Силабус освітнього компонента
Програма навчальної дисципліни

Інформаційна безпека хмарних сервісів

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
третій (освітньо-науковий)

Тип дисципліни
Вибіркова,

Семестр
3

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів
Детальніше про викладача на сайті кафедри

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

Загальна інформація

Анотація

Вивчення дисципліни має на меті формування світогляду, розвитку інтелекту, ерудиції, формування професійних компетенцій зі спеціальності кібербезпека. Дисципліна спрямована на оволодіння новітніми технологіями забезпечення кібербезпеки у хмарних середовищах.

Мета та цілі дисципліни

Оволодіння аспірантами базовими поняттями, теоретичними знаннями та практичними навичками використання хмарних та туманних технологій в різних галузях людської діяльності, а також налаштування сервісів хмарних обчислень, проектуванні корпоративних хмарних систем та розробки програм для роботи у хмарних середовищах.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК-1.Здатність до професійного спілкування іноземною мовою.
ЗК-3. Здатність до виявлення, генерування нових ідей, дослідження та вирішення проблем за професійним спрямуванням.

Результати навчання

РН-2. Вміння вести дискусії, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами.
РН-9. Вміння та навички спілкуватися в діалоговому режимі з широкою науковою спільнотою та громадськістю в галузі наукової та/або професійної діяльності з метою обговорення дискусійних питань, результатів досліджень, узгодження дій і спільної роботи на конференціях, симпозіумах, наукових семінарах, доводити результати досліджень та інновацій до колег, публічно представляти, захищати результати своїх досліджень, обговорювати їх і дискутувати з науково-професійною спільнотою, використовувати сучасні засоби візуальної презентації результатів дослідження.
РН-14. Вміння приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 20 год., лабораторні роботи – 20 год., самостійна робота – 80 год.

Передумови вивчення дисципліни (пререквізити)

Математичні методи, моделі та інформаційні технології у наукових дослідженнях, Моделювання механізмів кібербезпеки.

Особливості дисципліни, методи та технології навчання

Аспірант зобов'язаний відвідувати всі заняття згідно розкладу, не спізнюватися. Дотримуватися етики поведінки. Працювати з навчальною та додатковою літературою, з літературою на електронних носіях і в Інтернеті. При пропуску лекційних занять проводиться усна співбесіда за темою. З метою оволодіння необхідною якістю освіти з дисципліни потрібно відвідуваність і регулярна підготовленість до занять. Без особистої присутності аспіранта підсумковий контроль не проводиться.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Розуміння захисту.
Глибинна оборона. Керування операціями з кібербезпеки. Політики, правила та стандарти безпеки.
Тема 2. Захист систем та мереж.
Фізична безпека. Безпека застосунків. Підсилення захисту мережі: служби та протоколи. Укріплення мережі: сегментація. Захист бездротових та мобільних пристроїв. Стійкість кіберзахисту. Вбудовані та спеціалізовані системи.
Тема 3. Контроль доступу.
Засоби контролю доступу. Концепції контролю доступу. Керування обліковими записами. Використання та принципи роботи AAA.
Тема 4. Списки контролю доступу.
Введення в списки контролю доступу. Застосування шаблонної маски. Налаштування ACL. Синтаксис іменованого стандартного ACL та IPv4. Застосування ACL. Пом'якшення атак за допомогою ACL. ACL та IPv6.
Тема 5. Технології брандмауера.
Захист мережі за допомогою брандмауерів. Брандмауери в проектуванні мережі.
Тема 6. Брандмауери зональної політики.
Огляд ZPF. Функціонування ZPF. Налаштування ZPF.
Тема 7. Хмарна безпека.
Віртуалізація та хмарні обчислення. Домени хмарної безпеки. Безпека хмарної інфраструктури. Безпека хмарних застосунків. Безпека хмарних даних. Захист віртуальних машин.
Тема 8. Криптографія.
Конфіденційність. Приховування даних. Цілісність і автентичність. Використання хешів. Криптографія з відкритим ключем. Центри сертифікації і довірча система PKI. Застосування та вплив криптографії.
Тема 9. Технології та протоколи.
Моніторинг поширених протоколів. Технології безпеки.
Тема 10. Дані безпеки мережі.
Типи безпеки даних. Журнали кінцевого пристрою. Мережні журнали.
Тема 11. Оцінювання сповіщень.
Джерела сповіщень. Огляд оцінки сповіщень.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Огляд надавачів хмарних сервісів. Основні моделі надання хмарних послуг та їх реалізація.
Тема 2. Хмарні сервіси Google та Microsoft. Робота з Google Docs/Google Drive, Microsoft 365 Online/One Drive.
Тема 3. Реєстрація та налаштування сервісу хмарних обчислень Google App Engine (безкоштовна пробна версія).
Тема 4. Реалізація взаємодії з хмарним сервісом на основі API Blobstore.
Тема 5. Amazon AWS. Знайомство та налаштування. Реєстрація та адміністрування сервісу хмарних обчислень Heroku.

Тема 6. Приклади використання REST API у хмарних сервісах.
Тема 7. Створення та запуск web-додатків у середовищі Docker. DockerHub.

Самостійна робота

Самостійна робота аспіранта є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи аспіранти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Аспірантам 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.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Конспект лекцій з дисципліни «Грід-системи та технології хмарних обчислень» для студентів освітніх рівнів «бакалавр», «магістр» / Укладачі : Шимчук Г.В., Маєвський О.В., Назаревич О.Б., Стадник М.А. - Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2016. – 340 с. URL: https://elartu.tntu.edu.ua/bitstream/lib/20738/1/Hrid-systemy.pdf
2. Технології WEB, GRID, CLOUD для гарантоздатних IT-інфраструктур [Текст] / За ред. В.С. Харченка, А.В. Горбенка (ред.). – Харків: Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ». – 2013. – 868 с.
3. Хмарні сервіси і технології у науковій і педагогічній діяльності : Методичні рекомендації / Ю. Г. Носенко, М. В. Попель, М. П. Шишкіна / За ред. М. П. Шишкіної. – К. : ІІТЗН НАПН України, 2016. – 73 с. URL:
https://lib.iitta.gov.ua/id/eprint/706199/1/%D0%9C%D0%95%D0%A2%D0%9E%D0%94%D0%98%D0%A7%D0%9A%D0%90-2016%20final.pdf
4. Самсонов, В. В. Методи та засоби Інтернет-технологій : навч. посіб. для студ. ВНЗ / В. В. Самсонов, А. Л. Єрохін. - Х. : Компанія СМІТ, 2008. - 264 с. URL:
https://pdf.lib.vntu.edu.ua/books/2021/Samsonov_2008_264.pdf
5. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf
6. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с. URL:
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/.pdf2.pdf

Додаткова література

7. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010. — 379 p. — (Computer Communications and Networks). — ISBN 9781849962407. URL: https://link.springer.com/book/10.1007/978-1-84996-241-4
8. Michael Crump, Chris Pietschmann, Vahe Minasyan. The Developer's Guide to Azure. Microsoft Press, A division of Microsoft Corporation One Microsoft Way, Redmond, Washington 98052-6399.
9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL:
http://monograph.com.ua/pctc/catalog/view/64/52/231-1
10. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL:
http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2

11. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. URL: http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 25% семестрової оцінки;
•самостійна робота: 35% семестрової оцінки;
•іспит: 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

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

28.08.2024 — Завідувач кафедри Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП Олександр МІЛОВ