

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

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

Микола А. АНАСІЄВ

БЕЗПЕКА СЕРВЕРНИХ СИСТЕМ

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 СВСЕВ

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

Для рішення завдань бізнесу слід застосовувати не тільки ефективні та зручні ІТ-засоби, а й приділяти велику увагу побудові контуру безпеки серверних систем. Безпека рівня серверу є необхідною складовою побудови сучасної платформи, що не є напрямком затрат для підприємства, а навпаки сприяє розвитку бізнесу та пристосування до сучасних вимог ринкової економіки. Зараз серверні ресурси підприємства скоріш за все будуть обслуговувати кластери серверних рішень, наприклад, за управління системою Kubernetes чи ін. У курсі розглядаються, як рішення рівня одного сервера та декількох сервісів, а також системи корпоративного рівня та рівня приватної хмари (Cloud Computing).

Мета навчальної дисципліни “Безпека серверних систем” є засвоєння теоретичних основ, формування умінь з організації безпеки серверних систем та отримання знання технологій побудови систем рівня сучасного центру обробки даних. Предметом дисципліни є інструментальні засоби та основи їх застосування у галузі адміністрування серверних систем. Об’єктом – виконання процесів налагодження та адміністрування серверних систем, а також виконання завдань їх підтримки та супроводження.

Характеристика навчальної дисципліни

Курс	1М
Семестр	2
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 8. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю функціонування інформаційно-комунікаційних систем та технологій (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	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 частотої 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-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)

	<p>відкритих та закритих систем, тощо)</p> <p>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.</p> <p>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</p> <p>ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки</p>
--	--

Програма навчальної дисципліни

Змістовий модуль 1. Основи побудови серверних систем рівня сучасного центру обробки даних.

Тема 1. *Введення. Основні терміни та визначення.*

Тема 2. *Особливості побудови сучасного центру обробки даних. Безпека серверних платформ Windows та Linux.*

Тема 3. *Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології приватної хмари OpenStack. Засоби безпеки рівня серверу.*

Змістовий модуль 2. Практика адміністрування серверних систем на рівні центру обробки даних.

Тема 4. *Технологія Kubernetes для ефективного управління контейнерами віртуальних машин та відповідні засоби безпеки.*

Тема 5. *Застосування засобів автоматизації Ansible для розгортання серверних систем.*

Тема 6. *Технології хмарних обчислень Red Hat OpenShift.*

Тема 7. *Перспективи розвитку засобів безпеки у сучасному центрі обробки даних.*

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 особливості побудови сучасного центру обробки даних та застосовувати для рішення практичних завдань засоби безпеки серверних платформ Windows та Linux;

- використовувати засоби безпеки рівня серверної інфраструктури. Мати знання технології приватної хмари OpenStack. Вміти виконувати оцінку ризику вразливостей, обирати відповідні рішення протидії та застосовувати засоби безпеки рівня серверу;

- орієнтуватися у технології Kubernetes для ефективного управління контейнерами віртуальних машин та знати відповідні засоби безпеки для систем кластерів віртуальних контейнерів;

- застосовувати засоби автоматизації Ansible для розгортання серверних систем;

- мати навички працювати з технологією хмарних обчислень Red Hat OpenShift;

- формулювати прогноз щодо перспектив розвитку засобів безпеки у сучасному центрі обробки даних.

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 лекції – 14, контрольна робота – 20).

Лабораторні заняття: максимальна кількість балів становить 66 (виконання лабораторних робіт – 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 цей 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	Мак 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 з засобами контейнерної віртуалізації. Знайомства з засобами безпеки рівня веб-сервера та системи Docker.	Виконання лабораторної роботи	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 сучасного центру обробки даних. Безпека 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	Форми та види навчання	Форми оцінювання	Мак бал	
Тема 3	Аудиторна робота			
	Лекція	Лекція "Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології приватної хмари OpenStack. Засоби безпеки рівня серверу."	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №2. Знайомство з засобами моніторингу серверних систем.	Виконання лабораторної роботи	2
Тема 3	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 "Технологія Kubernetes для ефективного управління контейнерами віртуальних машин та відповідні засоби безпеки."	Робота на лекції	2
Тема 4	Лабораторне заняття	Лабораторна робота №2 (продовження).	Захист лабораторної роботи № 2	15
Тема 5	Аудиторна робота			
	Лекція	Лекція "Застосування засобів автоматизації Ansible для розгортання серверних систем."	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №3. Автоматизація розгортання серверних систем. Вбудова засобів безпеки рівня серверу у процесі автоматичного розгортання серверного рішення рівня кластеру віртуальних контейнерів.	Виконання лабораторної роботи	2
Тема 5	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	Форми та види навчання		Форми оцінювання	Мак бал
Тема 6	Аудиторна робота			
	Лекція	Лекція " Технології хмарних обчислень Red Hat OpenShift."	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 розвитку засобів безпеки у сучасному центрі обробки даних."	Робота на лекції	2
			Контрольна робота	20
	Лабораторне заняття	Лабораторна робота № 4. Розгортання інтелектуальної системи управління кластерами контейнерів Red Hat OpenShift.	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. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с.
2. Ушакова, І. О. Проектування інформаційних систем : практикум / Ушакова І. О. – Х.: ХНЕУ ім. С. Кузнеця, 2015. – 234 с.
3. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ: навч.-метод. посіб. / В. О. Алексієв.– Х. : ХНАДУ, 2008. – 208 с.
4. Девіс Дженніфер, Деніелс Кетрін. Філософія DevOps. Искусство управления ИТ. - СПб.: Питер, 2017. - 416 с.
5. Вольф Эберхард. Continuous delivery. Практика непрерывных апдейтов. - СПб.: Питер, 2018. - 320 с.
6. Таллоч Митч и команда Windows Azure. Знакомство с Windows Azure. Для ИТ-специалистов/ Таллоч М.; пер. с англ. – М.: ЭКОМ Паблицерз, 2014. — 154 с.
7. Риз Дж. Облачные вычисления: Пер. с англ. - СПб.: БХВ-Петербург, 2011. - 288 с.

Додаткова література

8. David Rensin. Kubernetes. Scheduling the Future at Cloud Scale, O'Reilly Media,

2015. – 138 p. [Electronic resource]. –Access mode: <https://www.openshift.com/resources/ebooks/kubernetes-ebook>.

9. Andrew Moore. OpenStack For Dummies. vScaler Limited Edition., John Wiley & Sons, Chichester, West Sussex, 2017. – 53 p. [Electronic resource]. – Access mode: <https://www.vscaler.com/openstack-for-dummies/>.

10. Jason Dobies, Joshua Wood. Kubernetes Operators., Red Hat, O’Reilly Media, 2020. – [Electronic resource]. –Access mode: https://www.redhat.com/cms/managed-files/cl-oreilly-kubernetes-operators-ebook-f21452-202001-en_2.pdf.

11. Stefano Picozzi, Mike Hepburn, Noel O’Connor. DevOps with OpenShift, Red Hat, O’Reilly Media, 2017. – 148 p. [Electronic resource]. –Access mode: <https://www.openshift.com/resources/ebooks/devops-with-openshift/>.

Інформаційні ресурси

12. Страх и ненависть DevSecOps [Электронный ресурс] / Habr, 2019. – Режим доступа : <https://habr.com/en/company/oleg-bunin/blog/448488/>.

13. Распределенные базы и хранилища данных : 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>.

14. 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-interopability/index.html>.

15. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Безпека серверних систем" <https://pns.hneu.edu.ua/course/view.php?id=7213>.