Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 5

ТЕОРІЯ ПРИЙНЯТТЯ РІШЕНЬ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Перший (бакалаврський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітньо-професійна програма	*Комп'ютерні системи і технології спеціального зв'язку*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (Денна)*
Рік підготовки, семестр	*III рік підготовки, осінній семестр*
Обсяг дисципліни	*3,5 кредити ECTS*
Семестровий контроль / контрольні заходи	*Екзамен*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лекції: Василь ЦУРКАН* *Практичні: Василь ЦУРКАН*
Розміщення курсу	*Google Classroom*

Київ – 2022

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Силабус освітнього компонента "Теорія прийняття рішень" складено відповідно до освітньої програми підготовки бакалаврів "Комп'ютерні системи і технології спеціального зв'язку" спеціальності 122 – Комп'ютерні науки.

Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: (ЗК1) Здатність до абстрактного мислення, аналізу та синтезу; (ЗК2) Здатність застосовувати знання у практичних ситуаціях; (ЗК3) Знання та розуміння предметної області та розуміння професійної діяльності; (ЗК6) Здатність вчитися й оволодівати сучасними знаннями; (ЗК7) Здатність до пошуку, оброблення та аналізу інформації з різних джерел; (ЗК11) Здатність приймати обґрунтовані рішення; (СК1) Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач у галузі комп'ютерних наук, аналізу та інтерпретування; (СК14) Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури; (СК15) Здатність до аналізу та функціонального моделювання бізнес-процесів, побудови та практичного застосування функціональних моделей організаційно-економічних і виробничо-технічних систем, методів оцінювання ризиків їх проектування.

Предмет навчальної дисципліни – моделі та методи моделювання загроз і оцінювання ризику безпеці програмного забезпечення.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (ПР1) Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук; (ПР2) Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об'єктів інформатизації; (ПР3) Використовувати знання закономірностей випадкових явищ, їх властивостей та операцій над ними, моделей випадкових процесів та сучасних програмних середовищ для розв'язування задач статистичної обробки даних і побудови прогнозних моделей; (ПР4) Використовувати методи обчислювального інтелекту, машинного навчання, нейромережевої та нечіткої обробки даних, генетичного та еволюційного програмування для розв'язання задач розпізнавання, прогнозування, класифікації, ідентифікації об'єктів керування тощо; (ПР16) Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

2. Пререквізити та постреквізити навчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни курсант повинен володіти освітніми компонентами "Математичний аналіз", "Теорія ймовірності, ймовірнісні процеси і математична статистика", "Дискретна математика". Компетенції, знання та уміння, одержані в процесі вивчення освітнього компонента необхідні для подальшого вивчення освітніх компонентів "Моделювання систем", "Основи створення КСЗІ та аудит кібербезпеки", "Проектування інформаційних систем".

3. Зміст навчальної дисципліни

Семестр 5

Семестровий (кредитний) модуль 1. Теорія прийняття рішень.

Розділ (змістовий модуль) 1. Теоретичні основи теорії прийняття рішень.

Тема 1. Теоретичні та прикладні аспекти теорії прийняття рішень.

Формальна постановка завдання прийняття рішень. Проблемні ситуації прийняття рішень. Процес прийняття рішень. Проблемна ситуація прийняття рішення. Формулювання проблемних ситуацій. Обирання варіантів прийняття рішень. Різновиди проблемних ситуацій. Представлення проблемних ситуацій. Правила обирання альтернатив прийняття рішень.

Тема 2. Теоретичні та прикладні аспекти ризик-орієнтованого прийняття рішень.

Узагальнена ризик-орієнтована модель. Ризик-орієнтована модель в аспекті вразливостей. Ризик-орієнтована модель в аспекті наслідків. Представлення ризик-орієнтованих моделей прийняття рішень. Моделювання загроз безпеці програмного забезпечення. Представлення програмного забезпечення у аспекті загроз.

Розділ (змістовий модуль) 2. Прикладні основи теорії прийняття рішень.

Тема 3. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення STRIDE.

Моделювання загроз безпеці програмного забезпечення методом STRIDE. Характеристика методу STRIDE. Атрибути мнемоніки STRIDE. Етапи використання методу STRIDE. Різновиди загроз безпеці програмного забезпечення методом STRIDE. Структурування інформації про загрози. Структурування інформації про властивості. Визначення різновидів загроз безпеці. Побудова моделі загроз безпеці програмного забезпечення методом STRIDE.

Тема 4. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення DREAD.

Моделювання загроз безпеці програмного забезпечення методом DREAD. Характеристика методу DREAD. Шкали оцінювання загроз методом DREAD. Етапи використання методу DREAD. Визначення шкали оцінювання загроз безпеці програмного забезпечення. Визначення критеріїв оцінювання загроз безпеці програмного забезпечення. Обирання шкали оцінювання загроз безпеці програмного забезпечення. Приклади шкал оцінювання загроз безпеці програмного забезпечення. Побудова моделі загроз безпеці програмного забезпечення за методом DREAD

Тема 5. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення діаграмою потоку даних.

Моделювання загроз безпеці програмного забезпечення діаграмою потоку даних. Характеристика діаграми потоку даних. Елементи діаграми потоку даних. Етапи побудови діаграми потоку даних. Способи представлення діаграми потоку даних. Типовий спосіб представлення діаграми потоку даних. Удосконалений спосіб представлення діаграми потоку даних. Автоматизований спосіб представлення діаграм потоку даних. Побудова моделі загроз безпеці програмного забезпечення на основі діаграми потоку даних.

Тема 6. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення методом LINDDU.

Моделювання загроз безпеці програмного забезпечення методом LINDDUN. Характеристика методу LINDDUN. Категорії загроз за методом LINDDUN. Етапи використання методу LINDDUN. Підтримання знань про загрози безпеці програмного забезпечення методом LINDDUN. Таблиця зіставлення елементів діаграми потоку даних стосовно загроз. Таксономія стратегій пом’якшення загроз за категоріями LINDDUN. Класифікація рішень забезпечення приватності програмного забезпечення. Побудова моделі загроз безпеці програмного забезпечення методом LINDDUN.

Тема 7. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення методом створення дерева атак.

Моделювання загроз безпеці програмного забезпечення методом створення дерева атак. Характеристика методу створення дерева атак. Способи використання дерева атак. Етапи використання методу створення дерева атак. Способи представлення дерева атак програмного забезпечення. Обрання способу представлення дерева атак. Спосіб представлення дерева атак “І”. Спосіб представлення дерева атак “АБО”. Побудова моделі загроз безпеці програмного забезпечення методом створення дерева атак.

Тема 8. Теоретичні та прикладні аспекти оцінювання ризиків інформаційної безпеки методом "Матриця "Наслідки – Вірогідність".

Оцінювання ризиків інформаційної безпеки методом "Матриця "Наслідки – Вірогідність". Характеристика методу оцінювання ризиків. Шкали оцінювання ризиків. Етапи використання методу оцінювання ризиків. Ідентифікування ризиків безпеки програмного забезпечення. Аналізування ризиків безпеки програмного забезпечення. Зіставлення ризиків безпеки програмного забезпечення. Візуалізування ризиків безпеки програмного забезпечення. Ранжування ризиків безпеки програмного забезпечення.

Тема 9. Теоретичні та прикладні аспекти оцінювання серйозності вразливостей програмного забезпечення.

Оцінювання серйозності вразливостей програмного забезпечення. Характеристика методу оцінювання уразливостей програмного забезпечення. Метрики серйозності уразливостей програмного забезпечення. Етапи використання методу оцінювання уразливостей програмного забезпечення. Формалізування метрик оцінювання серйозності вразливостей програмного забезпечення. Рівняння базових метрик оцінювання серйозності вразливостей. Рівняння часових метрик оцінювання серйозності вразливостей. Рівняння метрик середовища користувача при оцінюванні серйозності вразливостей. Побудова моделі оцінювання уразливостей програмного забезпечення.

4. Навчальні матеріали та ресурси

Основна література

1. Катренко А. В., Пасічник В. В., Пасько В. П. Теорія прийняття рішень. Київ : Видавнича група BHV, 2009. 448 с.

2. Волошин О. Ф., Мащенко С. О. Моделі та методи прийняття рішень : навч. посіб. для студ. вищ. навч. закл. Київ : Видавничо-поліграфічний центр «Київський університет», 2010. 336 с.

3. ISO/IEC 13335-1:2004. Information technology. Security techniques. Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management. [Valid from 2004-11-19]. URL: https://www.iso.org/standard/39066.html (accessed on: 29.04.2022).

4. ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management. [Valid from 2018-06-10]. URL: https://www.iso.org/standard/ 75281.html (accessed on: 29.04.2022).

5. Threat Modeling. Process. URL: https://owasp.org/www-community/Threat_Modeling_ Process (accessed on: 29.04.2022)

6. Shostack A. Threat Modeling. Designing for Security. Indianapolis : John Wiley & Sons, 2014. 590 p.

7. Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., Murukan, A. Improving web application security: Threats and countermeasures. Microsoft Corporation. URL: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10) (accessed on: 29.04.2022).

8. Tarandach I., Coles M. J. Threat Modeling. A Practical Guide for Development Teams. Sebastopol: O'Reilly Media, 2020, 201 p.

9. LINDDUN framework. URL: https://www.linddun.org/linddun (accessed on: 29.04.2022).

10. An Alternative: Attack Trees. URL: https://www.oreilly.com/library/view/ building-secure-servers/0596002173/ch01s03.html (accessed on: 29.04.2022).

11. Common Vulnerability Scoring System v3.1: Specification Document. . URL: https://www.first.org/cvss/v3.1/specification-document (accessed on: 29.04.2022).

12. Common Vulnerability Scoring System Version 3.1 Calculator. URL: https://www.first.org/cvss/calculator/3.1 (accessed on: 29.04.2022).

Додаткова література

1. Бутко М. П., Бутко І. М., Мащенко В. П. та ін. Теорія прийняття рішень : підручник. Київ : “Центр учбової літератури”, 2015. 360 с.
2. Бурячок В. Л., Толюпа С. В., Аносов А. О., Козачок В. А., Лукова-Чуйко Н. В. Системний аналіз та прийняття рішень в інформаційній безпеці : підручник. Київ : ДУТ, 2015. 345 с.
3. IEC 31010:2019. Risk management. Risk assessment techniques. [Valid from 2019-06-17]. URL: https://www.iso.org/standard/72140.html (accessed on: 29.04.2022).
4. Threat Modeling Manifesto. URL: https://www.threatmodelingmanifesto.org/ (accessed on: 29.04.2022).
5. Threat Modeling. URL: https://owasp.org/www-community/Threat_Modeling (accessed on: 29.04.2022).
6. Threat Modeling. URL: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling (accessed on: 29.04.2022).
7. DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis. URL: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/ (accessed on: 29.04.2022).
8. Create a threat model using data-flow diagram elements. URL: https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram-elements/ (accessed on: 29.04.2022).
9. Common Vulnerability Scoring System v3.1: Examples. URL: https://www.first.org/cvss/v3.1/examples (accessed on: 29.04.2022).

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні (семінарські) заняття	Лабораторні заняття (комп`ютерний практикум)	СР
Розділ (змістовий модуль) 1. *Теоретичні основи теорії прийняття рішень*						
Тема 1	**Теоретичні та прикладні аспекти теорії прийняття рішень.**	**8**	**2**	**4**	**0**	**2**
Заняття 1/1	Формальна постановка завдання прийняття рішень. 1. Поняття і різновиди рішень. 2. Формалізація прийняття рішень. 3. Завдання прийняття рішень. Основна література: [1–4] Додаткова література: [1–3]	**2,5**	2			0,5
Заняття 1/2	Обирання ситуації прийняття рішень. 1. Обирання об’єкту прийняття рішень. 2. Обирання проблемної ситуації прийняття рішень. 3. Обирання елементів ситуації прийняття рішень. Основна література: [1–4] Додаткова література: [1–3]	**2,5**		2		0,5

Заняття 1/3	Описання ситуації прийняття рішень. 1. Описання об’єкту прийняття рішень. 2. Описання проблемної ситуації прийняття рішень. 3. Описання елементів ситуації прийняття рішень. Основна література: [1–4] Додаткова література: [1–3]	**3**		2		1
Тема 2	**Теоретичні та прикладні аспекти ризик-орієнтованого прийняття рішень.**	**8**	**2**	**4**	**0**	**2**
Заняття 2/1	Метод моделювання загроз безпеці програмного забезпечення. 1. Поняття моделювання загроз безпеці програмного забезпечення. 2. Процес моделювання загроз безпеці програмного забезпечення. 3. Представлення програмного забезпечення у аспекті загроз. Основна література: [5, 6, 8] Додаткова література: [4–6]	**2,5**	2			0,5
Заняття 2/2	Етапи моделювання загроз безпеці програмного забезпечення. 1. Розкладання (декомпозиціювання) програмного забезпечення. 2. Визначення і ранжування загроз. 3. Визначення вимог безпеки програмного забезпечення. Основна література: [5, 6, 8] Додаткова література: [4–6]	**2,5**		2		0,5
Заняття 2/3	Декомпозиціювання програмного забезпечення у аспекті загроз. 1. Визначення інформації про модель загроз безпеці програмного забезпечення. 2. Визначення зовнішніх залежностей програмного забезпечення. 3. Визначення точок входу програмного забезпечення. 4. Визначення активів програмного забезпечення. 5. Визначення рівнів довіри програмного забезпечення. Основна література: [5, 6, 8] Додаткова література: [4–6]	**3**		2		1
Разом за розділом 1		**16**	**4**	**8**	**0**	**4**
Розділ (змістовий модуль) 2. *Прикладні основи теорії прийняття рішень*						
Тема 3	**Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення STRIDE.**	**8**	**2**	**4**	**0**	**2**

Заняття 3/1	Метод моделювання загроз безпеці програмного забезпечення STRIDE. 1. Характеристика методу STRIDE. 2. Атрибути мнемоніки STRIDE. 3. Етапи використання методу STRIDE. Основна література: [5, 6] Додаткова література: [5, 6]	**2,5**	2			0,5
Заняття 3/2	Різновиди загроз безпеці програмного забезпечення методом STRIDE. 1. Структурування інформації про загрози. 2. Структурування інформації про властивості. 3. Визначення різновидів загроз безпеці. Основна література: [5, 6] Додаткова література: [5, 6]	**2,5**		2		0,5
Заняття 3/3	Побудова моделі загроз безпеці програмного забезпечення методом STRIDE. 1. Визначення загроз безпеці програмного забезпечення. 2. Визначення вимог до безпеки програмного забезпечення. 3. Узагальнення результатів визначення загроз безпеці програмного забезпечення. Основна література: [5, 6] Додаткова література: [5, 6]	**3**		2		1
Тема 4	**Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення DREAD.**	**8,5**	**2**	**4**	**0**	**2,5**
Заняття 4/1	Метод моделювання загроз безпеці програмного забезпечення DREAD. 1. Характеристика методу DREAD. 2. Шкали оцінювання загроз методом DREAD. 3. Етапи використання методу DREAD. Основна література: [6–8] Додаткова література: [7]	**2,5**	2			0,5
Заняття 4/2	Визначення шкали оцінювання загроз безпеці програмного забезпечення. 1. Визначення критеріїв оцінювання загроз безпеці програмного забезпечення. 2. Обирання шкали оцінювання загроз безпеці програмного забезпечення. 3. Приклади шкал оцінювання загроз безпеці програмного забезпечення. Основна література: [6–8] Додаткова література: [7]	**3**		2		1

Заняття 4/3	Побудова моделі загроз безпеці програмного забезпечення за методом DREAD. 1. Визначення загроз безпеці програмного забезпечення. 2. Визначення шкали оцінювання загроз безпеці програмного забезпечення. 3. Оцінювання загроз безпеці програмного забезпечення. 4. Ранжування загроз безпеці програмного забезпечення. 5. Визначення вимог до безпеки програмного забезпечення. Основна література: [6–8] Додаткова література: [7]	**3**		2		1
Тема 5	**Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення діаграмою потоку даних.**	**8,5**	**2**	**4**	**0**	**2,5**
Заняття 5/1	Моделювання загроз безпеці програмного забезпечення діаграмою потоку даних. 1. Характеристика діаграми потоку даних. 2. Елементи діаграми потоку даних. 3. Етапи побудови діаграми потоку даних. Основна література: [6, 8] Додаткова література: [8]	**2,5**	2			0,5
Заняття 5/2	Способи представлення діаграми потоку даних. 1. Типовий спосіб представлення діаграми потоку даних. 2. Удосконалений спосіб представлення діаграми потоку даних. 3. Автоматизований спосіб представлення діаграм потоку даних. Основна література: [6, 8] Додаткова література: [8]	**3**		2		1
Заняття 5/3	Побудова моделі загроз безпеці програмного забезпечення на основі діаграми потоку даних. 1. Визначення процесів програмного забезпечення. 2. Визначення сховищ даних програмного забезпечення. 3. Визначення зовнішніх сутностей програмного забезпечення. 4. Визначення потоків даних програмного забезпечення. 5. Визначення меж довіри програмного забезпечення. Основна література: [6, 8] Додаткова література: [8]	**3**		2		1

Тема 6	**Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення методом LINDDUN.**	**8,5**	**2**	**4**	**0**	**2,5**
Заняття 6/1	Моделювання загроз безпеці програмного забезпечення методом LINDDUN. 1. Характеристика методу LINDDUN. 2. Категорії загроз за методом LINDDUN. 3. Етапи використання методу LINDDUN. Основна література: [9] Додаткова література: [5, 6]	**2,5**		2		0,5
Заняття 6/2	Підтримання знань про загрози безпеці програмного забезпечення методом LINDDUN. 1. Таблиця зіставлення елементів діаграми потоку даних стосовно загроз. 2. Таксономія стратегій пом'якшення загроз за категоріями LINDDUN. 3. Класифікація рішень забезпечення приватності програмного забезпечення. Основна література: [9] Додаткова література: [5, 6]	**3**		2		1
Заняття 6/3	Побудова моделі загроз безпеці програмного забезпечення методом LINDDUN. 1. Побудування діаграми потоку даних програмного забезпечення. 2. Виокремлення елементів діаграми потоку даних програмного забезпечення. 3. Зіставлення елементів діаграми потоку даних стосовно категорій загроз LINDDUN. Основна література: [9] Додаткова література: [5, 6]	**3**		2		1
Тема 7	**Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення методом створення дерева атак.**	**8,5**	**2**	**4**	**0**	**2,5**
Заняття 7/1	Моделювання загроз безпеці програмного забезпечення методом створення дерева атак. 1. Характеристика методу створення дерева атак. 2. Способи використання дерева атак. 3. Етапи використання методу створення дерева атак. Основна література: [6, 10] Додаткова література: [5, 6]	**2,5**	2			0,5

Заняття 7/2	Способи представлення дерева атак програмного забезпечення. 1. Обрання способу представлення дерева атак. 2. Спосіб представлення дерева атак “І”. 3. Спосіб представлення дерева атак “АБО”. Основна література: [6, 10] Додаткова література: [5, 6]	**3**	2			1
Заняття 7/3	Побудова моделі загроз безпеці програмного забезпечення методом створення дерева атак. 1. Створення кореневого вузла дерева атак. 2. Створення підвузлів кореневого вузла дерева атак. 3. Перевіряння повноти створеного дерева атак. 4. Обрізання створеного дерева атак. 5. Перевіряння створеного дерева атак. Основна література: [6, 10] Додаткова література: [5, 6]	**3**		2		1
Тема 8	**Теоретичні та прикладні аспекти оцінювання ризиків інформаційної безпеки методом “Матриця “Наслідки – Вірогідність”.**	**8,5**	**2**	**4**	**0**	**2,5**
Заняття 8/1	Оцінювання ризиків інформаційної безпеки методом “Матриця “Наслідки – Вірогідність”. 1. Характеристика методу оцінювання ризиків. 2. Шкали оцінювання ризиків. 3. Етапи використання методу оцінювання ризиків. Основна література: [3, 4] Додаткова література: [3]	**2,5**	2			0,5
Заняття 8/2	Різновиди шкал оцінювання ризиків інформаційної безпеки. 1. Якісна шкала оцінювання ризиків. 2. Напівкількісна шкала оцінювання ризиків. 3. Комбінована шкала оцінювання ризиків. Основна література: [3, 4] Додаткова література: [3]	**3**		2		1
Заняття 8/3	Оцінювання ризиків безпеки програмного забезпечення методом “Матриця “Наслідки – Вірогідність”. 1. Ідентифікування ризиків безпеки програмного забезпечення. 2. Аналізування ризиків безпеки програмного забезпечення. 3. Зіставлення ризиків безпеки програмного забезпечення.	**3**		2		1

	4. Візуалізування ризиків безпеки програмного забезпечення. 5. Ранжування ризиків безпеки програмного забезпечення. Основна література: [3, 4] Додаткова література: [3]					
Тема 9	**Теоретичні та прикладні аспекти оцінювання серйозності вразливостей програмного забезпечення.**	**8,5**	**2**	**4**	**0**	**2,5**
Заняття 9/1	Метод оцінювання серйозності вразливостей програмного забезпечення. 1. Характеристика методу оцінювання уразливостей програмного забезпечення. 2. Метрики серйозності уразливостей програмного забезпечення. 3. Етапи використання методу оцінювання уразливостей програмного забезпечення. Основна література: [11, 12] Додаткова література: [9]	**2,5**	2			0,5
Заняття 9/2	Формалізування метрик оцінювання серйозності вразливостей програмного забезпечення. 1. Рівняння базових метрик оцінювання серйозності вразливостей. 2. Рівняння часових метрик оцінювання серйозності вразливостей. 3. Рівняння метрик середовища користувача при оцінюванні серйозності вразливостей. Основна література: [11, 12] Додаткова література: [9]	**3**		2		1
Заняття 9/3	Побудова моделі оцінювання уразливостей програмного забезпечення. 1. Визначення базових метрик оцінювання уразливостей. 2. Визначення часових метрик оцінювання уразливостей. 3. Визначення метрик середовища користувача. 4. Визначення метрик оцінювання уразливостей калькулятором. 5. Зіставлення результатів оцінювання уразливостей. Основна література: [11, 12] Додаткова література: [9]	**3**		2		1
Разом за розділом 2		**59**	**14**	**28**	**0**	**17**
Разом за розділами		**75**	**18**	**36**	**0**	**21**
Екзамен		**30**	**0**	**0**	**0**	**30**
Всього годин		**105**	**18**	**36**	**0**	**51**

5. Самостійна робота курсанта

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
1	Тема 1. Теоретичні та прикладні аспекти теорії прийняття рішень. 1. Історія розвитку концепції прийняття рішень. 2. Проблеми структуризації прийняття рішень. 3. Етапи системного розв'язання проблем. 4. Розвиток теорії прийняття рішень у працях українських вчених.	2
2	Тема 2. Теоретичні та прикладні аспекти ризик-орієнтованого прийняття рішень. 1. Різновиди ризик-орієнтованих моделей. 2. Міри загроз інформаційній безпеці. 3. Вірогідність реалізації загрози інформаційні безпеці. 4. Імовірність реалізації загрози інформаційні безпеці.	2
3	Тема 3. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення STRIDE. 1. Особливості використання методу моделювання загроз інформаційній безпеці STRIDE. 2. Різновиди методу моделювання загроз інформаційній безпеці STRIDE. 3. Використання методу моделювання загроз інформаційній безпеці STRIDE з огляду на елемент. 4. Використання методу моделювання загроз інформаційній безпеці STRIDE з огляду на взаємодію.	2
4	Тема 4. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення DREAD. 1. Особливості використання методу моделювання загроз інформаційній безпеці DREAD. 2. Різновиди методу моделювання загроз інформаційній безпеці DREAD. 3. Атрибути оцінювання загроз на основі моделі STRIDE/DREAD від Microsoft. 4. Різновиди атрибутів загроз при моделюванні методом DREAD.	2,5
5	Тема 5. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення діаграмою потоку даних. 1. Інструментальні засоби представлення діаграм потоку даних. 2. Логічні та фізичні межі програмного забезпечення. 3. Рівні представлення діаграми потоку даних. 4. Контекст представлення потоку даних.	2,5
6	Тема 6. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення методом LINDDUN. 1. Різновиди категорій загроз приватності. 2. Каталог дерев загроз приватності. 3. Таксономія стратегій пом'якшення загроз приватності. 4. Класифікація технологій підвищення приватності.	2,5
7	Тема 7. Теоретичні та прикладні аспекти моделювання загроз безпеці програмного забезпечення методом створення дерева атак. 1. Дерево шахрайських атак. 2. Перспективи використання дерева атак. 3. Різновиди бібліотек атак. 4. Властивості бібліотек атак.	2,5
8	Тема 8. Теоретичні та прикладні аспекти оцінювання ризиків інформаційної безпеки методом "Матриця "Наслідки – Вірогідність".	2,5

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
	1. Класифікація методів оцінювання ризиків інформаційної безпеки. 2. Критерії обирання методу оцінювання ризиків інформаційної безпеки. 3. Обирання методу оцінювання ризиків інформаційної безпеки. 4. Характеристика методів оцінювання ризиків інформаційної безпеки.	
9	Тема 9. Теоретичні та прикладні аспекти оцінювання серйозності вразливостей програмного забезпечення. 1. Текстове представлення набору метрик CVSS. 2. Текстове представлення набору метрик атаки. 3. Шкали оцінювання серйозності вразливостей програмного забезпечення. 4. Визначення рівнянь базових, часових метрик і середовища користувача.	2,5
10	Підготовка до екзамену	30

Політика та контроль

6. Політика навчальної дисципліни (освітнього компонента)

При проведенні навчальних занять використовуються такі методи навчання:

- усне викладання матеріалу;
- обговорення навчального матеріалу;
- практична та самостійна робота зі застосуванням комп'ютерної техніки.

Відвідування занять є обов'язковим. Відсутність на заняттях з будь яких причин не вважається поважною причиною невиконання поставлених завдань.

Протягом навчальних занять усі мобільні телефони переводяться у беззвучний режим роботи. При цьому заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Електронні пристрої, включаючи мобільні телефони та ноутбуки можна використовувати лише за умови виробничої необхідності в них (за погодженням з викладачем).

Матеріали навчальної дисципліни розміщуються на вказаній сторінці Google Classroom. Очікується, що курсанти перевірятимуть свою електронну пошту і сторінку навчальної дисципліни в Google Classroom та своєчасно виконуватимуть поставлені завдання. Результати виконання завдань мають завантажуватися на персональних сторінках курсантів у Google Classroom. Крім того через сторінку Google Classroom курсанти можуть надсилати у вигляді відкритого чи приватного листа викладачу питання, що виникли під час виконання поставлених завдань.

Кожний курсант зобов'язаний дотримуватися принципів академічної доброчесності. Письмові завдання з використанням часткових або повнотекстових запозичень з інших робіт без зазначення авторства вважатимуться плагіатом. Використання будь-якої інформації (текст, фото, ілюстрації тощо) мають бути правильно процитовані з посиланням на автора. До курсантів, у роботах яких буде виявлено списування, плагіат чи інші прояви недоброчесної поведінки можуть бути застосовані штрафні бали.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даного кредитного модуля можна здійснювати віддалено з використанням технологій дистанційного навчання, зокрема, Google Classroom.

Навчальні матеріали та ресурси, зазначена у розділі 4 цієї робочої програми навчальної дисципліни (силабус) є відкритою інформацією, не містять відомостей з обмеженим доступом і можуть оприлюднюватися з використанням технологій дистанційного навчання. Тоді як робоча програма навчальної дисципліни (силабус) не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

7. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Рейтинг курсанта з навчальної дисципліни складається з балів за:

– виконання завдань на практичних заняттях;

– екзамен.

Практичне заняття оцінюється 6 балами, r_k :

– "відмінно" – повна відповідь (не менше 90% потрібної інформації) – 6 балів;

– "добре" – достатньо повна відповідь (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями – 5 балів;

– "задовільно" – неповна відповідь (не менше 60% потрібної інформації) та незначні помилки – 4 бали;

– "незадовільно" – відповідь не відповідає вимогам до "задовільно" – 0 балів.

Тобто максимум 6 · 10 = 60 балів.

Штрафні та заохочувальні бали нараховуються по 1 балу:

– заохочувальні бали нараховуються за своєчасне, оригінальне виконання завдань у межах навчальної дисципліни, $r_з$.

Тобто максимум +1 · 6 = + 6 балів.

– штрафні бали нараховуються за несвоєчасне виконання завдань, що виносяться на практичні заняття, або порушення принципів академічної доброчесності, $r_ш$.

Тобто максимум (–1) · 6 = – 6 балів.

Екзаменаційна контрольна робота оцінюється 4**0** балами. Проводиться в формі письмової відповіді за білетами. Екзаменаційний білет містить три питання (два – теоретичних, одне – практичне) з переліку, що наданий до робочої програми навчальної дисципліни (силабусу).

Кожне теоретичне питання оцінюється 10 балами за такими критеріями:

– "відмінно" – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд – 10 … 9 балів;

– "добре" – достатньо повна відповідь (не менше 75% потрібної інформації) з незначними неточностями – 8,5 … 7,5 балів;

– "задовільно" – неповна відповідь (не менше 60% потрібної інформації) з деякими помилками – 7 … 6 балів;

– "незадовільно" – незадовільна відповідь – 0 балів.

Практичне питання оцінюється 20 балами за такими критеріями:

– "відмінно" – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд – 20 … 18 балів;

– "добре" – достатньо повна відповідь (не менше 75% потрібної інформації) з незначними неточностями – 17 … 15 балів;

– "задовільно" – неповна відповідь (не менше 60% потрібної інформації) з деякими помилками – 14 … 12 балів;

– "незадовільно" – незадовільна відповідь – 0 балів.

Узагальнені результати оцінювання письмових відповідей екзаменаційної контрольної роботи оцінюються відповідно до таблиці.

Бали r_E	Оцінка
38…40	Відмінно
34…37	Дуже добре
30…33	Добре
26…29	Задовільно
24… 25	Достатньо
< 24	Незадовільно

Тож отримаємо

$$r_C = \sum_{k=1}^{10} r_k + \sum_{з=1}^{6} r_з + \sum_{ш=1}^{6} r_ш = 60 + 6 - 6 = 60,$$

$$RD = r_C + r_E = 60 + 40 = 100.$$

Умовою атестації курсанта є отримання не менше 50% від кількості балів на час її проведення.

Умовою допуску до екзамену є:

– не менш, ніж одна позитивна атестація з даної навчальної дисципліни;

– отримання стартового рейтингу не менше 60 % від r_C, тобто 36 балів.

Сума рейтингових балів переводиться до підсумкової оцінки згідно з таблицею.

Бали *RD*	Оцінка
100…95	Відмінно
94…85	Дуже добре
84…75	Добре
74…65	Задовільно
64…60	Достатньо
Менше 60	Незадовільно
Невиконання умов допуску до семестрового контролю та стартовий рейтинг менше 36 балів	Не допущено

9. Додаткова інформація з навчальної дисципліни

Орієнтовний перелік питань до екзаменаційних білетів:

1. Охарактеризувати формальну постановку завдання прийняття рішень.
2. Охарактеризувати класифікацію моделей і завдань прийняття рішень.
3. Охарактеризувати етапи прийняття рішень.
4. Охарактеризувати визначання варіантів рішень.
5. Охарактеризувати оцінювання якості варіантів рішень.
6. Охарактеризувати обирання варіанту рішень.
7. Охарактеризувати ризик-орієнтоване прийняття рішень.
8. Охарактеризувати узагальнену ризик-орієнтовану модель програмного забезпечення.
9. Охарактеризувати ризик-орієнтовану модель в аспекті вразливостей програмного забезпечення.
10. Охарактеризувати ризик-орієнтовану модель в аспекті наслідків реалізування загроз безпеці програмного забезпечення.
11. Охарактеризувати поняття моделювання загроз безпеці програмного забезпечення
12. Охарактеризувати процес моделювання загроз безпеці програмного забезпечення.
13. Охарактеризувати етапи моделювання загроз безпеці програмного забезпечення.
14. Охарактеризувати представлення програмного забезпечення у аспекті загроз.
15. Охарактеризувати метод моделювання загроз безпеці програмного забезпечення STRIDE.
16. Охарактеризувати атрибути мнемоніки STRIDE.
17. Охарактеризувати етапи використання методу STRIDE.
18. Охарактеризувати метод моделювання загроз безпеці програмного забезпечення DREAD.

19. Охарактеризувати шкалу оцінювання загроз методом DREAD.
20. Охарактеризувати етапи використання методу DREAD.
21. Охарактеризувати моделювання загроз безпеці програмного забезпечення діаграмою потоку даних.
22. Охарактеризувати елементи діаграми потоку даних.
23. Охарактеризувати етапи побудови діаграми потоку даних.
24. Охарактеризувати моделювання загроз безпеці програмного забезпечення методом LINDDUN.
25. Охарактеризувати категорії загроз за методом LINDDUN.
26. Охарактеризувати етапи використання методу LINDDUN.
27. Охарактеризувати моделювання загроз безпеці програмного забезпечення методом створення дерева атак.
28. Охарактеризувати способи використання дерева атак.
29. Охарактеризувати етапи використання методу створення дерева атак.
30. Охарактеризувати способи представлення дерева атак програмного забезпечення.
31. Охарактеризувати оцінювання ризиків інформаційної безпеки методом “Матриця “Наслідки – Вірогідність”.
32. Охарактеризувати шкали оцінювання ризиків інформаційної безпеки.
33. Охарактеризувати етапи оцінювання ризиків інформаційної безпеки методом “Матриця “Наслідки – Вірогідність”.
34. Охарактеризувати ідентифікування ризиків інформаційної безпеки методом “Матриця “Наслідки – Вірогідність”.
35. Охарактеризувати аналізування ризиків інформаційної безпеки методом “Матриця “Наслідки – Вірогідність”
36. Охарактеризувати зіставлення ризиків інформаційної безпеки методом “Матриця “Наслідки – Вірогідність”.
37. Охарактеризувати візуалізування ризиків інформаційної безпеки методом “Матриця “Наслідки – Вірогідність”.
38. Охарактеризувати оцінювання серйозності вразливостей програмного забезпечення.
39. Охарактеризувати метрики серйозності уразливостей програмного забезпечення.
40. Охарактеризувати етапи використання методу оцінювання уразливостей програмного забезпечення.