СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЇ»

Лектор курсу	Кожухівський Андрій Дмитрович, доктор технічних наук, професор.	**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** ikbdut@gmail.com; **сторінка курсу в GWE** https://classroom.google.com/c/NzA3NTIxNjI5Mjc1?cjc=wgfg46m
Галузь знань	12 «Інформаційні технології»	**Рівень вищої освіти**	магістр
Спеціальність	125 Кібербезпека та захист інформації	**Семестр**	1
Освітньо-професійна програма	Управління інформаційною та кібернетичною безпекою	**Тип дисципліни**	Вибіркова компонента освітньо-професійної програми

Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	36	-	96

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

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)**
КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

Програмні результати навчання (ПРН)

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та

критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

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.

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.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

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.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Розділ 1. Системи масового обслуговування			
Тема 1. ***Класифікація систем масового обслуговування.*** ***Рекомендовані джерела:*** 1-8			
Заняття1.1. Класифікація систем масового обслуговування.	Лекція 1 2 год	6*	Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитування
Заняття1.2. Класифікація систем масового обслуговування.	Практичне заняття 1 4 год		Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 2. ***Багатоканальні системи масового обслуговування.*** ***Рекомендовані джерела:*** 1–8			
Заняття 2.1 Багатоканальні системи масового обслуговування.	Лекція 2 2 год	6*	Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитування
Заняття 2.2 Багатоканальні системи масового обслуговування.	Практичне заняття 2 4 год		Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 3. ***Алгоритми моделювання систем масового обслуговування.*** ***Рекомендовані джерела:*** 1–8			

Заняття 3.1. Алгоритми моделювання систем масового обслуговування.	Лекція 3 2 год	6*	Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитування
Заняття 3.2. Алгоритми моделювання систем масового обслуговування.	Практичне заняття 3 4 год		Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
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 40	2	1. Використання математичних моделей систем захисту інформації.
		2	2. Використання математичних моделей для захисту інформаці
		2	3. Використання узагальнених алгоритмів імітаційного моделювання в системах захисту інформації.
Розділ 2. Мережі Петрі			
Тема 4. ***Теорія мереж Петрі.*** ***Рекомендовані джерела:*** 1-9			
Заняття 4.1. Теорія мереж Петрі.	Лекція 4 2 год	5*	Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитування
Заняття 4.2. Теорія мереж Петрі.	Практичне заняття 4 4 год		Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 5. ***Прикладне застосування мереж Петрі.*** ***Рекомендовані джерела:*** **8,9**			
Заняття 5.1. Прикладне застосування мереж Петрі.	Лекція 5 2 год	5*	Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитування
Заняття 5.1. Прикладне застосування мереж Петрі	Практичне заняття 5 4 год		Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування

Тема 4. Побудова моделей простих об'єктів	Самостійна робота	2	4.Побудова моделей простих об'єктів
Тема 5. Аналіз властивостей мереж за допомогою фундаментального рівняння та інваріантів		2	5. Аналіз властивостей мереж за допомогою фундаментального рівняння та інваріантів
Розділ 3. Основи моделювання систем			
Тема 6. ***Генератори випадкових величин.*** ***Рекомендовані джерела:*** 6–15			
Заняття 6.1. Генератори випадкових величин.	Лекція 6 2 год	6*	Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитування
Заняття 6.2. Генератори випадкових величин.	Практичне заняття 6 4 год		Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 7. ***Лінійні конгруентні генератори.*** ***Рекомендовані джерела:*** 1 - 15			
Заняття 7.1 Лінійні конгруентні генератори.	Лекція 7 2 год.	6*	Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитуванн
Заняття 7.2 Лінійні конгруентні генератори.	Практичне заняття 7 4 год		Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 8 . ***Перевірка послідовностей випадкових чисел*** ***Рекомендовані джерела:*** 1-15			
Заняття 8.1 . Перевірка послідовностей випадкових чисел.	Лекція 8 2 год	6*	Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитуванн
Заняття 8.2 . Перевірка послідовностей випадкових чисел.	Практичне заняття 8 4 год		Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 9. ***Моделювання неперервних випадкових величин.***			

<table>
<tr><td colspan="4"><u>Рекомендовані джерела:</u> 6–15</td></tr>
<tr><td>Заняття 9.1 Моделювання неперервних випадкових величин.</td><td>Лекція 9
2 год</td><td rowspan="2">6*</td><td>Пояснювально-ілюстартивний, лекція-візуалізація, бліц опитуванн</td></tr>
<tr><td>Заняття 9.1 Моделювання неперервних випадкових величин.</td><td>Практичне заняття 9
4 год</td><td>Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування</td></tr>
<tr><td rowspan="4">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.</td><td rowspan="4">Самостійна робота
56</td><td>2</td><td>6. Використання ресурсів комп’ютера для моделювання послідовностей псевдовипадкових чисел великої довжини.</td></tr>
<tr><td>2</td><td>7. Вибір параметрів лінійного конгруентного генератора для отримання послідовності з повним періодом</td></tr>
<tr><td>2</td><td>8. Оцінювання наближеності отриманого розподілу в порівнянні з рівномірним розподілом</td></tr>
<tr><td>2</td><td>9. Використання мови GPSS для моделювання випадкових величин.</td></tr>
<tr><td colspan="4">МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ</td></tr>
<tr><td colspan="4">Комп‘ютерне обладнання, мережа Інтернет ауд. 421.</td></tr>
<tr><td colspan="4">ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ</td></tr>
<tr><td colspan="4">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.- 174 с.
2. Криптографічні перетворювання: навчально-методичні матеріали до самостійної роботи для студентів спеціальностей 6.160.100 і 7.160.100 “Захист інформації в комп’ютерних системах та мережах”. Частина 1. Основи теорії чисел / Укл.: Ю.Г. Лега, А.Д. Кожухівський, О.А. Кожухівська, В.А. Лужецький.-Черкаси: ЧДТУ, 2008.- 32 с.
3. Кожухівський А.Д. Імітаційне моделювання систем та процесів в середовищі MATLAB. Практикум [Текст]/ А.Д. Кожухівський, О.А. Кожухівська.-Черкаси: Вид-во ЧДТУ.- 2009.
4. Моделювання обчислювальних процесів і систем. Практикум. Навчальний посібник [Текст] / [Ю.Г.Лега, А.Д.Кожухівський, О.А.Кожухівська,</td></tr>
</table>

Г.Т.Олійник]. – РВВ ЧДТУ, Черкаси: ЧДТУ, 2009. – 195 с.
5.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.
6. 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.
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 [Текст] / В.М.Томашевський.- К.:Видавнича група BHV.- 2005.- 352 с.
9. Стеценко І.В. Моделювання систем. Навчальний посібник [Текст] / І.В. Стеценко.- Черкаси: Видавництво “Маклаут”, 2011.- 502 с.
10. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І.Горбенко.- Харків: Видавництво “Форт”, 2012.- 870 с.
11. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ до виконання лабораторних робіт з дисципліни «ПРИКЛАДНА КРИПТОЛОГІЯ» / [А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, В.А. Савченко, В.В. Марченко, О.А. Кожухівська]. Мін-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2020.- 109 с.
12. Математичні методи криптології: Навчальний посібник [Електронний ресурс] / [А.Д. Кожухівський, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко]; Мін-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2021.- 243 с.
13.NIST SP 800-90. Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006.
14. AES discussion forum: [Electronnyi resurs]. Rezhym dostupa: http://aes.nist.gov
15. ISO/IEC 11770-3: 2008 Information technology – Security techniques – Key management Part 3: Mechanisms using asymmetric techniques.

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 магістр 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 магістр повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату магістр отримує за завдання 0 балів.
- Магістр, 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 магістр видаляється із заняття, за заняття отримує 0 балів.

*** КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання магістром мінімум 50 балів у сукупності за всіма темами дисципліни

Форми контролю	**Види навчальної роботи**	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	Виконання практичних завдань	52

	Самостійна робота	18
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 бал
ПІДСУМКОВЕ ОЦІНЮВАННЯ *залік*	Метою заліку 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	Магістр 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-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 магістр проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції магістра 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 відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Магістр 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 магістру самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (В)
75-81	Магістр 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	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (С)

	положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.		
64-74	Магістр 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	Магістр 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, магістр 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	Магістр може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни магістр виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необгрунтованими. Цілісність розуміння матеріалу з дисципліни у магістра 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	Магістр повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Магістр не допущений до здачі заліку.	**Незадовільний** Магістр 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*