



Силабус освітнього компонента Програма навчальної дисципліни



Розробка серверних додатків (Java Spring Boot)

Шифр та назва спеціальності

F5 – Кібербезпека та захист інформації

Спеціалізація

-

Освітня програма

Кібербезпека

Рівень освіти

Перший (бакалаврський)

Семестр

6

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Кафедра

Кібербезпеки (328)

Тип дисципліни

Вибіркова

Форма навчання

Денна, заочна

Мова викладання

Українська, англійська

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 багатoshарових 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 проєктів. 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

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

Результати навчання

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як

необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.

РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

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 проєкти, 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 IoT та DL.	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

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Розробка та захист RESTful веб-сервісу з використанням Spring Boot. У рамках контрольної роботи студент повинен створити серверний додаток на базі Spring Boot із реалізацією REST API.	0,4
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. Основи побудови мікросервісів, використання Eureka, Config Server, API Gateway.	8
Тема 2. Обробка асинхронних задач у Spring Boot. Використання @Async, черги повідомлень (RabbitMQ, Kafka).	8
Тема 3. Spring Boot і GraphQL. Розробка GraphQL API та відмінності від REST.	8
Тема 4. Spring Boot Actuator та моніторинг. Збір метрик, управління станом додатку, інтеграція з Prometheus/Grafana.	8
Тема 5. Spring Batch для обробки великих обсягів даних. Створення пакетних завдань, сценарії ETL.	8
Тема 6. Docker та контейнеризація Spring Boot додатків. Створення Docker-образів, робота з Docker Compose.	8
Тема 7. Spring Boot і Kubernetes. Розгортання додатків у Kubernetes, масштабування та управління.	8
Тема 8. Кешування у Spring Boot. Робота з Redis, використання @Cacheable, оптимізація продуктивності.	8
Тема 9. Робота з файлами та завантаження медіа у Spring Boot. Обробка завантаження файлів, збереження на диск чи у хмару (AWS S3).	10
Тема 10. Spring Boot і WebSockets. Реалізація реального часу: чати, нотифікації, push-повідомлення.	10
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%22+(6th+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](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 (Π , K , I , ...))

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 O 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)	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

Сергій ЄВСЕЄВ