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

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

ІНЖЕНЕРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ 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 ЄВСЕЄВ*

Харків
2020

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

Розробник:
Корольов Р.В., к.т.н., доцент 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:

Безпека в інформаційно-комунікаційних системах в сучасних умовах гібридних загроз базується на вмілому використанні програмних (програмно-апаратних) застосунках Інтернет-технологій, спеціальних механізмах послуг безпеки (шифруванні, цифрового підпису, функцій гешування). На сьогоднішній час багато експертів пропонує зосередитись на побудові системи безпеки тільки важливих бізнес-процесів інформаційно-комунікаційних систем, тому формування контуру безпеки стає найважливішим завданням служби (підрозділів безпеки).

Метою навчальної дисципліни "Інженерія безпеки інформаційно-комунікаційних систем" є навчання студентів принципам побудови комплексних систем захисту інформації для формування контуру безпеки бізнес-процесів в інформаційнокомунікаційних системах на основі Інтернет-технологій та застосунків

Результатами вивчення даної дисципліни є придбання навичок з нейтралізації типових мережевих загроз, використання протоколу SNMP для захисту мережі, захисту від шкідливого програмного забезпечення та захист електронної пошти та веб-трафіку.

Характеристика навчальної дисципліни

Курс	**1 р.н. (магістерський рівень)**
Семестр	**1**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	залік

Структурно-логічна схема вивчення навчальної дисципліни

Попередні дисципліни	Наступні дисципліни
Основи технічного захисту інформації	Дипломний проект
Організаційне забезпечення ЗІ	

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

Компетентності	Результати навчання
	(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).

Програма навчальної дисципліни

Змістовий модуль 1. Застосунки мережевої безпеки

Тема 1. *Сучасні загрози мережевої безпеки.*
Тема 2. *Забезпечення безпеки мережевих пристроїв.*
Тема 3. *Автентифікація, авторизація та облік.*
Тема 4. *Впровадження технологій брандмауера.*
Тема 5. *Впровадження системи запобігання вторгнень.*

Змістовий модуль 2. Мережева безпека

Тема 6. *Забезпечення безпеки локальної мережі (LAN).*
Тема 7. *Криптографічні системи захисту інформації.*
Тема 8. *Впровадження віртуальних приватних мереж (VPN).*
Тема 9. *Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA).*
Тема 10. *Управління безпечної мережею.*

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, дискусії, презентації, бесіди, індивідуальні та групові проєкти.

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, 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 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:

- вміння критично осмислювати, вибирати та використовувати необхідний науковий, методичний і аналітичний інструментарій для управління в непередбачуваних умовах;
- вміти приймати, обґрунтовувати та забезпечувати реалізацію управлінських рішень в непередбачуваних умовах, враховуючи вимоги чинного законодавства, етичні міркування та соціальну відповідальність;
- вміння забезпечувати особистий професійний розвиток та планувати власний часу.

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.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі накопичених балів за виконані поточні та контрольні завдання з лекційних та лабораторних занять, що відображає розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатність творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лабораторні заняття: максимальна кількість балів становить 70, а мінімальна – 35.

Контрольні роботи: максимальна кількість балів становить 10, а мінімальна – 5.

Лекційні заняття: максимальна кількість балів становить 20, а мінімальна – 10.

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

Підсумковий контроль: проводиться за накопиченими балами.

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 заліку, 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	Лекція №1. Сучасні загрози мережевої безпеки.	Робота на лекції	2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція №2. Забезпечення безпеки мережевих пристроїв.	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 1. Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак.	Захист лабораторної роботи	14
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція №3. Автентифікація, авторизація та облік.	Робота на лекції	2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 4.	***Аудиторна робота***			
	Лекція	Лекція №4. Впровадження технологій брандмауера.	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 2. Захист маршрутизатора для адміністративного доступу.	Захист лабораторної роботи	14
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 5.	***Аудиторна робота***			
	Лекція	Лекція №5. Впровадження системи запобігання вторгнень.	Робота на лекції	2
	Самостійна робота			
	Питання та завдання	Пошук, підбір та огляд		

	до самостійного опрацювання	літературних джерел за заданою тематикою		
Тема 6.	***Аудиторна робота***			
	Лекція	Лекція №6. Забезпечення безпеки локальної мережі (LAN).	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 3. Захист адміністративного доступу за допомогою AAA і RADIUS.	Захист лабораторної роботи	14
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 7.	***Аудиторна робота***			
	Лекція	Лекція №7. Криптографічні системи захисту інформації.	Робота на лекції	2
			Контрольна робота	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 8.	***Аудиторна робота***			
	Лекція	Лекція №8. Впровадження віртуальних приватних мереж (VPN).	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 4. Налаштування зональних міжмережевих екранів.	Захист лабораторної роботи	14
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 9.	***Аудиторна робота***			
	Лекція	Лекція №9. Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA).	Робота на лекції	2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 10.	***Аудиторна робота***			
	Лекція	Лекція №10. Управління безпечної мережею.	Робота на лекції	2

			Контрольна робота	5
	Лабораторне заняття	Лабораторна робота 5. Налаштування системи запобігання вторгнень (IPS).	Захист лабораторної роботи	14
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		

Рекомендована література

Основна

1. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С.Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6

2. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом "Родовід", 2014. – 428 с.

3. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

4. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

Додаткова

5. Хорошко В. А. Методы и средства зашиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

6. Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security - ESORICS 2016, Part I

Інформаційні ресурси в Інтернеті

7. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни "Інженерія безпеки інформаційно-комунікаційних систем" https://pns.hneu.edu.ua/course/view.php?id=7087.