Силабус курсу

БЕЗПЕКА ХМАРНИХ СЕРВІСІВ

Ступінь вищої освіти – бакалавр
Галузь знань – 01 Освіта / Педагогіка
Спеціальність – 015 Професійна освіта (за спеціалізаціями)
Спеціалізація – 015.39 Цифрові технології
Освітньо-професійна програма:
“Професійна освіта (Цифрові технології)”

Рік навчання: IV **Семестр:** VIII

Кількість кредитів: 5 **Мова викладання:** українська

Керівник курсу

ПІП к.т.н., доцент Івасьєв Степан Володимирович
Контактна інформація isv@wunu.edu.ua

Опис дисципліни

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.

Структура курсу

№	Тема	Результати навчання	Завдання
1	Віртуалізація як основа для виникнення і широкого розповсюдження хмарних сервісів.	Знати сутність віртуалізації, роль гіпервізора, відмінність між фізичними й віртуальними ресурсами та чому саме віртуалізація стала базою для хмарних обчислень. Вміти пояснювати, як віртуалізація серверів, сховищ і мереж дозволяє ефективніше використовувати ресурси та централізувати контроль безпеки. Розуміти, як ізолювання віртуальних машин підвищує безпеку та водночас створює нові виклики (атаки на гіпервізор, міжвіртуальні витоки).	Тести, питання
2	Види хмар і моделі обслуговування в хмарах. Стандарти та хмарні сервіси.	Знати класифікацію хмарних розгортань (публічна, приватна, гібридна, community cloud) та моделі обслуговування (IaaS, PaaS, SaaS), а також базові стандарти й рекомендації з безпеки (ISO/IEC 27017, 27018, NIST). Вміти описувати розподіл зон відповідальності за безпеку між провайдером і споживачем у різних моделях сервісів та оцінювати ризики для даних і додатків. Розуміти, як вибір моделі хмарного сервісу впливає на політику доступу, шифрування, аудит та відповідність регуляторним вимогам.	Тести, питання

3	Системи та мережі зберігання даних як обов'язкова складова частина хмарних сервісів.	Знати основні підходи до зберігання даних у хмарі: DAS, NAS, SAN, об'єктні сховища та їхні особливості з точки зору доступності, масштабованості й безпеки. Вміти пояснювати ризики централізованих систем зберігання (несанкціонований доступ, масові витоки даних, збої) та базові заходи їхнього захисту (сегментація, шифрування, контроль доступу, резервування). Розуміти, що надійна інфраструктура зберігання є критичною для безпечної роботи хмарних сервісів і впливає на виконання вимог до конфіденційності та цілісності.	Тести, питання
4	Платформи віртуалізації для Дата-центрів.	Знати основні платформи віртуалізації дата-центрів (VMware vSphere, Hyper-V, KVM та ін.), їхню типову архітектуру та ключові засоби безпеки (ізоляція ВМ, мережеві політики, рольове керування доступом). Вміти описувати, як на рівні платформи реалізуються оновлення, патч-менеджмент, моніторинг подій безпеки та резервне копіювання віртуальних ресурсів. Розуміти потенційні вектори атак на інфраструктуру віртуалізації (компрометація консолі керування, гіпервізора, мережі управління) та принципи їх мінімізації.	Тести, питання
5	Платформи віртуалізації для віртуалізації робочих місць користувачів VDI (Virtual Desktop Infrastructure).	Знати принципи роботи VDI, відмінність між традиційними робочими місцями та віртуальними десктопами, а також типові моделі розгортання (persistent/non-persistent). Вміти пояснювати переваги VDI з точки зору безпеки (централізоване зберігання даних, уніфіковані політики, контроль доступу, зменшення ризиків втрати пристрою) та типові заходи захисту (MFA, умовний доступ, моніторинг активності). Розуміти, як VDI інтегрується з хмарною інфраструктурою та які додаткові ризики виникають при віддаленому доступі користувачів.	Тести, питання
6	Особливості реалізації хмарних технологій.	Знати архітектурні особливості хмарних платформ (багатокористувацькість, еластичність, самообслуговування, автоматизоване масштабування) та їхній вплив на модель загроз. Вміти виділяти специфічні ризики хмарних середовищ: спільне використання ресурсів, можливість «витоку» між орендарями, залежність від провайдера, складність контролю фізичного рівня. Розуміти, як за допомогою сегментації, шифрування, журналювання, zero-trust-підходу та політик доступу компенсувати ці ризики й забезпечити прийнятний рівень безпеки.	Тести, питання
7	Технології SAN та NAS.	Знати відмінності між SAN (Storage Area Network) та NAS (Network Attached Storage), їх архітектуру, типові протоколи та сценарії використання в хмарних дата-центрах. Вміти пояснювати, які загрози характерні для SAN/NAS (несанкціонований доступ, перехоплення трафіку, збої в доступі до масивів) та які організаційні й технічні заходи потрібні	Тести, питання

		для їхнього захисту (VLAN, ACL, шифрування, розмежування прав адміністраторів). Розуміти, як вибір між SAN і NAS та їх конфігурація впливають на відмовостійкість, продуктивність і безпеку хмарних сервісів.	
8	Методи проектування хмарних сервісів та забезпечення безпеки.	Знати базові принципи secure-by-design для хмарних сервісів: моделювання загроз, мінімізація поверхні атаки, принцип найменших привілеїв, сегментація, шифрування та аудит. Вміти враховувати вимоги кібербезпеки на етапах проєктування хмарного рішення: визначати критичні активи, обирати механізми автентифікації, управління ключами, резервування й відновлення, відповідність стандартам і законодавству. Розуміти, що безпека хмарних сервісів є безперервним процесом, який включає оцінку вразливостей, моніторинг, реагування на інциденти та регулярний перегляд архітектурних рішень.	Тести, питання

Літературні джерела

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. Atrey Pradeep K., Senevirathna Kasun. SecureCSocial: Secure Cloud-Based Social Network. World Scientific, 2020. — 160 p.
3. Atchison L. Architecting for Scale. How to Maintain High Availability and Manage Risk in the Cloud. 2nd ed. — O'Reilly, 2020. — 257 p.
4. Benito A. Stradi-Granados. Cloud Computing for Engineering Applications. Springer, 2020. — 384 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.

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності. Списування під час проведення контрольних за ходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування тощо) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Політика щодо визнання результатів навчання

Відповідно до «Положення про визнання в Західноукраїнському національному університеті результатів попереднього навчання» (https://www.wunu.edu.ua/pdf/pologenya/Polozhennya_ruzult_poper_navch.pdf) здобувачам вищої освіти може бути зараховано результати навчання

(неформальної/інформальної освіти, академічної мобільності тощо) на підставі підтвердних документів (сертифікати, довідки, документи про підвищення кваліфікації тощо). Рішення про зарахування здобувачу результатів (певного освітнього компонента в цілому, або ж окремого виду навчальної роботи за таким освітнім компонентом) приймається уповноваженою Комісією з визнання результатів навчання за процедурою, визначеною вищезазначеним положенням.

Оцінювання

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**	**Модуль 4**
20 %	**20%**	**20 %**	**20%**	**5 %**	**15 %**
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінг	Самостійна робота
Оцінка визначається як середнє арифметичне з отриманих оцінок за перший змістовий модуль	Виконання модульного завдання	Оцінка визначається як середнє арифметичне з отриманих оцінок за другий змістовий модуль	Виконання модульного завдання	Оцінка за виконання завдання	Оцінка за виконання самостійного завдання

Шкала оцінювання

За шкалою ЗУНУ	**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)