Силабус освітнього компонента
Програма навчальної дисципліни

Безпека хмарних технологій

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
6

Мова викладання
Українська

Викладачі, розробники

ПОГАСІЙ Сергій Сергійович
Serhii.Pohasii@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Гарант освітньо-науової програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.

Детальніше про викладача на сайті кафедри

ДЖЕНЮК Наталія Володимирівна

nataliia.dzheniuk@khpi.edu.ua

Доцент кафедри кібербезпеки НТУ "ХПІ".

Кількість публікацій: понад 31, з них патентів на корисну модель 2, понад 13 наукових праць.
Фахівець з комп'ютерних мереж Cisco, кібербезпеки, інтернету речей, захисту мереж та аналітики вторгнень до мережі. Провідний лектор з дисциплін: «Безпека хмарних технологій».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека хмарних технологій" є вибірковою навчальною дисципліною. В курсі розглядаються методи та засоби забезпечення безпеки інформації та хмарних інформаційних технологій, що використовуються для її обробки.

Мета та цілі дисципліни

Формування системи знань студентів в області класичних прийомів безпеки для сьогоднішніх хмарних проблем безпеки. Забезпечення безпеки веб-сервісів та вирішення проблем, що виникають під час його вдосконалення. Аналіз останніх вразливостей хмарної безпеки, використовуючи стандартні, систематичні методи. Створення власних прикладів веб-служб та рішень безпеки для них.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 12 год., лабораторні роботи – 24 год., самостійна робота – 84 год.

Передумови вивчення дисципліни (пререквізити)

Технології програмування, Комп'ютерні мережі, Основи кібербезпеки.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до хмарних обчислень. Розгляд предмета та завдань дисципліни, визначення та еволюція хмарних обчислень, їхні переваги й недоліки, класифікація типів хмар, основні постачальники послуг та еталонна архітектура.	2
Тема 2. Елементний базис хмарних обчислень. Основи віртуалізації, типи гіпервізорів, контейнеризація та її інструменти (Docker, Kubernetes), роль віртуальних машин і контейнерів у побудові хмарних середовищ.	2
Тема 3. Моделі хмарних обчислень і моделі розгортання. Порівняння IaaS, PaaS, SaaS, FaaS; розгортання приватних, публічних і гібридних хмар; використання хмар для Big Data та високопродуктивних обчислень.	2
Тема 4. Безпека у хмарних сервісах. Основи забезпечення безпеки даних у хмарному середовищі, підходи до автентифікації, авторизації, захисту даних і управління доступом.	2
Тема 5. Загрози у хмарних обчисленнях та методи їхнього подолання. Аналіз ключових загроз, вразливостей і атак у хмарах, методи виявлення інцидентів та інструменти захисту.	2
Тема 6. Аналіз захищеності хмарних середовищ. Порівняння рівня безпеки сервісів Google Apps та Microsoft Office 365, оцінка ризиків та особливості захисту даних у різних провайдерів.	2
Загальна кількість годин	**12**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Огляд надавачів хмарних сервісів. Ознайомлення з основними провайдерами хмарних послуг (Google Cloud, Microsoft Azure, AWS), їхніми можливостями та сервісами.	3	0,1
Тема 2. Основні моделі надання хмарних послуг та їх реалізація. Вивчення моделей IaaS, PaaS, SaaS, FaaS, приклади їх реалізації на практиці та порівняння функціональності.	3	0,1
Тема 3. Захист даних в хмарах. Основи безпеки хмарних даних, шифрування, автентифікація та управління доступом у хмарних середовищах.	3	0,1
Тема 4. Хмарні сервіси Google. Захист Google Docs/Google Drive. Практичне вивчення захисних механізмів Google Docs і Google Drive, налаштування доступу та безпечного обміну файлами.	3	0,1
Тема 5. Хмарні сервіси Microsoft. Захист OneDrive. Ознайомлення з методами захисту файлів та даних у OneDrive, налаштування прав доступу та політик безпеки.	3	0,1
Тема 6. Хмарні сервіси Microsoft. Захист Microsoft 365 Online. Аналіз безпечної роботи з Microsoft 365 Online, управління	3	0,1

користувачами, контроль доступу та захист корпоративних даних.		
Тема 7. Налаштування середовища розробки Microsoft Azure. Практична робота з Microsoft Azure, створення середовищ розробки, управління ресурсами та інтеграція сервісів.	3	0,1
Тема 8. Захист бази даних SQL Microsoft Azure. Методи захисту SQL-баз даних у хмарі Azure, шифрування даних, налаштування ролей і політик доступу.	3	0,1
Загальна кількість годин	**24**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Елементний базис хмарних обчислень. Основи віртуалізації, типи гіпервізорів, контейнеризація та її інструменти (Docker, Kubernetes), а також роль віртуальних машин і контейнерів у побудові хмарних середовищ.	0,2
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу, підготовка до лабораторних занять, контрольних робіт та екзамену.

Опрацювання теоретичного матеріалу

Теми самостійного вивчення	Кількість годин
Тема 1. Історія та еволюція хмарних обчислень. Вивчення розвитку хмарних технологій, ключових етапів і впливу на IT-індустрію.	8
Тема 2. Архітектура хмарних сервісів. Огляд компонентів хмарних платформ, еталонна архітектура та взаємодія сервісів.	8
Тема 3. Моделі розгортання хмар (приватні, публічні, гібридні). Порівняння моделей розгортання, їх переваг, недоліків та сфер застосування.	8
Тема 4. Моделі надання послуг (IaaS, PaaS, SaaS, FaaS). Аналіз різних сервісних моделей та практичні приклади використання.	8
Тема 5. Віртуалізація та гіпервізори. Основи віртуалізації, типи гіпервізорів, роль у побудові хмарних середовищ.	8
Тема 6. Контейнеризація та оркестрація (Docker, Kubernetes). Принципи роботи контейнерів, управління масштабуванням та деплоєм за допомогою Kubernetes.	8
Тема 7. Безпека хмарних сервісів. Методи захисту даних, автентифікація та авторизація, управління доступом.	8

Тема 8. Аналіз загроз у хмарах. Основні види атак, вразливості хмарних систем та інструменти їхнього виявлення.	8
Тема 9. Захист корпоративних даних у Google Workspace та Microsoft 365. Практичне застосування політик безпеки, шифрування та контролю доступу.	10
Тема 10. Big Data та високопродуктивні обчислення у хмарах. Використання хмарних платформ для обробки великих обсягів даних та HPC-завдань.	10
Загальна кількість годин	**84**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

1. PaloAlto (Cloud Security Fundamentals): https://paloaltonetworksacademy.net/course/index.php.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Bhowmik S. Cloud Computing. Delhi : Cambridge University Press, 2017. 434 p. https://books.google.com.ua/books/about/Cloud_Computing.html?id=jeTFDgAAQBAJ&redir_esc=y.
2. Cloud Computing : Principles, Systems and Applications I Editors Nick Antonopoulos and Lee Gillam; second ed. Swindon : Springer International Publishing AG, 2017.410 p. https://download.e-bookshelf.de/download/0009/9634/13/L-G-0009963413-0020076340.pdf.
3. Collier M., Shahan R. Microsoft Azure Essentials - Fundamentals of Azure / second ed. Redmond : Microsoft Press, 2016. 250 p. https://books.google.com.ua/books/about/Microsoft_Azure_Essentials_Fundamentals.html?hl=el&id=EfFxBgAAQBAJ&redir_esc=y.
4. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P. https://books.google.com.ua/books/about/The_Internet_of_Things.html?id=oyyyBwAAQBAJ&redir_esc=y.
5. Аулов І.Ф., Дослідження моделі закроз ключових систем хмари та пропозиції захисту від них. Восточно-Европейский журнал передовых технологий 5/2 (77) 2015, ISSN 1729-3774, DOI: 10.15587/1729-4061.2015.50912, - С.13. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vejpte_2015_5(2)__2.
6. Войтович Н.В., Найдьонова А.В. Використання хмарних технологій Google та сервісів web 2.0 в освітньому процесі. Методичні рекомендації. – Дніпро: ДПТНЗ «Дніпровський центр ПТОТС», 2017 – 113 с. https://online.fliphtml5.com/arbd/jejq/#p=1.

Додаткова література

7. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P.
https://dl.matlabyar.com/siavash/ML/Book/Ethem%20Alpaydin-Introduction%20to%20Machine%20Learning-The%20MIT%20Press%20(2014).pdf.
8. C Nayan B. Ruparelia, Cloud Computing (MIT Press Essential Knowledge series), ASIN: B01FLE5JH8, 2016, 258 P.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Роман КОРОЛЬОВ