СИЛАБУС ДИСЦИПЛІНИ «БЕЗПЕКА РОЗРОБКИ І ПІДТРИМКИ ПРОГРАМНИХ ЗАСТОСУНКІВ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 4, семестр 8
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор дисципліни	**Шкарупило Вадим Вікторович, к.т.н., доцент (портфоліо)** 
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки, корпус. 15, к. 207, тел. 5278724** **e-mail shkarupylo.vadym@nubip.edu.ua**
Сторінка дисципліни в eLearn	**ЕНК (1 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=

ОПИС ДИСЦИПЛІНИ

Завдання навчальної дисципліни «Безпека розробки і підтримки програмних застосунків» – теоретична та практична підготовка здобувачів до розроблення та застосування сучасних технологій, підходів та практик для організації безпечних процесів розроблення і підтримки додатків (застосунків), призначених до функціонування в установах та на підприємствах, зокрема АПК.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною та практичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки.

Компетентності ОП:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності (КЗ):

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

Спеціальні (фахові, предметні) компетентності спеціальності (СК):

СК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

Програмні результати навчання (ПРН) ОП:

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

СТРУКТУРА ДИЦИПЛІНИ

Тема	**Години** (лекції/ лабораторні,)	Результати навчання	Завдання	Оцінювання
1 семестр				
Модуль 1. Заходи сприяння безпеці на етапах процесу розроблення.				
Тема лекційного заняття 1. Вступ до курсу.	**2/0**	Знати об'єкт, предмет курсу, вирішувані задачі, підходи до вирішення задач.	Опитування.	**2**
Тема лекційного заняття 2. Заходи сприяння безпеці на етапі аналізу вимог до системи.	**2/0**	Знати і вміти застосовувати заходи та підходи до сприяння безпеці розроблення і підтримки додатків на етапі аналізу вимог до розроблюваної системи.	Опитування.	**2**
Тема лекційного заняття 3. Заходи сприяння безпеці на етапі проєктування процесу розроблення.	**2/6**	Знати і вміти застосовувати заходи та підходи до сприяння безпеці розроблення і підтримки додатків на етапі проєктування процесу розроблення. Вміти використовувати сучасні формальні методи та засоби сприяння безпеці розроблюваних додатків на етапі проєктування процесу розроблення в автоматизованому режимі.	Виконання і захист звіту з лабораторної роботи. Опитування.	**30** **1**
Тема лекційного заняття 4. Заходи сприяння безпеці на етапі реалізації процесу розроблення.	**2/6**	Знати і вміти застосовувати заходи та підходи до сприяння безпеці розроблення і підтримки додатків на етапі реалізації процесу розроблення. Вміти використовувати сучасні методи та засоби сприяння безпеці розроблюваних додатків на етапі реалізації процесу розроблення в автоматизованому режимі.	Виконання і захист звіту з лабораторної роботи. Опитування.	**30** **1**
Тема лекційного заняття 5. Анотування і документування програмного коду.	**2/0**	Знати і вміти застосовувати інструменти анотування і документування програмного коду у якості засобів сприяння безпеці процесу розроблення на етапі реалізації процесу розроблення.	Опитування.	**2**
Тема лекційного заняття 6. Засоби контролю показників функціональних і нефункціональних характеристик.	**2/0**	Знати і вміти застосовувати засоби контролю показників функціональних і нефункціональних характеристик розроблюваного додатку на етапі реалізації процесу розроблення – як інструменти сприяння безпеці.	Опитування.	**2**

Модульний контроль			Підсумковий тест в ЕНК	**30**
Модуль 2. Безпека підтримки додатків.				
Тема лекційного заняття 7. Міжмережевий екран як засіб контролю трафіку.	**2/6**	Вміти застосовувати міжмережевий екран WAF (Web Application Firewall) у якості засобу сприяння безпеці шляхом здійснення контролю HTTPS-трафіку.	Виконання і захист звіту з лабораторної роботи. Опитування.	**30** **1**
Тема лекційного заняття 8. Статичне тестування безпеки.	**2/0**	Знати і вміти застосовувати технологію статичного тестування безпеки (SAST, Static Application Security Testing) – проводити статичний аналіз вихідного коду додатку, – дозволяє оцінити безпечність додатку ще до його запуску.	Опитування.	**2**
Тема лекційного заняття 9. Динамічне тестування безпеки.	**2/0**	Знати і вміти застосовувати технологію динамічного тестування безпеки (DAST, Dynamic Application Security Testing).	Опитування.	**2**
Тема лекційного заняття 10. Інтерактивне тестування безпеки.	**2/0**	Знати і вміти застосовувати технологію інтерактивного тестування безпеки (IAST, Interactive Application Security Testing).	Опитування.	**2**
Тема лекційного заняття 11. Інструментарій OWASP як сучасний набір засобів сприяння безпеці.	**2/0**	Знати особливості і специфіку застосування сучасного інструментарію сприяння безпеці додатків – OWASP (Open Web Application Security Project).	Опитування.	**2**
Тема лекційного заняття 12. Прикладне застосування інструментарію OWASP.	**2/6**	Вміти застосовувати інструменти OWASP у якості засобів сприяння безпеці вебдодатків, що функціонують згідно заданих прикладних сценаріїв.	Виконання і захист звіту з лабораторної роботи. Опитування.	**30** **1**
Модульний контроль			Підсумковий тест в ЕНК	**30**
Всього				**70**
Екзамен			**Тест, написання програм**	**30**
Всього за 1 семестр				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету).

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзаменів	**Заліків**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Hoffman A. Web Application Security: Exploitation and Countermeasures for Modern Web Applications: 1st Edition. O'Reilly, 2020. 311 p. ISBN: 978-1-492-08796-0