МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА»

Факультет математики та інформатики

Кафедра інформаційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека мереж

Освітня програма «Якість та безпека програмного забезпечення»

Спеціальність 121 Інженерія програмного забезпечення

Галузь знань 12 Інформаційні технології

Затверджено на засіданні кафедри
інформаційних технологій
Протокол № 1 від 29.08.2019 р.

м. Івано-Франківськ - 2019

ЗМІСТ

1. Загальна інформація

Назва дисципліни	Безпека мереж
Рівень вищої освіти	Другий (магістерський)
Викладач (-і)	Козленко Микола Іванович, доцент кафедри інформаційних технологій, канд. техн. наук, доцент
Контактний телефон викладача	+380 (342) 59-60-58
E-mail викладача	mykola.kozlenko@pnu.edu.ua
Формат дисципліни	Обов'язкова (цикл професійної підготовки)
Обсяг дисципліни	6 кредитів ECTS
Посилання на сайт дистанційного навчання	https://ceeq.pnu.edu.ua
Консультації	Вівторок 15.00 год. 319 ауд. адміністративного корпусу

2. Анотація до курсу

Предметом вивчення навчального курсу «Безпека мереж» є методи протистояння кіберзагрозам, виявлення вразливостей мереж та мережевого програмного забезпечення, методи розробки програмного забезпечення з мінімізацією кібер-ризиків, розслідування інцидентів. Даний курс базується на курсах «Операційні системи», «Організація комп'ютерних мереж», «Безпека програм і даних» першого (бакалаврського) рівня освіти.

3. Мета та цілі курсу

Метою дисципліни "Безпека мереж" є ознайомлення студентів з основними теоретичними положеннями про принципи, методики і методи запобігання кіберзагроз при розробці програмного забезпечення, освоєння студентами традиційних і сучасних методів забезпечення безпеки програмних засобів.

Цілі курсу:

- вивчення класифікації мережевих атак;
- освоєння використання засобів моніторингу для ідентифікації мережевих атак;
- використання методів запобігання зловмисного доступу до комп'ютерних мереж, хостів та даних;
- вивчення криптографії для задач безпеки мереж;
- дослідження вразливостей ендпоінтів для атак;
- аналіз даних інцидентів для ідентифікації вразливостей.

4. Результати навчання (компетентності)

- ЗК-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).
- СК-7. Здатність систематизувати професійні знання щодо створення і супроводження програмного забезпечення.
- СК-8. Здатність розробляти і координувати процеси, фази та ітерації життєвого циклу програмних систем на основі застосування відповідних моделей, методів та технологій розробки програмного забезпечення.

- ПР-1. Знати і системно застосовувати методи аналізу та моделювання прикладної області, виявлення інформаційних потреб і збору вихідних даних для проектування програмного забезпечення.
- ПР-2. Обґрунтовувати вибір методів формування вимог до програмної системи, розробляти, аналізувати та систематизувати вимоги.
- ПР-3. Знати і застосовувати базові концепції і методології моделювання інформаційних процесів.

- ПР-4. Оцінювати і вибирати методи і моделі розробки, впровадження, експлуатації програмних засобів та управління ними на всіх етапах життєвого циклу.
- ПР-6. Аналізувати, оцінювати і вибирати методи, сучасні програмно-апаратні інструментальні та обчислювальні засоби, технології, алгоритмічні та програмні рішення для ефективного виконання конкретних виробничих задач з програмної інженерії.
- ПР-7. Обґрунтовано вибирати парадигми і мови програмування для вирішення прикладних завдань; застосовувати на практиці системні та спеціалізовані засоби, компонентні технології (платформи) та інтегровані середовища розробки програмного забезпечення.
- ПР-8. Проводити аналітичне дослідження параметрів функціонування програмних систем для їх валідації та верифікації, а також проводити аналіз обраних методів, засобів автоматизованого проектування та реалізації програмного забезпечення.
- ПР-11. Набувати нові наукові і професійні знання, вдосконалювати, навички, прогнозувати розвиток програмних систем та інформаційних технологій.
- ПР-13(1). Знати і застосовувати на практиці різні методології та засоби реінжинірингу успадкованих програмних систем.

5. Організація навчання курсу

Обсяг курсу

Вид заняття	Загальна кількість годин
лекції	30
лабораторні	30
самостійна робота	120

Ознаки курсу

Семестр	Спеціальність	Рік навчання	Нормативний / вибірковий
1	121	1	нормативний

Тематика курсу

Тема, план	Форма заняття	Літера-тура	Завдання, год	Вага оцінки	Термін виконання
1. Основи безпеки програмного забезпечення	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
2. Безпека операційної системи Windows	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
3. Безпека операційної системи Linux	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
4. Мережеві протоколи і сервіси	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
5. Мережева інфраструктура	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
6. Принципи безпеки мереж	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
7. Мережеві атаки і захист мереж	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
8. Захист мереж	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
9. Роль криптографія в безпеці мережевого ПЗ	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
10. Безпека ендпоінтів та її аналіз	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
11. Моніторинг безпеки	Лекція	[1]-[11]	2	0,01	1 тиждень

	Лаб.		2	0,01	
12. Аналіз даних втручання	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
13. Розслідування і реагування на інциденти	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
14. Принципи розробка ПЗ з врахуванням питань безпеки	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	
15. Практичні аспекти забезпечення безпеки програмного забезпечення	Лекція	[1]-[11]	2	0,01	1 тиждень
	Лаб.		2	0,01	

6. Система оцінювання курсу

Загальна система оцінювання курсу	Сума балів	Оцінка ECTS	Оцінка за національною шкалою
	90 – 100	A	відмінно
	80 – 89	B	добре
	70 – 79	C	
	60 – 69	D	задовільно
	50 – 59	E	
	26 – 49	FX	незадовільно з можливістю повторного складання
	0 – 25	F	незадовільно з обов'язковим повторним вивченням дисципліни
Вимоги до письмових робіт	Контрольні робота в тестовій формі за кожною темою (15 балів)		
Лабораторні роботи	Лабораторні роботи за кожною темою (15 балів)		
Самостійна робота	Сертифікат про неформальну освіту або науково-дослідна робота або індивідуальне завдання (20 балів)		
Умови допуску до підсумкового контролю	До екзамену допускаються студенти, що набрали не менше 25 балів з 50 можливих за контрольні і лабораторні роботи, самостійну роботу.		
Підсумковий контроль	Екзамен в тестовій формі 50 балів (вага 0.5)		

7. Політика курсу

Студент, перед виконанням лабораторних робіт, отримує індивідуальне завдання та самостійно працює над його виконанням. За результатами виконання лабораторної роботи здається звіт, який захищається усно. Це сприяє розвитку навичок самостійної роботи над поставленою задачею та індивідуальному підходу у опануванні курсу із врахуванням можливостей та базового рівня студента.

Академічна доброчесність. Дотримання академічної доброчесності студентами передбачає:
- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання;
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:
- академічний плагіат оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

- самоплагіат оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів; фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;
- фальсифікація свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;
- списування виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання (контрольна робота, іспит тощо); повторне проходження відповідного освітнього компонента освітньої програми.

8. Рекомендована література

1. Домарев, В. В. Безопасность информационных технологий: системный поход.— К.: ООО «ТИД Диа Софт», 2004.— 992 с.
2. Кібербезпека: ризики та заходи: навч. посібник. / Ю.П. Лісовська/ – К. : Видавничий дім «КОНДОР», 2019. 272 с.
3. A Look Back at “Security Problems in the TCP/IP Protocol Suite” / Steven M. Bellovin AT&T Labs—Research https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf.
4. 12. Robert Lychev, Sharon Goldberg, Michael Schapira BGP Security in Partial Deployment: Is the Juice Worth the Squeeze? / https://arxiv.org/search/cs?searchtype=author&query=Lychev%2C+R
5. S. Fried DNS cache poisoning /http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
6. Hansen, L. and Niessanbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, pp. 1155-1175
7. McLean, S. 2013. Beware the Botnets: Cyber Security is a Board Level Issue. Intellectual Property & Technology Law Journal, 25 (12), pp. 22-27
8. Warner, M. 2012. Cybersecurity: A Pre-history. Intelligence and National Security, 27 (5), pp. 781-799
9. Vacca, JR. 2013. Cyber Security and IT infrastructure protection. Waltham: Steven Elliot
10. Роберт С. Безопасное программирование на С и С++ 2-ее изд.: Пер. с английского М. : ООО «И.Д. Вильямс», 2015 – 496 с. : ил.
11. ДСТУ ISO/IEC 27001:2015

Викладач **Козленко М.І**