МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Кафедра *Кібербезпеки*
(назва)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МОДЕЛЮВАННЯ КІБЕРФІЗИЧНИХ ДІЙ

(назва навчальної дисципліни)

рівень вищої освіти *другий (магістерський)*
перший (бакалаврський) / другий (магістерський)

галузь знань *12 Інформаційні технології*
(шифр і назва)

спеціальність *125 Кібербезпека*
(шифр і назва)

освітня програма *Кібербезпека*
(назви освітньої програми)

вид дисципліни *спеціальна (фахова) підготовка, вибіркова*
(загальна підготовка /спеціальна (фахова) підготовка; обов’язкова/вибіркова)

форма навчання *денна*
(денна / заочна/дистанційна)

Харків – 2022 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни
МОДЕЛЮВАННЯ КІБЕРФІЗИЧНИХ ДІЙ
(назва дисципліни)

Розробники:

проф, д.т.н., проф.		*Олександр МІЛОВ*
(посада, науковий ступінь та вчене звання)	(підпис)	(ініціали та прізвище)
(посада, науковий ступінь та вчене звання)	(підпис)	(ініціали та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри

кібербезпеки
(назва кафедри, яка забезпечує викладання дисципліни)

Протокол від “22” серпня 2022 року № 1

Завідувач кафедри кібербезпеки		*Сергій ЄВСЕЄВ*
(назва кафедри)	(підпис)	(ініціали та прізвище)

ЛИСТ ПОГОДЖЕННЯ

Шифр та назва освітньої програми _____125 “Кібербезпека”_____

_____

Кафедра _____кібербезпеки_____
(назва кафедри на якій викладається дисципліна)

Гарант ОП _____22.08.2022р _____*Олександр МІЛОВ*
(Підпис, дата) (ім’я та прізвище)

Завідувач кафедрою _____22.08.2022р _ *Сергій ЄВСЕЄВ* _
(Підпис, дата) (ім’я та прізвище)

ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

№ зп	Дата засідання кафедри-розробника РПНД	Номер протоколу	Підпис завідувача кафедри (яка викладає)	Підпис завідувача кафедри (на якій викладається)	Підпис гаранта освітньої програми
1					
2					
3					
4					
5					

МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни “Моделювання кіберфізичних дій” – підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також фахівців з моделювання кіберфізичних дій, на базі освоєння принципів та методів збору цифрової інформації для дослідження поведінки агентів систем безпеки, проведення статичного аналізу індивідуальної та групової поведінки учасників кіберфізичних дій, використовуючи інструменти та методи різноманітних напрямків кібербезпеки.

Компетентності та результати навчання

Компетентності	Результати навчання
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури	РН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів,

Компетентності	Результати навчання
	які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН21. Використовувати методи натурного, фізичного і

Компетентності	Результати навчання
	комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Структурно-логічна схема вивчення навчальної дисципліни

Попередні дисципліни:	Наступні дисципліни:
Математичні основи криптології	
Лінійна алгебра	
Основи криптографічного захисту	
Дискретна математика	
Інформатика	
Програмування	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Загальний обсяг (годин) / кредитів ECTS	З них		За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль	Семестровий контроль	
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари		Контрольні роботи (кількість робіт)	Залік	Екзамен
1	**150/5**	**64**	**86**	**32**	**32**	**-**	**-**	**2**	**+**	**-**

Співвідношення кількості годин аудиторних занять до загального обсягу складає 53 (%):

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
1	Л СР	2 2	***<u>Тема 1.</u> Вступ.*** Цілі та завдання навчальної дисципліни «Моделювання кіберфізичних дій». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів.	**1, 3**
	ЛЗ СР	2 3	***Лабораторне заняття № 1.*** Використання системи MATLAB для моделювання дій у кіберфізичних системах.	**3**
2	Л СР	2 2	***<u>Тема № 2.</u> Моделювання.*** Основні поняття моделювання, поняття системи та моделі, основні типи моделей, види моделей та їх класифікація за різними критеріями, вимоги до моделей.	**1, 3-5**
	ЛЗ СР	2 3	***Лабораторне заняття № 1.*** Використання системи MATLAB для моделювання дій у кіберфізичних системах.	**3**
3	Л СР	2 2	***<u>Тема 3.</u> Основні види моделювання. Формальні методи побудови моделей.*** Основні види моделювання (аналітичне, імітаційне, статистичне), їх характеристики та відношення між собою. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретично-множинний підхід.	**1, 3-5**
	ЛЗ СР	2 3	***Лабораторне заняття № 2.*** Використання системи SIMULINK ля моделювання дій у кіберфізичніх системах.	**3**
4	Л СР	2 2	***<u>Тема 4.</u> Принципи побудови моделей. Технологія моделювання.*** Основні принципи побудови моделей: інформаційної достатності, доцільності, здійсненності, множинності моделей, агрегації, параметризації, застосування методології ітераційного багаторівневого моделювання. Технологія моделювання: основні етапи, їх взаємозв'язок та характеристики.	**1, 3-5**
	ЛЗ	2	***Лабораторне заняття № 2.***	**3**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
	СР	3	Використання системи SIMULINK ля моделювання дій у кіберфізичних системах.	
5	Л СР	2 2	***<u>Тема 5.</u> Ідентифікація параметрів математичної моделі. Адекватність, чутливість, непротирічність моделі.*** Постановка завдання ідентифікації, основні етапи його вирішення та їх взаємозв'язок. Поняття адекватності, чутливості та непротирічності моделі, формальні способи їх перевірки.	**1, 3, 5**
	ЛЗ СР	2 3	***Лабораторне заняття № 3.*** Моделювання кінцевих автоматів як прототипів агентів кіберпростору.	**3**
6	Л СР	2 2	***<u>Тема № 6</u>. Структуровані підходи до збирання інформації.*** Методи розвідки із відкритим вихідним кодом. Огляд методів структурованого аналізу. Типи інформації, що збирається: ділова інформація (фінансова, клієнти, постачальники, партнери). Інформація про IT-інфраструктуру. Виявлення джерел інформації.	**1, 3-5**
	ЛЗ СР	2 3	***Лабораторне заняття № 3.*** Моделювання кінцевих автоматів як прототипів агентів кіберпростору.	**3**
7	Л СР	2 2	***<u>Тема 7.</u> Основні поняття і визначення, що використовуються при описі моделей безпеки комп'ютерних систем.*** Елементи теорії комп'ютерної безпеки. Сутність, суб'єкт, доступ, інформаційний потік. Класична класифікація загроз безпеки інформації. Види інформаційних потоків. Види політик управління доступом та інформаційними потоками. Витік права доступу і порушення безпеки КС. Математичні основи моделей безпеки.	**1, 3-5**
	ЛЗ СР	2 3	***Лабораторне заняття № 4.*** Моделювання кіберфізичних дій мережема Петрі.	**3**
8	Л СР	2 2	***<u>Тема № 8.</u> Соціальна інженерія*** Соціальна інженерія. Огляд проекту «Інструментарій соціальної інженерії».	**3-5**
	ЛЗ СР	2 3	***Лабораторне заняття № 4.*** Моделювання кіберфізичних дій мережема Петрі.	**3**
9	Л	2	***<u>Тема 9.</u> Системно-динамічні моделі дій у кіберпросторі. Мова системної динаміки.*** Концепція системної динаміки. Класифікація систем.	**1, 3-4, 6**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
	СР	2	Методи вивчення складних систем. Системний аналіз та системна динаміка. Понятийний апарат. Основні поняття. Типи зв'язків між елементами системи. Класифікація та позначення елементів моделі.	
	ЛЗ СР	2 3	***Лабораторне заняття № 5.*** Основи побудови системно-динамічних моделей за допомогою PowerSim. Побудова імітаційної моделі взаємодії «зловмисник-захісник».	**2**
10	Л СР	2 2	***<u>Тема 10.</u> Системно-динамічні моделі дій у кіберпросторі. Побудова імітаційних моделей.*** Формування цілей дослідження. Збір інформації про систему та процеси (етап референції). Побудова концептуальної моделі. Побудова машинної моделі. Проведення імітаційних експериментів та верифікація моделі. Обговорення моделі (дебрифінг). Поліпшення моделі	**1, 3-4, 6**
	ЛЗ СР	2 3	***Лабораторне заняття № 5.*** Основи побудови системно-динамічних моделей за допомогою PowerSim. Побудова імітаційної моделі взаємодії «зловмисник-захісник».	**2**
11	Л СР	2 3	***<u>Тема 11.</u> Теоретико-ігрові моделі дій у кіберпросторі.*** Елементи теорії ігор. Ігри та їх класифікація. Чисті стратегії гравців. Змішана стратегія гравців. Матричні ігри. Мінімаксні стратегії. Гра з сідловою точкою. Гра без сідловою точкою. Вирішення матричної гри. Критерії оптимальності стратегії адміністратора. Методи розв'язання матричних ігор. Домінування. Використання лінійного програмування. Біматричні ігри. Рівноваги Неша у кінцевій грі N осіб. Дилема ув'язненого. Програмне забезпечення знаходження рішення ігор. Нескінченні ігри.	**1, 3-4, 6**
	ЛЗ СР	2 3	***Лабораторне заняття № 6.*** Побудова та використання ігрової моделі «Відбиття атак у кіберпросторі».	**2**
12	Л СР	2 3	***<u>Тема 12.</u> Застосівання теорії ігор для моделювання кіберфізичних дій.*** Приклад матричної гри "зловмисник - адміністратор". Програмне застосування для вибору оптимального набору засобів захисту. Відображення	**1, 3-4, 6**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			атак у кіберпросторі. Вибір засобу ефективного захисту від DoS/DDoS-атак. Моделювання поведінки азартного зловмисника.	
	ЛЗ СР	2 3	***Лабораторне заняття № 6.*** Побудова та використання ігрової моделі «Відбиття атак у кіберпросторі».	**2**
13	Л СР	2 3	***<u>Тема 13.</u> Агентні моделі кіберфізичних дій.*** Об'єкти та агенти. Класифікація агентів кіберфізичних систем. Мультіагентні системи. Взаємодія агентів у кіберпросторі. Комунікація та координація кіберфізичних агентів. Кооперація та конфронтація агентів. Моделі конфліктних ситуацій у кіберпросторі.	**1, 3-4, 6**
	ЛЗ СР	2 3	***Лабораторне заняття № 6.*** Побудова та використання ігрової моделі «Відбиття атак у кіберпросторі».	**2**
14	Л СР	2 3	***<u>Тема 14.</u> Планування дій у кібер-фізичних системах.*** Планування дій. Планування при синтезі програм. Вчинки та поведінка.	**1, 3-4, 6**
	ЛЗ СР	2 3	***Лабораторне заняття № 7.*** Мультиагентна модель поведінки та гвзаємодії агентів в кіберфізичній системі.	**2**
15	Л СР	2 3	***<u>Тема 15.</u> Навчання у кіберфізичних системах.*** Моделі навчання. Навчання за прикладами. Навчальні системи.	**1, 3-4, 6**
	ЛЗ СР	2 3	***Лабораторне заняття № 7.*** Мультиагентна модель поведінки та гвзаємодії агентів в кіберфізичній системі.	**2**
16	Л СР	2 3	***<u>Тема 16.</u> Розпізнавання у кібер-фізичних системах.*** Проблема розпізнавання. Математична теорія розпізнавання образів. Розпізнавання атак. Розпізнавання зловмисників. Алгоритмічні основи знань.	**1, 3-4, 6**
	ЛЗ СР	2 3	***Лабораторне заняття № 7.*** Мультиагентна модель поведінки та гвзаємодії агентів в кіберфізичній системі.	**2**
Разом (годин)		**150**		

САМОСТІЙНА РОБОТА

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час.

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовування лекційного матеріалу	38
2	Підготовка до лабораторних занять	48
	Разом	**86**

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Не передбачено навчальним планом

МЕТОДИ НАВЧАННЯ

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

МЕТОДИ КОНТРОЛЮ

Поточний контроль при вивченні дисципліни реалізується у формі опитувань на лекційних заняттях, захисту лабораторних робіт та проведення контрольних робіт.

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

- з лекційного матеріалу – шляхом проведення тестування, презентацій докладів за темами лекційних занять;
- з лабораторних завдань – за допомогою перевірки виконаних завдань.

Семестровий контроль проводиться у формі заліку (з оцінкою) відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом.

Семестровий контроль проводиться в письмовій формі за контрольними завданнями, а також шляхом тестування з використанням технічних засобів.

Результати поточного контролю враховуються як допоміжна інформація для виставлення оцінки з даної дисципліни.

Студент вважається атестованим з навчальної дисципліни за умови повного відпрацювання усіх лабораторних робіт, виконання контрольних робіт та тестових опитувань, що передбачено навчальною програмою з дисципліни.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів для оцінювання успішності студента для залік

Контрольні роботи	Лабораторні роботи	КП	РГЗ	Індивідуальні завдання	Тощо	Залік	Сума
30	70	-	-	-	-	+	100

Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під **системою оцінювання** розуміють сукупність методів (письмові, усні і практичні тести, екзамени, проєкти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними **критеріями оцінювання** для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

Критерії оцінювання – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв’язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об’єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100 бальної шкали (табл. 2). Оцінки обов’язково переводять у національну шкалу (з виставленням державної семестрової оцінки „відмінно”, „добре”, „задовільно” чи „незадовільно”) та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ЄКТС

Рейтингова Оцінка, бали	**Оцінка ECTS та її визначення**	**Національна оцінка**	**Критерії оцінювання**	
			позитивні	**негативні**
			- **Глибоке знання** навчального матеріалу, що	Відповіді на запитання можуть містити **незначні неточності**

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
90-100	A	Відмінно	містяться в **основних і додаткових літературних джерелах;** **- вміння аналізувати** явища, які вивчаються, в їхньому взаємозв'язку і розвитку; **- вміння** проводити **теоретичні розрахунки**; **- відповіді** на запитання **чіткі, лаконічні, логічно послідовні;** **- вміння вирішувати складні практичні задачі.**	
82-89	B	Добре	**- Глибокий рівень знань** в обсязі **обов'язкового матеріалу**, - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **складні практичні задачі.**	Відповіді на запитання містять **певні неточності;**
75-81	C	Добре	**- Міцні знання** матеріалу, що вивчається, та його **практичного застосування;** **-** вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати	**-** невміння використовувати теоретичні знання для вирішення **складних практичних задач.**

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	**негативні**
			практичні задачі.	
64-74	Д	Задовільно	- Знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**; - вміння вирішувати прості **практичні задачі**.	Невміння давати **аргументовані відповіді** на запитання; - невміння **аналізувати** викладений матеріал і **виконувати розрахунки;** - невміння вирішувати **складні практичні задачі.**
60-63	Е	Задовільно	- Знання **основних фундаментальних положень** - вміння вирішувати найпростіші **практичні задачі**.	Незнання **окремих (непринципових) питань** з матеріалу модуля; - невміння **послідовно і аргументовано** висловлювати думку; - невміння застосовувати теоретичні положення при розвязанні **практичних задач**
35-59	FX (потрібне додаткове вивчення)	Незадовільно	**Додаткове вивчення** матеріалу може бути виконане **в терміни, що передбачені навчальним планом**.	Незнання **основних фундаментальних положень** навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; - невміння розв'язувати **прості практичні задачі.**
1-34	F (потрібне повторне вивчення)	Незадовільно	-	- Повна **відсутність знань** значної частини навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; -незнання основних фундаментальних положень; - невміння орієнтуватися під час розв'язання **простих практичних задач**

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Стандарт вищої освіти галузі знань 12 “Інформаційні технології” для другого (магістерського) рівня вищої освіти, який затверджено наказом Міністерства освіти і науки України від 18.03.2021 р. № 332 та введено в дію з 2021/2022 навчального року.
2. Робоча програма навчальної дисципліни.
3. Силабус навчальної дисципліни
4. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів «Новий світ-2000», 2020. – 241 с.
5. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ”: https://iiiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1	Томашевський В.М, Моделювання систем. – К. Видавнича група BHV, 2005. – 352 с.
2	Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів “Новий світ-2000”, 2020ю – 241 с.
3	Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0.

Допоміжна література

4	Жерновий Ю. В. Імітаційне моделювання систем масового обслуговування: Практикум. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2007. – 307 с.
5	Shoham, Yoav, and Kevin Leyton-Brown, «Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations». Cambridge University Press, 2009.
6	Sun, Ron, Cognition and Multi-Agent Interaction: From Cognitive Modeling to Social Simulation. Cambridge University Press, 2006. http://www.cambridge.org/uk/catalogue/catalogue.asp?isbn=0521839645

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. www.cyberpol.ru - Комп'ютерна злочинність і способи боротьби.
2. www.iso27000.ru - Інформаційний портал, присвячений питанням управління інформаційною безпекою.
3. www.itsec.ru - Інтернет-журнал “Інформаційна безпека”.
4. www.inside-zi.ru - Інформаційно-методичний журнал “Захист інформації. Інсайд”.
5. www.kaspersky.ru - Лабораторія Касперського.
6. www.drweb.com – Лабораторія DrWeb.
7. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ”: https://iiiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8