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

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

РОЗШИРЕНА МЕРЕЖЕВА ТА ХМАРНА БЕЗПЕКА

робоча програма навчальної дисципліни

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

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

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

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

Мережева та хмарна безпека є основною складовою побудови IT-інфраструктури будь-якої сучасної організації чи виробництва. Зараз великі корпоративні мережі поєднують, як наявні ресурси IT-підрозділу, так й ресурси, що орендуються як хмарні сервіси (Cloud Computing). Тому актуальною стає розширена мережева та хмарна безпека, що поєднує локальні засоби безпеки й відповідні ресурси та системні рішення захисту у хмарі.

У дисципліні розглядаються питання забезпечення кібербезпеки рівня окремого підприємства чи організації та засоби, які є складовими сервісу хмарних обчислень. Для отримання студентами практичного досвіду передбачено застосування ресурсів світової програми AWS Educate (https://aws.amazon.com/education/awseducate/). Це дозволить студентам оволодіти навичками роботи у реальному оточенні з засобами організації безпеки хмарного сервісу. Застосування ресурсів рівня локальної обчислювальної мережі ХНЕУ ім. С. Кузнеця та середовища віртуалізації Oracle VM VirtualBox забезпечує вивчення технічних засобів протидії кіберзагрозам на рівні приватної хмари та окремих серверних ресурсів.

Метою викладання дисципліни є формування теоретичних знань та практичних умінь побудови контуру безпеки IT-ресурсів підприємства, компанії чи організації на рівні засобів та технологій розширеної мережевої та хмарної безпеки.

Результатами вивчення даної дисципліни є придбання навичок з проектування та створення обчислювальної мережі для підприємств та організацій незалежно від їх розміру, з врахуванням адекватних засобів безпеки та побудови ефективної IT-інфраструктури. Також студенти мають розуміти та отримати комплекс практичних навичок щодо пошуку та побудови контуру захисту обчислювальної мережі.

Характеристика навчальної дисципліни

Курс	**1 М**
Семестр	**1**
Кількість кредитів ECTS	**3**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Інформаційні системи та інтернет технології	Науково-дослідна практика
Введення в мережі	Переддипломна практика
Комплексні системи захисту інформації	Дипломний проект

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
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. КФ-4. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки	ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; 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-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах

інформаційних технологій (в т.ч. хмарних технологій та додатків), а також безпеки бізнес/операційних процесів з метою забезпечення функціонування інформаційно-комунікаційних систем згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ-5. Здатність розробляти та впроваджувати систему управління інформаційними активами (ресурсами), володіти методами теорії ризик менеджменту та процесних моделей, розробляти моделі загроз й моделі порушника, а також забезпечувати штатне функціонування системи інформаційної безпеки та/або кібербезпеки організації з використанням сучасних технологій. КФ-6. Здатність планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів установи, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	інформаційної та/або кібербезпеки; 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-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); 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-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-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-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; 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-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві

Програма навчальної дисципліни

Змістовий модуль 1. Основи безпеки рівня веб-серверу.

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

Тема 2. *Особливості сучасних корпоративних мереж.*

Тема 3. *Засоби безпеки рівня корпоративної мережі.*

Тема 4. *Приватна хмара на основі технологій OpenShift та OpenStack й Proxmox VE.*

Змістовий модуль 2. Практика забезпечення безпеки веб-ресурсів.

Тема 5. *Публічні хмарні сервіси Amazon AWS, Microsoft Azure та Google Cloud Platform.*

Тема 6. *Побудова гібридної хмари.*

Тема 7. *Перспективи синергічного поєднання засобів безпеки рівня корпоративної мережі та хмарного сервісу.*

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 проєкти, майстер-класи.

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 – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, 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 сучасних корпоративних мереж, що будуються на платформі

Wondows Server та Linux;

– вміти налагоджувати та застосовувати на практиці засоби безпеки рівня корпоративної мережі;

– орієнтуватися у технологіях побудови та супроводження приватної хмари на основі технологій OpenShift, OpenStack та Proxmox VE;

– знати особливості публічних хмарних сервісів Amazon AWS, Microsoft Azure та Google Cloud Platform;

– розуміти особливості побудови гібридної хмари;

– вміти надати прогноз щодо перспективи синергічного поєднання засобів безпеки рівня корпоративної мережі та хмарного сервісу.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лекційні заняття: максимальна кількість балів становить 2,5 (робота на лекції).

Лабораторні заняття: максимальна кількість балів становить 57,5 (виконання лабораторних робіт – 2,5, захист лабораторних робіт – 40, контрольні роботи – 15), а мінімальна – 25.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням іспиту.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни. Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню структурної схеми побудови контуру безпеки корпоративної мережі компанії, виконання його оцінюється 10 балами; третє завдання – рішення евристичного завдання щодо планування розгортання контуру безпеки рівня хмарного сервісу, виконання його оцінюється 10 балами.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та 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. Особливості сучасних корпоративних мереж."*	Робота на лекції	0,5
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція *"Особливості сучасних корпоративних мереж."*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №1 *"Моделювання окремих сервісів корпоративних мереж та визначення їх засобів безпеки."*	Робота на лабораторній роботі	0,5
			Контрольна робота 1	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 3	***Аудиторна робота***			
	Лекція	Лекція *"Засоби безпеки рівня корпоративної мережі."*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №2 *"Моделювання побудови приватного хмарного сервісу. Визначення засобів безпеки приватної хмари"*	Робота на лабораторній роботі	0,5
			Захист лабораторної роботи № 1	10
	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 *" Приватна хмара на основі технологій OpenShift та OpenStack й Proxmox VE."*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №3 *"Робота з ресурсами публічного хмарного сервісу. Застосування політик безпеки."*	Робота на лабораторній роботі	1
			Захист лабораторної роботи № 2	10
	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 5	***Аудиторна робота***			
	Лекція	Лекція *"Публічні хмарні сервіси Amazon AWS, Microsoft Azure та Google Cloud Platform"*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №4. *"Огляд сучасних рішень мережевого апаратного устаткування. Визначення засобів безпеки як складової програмно-апаратного рішення"*	Робота на лабораторній роботі	0,5
			Захист лабораторної роботи № 3, 4	20
			контрольна робота 2	10
	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. Підготовка до екзамену		
Екзамен				40

Рекомендована література

Основна

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, 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. Глоба Л.С. Розробка інформаційних ресурсів та систем : у 2 т. / Л.С. Глоба // Київ – Т. 1 : Розподілені системи. Поняття розподіленого середовища, Зв'язок, Процеси, Іменування, Синхронизація. – 2013. – 378 с. [Електронний ресурс]. – Режим доступу: http://www.its.kpi.ua/ subjects/56/ Documents/ Глоба книга Том1.pdf.

4. Евсеев С. П. Концептуальная синергетическая модель оценки безопасности банковской безопасности в организациях банковского сектора / С. П. Евсеев, О. Г. Король // Матеріали Міжнародної науково-практичної конференції" Проблеми і перспективи розвитку IT-індустрії ": тези доповідей, 20–21 квітня 2017 р. – Х. : ХНЕУ імені Семена Кузнеця, 2017. – С. 51.

5. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ : навч.-метод. посіб. / В. О. Алексієв.– Х. : ХНАДУ, 2008. – 208 с.

6. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. – СПб.: Питер, 2020. – 448 с.

Додаткова

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. Proxmox VE Admin Guide for 6.x, 2020. – 462 p. [Electronic resource]. –Access mode: https://www.proxmox.com/en/downloads/item/proxmox-ve-admin-guide-for-6-x

10. AWS Security Incident Response Guide, 2020. - 65 p. [Electronic resource]. –Access mode: https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/ welcome.html? did=wp_card&trk=wp_card

Інформаційні ресурси

11. Создание и развертывание масштабируемого приложения для управления контактами в облаке [Электронный ресурс] / Викрам Васвани. IBM developerWorks, 2016. – Режим доступа : http://www.ibm.com/ developerworks/ru/ library/ cl-scalable-contacts-cloud1-app/index.html.

12. Разработка безопасных облачных приложений [Электронный ресурс] / Роби Сен. IBM developerWorks, 2016. – Режим доступа : http://www.ibm.com/developerworks/ru/library/cl-develop-secure-cloud-aware-applications/index.html.

13. 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.

14. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Розширена мережева та хмарна безпека" https://pns.hneu.edu.ua/course/view.php?id=7016.