МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра інформаційних систем

Затверджено
на засіданні кафедри
інформаційних систем
факультету прикладної математики та
інформатики
Львівського національного університету
імені Івана Франка
(протокол № 1 від 28.08.2023 р.)

Завідувач кафедри Георгій ШИНКАРЕНКО

_____

Силабус з навчальної дисципліни
“Надійність програмних систем”,
що викладається в межах ОПП Інформатика другого (магістерського) рівня вищої освіти для здобувачів зі спеціальності 122 – Комп’ютерні науки

Львів 2023 р.

Назва дисципліни	**Надійність програмних систем**
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра інформаційних систем
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 122 – комп'ютерні науки
Викладачі дисципліни	Жолткевич Григорій Миколайович, професор кафедри інформаційних систем, доктор техн. наук. (лекції та лабораторні заняття)
Контактна інформація викладачів	grygoriy.zholtkevych@lnu.edu.ua; Головний корпус ЛНУ ім. І. Франка, каб. 260. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/лабораторних занять (а також за розкладом консультацій кафедри).
Сторінка курсу	https://ami.lnu.edu.ua/course/nadiynist-prohramnykh-system-122-cs
Інформація про дисципліну	Дисципліна "Надійність програмних систем" є вибірковою дисципліною для спеціальності 122 – комп'ютерні науки для освітньої програми Інформатика, яка викладається в 1-му семестрі в обсязі 6-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Навчальну дисципліну розроблено так, щоб забезпечити розуміння студентами концепції надійності технічних систем, її особливості для програмних систем, а також ознайомити студентів з сучасною технологією забезпечення розробки надійного програмного забезпечення – сертифікованим програмування, спираючись на можливості The Coq Proof Assistant та сформувати загальні навички її використання. Курс представляє собою приклади застосування технології сертифікованого програмування для низки простих але типових задач програмування з поясненням загальних концепцій на цих прикладах. Кожна лекція передбачає обговорення на лабораторному занятті з широким залученням студентів до такого обговорення.
Мета та цілі дисципліни	***Метою*** *навчальної дисципліни є формування у студентів системи теоретичних знань і практичних навичок аналізу коректності програмного забезпечення з використанням програмних інструментів класу «помічник у доведенні (proof assistant)».* ***Завданням*** *вивчення навчальної дисципліни є сформувати у студентів теоретичні знання та практичні навички в області статичного аналізу програмного забезпечення; надати студентам уявлення про завдання та*

	цілі формальної верифікації програмного забезпечення; надати студентам теоретичні засади та практичні навички використання The Coq Proof Assistant для статичного аналізу програм.	
Література для вивчення дисципліни	Основна література:	
	1	Chlipala, Adam. Certified Programming with Dependent Types, MIT Press, 2019
	2	Bertot, Yves and Casteran, Pierre. Interactive Theorem Proving and Program Development. Coq' Art: The Calculus of Inductive Constructions, Springer, 2004
		Chlipala, Adam. Formal Reasoning About Programs, MIT Press, 2023
	3	Paulin-Mohring, Christine. Introduction to the Coq proof-assistant for practical software verification, Lecture Notes in Computer Science, vol 7682. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-35746-6_3
	4	The Coq Development Team. The Coq Reference Manual. 2023 https://coq.inria.fr/distrib/current/refman/
	5	The Coq Proof Assistant. Standard Library. 2023. https://coq.inria.fr/distrib/current/stdlib/
	Додаткова література:	
	6	Software Foundations Volume 1. Logical Foundation https://softwarefoundations.cis.upenn.edu/current/lf-current/index.html
	7	Software Foundations Volume 2. Programming Language Foundations https://softwarefoundations.cis.upenn.edu/current/plf-current/index.html
	8	Software Foundations Volume 3. Verified Functional Algorithms https://softwarefoundations.cis.upenn.edu/current/vfa-current/index.html
	9	Software Foundations Volume 5. Verifiable C https://softwarefoundations.cis.upenn.edu/current/vc-current/index.html
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 64 год., з них 32 години лекцій та 32 години лабораторних занять. Самостійної роботи: 116 годин.	
Очікувані результати навчання	**У результаті вивчення навчальної дисципліни студент повинен *знати:*** • концепцію надійності програмних систем, її особливості у контексті загального розуміння надійності технічних систем; • концепцію технології сертифікованого програмування і її теоретичні засади; • архітектуру системи The Coq Proof Assistant; • основні тактики системи The Coq Proof Assistant. ***вміти:*** • моделювати семантичні сутності за допомогою індуктивних визначень; • використовувати функціональну мову системи The Coq Proof Assistant; • використовувати основні тактики системи The Coq Proof Assistant	

	для доведення тверджень про програми; • використовувати модулі системи The Coq Proof Assistant для запобігання конфліктам іменування; • використовувати інструмент класів для побудови фреймворків верифікації. **Курс забезпечує набуття таких компетентностей: ІК, ЗК 1, ЗК 3-7, СК 1-6, СК 10 та програмних результатів навчання: ПРН 1-2, ПРН 6-7, ПРН 13, ПРН 16, ПРН 20.**
Ключові слова	Технічна система, програмна система, надійність, статичний аналіз, формальна верифікація, теорія типів, тактика, доведення
Формат курсу	Очний. Проведення лекцій, лабораторних занять і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці першого семестру.
Пререквізити	Для вивчення дисципліни студенти потребують базові знання, що формуються при підготовці рівня бакалавр з математичної логіки, дискретної математики, основ функціонального програмування, теорії алгоритмів
Навчальні методи та техніки, які будуть використовувати ся під час викладання курсу	Презентації, лекції, модульний контроль Індивідуальні завдання Індивідуальні мініпроєкти
Необхідне обладнання	Комп'ютер, Internet.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 40% семестрової оцінки; максимальна кількість балів 40; • індивідуальні завдання: 60% семестрової оцінки; максимальна кількість балів 60. Підсумкова максимальна кількість балів 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх самостійними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману. **Відвідування занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів, визначених для виконання всіх лабораторних робіт та індивідуальних завдань,

	передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. **Політика виставлення балів.** Враховуються бали, отримані при поточному опитуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях, не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до екзамену	Екзамен не передбачений
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенні курсу.

Схема курсу

Тиж.	**Тема, план, короткі тези**	**Форма діяльності (заняття)**	**Література. Ресурси в інтернеті**	**Завдання, год.**	**Термін виконання**
1	**Тема 1. Концепція надійності програмних систем** (надійність технічних систем, технічні системи з інтенсивним використанням програмного забезпечення, відомі катастрофічні інциденти, викликані помилками програмного забезпечення, два підходи до розуміння надійності програмних систем, концепція сертифікованого програмування)	лекція		2	
		самостійна робота		12	1 тиждень
	Тема 2. Задача розробки простого програмованого стекового обчислювача (встановлення The Coq Proof Assistant, інтерактивного середовища coqide, основи роботи з цими інструментами)	лабораторне заняття	[4-5]	2	
2	**Тема 2. Задача розробки простого програмованого стекового обчислювача** (моделювання мови виразів, моделювання стекового обчислювача, розробка компілятора, доведення коректності компілятора)	лекція	[1-5]	2	
		лабораторне заняття	[4-5]	2	
		самостійна робота		8	1 тиждень
3	**Тема 3. Задача розробки програмованого стекового обчислювача з типізацією значень** (моделювання мови типізованих виразів, концепція родин типів, моделювання	лекція	[1-5]	2	
		лабораторне занят-	[4-5]	2	

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Літерату-ра. Ресур-си в інте-рнеті	Завдання, год.	Термін виконан ня
	стекового обчислювача, що підтримує типізацію значень)	тя			
4	**Тема 3. Задача розробки програмованого стекового обчислювача з типізацією значень** (аналіз міні-проєкту)	лекція	[4-5]	2	
		лабораторне заняття	[4-5]	2	
		самостійна робота	[1-5]	6	1 тиждень
5	**Тема 4. Загальне уявлення про The Coq Proof Assistant** (архітектурні компоненти системи, мови системи, концепція «терм-тип-сорт»)	лекція	[1-4]	2	
		самостійна робота	[4]	2	
	Тема 5. Індуктивні визначення (перелічувані типи, рекурсивні типи, принципи індукції)	лабораторне заняття	[1-4]	2	
6	**Тема 5. Індуктивні визначення** (практикум з визначення індуктивних типів)	лабораторне заняття	[4-5]	2	
		самостійна робота	[1-4]	6	1 тиждень
	Тема 6. Функціональне програмування з The Coq Proof Assistant (основні конструкції мови Galinna)	лекція	[1-4]	2	
7	**Тема 6. Функціональне програмування з The Coq Proof Assistant** (залежні типи, специфіка застосування основних конструкцій мови Galinna у випадку залежних типів)	лекція	[1-4]	2	
		лабораторне заняття	[4-5]	2	
		самостійна робота	[1-5]	8	1 тиждень
8	**Тема 6. Функціональне програмування з The Coq Proof Assistant** (залежні типи, специфіка застосування основних конструкцій мови Galinna у випадку залежних типів)	лабораторне заняття	[4-5]	2	
		самостійна робота	[4]	8	1 тиждень
	Тема 7. Автоматизація доведення тверджень про програми (основні тактики, їх застосування, розробка тактик)	лекція	[1-4]	2	
		самостійна робота	[1-4]	8	1 тиждень
9	**Тема 7. Автоматизація доведення тверджень про програми** (простори імен, модульні типи, класи)	лекція	[1-4]	2	
		лабораторне заняття	[4-5]	2	
10	**Тема 7. Автоматизація доведення тверджень про програми** (практикум з управління просторами імен, модульних типів, класів)	лабораторне заняття	[4-5]	2	
		самостійна робота	[1-4]	10	1 тиждень

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література. Ресурси в інтернеті	Завдання, год.	Термін виконання
	Тема 8. Верифікація алгоритмів сортування (моделювання постановки задачі сортування засобами The Coq Proof Assistant)	лекція	[1-4]	2	
11	**Тема 8. Верифікація алгоритмів сортування** (верифікація алгоритму сортування злиттям)	лекція	[1-4]	2	
		самостійна робота	[1-5]	8	
	Тема 9. Верифікація деяких базових структур даних (побудова теорій стеків та черг)	лабораторне заняття	[1-4]	2	
		самостійна робота	[1-5]	8	
12-13	**Тема 9. Верифікація деяких базових структур даних** (побудова теорії словників)	лекція	[1-4]	4	
		самостійна робота	[1-5]	8	3 тижні
	Тема 9. Верифікація деяких базових структур даних (побудова теорії В-дерев)	лабораторне заняття	[1-5]	4	
14	**Тема 9. Верифікація деяких базових структур даних** (аналіз теорій стеків та черг)	лекція	[4-5]	2	
		самостійна робота	[4-5]	8	
		лабораторне заняття	[4-5]	2	
15	**Тема 9. Верифікація деяких базових структур даних** (аналіз теорії бінарних дерев)	лекція	[4-5]	2	
		самостійна робота	[4-5]	8	
		лабораторне заняття	[4-5]	2	
16	**Тема 9. Верифікація деяких базових структур даних** (аналіз теорії В-дерев)	лабораторне заняття	[4-5]	2	
		лекція	[4-5]	2	
		самостійна робота	[4-5]	8	