СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЇ»

Лектор курсу			Кожухівський Андрій Дмитрович, доктор технічних наук, професор.		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:** ikbdut@gmail.com; **сторінка курсу в Moodle –** http://dn.dut.edu.ua/course/view.php?id=447	
Галузь знань			12 «Інформаційні технології»		**Рівень вищої освіти**	Доктор філософії	
Спеціальність			Кібербезпека		**Семестр**	1,2	
Освітня програма			Доктор філософії кібербезпеки		**Тип дисципліни**	Професійної та практичної підготовки	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Основи наукових досліджень та організація науки
Освітні компоненти для яких є базовою	Вибіркові компоненти

Мета курсу:	Формування знань та вмінь застосування методів дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних з організацією, створенням методів і засобів забезпечення кібербезпеки при її зберіганні, обробці та передачі з використанням сучасних математичних методів, інформаційних технологій

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
	ФК-3. Організаційно-комунікативна компетентність **ФК-4. Професійна компетентність** **ФК-5. Загальнонаукова компетентність** **ФК-6. Політехнічна компетентність** **ФК-7. Інженерна компетентність**

Програмні результати навчання (ПРН)

ПРН-14. Володіти навиками роботи із спеціалізованими системами криптохзахисту та криптоаналізу, управляти змінами при роботі з існуючими системами криптографічного захисту.
ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.
ПРН-19. Уміти проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів й застосовувати їх на практиці.
ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, уразливостях мережевих та Web-ресурсів.
ПРН-22. Уміти розробляти та впроваджувати дослідницькі проекти в галузі знань «інформаційні технології» спеціальності «кібербезпека» для забезпечення безпеки мережевої інфраструктури.
ПРН-23. Бути здатним генерувати нові знання з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в

системах кібербезпеки.
ПРН-26. Уміти використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.
ПРН-27. Бути здатним оволодіти спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпековими технологіями.
ПРН-30. Бути здатним до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовий модуль 1. Системи масового обслуговування			
Тема 1. ***Класифікація систем масового обслуговування.*** ***Знати***: 1. Характеристики систем масового обслуговування. 2. Вхідний потік вимог. *Вміти:* застосовувати Застосовувати системи масового обслуговування в кібербезпеці. *Формування компетенцій:* ФК-3, ФК-4, ФК-5 *Програмні результати навчання:* ПРН-18, ПРН-19 ***Рекомендовані джерела:*** 1-8	Лекція 1 2 год	7*	Лекція-візуалізація
	Практичне заняття 1 2 год		Суть і основні характеристики СМО. Типи моделей систем масового обслуговування. Формула Литтла. Одноканальні системи масового обслуговування. Теорія СМО як науково-навчальна дисципліна.
Тема 2. ***Багатоканальні системи масового обслуговування.*** ***Знати***: Аналітичні залежності в замкнутому вигляді для розрахунків характеристик роботи багатоканальної СМО в стаціонарному режимі роботи ***Вміти***: Розраховувати значення деяких характеристик ефективності роботи СМО. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-30 ***Рекомендовані джерела:*** 1–8	Лекція 2 2 год	7*	Лекція-візуалізація
	Практичне заняття 2 2 год		Основи дискретно-подійного моделювання СМО. Деякі визначення, потрібні під час моделювання систем масового обслуговування. Простір станів системи масового обслуговування.
Тема 3. ***Алгоритми моделювання систем масового обслуговування.*** ***Знати***: Створення моделі системи як множини об'єктів, що взаємодіють між собою. ***Вміти***: Створювати моделі на основі об'єктного підходу, який передбачає створення моделі системи як множини об'єктів, що взаємодіють між собою. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7	Лекція 3 2 год	7*	Лекція-візуалізапція
	Практичне заняття 3 2 год		Мережі систем масового обслуговування. Операційний аналіз мереж систем масового обслуговування.

Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-30 ***Рекомендовані джерела:*** 1–8			
Тема 1. Основні підходи до побудови математичних моделей систем захисту інформації. Тема 2. Неперервні детерміновані моделі (Д – схеми). Дискретно – детерміновані моделі (F – схеми). Неперервно – стохастичні моделі (Q – схеми). Тема 3. Процедура імітаційного моделювання. Імітація функціонування системи. Узагальнені алгоритми імітаційного моделювання систем захисту інформації.	Самостійна робота		1. Використання математичних моделей систем захисту інформації. 2. Використання математичних моделей для захисту інформації. 3. Використання узагальнених алгоритмів імітаційного моделювання в системах захисту інформації.
Змістовий модуль 2. Мережі Петрі			
Тема 4. ***Теорія мереж Петрі.*** ***Знати***: Зазначати режим доступу до маркерів, тобто задати, яким чином маркери (дані) надходять до вузлів та як вони з них вилучаються. ***Вміти.*** Визначати основні режими доступу до вузлів у розширеннях мереж Петрі ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1-8	Лекція 4 2 год Практичне заняття 4 2 год	8*	Лекція-візуалізація Вхідна і вихідна мультимножина місць і переходів. Маркована мережі Петрі. Операції злиття в кольорових мережах. Точки доступу мережі Петрі. Стани мережі Петрі.
Тема 5. ***Прикладне застосування мереж Петрі.*** ***Знати***: Поняття дуги, що використовується для моделювання фіксованих потоків даних. ***Вміти.*** Визначати правило спрацювання переходів. Застосування змінних у відповідності з послідовністю перегляду вхідних дуг переходу. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1-8	Лекція 5 2 год Практичне заняття 5 2 год	8*	Лекція-візуалізація Конвейєрно-складські задачі. Моделі на базі мереж Петрі в мовах програмування. Моделювання паралельних процесів засобами мереж Петрі. Класичні задачі, що мають розв’язок засобами мереж Петрі
Тема 4. Побудова моделей простих об'єктів Тема 5. Аналіз властивостей мереж за допомогою фундаментального рівняння та інваріантів	Самостійна робота		4.Побудова моделей простих об'єктів 5. Аналіз властивостей мереж за допомогою фундаментального рівняння та інваріантів

Змістовий модуль 3. Основи моделювання систем			
Тема 6. ***Генератори випадкових величин.*** ***Знати***: Методи генерування псевдовипадкових чисел ***Вміти***: Використовувати ресурси комп'ютера для моделювання послідовностей псевдовипадкових чисел великої довжини. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1–8	Лекція 6 2 год	8*	Лекція-візуалізація
	Практичне заняття 6 2 год		Способи генерування випадкових величин. Генерування рівномірно розподілених в інтервалі (0;1) випадкових величин на основі рекурсивних формул. Тестування генераторів рівномірно розподілених в інтервалі (0,1) випадкових чисел.
Тема 7. ***Лінійні конгруентні генератори.*** ***Знати***: властивості конгруентності ***Вміти***: вибирати параметри лінійного конгруентного генератора для отримання послідовності з повним періодом ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1–8	Лекція 7 2 год.	8*	Лекція-візуалізація
	Практичне заняття 7 2 год		Об'єднання лінійних конгруентних генераторів. Регістри зсуву з лінійним зворотнім зв'язком.
Тема 8 . *Перевірка послідовностей випадкових чисел* **.** ***Знати***: методи моделювання неперервних випадкових величин. ***Вміти***: використання мови GPSS для моделювання випадкових величин. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1-8	Лекція 8 2 год	8*	Лекція-візуалізація
	Практичне заняття 8 2 год		Основні вимоги до засобів формування випадкових та псевдовипадкових послідовностей.
Тема 9. ***Моделювання неперервних випадкових величин.*** ***Знати***: методи моделювання неперервних випадкових величин.	Лекція 9 2 год	8*	Лекція-візуалізація

Вміти: використання мови GPSS для моделювання випадкових величин. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1–8	Практичне заняття 9 2 год		Моделювання систем як засіб наукового пізнання. Етапи процесу моделювання. Системні принципи моделювання. Методи моделювання систем. Проведення заліку
Тема 6. Основні підходи до побудови математичних моделей систем захисту інформації. **Тема 7.** Неперервні детерміновані моделі (Д – схеми). Дискретно – детерміновані моделі (F – схеми). Неперервно – стохастичні моделі (Q – схеми). **Тема 8.** Процедура імітаційного моделювання. Імітація функціонування системи. Узагальнені алгоритми імітаційного моделювання систем захисту інформації. **Тема 9.** Моделювання мережі масового обслуговування з використанням мови імітаційного моделювання GPSS.	Самостійна робота		6. Використання ресурсів комп'ютера для моделювання послідовностей псевдовипадкових чисел великої довжини. 7. Вибір параметрів лінійного конгруентного генератора для отримання послідовності з повним періодом 8. Оцінювання наближеності отриманого розподілу в порівнянні з рівномірним розподілом. 9. Використання мови GPSS для моделювання випадкових величин.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерне обладнання, мережа Інтернет ауд. 421.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Імітаційне моделювання систем масового обслуговування / [В.Б. Толубко, А.Д. Кожухівський, В.В. Вишнівський, Г.І. Гайдур, О.А. Кожухівська].- Навч. посібник (Електронне видання).-К.: ДУТ.-2018.- 175 с.
2. Кожухівський А.Д. Імітаційне моделювання систем та процесів в середовищі MATLAB. Практикум [Текст]/ А.Д. Кожухівський, О.А. Кожухівська.- Черкаси: Вид-во ЧДТУ.- 2009.
3. Моделювання обчислювальних процесів і систем. Практикум. Навчальний посібник [Текст] / [Ю.Г.Лега, А.Д.Кожухівський, О.А.Кожухівська, Г.Т.Олійник]. – РВВ ЧДТУ, Черкаси: ЧДТУ, 2009. – 195 с.
4.Кожухівський А.Д., Основи комп`ютерної безпеки в спеціалізованих телекомунікаційних мережах. Навчальний посібник [Текст] / А.Д.Кожухівський, А.В.Сагун , Д.В. Копил.- РВВ ЧДТУ, Черкаси, 2009. – 132 с.
5. Лега Ю.Г., Методи імітаційного моделювання систем та процесів. Практикум. Навчальний посібник [Текст] / Ю.Г.Лега, А.Д. Кожухівський, О.А.Кожухівська. – Черкаси: Вид – во ЧДТУ, 2010. – 247 с.
6.Девянін П.Н. Моделі безпеки комп'ютерних систем: Навч. посібник для студ. висш. навч. закладів [Текст]/ Петро Миколайович Девянін. - М.: Видавничий центр «Академія», 2005. - 144 с.
7. Зайцев Д.А. Мережі Петрі і моделювання систем. Методичні вказівки до практичних занять і лабораторних робіт для підготовки магістрів з напрямку «Телекомунікації». Укл Д.А.Зайцев.- Одеса, 2006.- 42 с.
8. Томашевський В.М. Моделювання систем / В.М.Томашевський.- К.:Видавнича група BHV.- 2005.- 352 с.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо аспірант відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації аспірант повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату аспірант отримує за завдання 0 балів.
- Аспірант, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни аспірант видаляється з заняття, за заняття отримує 0 балів.

*** КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання аспірантом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,5 бала
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***залік***	Метою залік є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій формі.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Аспірант демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що	Відмінно / Зараховано (А)

	бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	відносяться до дисципліни, яка вивчається.	
82-89	Аспірант демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (B)
75-81	Аспірант в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Аспірант засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Аспірант має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, аспірант з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	**Незадовільний** Аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*