



Силабус освітнього компонента Програма навчальної дисципліни



Розробка серверних додатків (Java Spring Boot)

Шифр та назва спеціальності

K4 – Управління інформаційною безпекою

Спеціалізація

-

Освітня програма

Управління інформаційною безпекою

Рівень освіти

Перший (бакалаврський)

Семестр

6

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Кафедра

Кібербезпеки (328)

Тип дисципліни

Вибіркова

Форма навчання

Денна

Мова викладання

Українська

Викладачі, розробники



ДУНАЄВ Сергій Владиславович

Serhii.Dunaiev@cs.khpi.edu.ua

Асистент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: 5, з них 3 статті, що реферуються у науково метричних базах Scopus. Лектор з дисциплін: "Веб-програмування" та інших у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)



ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.

Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.

Загальна інформація

Анотація

Курс "Розробка серверних додатків (Java Spring Boot)" присвячений вивченню принципів та технологій створення серверних веб-додатків на базі Java із використанням фреймворку Spring Boot. Основна увага приділяється архітектурі багатошарових додатків, розробці RESTful API, управлінню базами даних через ORM (наприклад, Hibernate), та впровадженню безпеки через такі стандарти, як OAuth 2.0 та JWT.

Мета та цілі дисципліни

Метою курсу "Розробка серверних додатків (Java Spring Boot)" є навчити студентів принципам та підходам розробки сучасних серверних додатків, що відповідають вимогам реальних проектів. Студенти отримають знання та практичні навички у створенні, налаштуванні та розгортанні серверних веб-додатків з використанням фреймворку Spring Boot, освоюють роботу з базами даних, безпекою та інтеграцією серверних рішень з іншими системами. Курс також спрямований на розвиток розуміння архітектурних шаблонів, кращих практик програмування та використання інструментів для ефективної розробки серверних частин додатків.

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.

ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

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.

РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

PH11. 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.

PH12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

PH14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

PH16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

PH17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

PH18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

PH19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

PH20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

PH21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

PH22. 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)

Іноземна мова, Основні поняття про серверні додатки.

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 проекти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до Java Spring Boot та архітектура серверних додатків. Ознайомлення з фреймворком Spring Boot, його місцем у розробці корпоративних додатків. Архітектурні підходи (моноліт, мікросервіси), концепції IoC та DI.	2
Тема 2. Розробка RESTful веб-сервісів. Принципи REST-архітектури, створення API з використанням Spring Boot. Маршрутизація запитів, обробка JSON/XML. Практика створення CRUD-операцій.	2

Тема 3. Робота з базами даних: Spring Data JPA та Hibernate. Основи ORM, взаємодія з реляційними базами даних через Spring Data JPA. Використання Hibernate для збереження та отримання даних. Налаштування репозиторіїв, запити.	2
Тема 4. Аутентифікація та авторизація: Безпека у Spring Boot. Основи безпеки веб-додатків. Використання Spring Security для аутентифікації та авторизації. Ролі користувачів, токени (JWT), інтеграція OAuth2.	2
Тема 5. Тестування серверних додатків. Види тестування: модульне, інтеграційне, навантажувальне. Використання JUnit, Mockito, Spring Boot Test. Автоматизація тестування.	2
Тема 6. Деплой серверних додатків та CI/CD. Розгортання додатків на локальних і хмарних серверах. Інструменти CI/CD (Jenkins, GitHub Actions). Контейнеризація з Docker, оркестрація з Kubernetes.	2
Загальна кількість годин	12

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Створення базового Spring Boot додатку. Ознайомлення з архітектурою Spring Boot. Створення базового проєкту, структура додатку, налаштування конфігурації та запуск першого сервісу.	4	0,1
Тема 2. Розробка RESTful API. Реалізація REST-контролерів. Обробка HTTP-запитів (GET, POST, PUT, DELETE). Формування відповідей у форматі JSON.	4	0,1
Тема 3. Інтеграція з базою даних через Spring Data JPA. Створення моделей і репозиторіїв. Виконання CRUD-операцій із використанням Spring Data JPA. Робота з H2/ MySQL базою даних.	4	0,1
Тема 4. Реалізація безпеки в Spring Boot за допомогою Spring Security. Впровадження аутентифікації та авторизації користувачів. Налаштування ролей і доступів. Реалізація захисту API.	4	0,1
Тема 5. Тестування Spring Boot додатків. Використання JUnit і Mockito для написання юніт-тестів. Тестування REST API за допомогою Postman. Перевірка працездатності сервісів.	4	0,1
Тема 6. Деплой Spring Boot додатку на хмару (Heroku або AWS). Підготовка додатку до розгортання. Використання систем CI/CD. Деплой у хмарне середовище, перевірка працездатності додатку онлайн.	4	0,1
Загальна кількість годин	24	$\sum_{i=1}^n a_i = 0,6$

Контрольні роботи

За наявності

Тема 1. Розробка та захист RESTful веб-сервісу з використанням Spring Boot.

0,4

У рамках контрольної роботи студент повинен створити серверний додаток на базі Spring Boot із реалізацією REST API.

Загалом

$$\sum_{i=1}^m b_i = 0,4$$

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. Мікросервісна архітектура та Spring Cloud.

8

Основи побудови мікросервісів, використання Eureka, Config Server, API Gateway.

Тема 2. Обробка асинхронних задач у Spring Boot.

8

Використання @Async, черги повідомлень (RabbitMQ, Kafka).

Тема 3. Spring Boot і GraphQL.

8

Розробка GraphQL API та відмінності від REST.

Тема 4. Spring Boot Actuator та моніторинг.

8

Збір метрик, управління станом додатку, інтеграція з Prometheus/Grafana.

Тема 5. Spring Batch для обробки великих обсягів даних.

8

Створення пакетних завдань, сценарії ETL.

Тема 6. Docker та контейнеризація Spring Boot додатків.

8

Створення Docker-образів, робота з Docker Compose.

Тема 7. Spring Boot і Kubernetes.

8

Розгортання додатків у Kubernetes, масштабування та управління.

Тема 8. Кешування у Spring Boot.

8

Робота з Redis, використання @Cacheable, оптимізація продуктивності.

Тема 9. Робота з файлами та завантаження медіа у Spring Boot.

10

Обробка завантаження файлів, збереження на диск чи у хмару (AWS S3).

Тема 10. Spring Boot і WebSockets.

10

Реалізація реального часу: чати, нотифікації, push-повідомлення.

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. Онлайн-курс CISCO «Java 2»

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Craig Walls, "Spring in Action" (6th Edition)

[https://www.google.com.ua/books/edition/Spring+in+Action+Sixth+Edition/2zVbEAAAQBAJ?hl=ru&gbpv=1&dq=Craig+Walls,+%22Spring+in+Action%22+\(6th+Edition\)&printsec=frontcover](https://www.google.com.ua/books/edition/Spring+in+Action+Sixth+Edition/2zVbEAAAQBAJ?hl=ru&gbpv=1&dq=Craig+Walls,+%22Spring+in+Action%22+(6th+Edition)&printsec=frontcover)

2. Mark Heckler, "Spring Boot: Up and Running" (1st Edition)

[https://www.google.com.ua/books/edition/Spring+Boot+Up+and+Running/RQUaEAAAQBAJ?hl=ru&gbpv=1&dq=Mark+Heckler,+%22Spring+Boot:+Up+and+Running%22+\(1st+Edition\)&pg=PR4&printsec=frontcover](https://www.google.com.ua/books/edition/Spring+Boot+Up+and+Running/RQUaEAAAQBAJ?hl=ru&gbpv=1&dq=Mark+Heckler,+%22Spring+Boot:+Up+and+Running%22+(1st+Edition)&pg=PR4&printsec=frontcover)

3. Josh Long, Kenny Bastani, "Cloud Native Java"

<https://www.google.com.ua/books/edition/Cloud+Native+Java/dZAwDwAAQBAJ?hl=ru&gbpv=1&dq=Josh+Long,+Kenny+Bastani,+%22Cloud+Native+Java%22&printsec=frontcover>

Додаткова література

4. Madhusudhan Konda, "Just Spring Data Access"

<https://www.google.com.ua/books/edition/Just+Spring+Data+Access/LalyxM305ogC?hl=ru&gbpv=1&dq=Madhusudhan+Konda,+%22Just+Spring+Data+Access%22&printsec=frontcover>

5. Dan Vega, "Spring Boot Essentials" (YouTube course)

https://www.youtube.com/results?search_query=Dan+Vega+Spring+Boot+Essentials

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
0,6	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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, К, 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 БУСЕБ

30.08.2025



Гарант ОП
Роман КОРОЛЬОВ