МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

РОЗШИРЕНЕ АДМІНІСТРУВАННЯ СЕРВЕРНИХ СЕРВІСІВ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***другий (магістерський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***вибіркова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЄЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Алексієв В.О., д.т.н., проф. кафедри КІТ.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Рішення завдань адміністрування серверних систем для побудови засобів Інтернету речей (IoT, Internet of Things) обмежується не тільки автоматизацією на рівні DevOps щодо розгортання сервісів, а й поруч із цим характеризується комплексом дій щодо забезпечення моніторингу та налагодження взаємодії чималої кількості розподілених у просторі компонентів системи. Відповідна архітектура системи потребує застосування новітніх підходів щодо виконання завдань системного адміністратору з налагодження працездатності починаючи з окремого компоненту системи до комплексу IoT-рішення загалом.

Мета навчальної дисципліни "Розширене адміністрування серверних сервісів" є засвоєння теоретичних основ, формування умінь з розширеного адміністрування серверних сервісів та отримання знання технологій неперервної інтеграції та доставки веб-сервісів, поруч із забезпеченням безпеки відповідних операцій. Предметом дисципліни є інструментальні засоби та основи їх застосування у галузі розширеного адміністрування серверних сервісів. Об'єктом – неперервна інтеграція та доставка веб-сервісів користувачам.

Характеристика навчальної дисципліни

Курс	**1М**
Семестр	**1**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Інформаційні системи та інтернет технології	Науково-дослідна практика
Комплексні системи захисту інформації	Переддипломна практика
Знання особливостей побудови корпоративних мереж	Дипломний проект

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (інформаційних, інформаційно-телекомунікаційних, автоматизованих).	ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому ПРН-9 – проектувати, впроваджувати,

	супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства)
КФ 3. Здатність розробляти й впроваджувати систему менеджменту інформаційної безпеки та/або кібербезпеки організації, формувати стратегію і політики інформаційної безпеки різних рівнів на базі світових й вітчизняних стандартів з урахуванням кращих практик галузі інформаційних технологій та їх безпеки.	ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства) ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам),

	проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо) ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки
КФ 7. Здатність аналізувати причини та наслідки збоїв або відмов функціонування інформаційних систем, що викликані реалізацією різного класу кіберінцидентів, а також розробляти й впроваджувати методи і заходи відновлення штатного функціонування інфраструктури організації в цілому.	ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо) ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо) ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства) ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки

Програма навчальної дисципліни

Змістовий модуль 1. Основи застосування методології DevOps.

Тема 1. *Введення. Основні терміни та визначення.*
Тема 2. *Особливості побудови та розгортання сучасних веб-застосунків на базі мікросервісної архітектури. Особливості серверних платформ Windows та Linux.*
Тема 3. *Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології віртуалізації Docker.*

Змістовий модуль 2. Практика застосування та безпека мікросервісів.

Тема 4. *Поняття гнучкого (Agile) управління розробкою програмних продуктів. Основи розгортання систем CI/CD (Continuous Integration та Continuous Delivery).*
Тема 5. *Взаємодія між веб-сервісами. Інтерфейс взаємодії мікросервісів та його безпека. Інтерфейс REST та системи обміну повідомленнями MQ (Messages queue).*
Тема 6. *Технології хмарних обчислень (Cloud Computing) та мікросервіси.*
Тема 7. *Перспективи розробки веб-застосувань у сенсі залучення засобів DevOps.*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

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 проблемні лекції, презентації, бесіди, індивідуальні та групові міні-проекти.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту поставити залік, – 60 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- знати та застосовувати для рішення практичних завдань особливості побудови та розгортання сучасних веб-застосунків на базі мікросервісної архітектури. Особливості серверних платформ Windows та Linux;
- налагоджувати засоби безпеки рівня серверної інфраструктури. Розуміти особливості застосування технології віртуалізації Docker;
- мати навички працювати за методологією гнучкого (Agile) управління розробкою програмних продуктів. Орієнтуватися у сучасних технологіях розгортання систем CI/CD (Continuous Integration та Continuous Delivery);
- налагоджувати взаємодія між веб-сервісами. Знати інтерфейси взаємодії мікросервісів та забезпечувати їх безпеку. Розуміти теоретичні основи застосування інтерфейсу REST та системи обміну повідомленнями MQ (Messages queue);

- вміти обирати ефективні технології хмарних обчислень (Cloud Computing) та розгортати у середовищі хмари мікросервіси.

- формулювати прогноз щодо перспектив розробки веб-застосувань у сенсі адміністрування серверних сервісів та напрямку DevOps.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: максимальна кількість балів становить 34 (робота на лекціях – 14, контрольна робота – 20).

Лабораторні заняття: максимальна кількість балів становить 66 (робота на лабораторних заняттях – 6, захист лабораторних робіт – 60), а мінімальна – 35.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями та контрольних робіт за лабораторними роботами дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням отриманих балів у продовж семестру.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція *"Введення. Основні терміни та визначення"*	Робота на лекції	2

	Лабораторне заняття	Лабораторна робота №1 Розгортання веб-серверу у середовищі віртуальної машини. Знайомства з засобами безпеки рівня веб-сервера.	Робота на лабораторній роботі	2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Лекція	Лекція *" Особливості побудови та розгортання сучасних веб-застосунків на базі мікросервісної архітектури. Особливості серверних платформ Windows та Linux."*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №1 (продовження)	Захист лабораторних робіт № 1	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *" Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології віртуалізації Docker."*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №2. Установка та налагодження веб-серверу на базі брокера повідомлень за протоколом MQTT або ін.	Робота на лабораторній роботі	2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *" Поняття гнучкого (Agile) управління розробкою програмних продуктів. Основи розгортання систем CI/CD (Continuous Integration та Continuous*	Робота на лекції	2

		Delivery)."		
	Лабораторне заняття	Лабораторна робота №2 (продовження).	Захист лабораторної роботи № 2	15
Тема 5	***Аудиторна робота***			
	Лекція	Лекція*" Взаємодія між веб-сервісами. Інтерфейс взаємодії мікросервісів та його безпека. Інтерфейс REST та системи обміну повідомленнями MQ (Messages queue)."*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №3. Тестування роботи розподіленої системи реєстрації та обробки даних за технологією Інтернета речей (IoT).	Робота на лабораторній роботі	2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *" Технології хмарних обчислень (Cloud Computing) та мікросервіси."*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №3. (продовження)	Захист лабораторної роботи № 3	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *" Перспективи розробки веб-застосувань у сенсі залучення засобів DevOps."*	Робота на лекції	2
			Контрольна робота	20
	Лабораторне заняття	Лабораторна робота № 4. Розгортання інтелектуальної системи рівня розумного будинку. Застосування платформи IFTTT.	Захист лабораторної роботи № 4	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Рекомендована література

Основна

1. Ушакова, І. О. Проектування інформаційних систем : практикум / Ушакова І. О. – Х.: ХНЕУ ім. С. Кузнеця, 2015. – 234 с.
2. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ: навч.-метод. посіб. / В. О. Алексієв.– Х. : ХНАДУ, 2008. – 208 с.
3. Дэвис Дженнифер, Дэниелс Кэтрин. Философия DevOps. Искусство управления IT. - СПб.: Питер, 2017. - 416 с.
4. Вольф Эберхард. Continuous delivery. Практика непрерывных апдейтов. - СПб.: Питер, 2018. - 320 с.
5. Стеллман Эндрю. Постигая Agile. Ценности, принципы, методологии / Эндрю Стеллман, Дженни-фер Грин ; пер. сангл. С.Пасерба.- М.: Манн, Иванов и Фербер, 2017.— 448 с.
6. Ньюмен С. Создание микросервисов/ С.Ньюмен.–СПб.: Питер, 2016. – 304 с.
7. Таллоч Митч и команда Windows Azure. Знакомство с Windows Azure. Для ИТ-специалистов/ Таллоч М.; пер. с англ. – М.: ЭКОМ Паблишерз, 2014. — 154 с.
8. Риз Дж. Облачные вычисления: Пер. с англ. - СПб.: БХВ-Петербург, 2011. - 288 с.
9. Johansson L., Vinka. E. The optimal RabbitMQ guide. From Beginner to Advanced - An introduction to RabbitMQ and CloudAMQP. - 84codes AB, 2020. – 138 p. . [Electronic resource]. –Access mode: https://www.cloudamqp.com/rabbitmq_book_success.html
10. Maarten van SteenAndrew S. Tanenbaum. Distributed Systems. Third edition., Maarten van Steen, 2018. – p. [Electronic resource]. – Access mode: https://www.distributed-systems.net/index.php/contact/

Додаткова література та інформаційні ресурси

11. Страх и ненависть DevSecOps [Электронный ресурс] / Habr, 2019. – Режим доступа : https://habr.com/en/company/oleg-bunin/blog/448488/.
12. Настройка среды непрерывного развертывания с помощью Jenkins [Электронный ресурс] / На Лв, Чжао Чжо, Янь Чжэ, Чэнь Сяо Лун. IBM developerWorks, 2015. – Режим доступа : https://www.ibm.com/ developerworks/ru/library/d-continuous-delivery-framework-jenkins/.
13. Микрослужбы в действии: Введение в микрослужбы [Электронный ресурс] / Рик И. Осовский. IBM developerWorks, 2015. – Режим доступа : https://www.ibm.com/developerworks/ru/library/cl-bluemix-microservices-in-action-part-1-trs.
14. Распределенные базы и хранилища даннях : Электронный учебник / Н. Аносова, О. Бородин, Е. Гаврилов и др. – НОУ "ИНТУИТ" [Электронный ресурс]. – Режим доступа : http://www.intuit.ru/ studies/ courses/1145/214/info.
15. Облачные стандарты: средства взаимодействия приложений в облаке [Электронный ресурс] / Кэйн Скарлетт. IBM developerWorks, 2016. – Режим доступа : http://www.ibm.com/ developerworks/ ru/library /cl-tools-to-ensure-cloud-application-interoperability/index.html.
16. Create REST applications with the Slim micro-framework [Electronic resource] / Vikram Vaswani. IBM developerWorks, 2012. – Access mode : http://www.ibm.com/developerworks/library/x-slim-rest/.
17. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Розширене адміністрування серверних сервісів" https://pns.hneu.edu.ua/ course/view.php?id=7018.