Силабус освітнього компонента
Програма навчальної дисципліни

Безпека хмарних технологій

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
6

Мова викладання
Українська

Викладачі, розробники

ПОГАСІЙ Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua
Кандидат економічних наук, доцент, доцент 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. 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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-9. Здатність організації реагування на загрози на об’єктах критичної інфраструктури, установах та підприємствах.
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. 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.
ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об’єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. 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.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. 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 – 24 год., лабораторні роботи – 12 год., самостійна робота – 84 год.

Передумови вивчення дисципліни (пререквізити)

Антивірусний захист інформації.

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

Теми лекційних занять

Тема 1. Вступ до хмарних обчислень.
Предмет, мета та задачі дисципліни. Програмні результати навчання. Визначення хмарних обчислень. Характеристика хмарних обчислень. Історія та еволюція хмарних обчислень. Переваги та недоліки хмарних обчислень.Типи хмарних обчислень. Варіанти використання хмарних обчислень. Хмарна економетрика. Основні постачальники хмарних послуг та їх послуги. Еталонна архітектура хмарних обчислень.
Тема 2. Елементний базис хмарних обчислень.
Поняття віртуалізації. Типи віртуалізації. Поняття гіпервізора. Типи гіпервізорів. Огляд гіпервізорів: Hyper-V, VMware, KVM. Поняття віртуального контейнера. Класифікація контейнерів. Огляд інструментів для контейнеризації: OpenVZ, LXC Linux Containers. Огляд інструменту для реалізації контейнерів на ОС Linux - Docker. Огляд інструменту для автоматизації управління контейнерами (оркестрації) - Kubernetes. Java Virtual Machine.
Тема 3. Моделі хмарних обчислень.

Інфраструктура як послуга (IaaS). Платформа як послуга (PaaS). Програмне забезпечення як послуга (SaaS). Функція як послуга (FaaS).
Тема 4. Моделі розгортання систем хмарних обчислень.
Приватна хмара (Private Cloud). Публічна хмара (Public Cloud). Гібридна хмара (Hybrid Cloud). Високопродуктивні обчислення в хмарах (HPC Cloud). Хмара великих даних (Big Data Cloud).
Тема 5. Архітектура і пропозиції від провідних компаній надання хмарних послуг.
Хмарна платформа Microsoft Azure. Хмарна платформа Amazon Web Services. Хмарна платформа IBM Cloud. Хмарна платформа Google Cloud Platform. Хмарна PaaS платформа Heroku. Хмарна IaaS платформа DigitalOcean. Локальна платформа як сервіс OpenShift Container Platform. Комплекс проектів вільного програмного забезпечення для створення інфраструктури хмарних сервісів та сховищ OpenStack..
Тема 6. Безпека у хмарних сервісах.
Тема 7. Загрози для безпеки у хмарі та пропозиції захисту від них.
Тема 8. Використання хмарного сервісу Google Apps.
Сховище Google Drive, обліковий запис, робота з таблицями та документами.
Тема 9. Захист хмарного сервісу Google Apps.
Створення сайтів на Google Sites.
Тема 10. Захист хмарного сервісу Google Apps.
Створення форми засобами Google Forms (переваги використання хмарних сервісів для створення Інтернет-опитувань).
Тема 11. Використання хмарного середовища SkyDrive (сервіс Microsoft).
Створення опитувань (переваги використання хмарних сервісів для створення Інтернет-опитувань).
Тема 12. Хмаро орієнтований пакет програм Microsoft Office 365 та робота в ньому.
Тема 13. Аналіз захищеності хмарних середовищ Google Apps та Microsoft Office 365.
Тема 14. Розгортання веб-сайту в Microsoft Azure за допомогою Служби додатків.
Тема 15. Робота з реляційними даними в Microsoft Azure.
Тема 16. Хмарна технологія для створення динамічних презентацій Prezi.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Огляд надавачів хмарних сервісів.
Тема 2. Основні моделі надання хмарних послуг та їх реалізація.
Тема 3. Захист даних в хмарах.
Тема 4. Хмарні сервіси Google. Захист Google Docs/Google Drive.
Тема 5. Хмарні сервіси Microsoft. Захист One Drive.
Тема 6. Хмарні сервіси Microsoft. Захист Microsoft 365 Online.
Тема 7. Налаштування середовища розробки Microsoft Azure.
Тема 8. Захист бази даних SQL Microsoft Azure.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
PaloAlto (Cloud Security Fundamentals)
https://paloaltonetworksacademy.net/course/index.php.

Література та навчальні матеріали

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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•залік: 40% семестрової оцінки.

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

Студент 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

28.08.2024 — Завідувач кафедри — Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП — Роман КОРОЛЬОВ