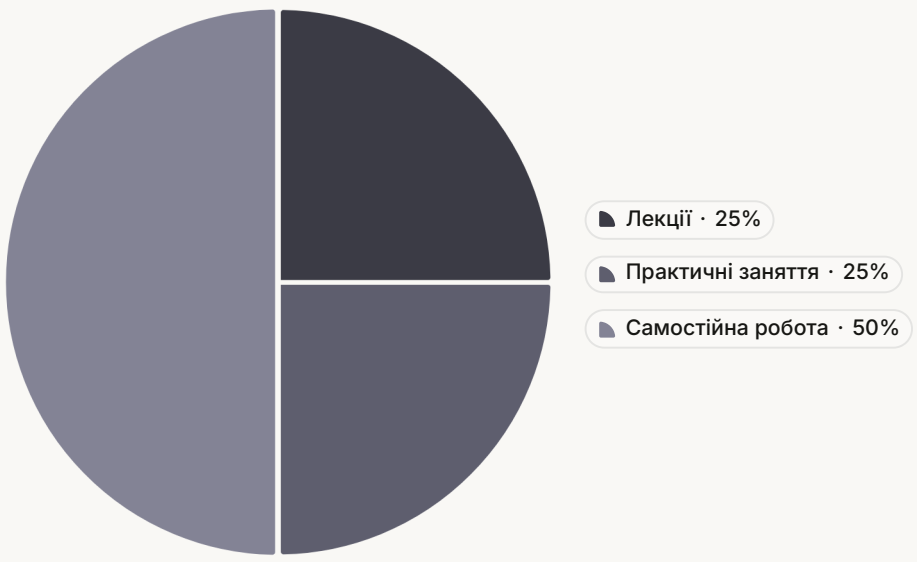
Стратегічне планування та економічна зрілість ІБ. Моделі зрілості ІБ та їх вплив на економічні показники (CMMI, C2M2). Стратегія розвитку СУІБ з урахуванням ресурсних обмежень. Вимірювання ефективності ІБ: KPI та метрики безпеки. Економічна ефективність відповідності нормативним вимогам (compliance). Тенденції та перспективи ринку кібербезпеки в умовах цифровізації.

Тема 4.4

Комплексний аналіз та захист критичної інформаційної інфраструктури. Економічні особливості захисту об'єктів КІІ. Оцінка вартості захисту критичних систем. Державне фінансування кібербезпеки в Україні. Публічно-приватне партнерство у сфері захисту КІІ. Економічні наслідки кіберзагроз для критичних секторів: енергетика, фінанси, транспорт, охорона здоров'я.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Інформація як економічний ресурс	2	2	4
	Тема 1.2 — Ринок засобів і послуг захисту інформації	2	2	4
	Тема 1.3 — Збитки від порушень інформаційної безпеки	2	2	4
	Тема 1.4 — Нормативно-правові основи економіки ЗІ	2	2	4
Модуль 2	Тема 2.1 — Концепція ризику в економіці ІБ	2	2	4
	Тема 2.2 — Методи кількісного аналізу ризиків	2	4	4
	Тема 2.3 — Страхування кіберризиків	2	2	4
Модуль 3	Тема 3.1 — Структура витрат на інформаційну безпеку	2	4	6
	Тема 3.2 — Показники ефективності інвестицій (ROSI)	4	4	6
	Тема 3.3 — Бюджетування інформаційної безпеки	2	2	6
Модуль 4	Тема 4.1 — Економічний аналіз кіберінцидентів	2	2	6
	Тема 4.2 — Економіка хмарної та розподіленої безпеки	2	2	6
	Тема 4.3 — Стратегічне планування та зрілість ІБ	2	2	6
	Тема 4.4 — Захист критичної інформаційної інфраструктури	2	2	6
Разом		**30**	**30**	**60**



Структура навчального часу

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

- **Лекції (30 год. — 25%):** подача ключового теоретичного та аналітичного матеріалу
- **Практичні (30 год. — 25%):** розрахунки ROSI/ALE, аналіз ризиків, кейси, побудова бюджетів ІБ
- **Самостійна робота (60 год. — 50%):** поглиблене вивчення, підготовка аналітичних проектів

Практичні заняття становлять **25% обсягу дисципліни** — студенти набувають навичок реальних розрахунків економічної ефективності заходів захисту інформації.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з економіки захисту інформації та управління ризиками ІБ, нормативними документами, науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння методів оцінки ефективності заходів захисту.

Індивідуальні завдання

Виконання розрахункових завдань: оцінка ризиків ІБ за методологією FAIR, розрахунок показників ROSI та ALE для конкретних сценаріїв загроз, побудова бізнес-кейсу для обґрунтування інвестицій у систему захисту інформації підприємства.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: Держспецзв'язку (**cip.gov.ua**), НКЦК (**ncscc.gov.ua**), Верховна Рада (**zakon.rada.gov.ua**). Аналіз звітів IBM Cost of a Data Breach, Verizon DBIR, аналітики ринку кібербезпеки.

Підготовка до занять

Підготовка до практичних занять шляхом опрацювання методик розрахунку ризиків та показників ефективності; повторення теоретичного матеріалу; підготовка до тестувань через засвоєння ключових термінів, формул та визначень; систематизація знань перед модульними контрольними роботами.

Методи викладання

→ Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, таблиць, графіків і прикладів розрахунків; студенти ведуть конспекти та задають уточнювальні запитання щодо методів оцінки ефективності ЗІ.

→ Кейс-стаді

Аналіз реальних кіберінцидентів з позиції економічних наслідків; студенти розраховують збитки, оцінюють ROSI впроваджених контрзаходів та обґрунтовують оптимальні рішення щодо управління ризиками.

→ Практичні вправи

Розрахунки ALE, SLE, ROSI, TCO та NPV для проектів ІБ; побудова матриць ризиків; розробка бюджетів інформаційної безпеки та бізнес-кейсів для обґрунтування інвестицій у засоби захисту.

→ Робота з нормативними документами

Опрацювання стандартів ISO/IEC 27001, 27005, законодавства України у сфері ІБ; формування навичок аналізу регуляторних вимог та розрахунку витрат на відповідність (compliance costs).

→ Самостійне дослідження

Підготовка аналітичних проектів з оцінки економічної ефективності системи ЗІ для модельного підприємства; розвиток навичок самостійного економічного аналізу та презентації результатів.

Форми контролю знань

1

Поточний контроль

Завдання: розрахункові, аналітичні та тестові вправи за темами змістовного модуля. Оцінюються точність обчислень показників ризику та ефективності (ALE, ROSI, TCO), якість аналізу кейсів і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, письмові розрахункові завдання, розбір нормативних актів та участь у вирішенні економічних кейсів із ЗІ.

2

Проміжний контроль

Самостійна розрахунково-аналітична робота — комплексне завдання, що охоплює теми змістовного модуля: оцінка ризиків за кількісною методологією, розрахунок показників ефективності заходів захисту, обґрунтування бюджету ІБ або бізнес-кейс для конкретного підприємства. Оцінюються повнота, правильність розрахунків та обґрунтованість висновків. Проводиться після кожного змістовного модуля.

3

Підсумковий контроль

Іспит відповідно до навчального плану. Форма проведення — тестування та письмові задачі з усіх чотирьох модулів курсу (розрахункові завдання, аналіз сценаріїв, обґрунтування рішень). 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).

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

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: підручник. — Житомир : ЖНАЕУ, 2023. — 636 с.
2. Дудикевич В. Б., Хорошко В. О. Захист інформації в інформаційно-комунікаційних системах: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 312 с.
3. Корченко О. Г., Архипов О. Є. Системи захисту інформації: стандарти та нормативна база: підручник. — Київ : НАУ, 2022. — 398 с.
4. Петров В. В., Смерницький Д. В. Правові основи захисту інформації з обмеженим доступом: навч. посіб. — Харків : ХНУРЕ, 2023. — 224 с.
5. Леськів А. В., Паращук С. Д. Електронний документообіг та захист інформації в органах державної влади: навч. посіб. — Київ : Видавничий дім «Академперіодика», 2024. — 268 с.
6. Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки: підручник. — Київ : ДУІКТ, 2022. — 476 с.
7. Криворучко О. В., Десятко А. М., Чубаєвський В. І. Methods and Means of Information Protection: навч. посіб. — Київ : ДТЕУ, 2023. — 284 с.
8. Рудик О. М., Сергієнко І. В. Організація архівної справи та захист документаційного фонду: навч. посіб. — Київ : Алерта, 2024. — 256 с.
9. Білоус С. П., Власенко А. Ю. Управління ризиками підприємства в умовах цифровізації: навч. посіб. — Київ : Цифрова економіка та економічна безпека, 2023. — 198 с.
10. Гайдамака А. В., Козловський С. В. Організація спеціального діловодства та захист інформації: навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 248 с.

Офіційні інтернет-ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. — URL: **https://cip.gov.ua/**
2. Національний координаційний центр кібербезпеки. — URL: **https://ncscc.gov.ua/**
3. Офіційний сайт Верховної Ради України. — URL: **https://zakon.rada.gov.ua/**
4. Офіційний сайт Кабінету Міністрів України. — URL: **https://www.kmu.gov.ua/**
5. Міністерство цифрової трансформації України. — URL: **https://thedigital.gov.ua/**
6. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
7. Науково-технічний журнал «Кібербезпека: освіта, наука, техніка». — URL: **https://csecurity.kubg.edu.ua/**
8. Журнал «Захист інформації» (електронне видання). — URL: **https://захист-інформації.укр/**

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