Силабус освітнього компонента
Програма навчальної дисципліни

Архітектура корпоративних інформаційних систем

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
7

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

Загальна інформація

Анотація

Дисципліна «Архітектура корпоративних інформаційних систем» завершує цикл дисциплін по розробці, впровадженню та підтримці інформаційних систем рівня корпорацій. Студенти отримають розуміння архітектурних концепцій та інтеграції хмарних рішень, що допоможе їм стати компетентними фахівцями у сфері розробки та впровадження інформаційних систем для сучасного бізнесу.
Курс викладається практикуючем фахівцем, що зумовлює практичну спрямованість дисципліни та використання досвіду реальних проєктів IT-компанії Academy Smart.

Мета та цілі дисципліни

Формування у студентів поглиблених знань з теорії та навичок практичної розробки архітектури програмного забезпечення для великих підприємств, корпорацій та інших бізнес-структур будь-якої галузі економіки та форми власності.

Формат занять

Лекції, лабораторні роботи, самостійна робота. Підсумковий контроль — іспит.

Компетентності

КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
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-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
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-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
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 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Бази даних корпоративних інформаційних систем

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. Основні поняття архітектури корпоративних інформаційних систем
Тема 2. Моделі надання програм споживачам
Тема 3. Роль форматів обміну даними у корпоративних інформаційних системах
Тема 4. Особливості клієнт-серверної архітектури в корпоративних інформаційних системах
Тема 5. Безпека передачі даних у корпоративних інформаційних системах

Теми практичних занять

Практичні заняття в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Розгортання мікросервісної архітектури в AWS
Тема 2. Використання Firebase у корпоративних інформаційних системах
Тема 3. Використання JSON для обміну даними між сервісами

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:
CCNA2
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література

1. Richards, M., Ford N. (2020). Fundamentals of Software Architecture: An Engineering Approach. O'Reilly Media, 432 p.
https://books.google.com.ua/books?id=xa7MDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
2. Newman, S. (2021). Building Microservices: Designing Fine-Grained Systems. 2nd ed. O'Reilly Media, 616 p.
https://h.twirpx.link/file/3802294/
3. Blokdyk, G. (2011). Client Server Complete Self-Assessment Guide. 5STARCooks, 311 p.
https://books.google.com.ua/books/about/Client_Server_Complete_Self_Assessment_G.html?id=dSJb0AEACAAJ&redir_esc=y
4. Newman, S. (2019). Monolith to Microservices: Evolutionary Patterns to Transform Your Monolith. 1st ed. O'Reilly Media, 272 p.
https://www.google.com.ua/books/edition/Monolith_to_Microservices_Evolutionary_P/sIczEAAAQBAJ?hl=ru&gbpv=1&dq=Newman,+S.+(2019).+Monolith+to+Microservices:+Evolutionary+Patterns+to+Transform+Your+Monolith.+1st+ed.+O%27Reilly+Media,+272+%D1%80.&printsec=frontcover.

Додаткова література

5. Hohpe, G. (2020). The Software Architect Elevator: Redefining the Architect's Role in the Digital Enterprise. 1st ed. O'Reilly Media, 368 p.
https://www.google.com.ua/books/edition/The_Software_Architect_Elevator/X-_bDwAAQBAJ?hl=ru&gbpv=1&dq=Hohpe,+G.+The+Software+Architect+Elevator:+Redefining+the+Architect%27s+Role+in+the+Digital+Enterprise&printsec=frontcover
6. Introducing JSON. [Electronic resource]. – Access mode : https://www.json.org/json-en.html

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 30% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 20% 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

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