



«Затверджую»

Завідувач кафедри кібербезпеки та комп'ютерної інженерії

 /д.т.н., проф. Юрій ХЛАПОНІН/

« 29 » 08 2022 р.

Розробник силабусу

 /к.т.н., доц. Володимир ВИШНЯКОВ/



СИЛАБУС ЗАХИСТ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

назва освітньої компоненти(дисципліни)

1) Шифр за ОП: ВК				
2) Навчальний рік: 2022/2023				
3) Освітній рівень: перший рівень вищої освіти (бакалавр)				
4) Форма навчання: денна, заочна, дуальна, дистанційна, змішана				
5) Галузь знань: 12 «Інформаційні технології»				
6) Спеціальність: 126 "Інформаційні системи та технології "				
8) Компонента спеціальності: вибіркова				
9) Семестр: -				
10) Цикл дисципліни: вибіркова компонента ОП				
11) Контактні дані викладача: к.т.н., доц. Володимир ВИШНЯКОВ vyshniakov.vm@knuba.edu.ua (068)554-80-74 https://www.knuba.edu.ua/faculties/fait/kafedri-fait/kafedra-kbki/sklad-kafedri/vishnyakov-volodimir-mixajlovich/				
12) Мова навчання: українська				
13) Пререквізити: «Математика», «Теорія імовірностей», «Основи програмування та алгоритмічні мови», «Системи програмування та операційні системи», «Комп'ютерні мережі»				
14) Мета курсу: полягає у наданні студентам теоретичних знань та практичних навичок, що необхідні для побудови та підтримки сучасних систем захисту даних на базі міжнародних та українських нормативних документів відповідно до обраного ними напрямку підготовки.				
15) Результати навчання:				
№	Програмний результат навчання	Метод перевірки навчального ефекту	Форма проведення занять	Посилання на компетентності
1.	ПР2. Застосовувати знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів та дискретного аналізу при розв'язанні задач проектування і використання інформаційних систем та технологій	Обговорення під час занять	Лекції, лабораторні роботи	ІК КС1, КС2, КС3, КС4, КС5, КС6, КС12

2.	ПР3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій	Обговорення під час занять	Лекції, лабораторні роботи	ІК КС1, КС2, КС3, КС4, КС5, КС6, КС12
3.	ПР5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій	Обговорення під час занять	Лекції, лабораторні роботи	ІК КС1, КС2, КС3, КС4, КС5, КС6, КС12
4.	ПР 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ з метою їх запровадження у професійній діяльності.	Обговорення під час занять	Лекції, лабораторні роботи	ІК КС1, КС2, КС3, КС4, КС5, КС6, КС12
5.	ПР7. Обґрунтувати вибір технічної структури та розробляти відповідне програмне забезпечення, що входить до складу інформаційних систем та технологій	Обговорення під час занять	Лекції, лабораторні роботи	ІК КС1, КС2, КС3, КС4, КС5, КС6, КС12

16) Структура курсу:

Лекції, год	Практичне заняття, год	Лабораторні заняття, год	Курсовий проект/ курсова робота РГР/Контрольна робота	Самостійні роботи здобувача, год	Форма підсумкового контролю
20	-	20	РГР	50	залік
Сума годин:					
Загальна кількість (кредитів ECTS)				90 (3,0)	
Кількість годин (кредитів ECTS) аудиторного навантаження:				40 (1,33)	

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

Лекції:

Модуль 1. Захист даних в інформаційних системах.

Змістовий модуль 1. Основи побудови систем захисту даних

Тема 1. Державні стандарти та інші нормативні документи щодо систем захисту даних.

Тема 2. Принципи розробки систем захисту даних

Змістовий модуль 2. Характеристики захищаних об'єктів та систем захисту даних

Тема 1. Класифікація об'єктів захисту та загроз в інформаційних системах.

Тема 2. Функціональні послуги захисту даних та механізми для їх реалізації.

Змістовий модуль 3. Математичні основи криптографічного захисту даних

Тема 1. Математичні задачі, на яких засновано криптографічні перетворення.

Тема 2. Поля Галуа та їх значення для теорії кодування.

Змістовий модуль 4. Криптографічні методи захисту даних

Тема 1. Криптографія та криптоаналіз.

Тема 2. Принципи побудови захищених систем зв'язку.

Змістовий модуль 5. Захист даних в IP-мережах

Тема 1. Основні компоненти систем захисту даних в IP-мережах.

Тема 2. Політика IP-безпеки.

Лабораторні заняття:

№ з/п	Назва теми
1	Ознайомлення з механізмами ідентифікації та автентифікації користувачів на рівні операційних систем
2	Практичне знайомство із засобами захисту даних від несанкціонованого доступу в сучасних операційних системах
3	Ознайомлення з механізмами для забезпечення конфіденційності та цілісності даних на рівні прикладного програмного забезпечення
4	Ознайомлення з механізмами ідентифікації та автентифікації користувачів для захисту мережевих інформаційних ресурсів від несанкціонованого доступу
5	Ознайомлення з механізмами шифрування даних та цифровим підписом
6	Практичне знайомство з протоколами, що забезпечують безпечність передавання даних
7	Принципи фільтрації IP-пакетів
8	Побудова IP-тунелів

Практичні заняття: не передбачено НП

Курсовий проект/курсова робота/РГР/Контрольна робота:

Розрахунково-графічна робота. Побудова структурної схеми критеріїв оцінки захисту даних для заданих рівнів гарантії в умовах довірчої або адміністративної конфіденційності та цілісності.

1. Доповнити задані для свого варіанту завдання до курсової роботи критерії оцінки захисту даних необхідними умовами згідно нормативному документу НД ТЗІ 2.5-004-99.

2. Зобразити структурну схему критеріїв для свого варіанту завдання.

3. Описати вимоги до архітектури КЗЗ, керуючись пунктом 10.1 Нормативного документу НД ТЗІ 2.5-004-99.

4. Описати вимоги до середовища розробки КЗЗ, керуючись пунктом 10.2 Нормативного документу НД ТЗІ 2.5-004-99

5. Описати вимоги до послідовності розробки КЗЗ, керуючись пунктом 10.3 Нормативного документу НД ТЗІ 2.5-004-99

6. Описати вимоги до середовища функціонування КЗЗ, керуючись пунктом 10.4 Нормативного документу НД ТЗІ 2.5-004-99

Самостійна робота студента (СРС):

№ з/п	Назва теми
1	Законодавство України про захист даних в інформаційних системах..
2	Нормативні документи Служби спеціального зв'язку і захисту інформації щодо технічного захисту інформації.
3	Криптографічний захисту інформації.

18) Основна література:

1. НД ТЗІ 1.5-002-2012. Класифікатор засобів технічного захисту інформації. Адміністрація Держспецзв'язку, 2012.
2. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. – Чинний з 01.01.1997.
3. Вишняков В.М. Захист інформації в комп'ютерних системах. Навчальний посібник. – К.: КНУБА, 2022. – 128 с.
4. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 14 с.
5. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 53 с.

19) Додаткова література:

1. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 24 с.
2. Вишняков В.М. Принципи побудови комп'ютерних мереж. Навчальний посібник. – К.: КНУБА, 2022. – 128 с.
<http://library.knuba.edu.ua>

20) Система оцінювання навчальних досягнень (розподіл балів):

Поточне оцінювання					РГР	Сума
Змістові одулі						
1	2	3	4	5		
14	14	14	14	14	30	100

21) Умови допуску до підсумкового контролю:

- відвідування лекцій;
- виконання лабораторних робіт;
- виконання РГР;
- 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:

<https://org2.knuba.edu.ua/course/view.php?id=263>