Силабус освітнього компонента
Програма навчальної дисципліни

Архітектура корпоративних інформаційних систем

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
7

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-наукової 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

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 заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
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.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
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 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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Основні поняття архітектури корпоративних інформаційних систем. Визначення архітектури КІС, її компоненти та вимоги до продуктивності, масштабованості й надійності.	3
Тема 2. Моделі надання програм споживачам. Розгляд моделей On-premises, SaaS, PaaS, IaaS та їх застосування у корпоративних системах.	3
Тема 3. Роль форматів обміну даними у корпоративних інформаційних системах. Стандарти обміну даними (XML, JSON, CSV) та їх значення для інтеграції корпоративних додатків.	3
Тема 4. Особливості клієнт-серверної архітектури в корпоративних інформаційних системах. Принципи побудови клієнт-серверної моделі, трирівнева архітектура, переваги й недоліки.	3
Тема 5. Безпека передачі даних у корпоративних інформаційних системах. Методи захисту даних під час передавання: шифрування, VPN, механізми аутентифікації й авторизації.	4
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1 Розгортання мікросервісної архітектури в AWS. Практичне ознайомлення з побудовою та розгортанням мікросервісної архітектури у хмарному середовищі Amazon Web Services.	4	0,1
Тема 2. Використання Firebase у корпоративних інформаційних системах. Дослідження можливостей Firebase для зберігання даних, автентифікації користувачів та інтеграції з корпоративними системами.	6	0,15
Тема 3. Використання JSON для обміну даними між сервісами. Вивчення принципів формування та обробки JSON-файлів для забезпечення взаємодії між різними сервісами корпоративної системи.	6	0,15
Загальна кількість годин	**16**	$\sum_{i=1}^{m} a_i$=0,4

Контрольні роботи

Теми контрольних робіт	Вагові

	коефіцієнти b
Тема 1. Архітектурні основи корпоративних інформаційних систем. Включає аналіз основних понять архітектури КІС, моделей надання програм (On-premises, SaaS, PaaS, IaaS) та ролі форматів обміну даними в інтеграції систем.	0,1
Тема 2. Клієнт-серверна архітектура та безпека передачі даних у корпоративних системах. Охоплює особливості клієнт-серверної архітектури, трирівневу модель та сучасні методи забезпечення безпеки передачі даних у корпоративних мережах.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи мікросервісної архітектури. Переваги та недоліки мікросервісів, порівняння з монолітними системами.	5
Тема 2. Хмарні сервіси AWS для корпоративних систем. Огляд ключових сервісів AWS (EC2, S3, Lambda, API Gateway) та їх застосування.	5
Тема 3. Оркестрація контейнерів у корпоративних системах. Використання Docker та Kubernetes для розгортання мікросервісів.	6
Тема 4. Аутентифікація та авторизація у Firebase. Механізми захисту доступу користувачів у корпоративних додатках.	6
Тема 5. Cloud Firestore та Realtime Database. Особливості роботи з базами даних у Firebase та їх інтеграція.	6
Тема 6. Принципи обміну даними у форматі JSON. Структура JSON-документів, їх переваги та застосування в інтеграції сервісів.	6
Тема 7. REST API та JSON. Роль REST API у взаємодії сервісів і використання JSON як стандарту обміну даними.	6
Тема 8. GraphQL як альтернатива REST. Порівняння підходів REST і GraphQL для корпоративних систем.	6
Тема 9. Захист даних у хмарних сервісах. Шифрування, керування ключами та безпечний обмін даними в AWS і Firebase.	6
Тема 10. Сучасні тенденції у використанні мікросервісів і хмарних технологій. Актуальні тренди: serverless-архітектура, edge-computing, інтеграція AI-сервісів.	6
Загальна кількість годин	**58**

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. Онлайн-курс CISCO «CCNA2»
https://www.netacad.com/catalogs/learn?category=course

Література, навчальні матеріали та інформаційні ресурси

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

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
0,4	0,2		0,4

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