Силабус навчальної дисципліни
"ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ"

Спеціальність	*125 Кібербезпека*
Освітня програма	*125 Кібербезпека*
Освітній рівень	*Магістр*
Статус дисципліни	*Базова*
Мова викладання	*Українська*
Курс / семестр	*1 р.н., 2 семестр*
Кількість кредитів ЄКТС	*4*
Розподіл за видами занять та годинами навчання	*Лекції – 10 год.*
	Практичні (семінарські) – …. год.
	Лабораторні – 20 год.
	Самостійна робота – 90 год.
Форма підсумкового контролю	*Екзамен*
Кафедра	*Кібербезпеки та інформаційних технологій, м. Харків, пр-т Науки 9-А, 057-702-18-31, http://www.kafcbit.hneu.edu.ua/*
Викладач (-і)	*Мілов Олександр Володимирович*
Контактна інформація викладача (-ів)	*oleksandr.milov@hneu.net*
Дні занять	*середа*
Консультації	*Вівторок 13.55; дистанційні; відповідно до графіку; індивідуальні*

Мета навчальної дисципліни "Цифрова криміналістика" є підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також фахівців з тестування на проникнення та етичного хакінгу.

Передумови для навчання

Математичні основи криптології. Основи криптографічного захисту.

Зміст 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

Матеріально-технічне (програмне) забезпечення дисципліни

Internet, ОС Linux, WordPress: WPScanner, Plecost, Kali Linux, W3af , SlowHTTPTest, Hashcat

Сторінка курсу на платформі Moodle (персональна навчальна система) Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Тестування на проникнення» https://pns.hneu.edu.ua/course/view.php?id=5684	*Посилання:*

Рекомендовані джерела

Базова

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

Система оцінювання результатів навчання

*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.

Більш детальна інформація щодо оцінювання наведена в технологічній карті дисципліни.

Накопичування рейтингових балів з навчальної дисципліни *(приклад)*	
Види навчальної роботи	**Мах кількість балів**
Лекційні заняття	**8**
Експрес-опитування	**9**
Лабораторні заняття	**8**
Захист лабораторних робіт	**15**
Поточні КР	**20**
Екзамен (за наявності)	**40**
Максимальна кількість балів	**100**

Відповідність шкали оцінювання ЄКТС національній системі оцінювання та ХНЕУ ім. С. Кузнеця			
Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену (іспиту), диференційованого заліку, курсового проекту (роботи), практики, тренінгу	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
1 – 34	F		
Політики навчальної дисципліни *Політика дотримання академічної доброчесності,* *Політика щодо пропусків занять,* *Політика щодо виконання завдань пізніше встановленого терміну,* *тощо*			
Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у Робочій програмі навчальної дисципліни «Тестування на проникнення», 2020.			

Силабус затверджено на засіданні кафедри «31» серпня 2020 р. Протокол № 2