

Назва курсу	«Безпека хмарних сервісів»
Викладач (-і)	Івасьєв Степан Володимирович
Профайл викладача (-ів)	http://www.wunu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
Контактний тел.	+380352-475050 ext. 56501
E-mail:	isv@wunu.edu.ua

1. Анотація до курсу. Завданням дисципліни «Безпека хмарних сервісів» є здобуття студентами загальних теоретичних та практичних знань у галузі створення хмарних сервісів та використання хмарних технологій при розробці програмного забезпечення та наукових досліджень. Надання оцінки і рекомендацій, щодо безпеки цих сервісів. Проектування захищених сховищ даних.

2. Мета та цілі курсу.

Метою вивчення дисципліни «Безпека хмарних сервісів» є формування у студентів достатньо широкої підготовки в галузі захисту хмарних сховищ даних, ознайомлення із загальною концепцією розподілених баз даних як необхідного елементу сучасних інформаційних технологій, висвітлення теоретичних та організаційно-методичних питань розробки, функціонування та захисту хмарних сервісів, вивчення конкретних систем управління хмарними сховищами даних, набуття навиків практичної роботи по проектуванню захищеної розподіленої бази даних, її створенні, управлінню хмарними сервісами, подальшу можливість використання нових принципів роботи з даними та їхнього захисту від можливих кібератак.

3 Загальна інформація про дисципліну

Ступінь вищої освіти	бакалавр
Освітня програма	Технології IoT
Курс (рік навчання)	4
Семестр	7
Нормативна \ вибіркова	вибіркова
Загальна кількість год/ кредитів	150/5

4. Перелік тем

1. Віртуалізація як основа для виникнення і широкого розповсюдження хмарних сервісів.
2. Види хмар і моделі обслуговування в хмарах. Стандарти та хмарні сервіси.
3. Системи та мережі зберігання даних як обов'язкова складова частина хмарних сервісів.
4. Платформи віртуалізації для Дата-центрів.
5. Платформи віртуалізації для віртуалізації робочих місць користувачів VDI (Virtual Desktop Infrastructure).
6. Особливості реалізації хмарних технологій.
7. Технології SAN та NAS.
8. Методи проектування хмарних сервісів та забезпечення безпеки.

5. Рекомендовані джерела інформації

1. Añel Juan A. et al. Cloud and Serverless Computing for Scientists: A Primer/ Juan A. Añel, Diego P. Montes, Javier Rodeiro Iglesias. — Springer, 2020. — 94 p.

2. Atchison L. Architecting for Scale. How to Maintain High Availability and Manage Risk in the Cloud. 2nd ed. — O'Reilly, 2020. — 257 p.
3. Benito A. Stradi-Granados. Cloud Computing for Engineering Applications. Springer, 2020. — 384 p.
4. Atrey Pradeep K., Senevirathna Kasun. SecureCSocial: Secure Cloud-Based Social Network. World Scientific, 2020. — 160 p.
5. Gai Silvano. Building a Future-Proof Cloud Infrastructure: A Unified Architecture for Network, Security, and Storage Services. Addison Wesley, 2020. — 343 p.
6. Vacca John R. Cloud Computing Security: Foundations and Challenges. 2nd Edition. — CRC Press, 2021. — 522 p.

6. Система оцінювання та вимоги.

Підсумковий бал (за 100-бальною шкалою) з дисципліни “Безпека хмарних сервісів” визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3
40 %	40 %	5%	15%
Поточне оцінювання	Модульний контроль 1	Тренінг	Самостійна робота.
Середнє арифметичне з оцінок, отриманих за виконання лабораторних робіт	Оцінка за контрольну модульну роботу	Оцінка за виконання завдання тренінгу	Оцінка за виконання завдання самостійної роботи

Будь-яке завдання, за яке студент отримав оцінку, яка його не задовольняє, може бути повторно перездано протягом наступних двох тижнів.

Незадовільну оцінку за заліковий модуль студент може перездати до здачі наступного модуля.

Шкала оцінювання

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60–64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)
1–34		F (незадовільно з обов'язковим повторним курсом)

7. Навчальні ресурси

№	Найменування
1.	Обладнання: проектор, комп'ютери з доступом до мережі Інтернету.
2.	Програмне забезпечення: Доступ до наукометричних баз: Web of Science, Scopus, Ubuntu server

8. Політики курсу.

Академічна доброчесність. Дотримання академічної доброчесності студентами передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використанні методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадкування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідомо зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.