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

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ

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:
Мілов О. В., к.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

Процес тестування на проникнення призначено для освоєння принципів та методів збору цифрової інформації для дослідження вразливостей операційних систем Linux та Windows, проведення статичного аналізу вразливостей інформаційних систем, використовуючи інструменти та методи тестування на проникнення.

Предметом навчальної дисципліни «Тестування на проникнення та етичний хакінг» є основні поняття та методи тестування на проникнення, навики збору інформації та тестування вразливостей операційних систем Windows та Linux за допомогою інструментів з відкритим кодом.

Метою викладання дисципліни є підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також фахівців з тестування на проникнення та етичного хакінгу.

Результатами вивчення даної дисципліни є придбання знань та вмінь щодо виявлення випадків порушень кібербезпеки та аналізу цифрової інформації.

Характеристика навчальної дисципліни

Курс	**1 М**
Семестр	**2**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Математичні основи криптології	Основи криптографічного захисту

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
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	ПРН2 – 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; ПРН8 – 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-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-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
КФ 10. Здатність розробляти, впроваджувати, та супроводжувати бізнес / операційні процеси з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої стратегії і політики інформаційної безпеки та / або кібербезпеки організації.	ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; 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-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-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві
КФ 11. Здатність розробляти, впроваджувати і супроводжувати системи аудиту та моніторингу якості бізнес/операційних процесів інформаційно-комунікаційних систем та технологій, а також системи менеджменту інформаційної безпеки та/або кібербезпеки організації в цілому.	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-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

Програма навчальної дисципліни

Змістовий модуль 1. Основи етичного хакінгу

Тема 1. *Введення в етичний хакінг*

Тема 2. *Методологія тестування на проникнення*

Тема 3. *Основи етичного хакінгу*

Тема 4. *Інструменти збору інформації для тестування на проникнення*

Змістовий модуль 2. Спеціалізоване програмне забезпечення для тестування на проникнення

Тема 5. *Базові методи використання спеціалізованого програмного забезпечення*
Тема 6. *Тестування на проникнення бездротових мереж*
Тема 7. *Стрес-тести мережі*
Тема 8. *Аналіз вразливостей в веб-додатках*

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:

- встановлювати і настроювати програмне забезпечення для тестування на проникнення;
- виконувати пошук та аналіз вразливостей інформаційних систем;
- застосовувати Kali Linux;
- самостійно виконувати збір та аналіз цифрової інформації для етичного хакінгу;
- розробляти методи реагування та випадки порушень кібербезпеки;
- застосовувати інструменти тестування на проникнення для організації захисту даних в ОС Windwos, Linux.

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 14 (робота на лекції – 8, експрес-опитування – 6).

Лабораторні заняття: максимальна кількість балів становить 46 (виконання лабораторних робіт – 8, захист лабораторних робіт – 20, контрольні роботи – 18), а мінімальна – 30.

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 проведенню аналізу вразливостей в ОС та Linux, виконання його оцінюється 10 балами; третє завдання – розрахункове, 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	Лекція *"Введення в етичний хакінг"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №1 *"Встановлення та настройка Kali*	Виконання лабораторної	1

		Linux"	роботи	
	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 *"Методологія тестування на проникнення"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2 *"Встановлення та настройка Metasploit"*	Виконання лабораторної роботи	1
			Захист лабораторної роботи № 1	4
	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 *"Основи етичного хакінгу"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3. *"Тестування паролів WPA2 / WPA за допомогою Hashcat в Kali Linux"*	Виконання лабораторної роботи	1
			Захист лабораторної роботи № 2	4
	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 "Інструменти збору інформації для тестування на проникнення"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3. *"Тестування паролів WPA2 / WPA за допомогою Hashcat в Kali Linux"*	Виконання лабораторної роботи	1
			Захист лабораторної роботи № 3	4
			Контрольна робота 1	9

	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 *"Базові методи використання спеціалізованого програмного забезпечення"*	Робота на лекції	1
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота №4. *"Стрес-тест мережі (DoS веб-сайту) з SlowHTTPTest в Kali Linux"*	Виконання лабораторної роботи	1
Тема 6	***Аудиторна робота***			
	Лекція	Лекція "*Тестування на проникнення бездротових мереж"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №4. *"Стрес-тест мережі (DoS веб-сайту) з SlowHTTPTest в Kali Linux"*	Виконання лабораторної роботи	1
			Захист лабораторної роботи № 4	4
	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		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Стрес-тести мережі"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5. *"Сканування на уразливості WordPress: WPScanner і Plecost. Робота з W3af в Kali Linux "*	Виконання лабораторної роботи	1
	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		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Стрес-тести мережі"*	Робота на лекції	1
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота №5. *"Сканування на уразливості*	Виконання лабораторної	1

		WordPress: WPScanner і Plecost. Робота з W3af в Kali"	роботи	
			Захист лабораторної роботи № 5	4
			Контрольна робота 2	9
	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. Тестирование на проникновение или пентест [Электронный ресурс]. – URL: http: //deflab.ru/blog/metodi-i-sredstva-zashiti/testirovanie-naproniknoveniepentest.html

2. Тестирование на проникновение в соответствии с требованиями СТО БР ИББС-1.0–2014 [Электронный ресурс]. – URL: https: //habrahabr.ru/company/pentestit/blog/255113.

3. Этичный хакинг и тестирование на проникновение [Электронный ресурс]. – URL: http: //www.slideshare.net/heirhabarov/publ-57821636

4. Статистика уязвимостей корпоративных информационных систем 2014 [Электронный ресурс]. – URL: https: //www.ptsecurity.ru/download/PT_Corporate_vulnerability_2015_rus.pdf .

5. Скабцов Н.В. Аудит безопасности информационных систем. – СПб.: Питер, 2018, – 272 с.

6. Стародубцев Ю.И. Управление качеством информационных услуг / Ю.И. Стародубцев, А.Н. Бегаев, М.А. Дятлова; под общ. ред. Ю.И. Стародубцева. – СПб: Изд-во Политехн. Ун-та, 2017, – 454 с.

7. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. – NY.: Press.Inc, 2014, – 478 с.

8. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.

9. Бегаев А.Н., Тарасюк М.В. Контроль безопасности программного кода в составе объекта информатизации // Защита информации. Инсайд. 2013. № 5 (53). С. 63- 67.

10. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд. 2010. № 6 (36). С. 72-73.

Додаткова

11. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4 (7). С. 69-74.

12. Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг. СПб.: Изд-во Политехн. ун-та, 2017. 454 с.

13. Dorofeev A.V., Rautkin Y.V. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII AllRussian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 49-53.

14. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети Интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41-53.

15. Doroveev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city // Communications in Computer and Information Science. 2016. V. 674. P. 441-449

Інформаційні ресурси.

16. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Тестування на проникнення та етичний хакінг" https://pns.hneu.edu.ua/course/view.php?id=5684.