«Затверджую»

Завідувач кафедри інформаційних технологій
проектування та прикладної математики

_____ /д.т.н., проф. Олександр ТЕРЕНТЬЄВ/

«__19__» _вересня__2023 р.

Розробник силабусу

_____ /ас. Ольга СЕРПІНСЬКА./

СИЛАБУС

ТЕОРІЯ АЛГОРИТМІВ

назва освітньої компоненти(дисципліни)

Шифр за ОП: ВК
Навчальний рік:2023/2024
Освітній рівень: перший рівень вищої освіти (бакалавр)
Форма навчання: денна
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека»
8) Компонента спеціальності: вибіркова
9) Семестр: 7
10) Цикл дисципліни:вибіркова компонента ОП
11) Контактні дані викладача: ас. Серпінська О.І., o.serpinska@gmail.com, (044) 241-54-02
12) Мова навчання: українська
13) Пререквізити: «Основи програмування», «Об'єктно-орієнтоване програмування», «Математичний аналіз», «Дискретна математика»
14) Мета курсу: отримання студентами ґрунтовної математичної підготовки та знань теоретичних, методичних і алгоритмічних основ інформаційних технологій для їх використання під час розв`язання прикладних і наукових завдань в області інформаційних систем і технологій, забезпечення теоретичної і інженерної підготовки фахівців у галузі проектування, впровадження і використання інформаційних систем.

15) Програмні компетентності:

Інтегральна Компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\ абокібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності (КФ)	КФ 2. Здатність до використання інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмноапаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційнотелекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

16). Програмні результати навчання:

№	Програмний результат навчання	Метод перевірки навчального ефекту	Форма проведення занять	Посилання на компетентності
1.	ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;	Обговорення під час занять	Лекції, лабораторні роботи	**КЗ3**
2.	ПРН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;	Обговорення під час занять	Лекції, лабораторні роботи	**ІК** **КЗ5** КФ2

3.	ПРН 7. Діяти на основівзаконодавчої та нормативно-правовоїбазиУкраїни та вимогвідповіднихстандартів, у тому числіміжнародних в галузіінформаційної та /абокібербезпеки;	Обговорення під час занять	Лекції, лабораторні роботи	**КЗ6 КЗ7**
4.	ПРН10. Виконуватианаліз та декомпозиціюінформаційно-телекомунікаційних систем;	Обговорення під час занять	Лекції, пактичні заняття	**КФ2**
5.	ПРН11. Виконуватианаліззв'язківміжінформаційнимипроцесами на віддаленихобчислювальних системах;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ2 КФ3**
6.	ПРН13. Аналізувати проектиінформаційно-телекомунікаційних систем базуючись на стандартизованихтехнологіях та протоколах передачіданих;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ2 КФ3**
7.	ПРН16. Реалізовуватикомплекснісистемизахистуінформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правовихдокументів;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7**
8.	ПРН17. Забезпечувати процеси захисту та функціонування інформаційнотелекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
9.	ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\абокібербезпеки;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
10.	ПРН23. Реалізовувати заходи з протидіїотриманнюнесанкціонованого доступу до інформаційнихресурсів і процесіввінформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
11.	ПРН24. Вирішуватизадачіуправління доступом до інформаційнихресурсів та процесіввінформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**

12.	ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
13.	ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
14.	ПРН27. Вирішуватизадачізахиступотоківданих в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ2 КФ4 КФ7 КФ11**
15.	ПРН30. Здійснюватиоцінюваннямożливостінесанкціонованого доступу до елементівінформаційно-телекомунікаційних систем;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ2 КФ4 КФ7 КФ11**
16.	ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
17.	ПРН36. Виявлятинебезпечнісигналитехнічнихзасобів;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
18.	ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
19.	ПРН39. Проводитиатестацію (спираючись на облік та обстеження) режимнихтериторій (зон), приміщеньтощо в умовахдодержання режиму секретностіізфіксуваннямрезультатів у відповідних документах;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
20.	ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
21.	ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**

22.	ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
23.	ПРН49. Забезпечуватиналежнефункціонуваннясистемимоніторингуінформаційнихресурсів і процесіввінформаційно-телекомунікаційних системах;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
24.	ПРН50. Забезпечувати) функціонуванняпрограмних та програмно-апаратнихкомплексіввиявленнявторгненьрізнихрівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
25.	ПРН51. Підтримуватипрацездатність та забезпечуватиконфігурування систем виявленнявторгнень в інформаційно-телекомунікаційних системах;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**
26.	ПРН53. Вирішуватизадачіаналізупрограмного коду на наявністьможливихзагроз;	Обговорення під час занять	Лекції, лабораторні роботи	**КФ4 КФ7 КФ11**

16) Структура курсу:

Лекції, год	Практичне заняття, год	Лабораторні заняття, год	Курсовий проект/ курсова робота РГР/Контрольна робота	Самостійні робота здобувача, год	Форма підсумкового контролю
20		20		20	Залік

Сума годин: 60	
Загальна кількість (кредитів ECTS)	60 (2)
Кількість годин (кредитів ECTS) аудиторного навантаження:	40(2)

17) Зміст курсу: (окремо для кожної форми занять – Л/Пр/Лаб/ КР/СРС)

Лекції:

<u>Модуль 1. Алгоритми: побудова та аналіз</u>

Змістовий модуль 1. Аналіз алгоритмів та алгоритмічні стратегії.

1.1. Основи аналізу алгоритмів.
1.2. Асимптотичний аналіз. Оцінки складності алгоритмів.
1.3. Структури даних.
1.4. Рекурсивні функції і алгоритми.
1.5. Теорія скінченних автоматів.

Змістовий модуль 2. Фундаментальні алгоритми та їх побудова.

2.1.Алгоритми сортування та їх аналіз.
2.2.Алгоритми пошуку підрядків в рядках.
2.3.Алгоритми побудови мереж і потоків.
2.4.Алгоритми стиснення інформації.
2.5.Криптографічні алгоритми.

Лабораторні заняття:

Змістовий модуль 1. Аналіз алгоритмів та алгоритмічні стратегії

1.Властивості і способи опису алгоритмів.

2.Аналіз алгоритмів.
3. Структури даних. Статичні структури даних.
4. Структури даних. Динамічні структури даних.
5.Рекурсивні алгоритми (програмна реалізація).
6.Машини Тьюрінга. Автомати Маркова. Машина Поста.

Змістовий модуль 2. Фундаментальні алгоритми та їх побудова.

1.Основні методи сортування масивів (розрахунки вручну та програмна реалізація).
2.Алгоритми пошуку в рядках (розрахунки вручну та програмна реалізація).
3.Алгоритми побудови мереж і потоків (розрахунки вручну та програмна реалізація).
4.Алгоритми стиснення інформації (розрахунки вручну та програмна реалізація).
5.Криптографічні алгоритми (розрахунки вручну та програмна реалізація)

Практичні заняття:не передбачено НП

Курсовий проект/курсова робота/РГР/Контрольна робота:не передбачено НП

Самостійна робота студента(СРС):

1. Виконання лабораторних робіт.
2. Підготовка до лекцій.
3. Підготовка до заліку.

18) Основна література:

1. Нікольський Ю. В., Пасічник В. В., Щербина Ю. М. Дискретна математика: підручник. – Львів: Магнолія-2006, 2010.- 431с. (укр. мова, 20 примірників).
2. Заяць В. М. Методи, алгоритми та програмнізасоби для моделювання і аналізудинамікискладнихоб'єктів і систем на основідискретних моделей: Монографія. – Львів: НовийСвіт-2000, 2009. – 399с. (укр. мова, 2 примірники).
3. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ: Пер. с англ. – М.: Центр непрер. матем. образ-я, 2000. - 960 с.

19) Додаткові джерела:

1. Бартків А.Б., Гринчишин А.Т., Ломакович А.М. та ін. TURBO PASCAL: Алгоритми і програми:Числені методи в фізиці та математиці: Навч. посібник для студ. пед. ін-ів.- К.: Вища школа, 1992. – 248 с. (укр. мова, 24 примірника).
2. Блохін Л. М., Бориченко М.Ю., Кривоносенко О.П., Безкоровайний Ю.М. Базові алгоритми статистичної динаміки: Навч. посібник для студ. вищ. навч. закл. – К.: Книжкове вид-во НАУ, 2007. – 18 с. (укр. мова, 3 примірника).
3. Бех О. В., Городня Т. А., Щербак А. Ф. Збірник задач з математичного програмування: Навч. посібник для студ. вищ. навч. закл. - Львів: Магнолія, 2007.- 211 с. (укр. мова, 5 примірників).
3. Ахо, Альфред, В., Хопкрофт, Джон, Ульман, Джефри, Д. Структуры данных и алгоритмы.: Пер. с англ.: М.: Издательский дом «Вильямс», 2003.-384 с. (рос. мова, електронний варіант).

20) Система оцінювання навчальних досягнень (розподіл балів):

Поточне оцінювання		Підсумковий контроль (залік)	Сума
Змістовні модулі			
1	**2**		
30	45	25	100

21) Умови допуску до підсумкового контролю:

- відвідування лекцій;
- виконання лабораторних робіт;
- дотримання термінів виконання робіт;
- дотримання умов академічної доброчесності.

22) Політика щодо академічної доброчесності:розуміння здобувачами вищої освіти етичного кодексу університету та норм академічної доброчесності (вимог щодо оригінальності текстів та допустимого відсотку співпадінь))

23) Посилання на сторінку електронного навчально-методичного комплексу дисципліни:

http://org2.knuba.edu.ua/course/view.php?id=893