Силабус дисципліни «Теорія ризиків»

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: Теорія ризиків

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 «Теорія ризиків» формує у студентів спеціальності «Комп'ютерна інженерія» систему знань, умінь і навичок у сфері ідентифікації, аналізу, оцінювання та управління ризиками в інформаційно-комунікаційних системах. Курс спрямований на опанування концептуальних основ теорії ризиків, методів кількісного та якісного оцінювання, стандартів ризик-менеджменту, а також сучасних інструментів мінімізації ризиків інформаційної безпеки в комп'ютерних мережах і ІКС.

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 технічної і нормативної інформації у сфері ризик-менеджменту та захисту інформації: виявлення факторів ризику, порівняння методологічних підходів, формування обґрунтованих висновків щодо стратегій управління ризиками. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки аналітичних матеріалів і моделей оцінювання ризиків.

Здатність до усної та письмової фахової комунікації: чітко пояснювати вимоги стандартів ризик-менеджменту, аргументовано обґрунтовувати рішення щодо вибору методів оцінювання та мінімізації ризиків. Відповідальність, ініціативність і готовність до командної роботи під час виконання практичних завдань.

- Аналізувати нормативно-правові акти та стандарти у сфері управління ризиками ІБ
- Планувати власну діяльність і дотримуватися дедлайнів
- Коректно спілкуватися в академічному та фаховому середовищі
- Брати участь у командній роботі та розподіляти обов'язки

Фахові компетентності

Розуміння сутності та закономірностей теорії ризиків, її місця у системі захисту інформації в інформаційно-комунікаційних системах. Знання ключових понять, концептуальних моделей і методів ідентифікації, аналізу, оцінювання та управління ризиками, вміння застосовувати їх у практичній діяльності фахівця з інформаційної безпеки.

Здатність застосовувати кількісні та якісні методи оцінювання ризиків для забезпечення конфіденційності, цілісності та доступності інформації в умовах функціонування сучасних ІКС, зокрема з урахуванням вимог міжнародних стандартів ISO/IEC 27005 та NIST SP 800-30.

- Характеризувати концептуальні основи та класифікацію ризиків
- Застосовувати методи ідентифікації загроз та вразливостей
- Виконувати кількісне та якісне оцінювання ризиків ІБ
- Розробляти стратегії та плани управління ризиками
- Застосовувати стандарти ризик-менеджменту до реальних ІКС

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять теорії ризиків: ризик, загроза, вразливість, актив, ймовірність реалізації, величина збитку, прийнятний ризик, залишковий ризик, ризик-апетит. Характеризувати нормативно-правову базу та міжнародні стандарти, що регламентують управління ризиками інформаційної безпеки в Україні та світі.

2

Аналіз та оцінювання

Аналізувати інформаційні системи з точки зору ризиків, ідентифікувати загрози та вразливості, оцінювати ймовірність та потенційні наслідки реалізації ризиків. Застосовувати кількісні та якісні методи оцінювання ризиків (CRAMM, FRAP, OCTAVE, NIST) та порівнювати їх ефективність для конкретних умов ІКС.

3

Застосування знань

Розробляти моделі ризиків для інформаційно-комунікаційних систем, формувати плани обробки ризиків і стратегії їх мінімізації. Застосовувати інструментарій ризик-менеджменту відповідно до вимог стандартів ISO/IEC 27005:2022, NIST SP 800-30 та методики Держспецзв'язку України.

4

Комунікація та рефлексія

Аргументовано викладати власну позицію щодо вибору методів оцінювання та управління ризиками в конкретних умовах функціонування ІКС. Формувати професійну відповідальність і розуміння важливості систематичного управління ризиками у фаховій діяльності фахівця із захисту інформації.

Модуль 1. Концептуальні основи теорії ризиків

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Поняття та сутність ризику. Місце теорії ризиків у системі захисту інформації. Основні терміни та визначення: ризик, загроза, вразливість, актив, інцидент, збиток. Класифікація ризиків за природою, джерелом та наслідками. Принципи системного підходу до аналізу ризиків в ІКС.

Тема 1.2

Нормативно-правова база та стандарти ризик-менеджменту. Закони України «Про інформацію», «Про кіберзахист», «Про захист інформації в інформаційно-комунікаційних системах». Стандарти ISO/IEC 27001, ISO/IEC 27005:2022, NIST SP 800-30, DSTU ISO 31000. Методика оцінювання ризиків кібербезпеки Держспецзв'язку України (2023).

Тема 1.3

Моделі та концепції ризиків в ІКС. Математичні основи теорії ризиків: теорія ймовірностей, теорія ігор, теорія нечітких множин. Моделі ризиків інформаційної безпеки. Концепція прийнятного та залишкового ризику. Ризик-апетит організації та толерантність до ризиків.

Тема 1.4

Процес управління ризиками: загальна структура. Контекст управління ризиками. Ідентифікація, аналіз, оцінювання, обробка, моніторинг і перегляд ризиків. Організаційна структура управління ризиками в ІКС. Документування та звітність у процесі управління ризиками.

Модуль 2. Ідентифікація та аналіз ризиків

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Ідентифікація активів та загроз в ІКС. Класифікація інформаційних активів та їх цінність для організації. Методи інвентаризації та оцінювання активів. Каталоги загроз та вразливостей. Джерела загроз: антропогенні, техногенні, природні. Методи ідентифікації загроз у комп'ютерних мережах.

Тема 2.2

Аналіз вразливостей інформаційних систем. Поняття вразливості та методи її оцінювання. Системи оцінювання вразливостей: CVSS, CVE. Методи виявлення вразливостей у програмному забезпеченні та мережевій інфраструктурі. Зв'язок між вразливостями, загрозами та ризиками. Аналіз сценаріїв реалізації загроз.

Тема 2.3

Якісні методи аналізу ризиків. Матричний метод оцінювання ризиків. Метод FRAP (Facilitated Risk Analysis Process). Методологія OCTAVE. Метод дерева відмов та дерева атак. Метод HAZOP для аналізу небезпек. Переваги та обмеження якісних методів для задач захисту інформації в ІКС.

Тема 2.4

Кількісні методи оцінювання ризиків. Кількісне оцінювання: ймовірність реалізації загрози, очікувані втрати (SLE, ALE, ARO). Статистичні методи та моделі. Баєсівський метод оцінювання ризиків кібербезпеки. Метод CRAMM. Застосування нейронних мереж та машинного навчання для оцінювання ризиків у розподілених ІС.

Модуль 3. Управління ризиками та стратегії їх обробки

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Стратегії обробки ризиків. Варіанти реагування на ризики: прийняття, уникнення, передача (страхування), зниження. Вибір стратегії обробки ризику з урахуванням вартості заходів та величини можливого збитку. Розробка плану обробки ризиків. Залишковий ризик та критерії його прийнятності.

Тема 3.2

Технічні та організаційні заходи зниження ризиків. Класифікація захисних заходів (контролів): превентивні, детектуючі, коригувальні. Контроль доступу, криптографічний захист, резервування. Організаційні заходи: політики безпеки, навчання персоналу, розподіл обов'язків. Ефективність заходів та оцінювання їх впливу на рівень ризику.

Тема 3.3

Управління ризиками в умовах кіберзагроз. Специфіка кіберризиків для об'єктів критичної інфраструктури. Методологія COBIT 5 for Risk та COBIT 2019. Управління ризиками в розподілених інформаційних системах, хмарних середовищах та системах IoT. Реагування на кіберінциденти в контексті управління ризиками.

Модуль 4. Моніторинг, аудит ризиків та ризик-менеджмент в ІКС

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

Моніторинг та перегляд ризиків. Безперервний моніторинг ризиків як елемент системи управління ІБ. Показники ефективності управління ризиками (KRI). Системи SIEM та їх роль у моніторингу ризиків. Порядок перегляду та актуалізації реєстру ризиків. Звітність перед керівництвом організації.

Тема 4.2

Аудит системи управління ризиками. Поняття та цілі аудиту ризиків в ІКС. Внутрішній і зовнішній аудит системи управління інформаційною безпекою. Аудит відповідно до ISO/IEC 27001 та вимог Держспецзв'язку. Процедури аудиту, методи збирання доказів. Результати аудиту та коригувальні дії.

Тема 4.3

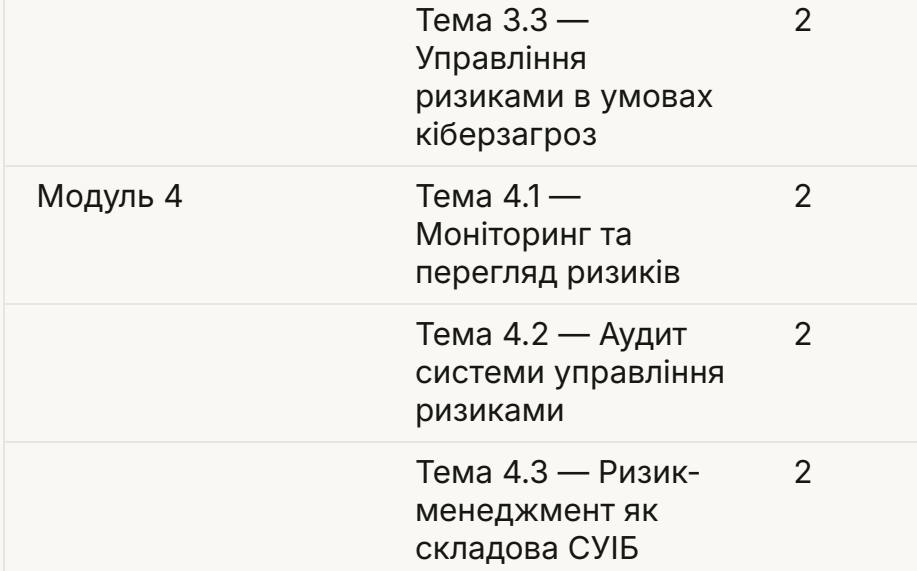
Ризик-менеджмент як складова СУІБ організації. Інтеграція управління ризиками в систему управління інформаційною безпекою (СУІБ). Цикл PDCA в управлінні ризиками. Зрілість процесів управління ризиками. Актуальні зміни нормативно-правового регулювання в умовах воєнного стану та кіберпротистояння.

Тема 4.4

Практика ризик-менеджменту в українських ІКС. Особливості застосування методів оцінювання ризиків у державних органах та підприємствах. Методика оцінювання ризиків кібербезпеки відповідно до Постанови КМУ № 497 від 16.05.2023. Приклади оцінювання ризиків для об'єктів критичної інфраструктури України.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Поняття та сутність ризику	2	2	4
	Тема 1.2 — Нормативно-правова база та стандарти	2	2	4
	Тема 1.3 — Моделі та концепції ризиків в ІКС	2	2	4
	Тема 1.4 — Процес управління ризиками: структура	2	2	4
Модуль 2	Тема 2.1 — Ідентифікація активів та загроз	2	2	4
	Тема 2.2 — Аналіз вразливостей інформаційних систем	2	2	4
	Тема 2.3 — Якісні методи аналізу ризиків	2	4	4
	Тема 2.4 — Кількісні методи оцінювання ризиків	2	4	6
Модуль 3	Тема 3.1 — Стратегії обробки ризиків	2	2	4
	Тема 3.2 — Технічні та організаційні заходи зниження ризиків	2	4	6
	Тема 3.3 — Управління ризиками в умовах кіберзагроз	2	2	6
Модуль 4	Тема 4.1 — Моніторинг та перегляд ризиків	2	2	4
	Тема 4.2 — Аудит системи управління ризиками	2	2	6
	Тема 4.3 — Ризик-менеджмент як складова СУІБ	2	2	6
	Тема 4.4 — Практика ризик-менеджменту в українських ІКС	2	2	4
Разом		**30**	**30**	**60**



Структура навчального часу

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

- **Лекції (30 год. — 25%):** подача ключового теоретичного матеріалу з теорії ризиків
- **Практичні (30 год. — 25%):** відпрацювання методів оцінювання ризиків, аналіз кейсів, моделювання загроз
- **Самостійна робота (60 год. — 50%):** поглиблене вивчення, підготовка завдань та реєстрів ризиків

Самостійна робота становить **50% обсягу дисципліни** — студенти навчаються самостійно застосовувати методи аналізу та оцінювання ризиків для реальних ІКС.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з теорії ризиків та захисту інформації, міжнародними стандартами ризик-менеджменту, науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння методів оцінювання ризиків різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань: побудова реєстру ризиків для модельної ІКС, розроблення матриці ризиків, порівняльний аналіз методів CRAMM, FRAP, OCTAVE, підготовка аналітичних записок з актуальних питань ризик-менеджменту в умовах кіберзагроз.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: Держспецзв'язку (**cip.gov.ua**), Верховна Рада (**zakon.rada.gov.ua**), NIST (**csrc.nist.gov**). Аналіз методики оцінювання ризиків кібербезпеки КМУ та чинних нормативних актів.

Підготовка до занять

Підготовка до практичних занять шляхом вивчення методів оцінювання ризиків, повторення теоретичного матеріалу; підготовка до тестувань через засвоєння ключових термінів і визначень; систематизація знань перед контрольними роботами та захистом практичних завдань.

Методи викладання

→ Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, таблиць і прикладів з нормативних актів та стандартів; студенти ведуть конспекти та задають уточнювальні запитання.

→ Кейс-стаді

Аналіз реальних ситуацій кіберінцидентів та витоків інформації в ІКС; студенти ідентифікують ризики, оцінюють їх величину, пропонують заходи зниження та обґрунтовують висновки.

→ Практичні вправи

Побудова моделей загроз та вразливостей, складання реєстрів ризиків, розроблення матриць ризиків та планів їх обробки для модельних інформаційно-комунікаційних систем.

→ Робота зі стандартами

Опрацювання міжнародних і національних стандартів ризик-менеджменту (ISO/IEC 27005, NIST SP 800-30, DSTU ISO 31000); формування навичок їх застосування до реальних задач захисту інформації.

→ Самостійне дослідження

Підготовка аналітичних записок, рефератів і презентацій за обраною темою; розвиток навичок самостійного пошуку та систематизації наукової та нормативної інформації у сфері теорії ризиків.

Форми контролю знань

1

Поточний контроль

Завдання: аналітичні та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання завдань, якість відповідей і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, письмові відповіді, розбір стандартів та участь у вирішенні кейсів з оцінювання ризиків ІКС.

2

Проміжний контроль

Самостійна робота — комплексне практичне завдання, яке охоплює теми змістовного модуля (побудова реєстру ризиків, застосування обраного методу оцінювання, розроблення плану обробки ризиків для модельної ІКС). Оцінюються повнота відповіді, правильність розрахунків та обґрунтованість висновків. Проводиться після кожного змістовного модуля.

3

Підсумковий контроль

Іспит відповідно до навчального плану. Форма проведення — тестування та письмові відповіді на питання з усіх чотирьох модулів курсу. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали оцінювання: 100-бальна система з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

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

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Коломійцев О. В., Панченко В. І., Лисиця Д. О. Теорія ризиків: навч. посіб. для студентів спеціальності 123 «Комп'ютерна інженерія». — Харків : НТУ «ХПІ», 2023.
2. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: підручник. — Житомир : ЖНАЕУ, 2023. — 636 с.
3. Дудикевич В. Б., Хорошко В. О. Захист інформації в інформаційно-комунікаційних системах: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 312 с.
4. Корченко О. Г., Архипов О. Є. Системи захисту інформації: стандарти та нормативна база: підручник. — Київ : НАУ, 2022. — 398 с.
5. Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки: підручник. — Київ : ДУІКТ, 2022. — 476 с.
6. Петров В. В., Смерницький Д. В. Правові основи захисту інформації з обмеженим доступом: навч. посіб. — Харків : ХНУРЕ, 2023. — 224 с.
7. Палко Д., Мирутенко Л. Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах // Кібербезпека: освіта, наука, техніка. — 2024. — Вип. 2(26). — С. 487–502.
8. Леськів А. В., Паращук С. Д. Електронний документообіг та захист інформації в органах державної влади: навч. посіб. — Київ : Академперіодика, 2024. — 268 с.
9. Методика оцінювання ризиків кібербезпеки: затв. наказом Держспецзв'язку відповідно до постанови КМУ від 16.05.2023 № 497. — Київ, 2023.
10. Рудик О. М., Сергієнко І. В. Організація архівної справи та захист документаційного фонду: навч. посіб. — Київ : Алерта, 2024. — 256 с.

Офіційні інтернет-ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. — URL: **https://cip.gov.ua/**
2. Офіційний сайт Верховної Ради України. — URL: **https://zakon.rada.gov.ua/**
3. Офіційний сайт Кабінету Міністрів України. — URL: **https://www.kmu.gov.ua/**
4. Національний інститут стандартів і технологій США (NIST). — URL: **https://csrc.nist.gov/**
5. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
6. Міністерство цифрової трансформації України. — URL: **https://thedigital.gov.ua/**
7. Науково-технічний журнал «Кібербезпека: освіта, наука, техніка». — URL: **https://csecurity.kubg.edu.ua/**
8. Репозиторій НТУ «ХПІ» (навч. посіб. з теорії ризиків). — URL: **https://repository.kpi.kharkov.ua/**

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