Чернівецький національний університет імені Юрія Федьковича

Навчально-науковий інститут *фізико-технічних та комп'ютерних наук*
Кафедра *програмного забезпечення комп'ютерних систем*

"**ЗАТВЕРДЖУЮ**"
Директор навчально-наукового інституту
фізико-технічних та комп'ютерних наук
_____ Олег АНГЕЛЬСЬКИЙ
"*31*" *серпня* 2023 року

РОБОЧА ПРОГРАМА
навчальної дисципліни

БЕЗПЕКА WEB-ДОДАТКІВ
вибіркова

Освітньо-професійна програма *«Інформаційні системи та технології»*

Спеціальність *126 Інформаційні системи та технології*

Галузь знань *12 Інформаційні технології*

Рівень вищої освіти *перший бакалаврський*

Мова навчання *українська*

Чернівці 2023 рік

Робоча програма навчальної дисципліни «БЕЗПЕКА WEB-ДОДАТКІВ» складена відповідно до освітньо-професійної програми першого (бакалаврського) рівня вищої освіти *«Інформаційні системи та технології»* за спеціальністю *126 Інформаційні системи та технології* галузі знань *12 Інформаційні технології*, затвердженої Вченою радою Чернівецького національного університету імені Юрія Федьковича (Протокол № *7* від «*31*» *серпня* 2020 року).

Розробник: *Прохоров Георгій Валерійович, доцент кафедри програмного забезпечення комп'ютерних систем, кандидат фізико-математичних наук*

Погоджено з гарантом ОПП і затверджено на засіданні кафедри
інформаційних технологій та комп'ютерної фізики

Протокол № *1* від "*28*" *серпня* 2023 року

Завідувачка кафедри ІТКФ _____ Борча М.Д.

Робоча програма затверджена на засіданні кафедри
програмного забезпечення комп'ютерних систем

Протокол № *1* від "*29*" *серпня* 2023 року

Завідувач кафедри ПЗКС _____ Остапов С.Е.

Схвалено методичною радою навчально-наукового інституту
фізико-технічних та комп'ютерних наук

Протокол № *1* від "*29*" *серпня* 2023 року

Голова методичної ради ННІФТКН _____ Струк Я.М.

1. Мета навчальної дисципліни.

Навчальна дисципліна «Безпека web-додатків» призначена для формування у студентів знань, вмінь та навичок з сучасних методів та засобів дослідження програмного забезпечення на безпеку, які будуть корисними при проведенні власних розробок при підготовці дипломної роботи, а також при подальших наукових роботах для створення сучасних інформаційних систем.

Мета навчальної дисципліни: Забезпечення підготовки студентів технічної спеціальності 126 Інформаційні системи та технології. А саме - формування навиків аналізу та вирішення задач з безпеки інформаційних систем, які доцільно вирішувати засобами інтелектуальних систем; вміти використовувати сучасні інформаційні технології для створення та дослідження безпечних інтелектуальних систем для широкого застосунку.

Він є одним з основних курсів, призначеним для набуття студентами базових знань з основ надійності програмного забезпечення у сфері комп'ютерних наук, які необхідні у подальшому навчанні, а також у практичній діяльності на виробництві.

Навчальна дисципліна «Безпека web-додатків» являється логічним продовження попередніх курсів «Об'єктно-орієнтоване програмування» , «Технології Java», «Безпека програм та даних», «Технології захисту інформації», а саме **практичним** втіленням набутих попередніх теоретичних знань на прикладі створення системи безпеки веб-додатка.

2. Результати навчання.

Відповідно до освітньо-професійної програми підготовки бакалаврів галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології вивчення дисципліни сприяє формуванню наступних компетентностей та програмних результатів навчання:

Загальних компетентностей:

КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 2. Здатність застосовувати знання у практичних ситуаціях.

КЗ 3. Здатність до розуміння предметної області та професійної діяльності.

КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальних (фахових, предметних) компетентностей:

КС 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем.

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

Програмними результатами навчання є:

ПРН 3. **Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.

ПРН 5. **Аргументувати** вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

ПРН 9. **Здійснювати** системний аналіз архітектури підприємства та його ІТінфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.
ПРН 10. **Розуміти і враховувати** соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень.

3. Опис навчальної дисципліни
3.1. Загальна інформація

«Безпека web-додатків»													
Форма навчання	Рік підготовки	Семестр	Кількість			Кількість годин							Вид підсум-кового контролю
			кредитів	годин	змістових модулів	лекції	практичні	семінарські	лабораторні	самостійна робота	індивідуальні завдання	курсова робота	
Денна	4	7	4	120	2	30	-	-	30	60	-	-	Залік
Заочна	-	-	-	-	-	-	-		-	-	-	-	-

3.3. Структура змісту 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*
Теми лекційних занять	**Змістовий модуль 1 –Тестування серверної частини**											
Тема 1 Фундаментальні поняття і визначення теорії безпеки програмних продуктів.	14	4	-	-	-	10	-	-	-	-	-	-
Тема 2 . Критерії безпеки. Рівні та повнота безпеки.	26	6	-	6	-	14	-	-	-	-	-	-
Тема 3. Сервіс-орієнтована архітектура. Поняття сервісу. Архітектура REST. Веб-сервіси RESTful. Безпека REST API, етапи.	12	2	-	4	-	6	-	-	-	-	-	-

Тема 4. Введення Spring Security. Сценарії тестування рівнів безпеки серверного веб-додатка.	16	4	-	2	-	10	-	-	-	-	-	-
Разом за ЗМ1	68	16	-	12	-	40	-	-	-	-	-	-
Теми лекційних занять	**Змістовий модуль 2**											
Тема 5. Базовий рівень безпеки веб-додатка. Архітектура та імплементація.	26	8	-	8	-	10	-	-	-	-	-	-
Тема 6. Технологія JWT. Архітектура. Рівні складності. Мікросервісна реалізація.	26	6		10		10	-	-	-	-	-	-
Разом за ЗМ 2	52	14	-	18	-	20	-	-	-	-	-	-
Усього годин	120	30	-	30	-	60	-	-	-	-	-	-

3.3. Зміст завдань для самостійної роботи

№	Назва теми
1	Аналіз безпеки складних технічних систем
2	Методи тестування стійкості систем до кібер-атак.
3	Математичні моделі функціонування елементів і систем в сенсі їх безпеки
4	Технології розробки безпечних програмних систем

4. Форми і методи навчання

Форми навчання – це лекції-візуалізації (із застосуванням комп'ютерної техніки), лекції-дискусії, лабораторні заняття з виконанням індивідуальних завдань, заняття з використанням систем електронного навчання Moodle; індивідуальні та групові консультації, самостійна робота (індивідуальна під керівництвом викладача-тьютора); використання елементів дистанційного навчання (за потреби): відеолекції, відеозаняття і відеоконференції засобами Google Meet, Zoom тощо.

Підходи до навчання – використовуються студентоцентрований, проблемноорієнтований, діяльнісний, комунікативний, професійно-орієнтований, міждисциплінарний підходи.

Для викладання навчальної дисципліни використовуються наступні ***методи навчання:***

- ☑ *пояснювально-ілюстративні* (спрямовані на повідомлення готової інформації різними засобами (словесними, наочними, практичними) та усвідомлення і запам'ятовування цієї інформації студентами);
- ☑ *компетентнісний* (навчання, спрямоване на розвиток навичок, умінь і якостей, які знадобляться в професійній діяльності);

- ☑ *репродуктивний* (використовується під час лабораторних занять, а також під час самостійної роботи студентів; передбачає роботу студентів за визначеним алгоритмом);
- ☑ *частково-пошукові або евристичні* (організація активного пошуку розв'язання поставлених або самостійно сформульованих пізнавальних завдань, над якими студенти працюють самостійно під керівництвом педагога або на основі евристичних програм та вказівок).

5. Система контролю та оцінювання

Форми та засоби оцінювання

- опитування теоретичного матеріалу;
- лабораторні роботи;
- індивідуальні проєкти (презентація);
- презентації результатів виконаних завдань та досліджень;
- тестові завдання.

Види та форми контролю

Форми поточного контролю:

- усна (відповідь студента під час лабораторного заняття).
- захист і презентації результатів виконаних лабораторних / практичних завдань.
- письмова (тестування).

Форма підсумкового контролю – залік.

6. Критерії оцінювання результатів навчання з навчальної дисципліни

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-50%). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт, заліків або іспитів заборонені (в т.ч. із використанням мобільних девайсів).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в online формі за погодженням із керівником курсу.

Критеріями оцінювання є:

- <u>при усних відповідях:</u> повнота розкриття питання; логіка викладання матеріалу; використання основної та додаткової літератури; аналітичні міркування, уміння робити порівняння, висновки; уміння аналізувати теоретичні проблеми з урахуванням світової і вітчизняної практики;
- <u>при виконанні письмових завдань:</u> повнота розкриття питання, аргументованість і логіка викладення матеріалу, використання літературних джерел, законодавчих актів, прикладів та фактичного матеріалу тощо; цілісність, системність, логічність, уміння формулювати висновки; акуратність оформлення письмової роботи.

Проведення підсумкового контролю здійснюється у формі передбаченою навчальним планом в обсязі навчального матеріалу, визначеного навчальною програмою дисципліни і в терміни, передбачені графіком навчального процесу.

Загальна підсумкова оцінка з дисципліни (максимум 100 балів) визначається як сума балів поточного і модульного контролю та результатів заліку/іспиту (як

можливість отримання додаткових балів, якщо набрані протягом семестру бали не влаштовують студентів). У випадку отримання менше 50 балів за результатами загального підсумкового контролю, студент обов'язково здійснює перескладання для ліквідації академічної заборгованості.

Загальні вимоги для одержання підсумкової оцінки:

- «відмінно» – студент вільно володіє матеріалом дисципліни; може самостійно і грамотно провести всі необхідні розробки і викладки з усіх передбачених програмою питань, може розв'язувати нестандартні задачі, відповідь охоплює не менше 90% матеріалу питань в білеті.
- «добре» – студент вільно орієнтується у матеріалі дисципліни; може грамотно відтворити лекційний матеріал; може розв'язувати всі стандартні задачі з матеріалу дисципліни; відповідь охоплює не менше 75% матеріалу питань в білеті.
- «задовільно» – студент знає основні поняття і твердження, але не всі може відповідно обґрунтувати; може розв'язати прості стандартні задачі; відповідь охоплює не менше 60% матеріалу питань в білеті.
- «незадовільно» – вимоги позитивних оцінок не виконуються, відповідь містить менше 60% потрібного матеріалу питань білету.

Шкала оцінювання знань студентів: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для іспиту, курсового проєкту (роботи), практики	для заліку
90-100	**A**	відмінно	зараховано
80-89	**B**	добре	
70-79	**C**		
60-69	**D**	задовільно	
50-59	**E**		
35-49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Розподіл балів, які отримують студенти

Поточне оцінювання (*аудиторна та самостійна робота*)								Кількість балів (залік)	Сумарна к-ть балів
Змістовий модуль №1				Змістовий модуль № 2					
Т1	Т2	Т3	Т4	Т5.1	Т5.2	Т5.3	Т5.4	40	100
0	10	10	10	7,5	7,5	7,5	7,5		

7. Рекомендована література

1) ДСТУ ISO/IEC 2382-14:2005 Інформаційні технології. Словник термінів. Частина 14. Безвідмовність, ремонтопридатність і готовність;
2) ГОСТ 19.301-79 (СТ СЗВ 3747-82). Єдина система програмної документації. Програма та методка випробувань. Вимоги до змісту та оформлення.
3) Яковина В. С., Сенів М. М. Основи теорії надійності програмних систем. Навчальний посібник. Львів : Видавництво Львівської політехніки, 2020. 248 с.

4) Marvin Rausand, Anne Barros, Arnljot Hoyland. System reliability theory: models, statistical methods and applications. Wiley, 3rd edition, 2020. 864p.
5) Svyatoslav Kulikov. Software testing. Base course, 3rd Edition/ EPAM Systems, 2022.-278p.
6) Daniel Galin Software Quality Concepts and Practice / USA.: Wiley-IEEE Press, 2018. – 711 p.
7) Claude Y. LaporteAlain Software Quality Assurance, First Edition/ USA: Wiley-IEEE Press, 2017. – 596 p.
8) Karl Wiegers and Joy Beatty. Software Requirements, Third Edition/Published by Microsoft Press A Division of Microsoft Corporation One Microsoft Way Redmond, Washington, 2013. - 673p.

8. Інформаційні ресурси

1. International Software Testing Qualification Board Glossary. URL: https://glossary.istqb.org/en/search/ (дата звернення 20.03.2023).
2. Guide to the Software Engineering Body of Knowledge. Version 3.0 Editors: Pierre Bourque, Richard E. (Dick) Fairley. IEEE Computer Society, 2014 URL: https://ieeecs-media.computer.org/media/education/swebok/swebok-v3.pdf (дата звернення 20.03.2023).
3. 1An Introduction to Software Testing Life Cycle (STLC): Definition and Phases. URL: https://www.sealights.io/software-quality/an-introduction-to-software testing-life-cycle-stlc-definition-and-phases/ (дата звернення 20.03.2023).
4. Reid S. ISO/IEC/IEEE 29119: The New International Software Testing Standards. URL: http://www.stureid.info/wp-content/uploads/2015/08/ISO-29119- The-New-International-Software-Testing-Standards.pdf. (дата звернення 20.03.2023).
5. Certified Tester Foundation Level Syllabus. Version 2018 V3.1.1. International Software Testing Qualifications Board. URL: https://istqb-main-web prod.s3.amazonaws.com/media/documents/ISTQB-CTFL_Syllabus_2018_v3.1.1.pdf. (дата звернення 20.03.2023).
6. WebDriver. W3C Working Draft. URL: https://www.w3.org/TR/webdriver/ (дата звернення 25.03.2022).