Форма № Н - 3.04

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра ___ комп'ютерних систем, мереж та кібербезпеки _____

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"___" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
"Безпека розробки і підтримки програмних застосунків"

спеціальність _____125 – «Кібербезпека»_____
освітня програма _____«Кібербезпека»_____
Факультет (ННІ)_____ інформаційних технологій _____
Розробники: _____ доцент, к.т.н., доцент Шкарупило В.В. _____

Київ – 2023 р.

Робоча програма з дисципліни «Безпека розробки і підтримки програмних застосунків» для студентів ОС Бакалавр зі спеціальності 125 – «Кібербезпека».

„17” травня 2023 р. − 10 с.

Розробники: Шкарупило Вадим Вікторович, кандидат технічних наук, доцент

Робоча програма затверджена на засіданні кафедри комп’ютерних систем, мереж та кібербезпеки

Протокол від “17” травня 2023 р. № 10

Завідувач кафедри комп’ютерних систем, мереж та кібербезпеки

_____ (Касаткін Д.Ю.)
(підпис)

Схвалено вченою радою факультету інформаційних технологій

Протокол від “_18_”_____05_____2023 р. № _10_

“_____”_____2023 р. Голова _____(Глазунова О.Г.)
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни.

Безпека розробки і підтримки програмних застосунків
(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
Освітньо-кваліфікаційний рівень	бакалавр	
Характеристика навчальної дисципліни		
Вид	Вибіркова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки (курс)	2023-2024 (4)	-
Семестр	8	-
Лекційні заняття	24 год.	-
Практичні, семінарські заняття	-	-
Лабораторні заняття	24 год.	-
Самостійна робота	102 год.	-
Індивідуальні завдання	-	-
Кількість тижневих годин для денної форми навчання: аудиторних	4	

2. Мета, завдання та компетентності навчальної дисципліни.

Мета – набуття здобувачами знань та вмінь здійснення безпечних розроблення і підтримки додатків у процесі життєвого циклу.

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.

Вимоги щодо знань і вмінь, набутих внаслідок вивчення дисципліни.

Внаслідок вивчення дисципліни студенти повинні:

знати: предмету курсу, вирішувані задачі, підходів до вирішення задач; заходи та підходи до сприяння безпеці розроблення і підтримки додатків на етапах аналізу вимог, проєктування, реалізації процесу розроблення; інструменти

анотування і документування програмного коду у якості засобів сприяння безпеці процесу розроблення на етапі реалізації процесу розроблення; засоби здійснення контролю показників функціональних і нефункціональних характеристик розроблюваного додатку на етапі реалізації процесу розроблення – як інструменти сприяння безпеці; аспекти застосування міжмережевого екрану WAF (Web Application Firewall) у якості засобу сприяння безпеці шляхом здійснення контролю HTTPS-трафіку; технології статичного тестування безпеки (SAST, Static Application Security Testing), динамічного тестування безпеки (DAST, Dynamic Application Security Testing), інтерактивного тестування безпеки (IAST, Interactive Application Security Testing); особливості і специфіку застосування сучасного інструментарію сприяння безпеці додатків – OWASP (Open Web Application Security Project).

Вміти: вирішувати задачі, застосовувати підходи до вирішення задач дисципліни; застосовувати заходи та підходи до сприяння безпеці розроблення і підтримки додатків на етапах аналізу вимог, проєктування, реалізації процесу розроблення; застосовувати інструменти анотування і документування програмного коду у якості засобів сприяння безпеці процесу розроблення на етапі реалізації процесу розроблення; застосовувати засоби здійснення контролю показників функціональних і нефункціональних характеристик розроблюваного додатку на етапі реалізації процесу розроблення – як інструменти сприяння безпеці; застосовувати міжмережевий екран WAF (Web Application Firewall) у якості засобу сприяння безпеці шляхом здійснення контролю HTTPS-трафіку; застосовувати технології статичного тестування безпеки (SAST, Static Application Security Testing), динамічного тестування безпеки (DAST, Dynamic Application Security Testing), інтерактивного тестування безпеки (IAST, Interactive Application Security Testing); застосовувати сучасний інструментарій сприяння безпеці додатків – OWASP (Open Web Application Security Project).

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):

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.

3. Програма та структура навчальної дисципліни для:
– повного терміну денної форми навчання.

Змістовий модуль 1. Заходи сприяння безпеці на етапах процесу розроблення.

Тема лекційного заняття 1. Вступ до курсу:
Вивчення об’єкту, предмету курсу, вирішуваних задач, підходів до вирішення задач.

Тема лекційного заняття 2. Заходи сприяння безпеці на етапі аналізу вимог до системи:
Вивчення застосування заходів та підходів до сприяння безпеці розроблення і підтримки додатків на етапі аналізу вимог до розроблюваної системи.

Тема лекційного заняття 3. Заходи сприяння безпеці на етапі проєктування процесу розроблення.
Вивчення заходів та підходів до сприяння безпеці розроблення і підтримки додатків на етапі проєктування процесу розроблення. Вивчення сучасних формальних методів та засобів сприяння безпеці розроблюваних додатків на етапі проєктування процесу розроблення в автоматизованому режимі.

Тема лекційного заняття 4. Заходи сприяння безпеці на етапі реалізації процесу розроблення.
Вивчення заходів та підходів до сприяння безпеці розроблення і підтримки додатків на етапі реалізації процесу розроблення. Вивчення сучасних формальних методів та засобів сприяння безпеці розроблюваних додатків на етапі реалізації процесу розроблення в автоматизованому режимі.

Тема лекційного заняття 5. Анотування і документування програмного коду.
Вивчення інструментів анотування і документування програмного коду у якості засобів сприяння безпеці процесу розроблення на етапі реалізації процесу розроблення.

Тема лекційного заняття 6. Засоби контролю показників функціональних і нефункціональних характеристик.
Вивчення засобів здійснення контролю показників функціональних і нефункціональних характеристик розроблюваного додатку на етапі реалізації процесу розроблення – як інструменти сприяння безпеці.

Змістовий модуль 2. Безпека підтримки додатків.

Тема лекційного заняття 7. Міжмережевий екран як засіб контролю трафіку:
Вивчення застосування міжмережевого екрану WAF (Web Application Firewall) у якості засобу сприяння безпеці шляхом здійснення контролю HTTPS-трафіку.

Тема лекційного заняття 8. Статичне тестування безпеки:

Вивчення технології статичного тестування безпеки (SAST, Static Application Security Testing) – проведення статичний аналіз вихідного коду додатку, – дозволяє оцінити безпечність додатку ще до його запуску.

Тема лекційного заняття 9. Динамічне тестування безпеки:

Вивчення технології динамічного тестування безпеки (DAST, Dynamic Application Security Testing).

Тема лекційного заняття 10. Інтерактивне тестування безпеки:

Вивчення технології інтерактивного тестування безпеки (IAST, Interactive Application Security Testing).

Тема лекційного заняття 11. Інструментарій OWASP як сучасний набір засобів сприяння безпеці:

Вивчення особливостей і специфіки застосування сучасного інструментарію сприяння безпеці додатків – OWASP (Open Web Application Security Project).

Тема лекційного заняття 12. Прикладне застосування інструментарію OWASP:

Вивчення застосування інструментів OWASP у якості засобів сприяння безпеці вебдодатків, що функціонують згідно заданих прикладних сценаріїв.

Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	Усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Заходи сприяння безпеці на етапах процесу розроблення.												
Тема лекційного заняття 1. Вступ до курсу.	10	2		0		8						
Тема лекційного заняття 2. Заходи сприяння безпеці на етапі аналізу вимог до системи.	11	2		0		9						
Тема лекційного заняття 3. Заходи сприяння безпеці на етапі проєктування процесу розроблення.	16	2		6		8						
Тема лекційного заняття 4. Заходи сприяння безпеці на етапі реалізації процесу розроблення.	17	2		6		9						
Тема лекційного заняття 5. Анотування і документування програмного коду.	10	2		0		8						
Тема лекційного заняття 6. Засоби контролю показників функціональних і нефункціональних	11	2		0		9						

характеристик.												
Разом за змістовим модулем 1	**75**	**12**		**12**		**51**						
Змістовий модуль 2. Безпека підтримки додатків.												
Тема лекційного заняття 7. Міжмережевий екран як засіб контролю трафіку.	16	2		6		8						
Тема лекційного заняття 8. Статичне тестування безпеки.	11	2		0		9						
Тема лекційного заняття 9. Динамічне тестування безпеки.	10	2		0		8						
Тема лекційного заняття 10. Інтерактивне тестування безпеки.	11	2		0		9						
Тема лекційного заняття 11. Інструментарій OWASP як сучасний набір засобів сприяння безпеці.	10	2		0		8						
Тема лекційного заняття 12. Прикладне застосування інструментарію OWASP.	17	2		6		9						
Разом за змістовим модулем 2	**75**	**12**		**12**		**51**						
Усього годин за курс	**150**	**24**		**24**		**102**						

4. Теми лабораторних занять.

№ з/п	Назва теми	Кількість годин
1	Засоби сприяння безпеці при проєктуванні.	6
2	Засоби сприяння безпеці при реалізації.	6
3	Застосування міжмережевого екрану.	6
4	Застосування інструментарію OWASP.	6
	Разом за семестр	**24**
	Разом	**24**

5. Теми самостійної роботи.

№ з/п	Назва теми	Кількість годин
1	Прикладні сценарії, що обґрунтовують потребу сприяння безпеці процесів розроблення і підтримки додатків.	8
2	Форми подань формулювань вимог до розроблюваної системи.	9
3	Інструменти автоматизації реалізації заходів безпеки на етапі проєктування процесу розроблення.	8
4	Інструменти автоматизації реалізації заходів безпеки на етапі реалізації процесу розроблення.	9
5	Роль документування у напрямі сприяння безпечності програмного коду.	8
6	Порівняльний аналіз засобів контролю показників функціональних і нефункціональних характеристик розроблюваного додатку, застосовуваних на етапі реалізації процесу розроблення.	9
7	Поширені реалізації міжмережевих екранів. Порівняльна характеристика.	8

8	Інструментарій автоматизації процесу статичного аналізу коду.	9
9	Інструментарій автоматизації процесів динамічного тестування безпеки.	8
10	Програмні засоби забезпечення інтерактивної перевірки безпеки. Порівняльний аналіз.	9
11	Ідеологія фундації OWASP. Напрями діяльності.	8
12	Програмний інструментарій у межах проєкту OWASP. Порівняльна характеристика.	9
	Разом	**102**

6. Зразки контрольних питань, тестів для визначення рівня засвоєння знань студентами.

1. Аналіз історичного розвитку напрацювань у сфері сприяння безпеці розроблюваних додатків.
2. Аналіз інтерфейсів додатків як підхід до сприяння безпеці додатків.
3. Аналіз структури додатків. Виявлення залежностей від напрацювань третіх сторін як шлях до сприяння безпеці.
4. Шляхи виявлення «слабких сторін» розроблюваного додатку на архітектурному рівні.
5. Аналіз підходів, застосовуваних зловмисниками, для порушення безпеки додатків.
6. Регресійне тестування як шлях сприяння безпеці додатку.
7. Шляхи безпечної реалізації засобів автентифікації у додатках.
8. Шляхи безпечної реалізації засобів авторизації у додатках.
9. Підходи до проєктування безпечної архітектури додатків.
10. Архетипні уразливості програмного коду при його статичному аналізі.
11. Шляхи відтворення виявлених уразливостей програмного коду.
12. Моделювання дерева залежностей як інструмент досягнення безпеки по відношенню до напрацювань третіх сторін.

7. Методи навчання.

Під час викладання курсу використовуються наступні методи навчання:

– розповідь – для оповідної, описової форми розкриття навчального матеріалу;

– пояснення – для розкриття сутності певного явища, закону, процесу;

– бесіда – для усвідомлення, за допомогою діалогу, нових явищ, понять;

– ілюстрація – для розкриття предметів і процесів через їх символічне зображення (рисунки, схеми, графіки);

– лабораторна робота – для використання набутих знань при виконанні лабораторних завдань;

– аналітичний метод – для мисленнєвого або практичного розкладу цілого на частини з метою вивчення їх суттєвих ознак;

– проблемний виклад матеріалу – для створення проблемної ситуації.

8. Форми контролю.

Наприкінці кожного змістовного модуля проводиться контрольна робота.

Перший змістовий модуль – захист двох лабораторних робіт, усне опитування, контрольна робота – тест.

Другий змістовий модуль – захист двох лабораторних робіт, усне опитування, контрольна робота – тест, екзамен.

9. Розподіл балів, які отримують студенти.

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг студента, бали	**Оцінка національна за результати складання**	
	екзаменів	**заліків**
90-100	**Відмінно**	**Зараховано**
74-89	**Добре**	
60-73	**Задовільно**	
0-59	**Незадовільно**	**Не зараховано**

Для визначення рейтингу студента (слухача) із засвоєння дисципліни $\mathbf{R_{ДИС}}$ (до 100 балів) одержаний рейтинг з атестації (до 30 балів) додається до рейтингу студента (слухача) з навчальної роботи $\mathbf{R_{НР}}$ (до 70 балів): $\mathbf{R_{ДИС} = R_{НР} + R_{АТ}}$.

Оцінка виконання та захисту лабораторних робіт за кожний модуль здійснюється у наступній відповідності:

№ лабораторної роботи	**Кількість балів**	**Загальна кількість балів**
1 модуль		
Лабораторна робота № 1	30	70
Лабораторна робота № 2	30	
Самостійна робота	10	
Модульна контрольна		30
2 модуль		
Лабораторна робота № 3	30	70
Лабораторна робота № 4	30	
Самостійна робота	10	
Модульна контрольна		30

10. Навчально-методичне забезпечення.

1. Методичні вказівки до лабораторних робіт з дисципліни "Безпека розробки і підтримки додатків" для студентів спеціальності 125 "Кібербезпека" всіх форм навчання / Укл.: В.В. Шкарупило. – Київ: НУБіП, 2023. (у процесі розроблення).

11. Рекомендовані джерела інформації.

Базові:

1. Huseby S.H. Innocent Code: A Security Wake-Up Call for Web Programmers: 1st Edition. Wiley, 2004. 248 p. ISBN-13: 978-0470857441

Допоміжні:

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

2. What is OWASP, and Why it Matters for AppSec. URL: https://web.archive.org/web/20180411030013/https://www.contrastsecurity.com/security-influencers/what-is-owasp-and-why-it-matters-for-appsec (дата звернення: 08.05.2022).

3. Startling Results Reveal Significant Static and Dynamic Weaknesses. URL: https://web.archive.org/web/20171030064940/https://www.contrastsecurity.com/owasp-benchmark (дата звернення: 08.05.2022).

4. ДСТУ ISO/IEC 2382:2017 (ISO/IEC 2382:2015, IDT) Інформаційні технології. Словник термінів.

5. ДСТУ EN 61508-1:2019 Функційна безпечність електричних, електронних, програмованих електронних систем, пов'язаних із безпекою. Частина 1. Загальні вимоги (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=84383 (дата звернення: 08.05.2022).