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

Затверджено
на засіданні кафедри прикладної математики
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(протокол № 1 від 31 серпня 2023 р.)

Завідувач кафедри

Юрій ЯЩУК

Силабус з навчальної дисципліни
“Захист інформації”,
що викладається в межах першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 113 – прикладна математика

Львів 2023 р.

Назва дисципліни	**Захист інформації**
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 прикладної математики
Галузь знань, шифр та назва спеціальності	11 – математика та статистика 113 – прикладна математика
Викладачі дисципліни	Марчук Юрій Богданович, асистент кафедри прикладної математики, Переймибіда Андрій Андрійович, кандидат фізико-математичних наук, доцент кафедри прикладної математики (лабораторні заняття)
Контактна інформація викладачів	Yurii.Marchuk@lnu.edu.ua; https://ami.lnu.edu.ua/employee/marchuk-yu-biu andrii.pereimybida@lnu.edu.ua; https://ami.lnu.edu.ua/employee/pereymybida-andriy-andriyovych Головний корпус ЛНУ ім. І. Франка, каб. 378. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/course/zakhyst-informatsii-pm
Інформація про дисципліну	Дисципліна “Захист інформації” є дисципліною на вибір зі спеціальності 113 – прикладна математика для освітньої програми “Прикладна математика”, яка викладається в 8-му семестрі в обсязі 4-и кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс “Захист інформації ” охоплює такі розділи: методології захисту інформації, елементарна криптограція, шифрування, безпечна взаємодія бекенд сервісів, безпечна реалізація веб-додатків. Викладення матеріалу здійснюється за допомогою сучасних термінів та понять з галузі інформаційних технологій.
Мета та цілі дисципліни	***Метою*** курсу є ґрунтовне ознайомлення студентів із підходами організації забезпечення захисту інформації. ***Завданням*** вивчення навчальної дисципліни є формування у студентів теоретичних знань в області захисту інформації; здобуття студентами практичних навичок захисту інформації.
Література для вивчення дисципліни	Основна література 1. Eduardo Fernandez-Buglioni. Security patterns in practice: Designing Secure Architectures using software. – Wiley: 2013 – 582p. 2. Loren Kohnfelder. Designing Secure Software. – No Starch Press: 2021 – 312p. 3. David Wong. Real-World Cryptography. – Manning Publications: 2021 – 400p. 4. Charles Pfleeger. Security in Computing, 6th Edition //Charles Pfleeger, Shari Lawrence Pfleeger, Lizzie Coles-Kemp – Addison-Wesley Professional: 2023 – 1040p. 5. Jean-Philippe Aumasson. Serious Cryptography. – No Starch Press: 2017 – 312p

	6. David Pointcheval. Asymmetric Cryptography – Wiley-ISTE: 2023 – 304p. 7. Sam Newman. Building Microservices, 2nd Edition – O'Reilly Media, Inc: 2021 – 612p. 8. Wajjakkara Kankanamge. Microservices Security in Action //Wajjakkara Kankanamge, Anthony Nuwan Dias, Prabath Siriwardena – Manning Publications: 2020 – 616p. 9. Chris Richardson. Microservices Patterns – Manning Publications: 2018 – 520p. 10. Bryan Sullivan. Web Application security, a beginner's guide //Bryan Sullivan, Vincent Liu – McGraw-Hill: 2011 – 384p. 11. Andrew Hoffman. Web Application Security – O'Reilly Media, Inc: 2020 – 327p. 12. Matthew Baker. Secure Web Application Development: A Hands-On Guide with Python and Django – Apress: 2022 – 471p. 13. Adam Shostack. Threat Modeling: Designing for Security. – Willet: 2014 – 624p. 14. Derek Fisher. Application Security Program Handbook – Manning Publications: 2023 – 296p.
Обсяг курсу	Загальний обсяг: 120 год. З них, аудиторних занять: 56 год., з них 28 години лекцій, 28 години лабораторних робіт та 64 год. самостійної роботи
Очікувані результати навчання	Після завершення цього курсу студент буде: ***Знати***: - підходи та шаблони розробки алгоритмів шифрування, - техніки розробки криптографічних алгоритмів - техніки безпечної взаємодії мікросервісів - захист інформації у ВЕБ-додатках ***Вміти***: - розробляти алгоритми шифрування та дешифрування, - розроблятити безпечні бекенд додатки мікросервісної архітектури, - розроблятити безпечні Веб-додатки
Ключові слова	Захист, шифрування, дешифрування, криптографія.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Подано нижче у таблиці Схема курсу "Захист інформації"
Підсумковий контроль, форма	Залік
Пререквізити	Для вивчення курсу студенти потребують базових знань з - Основ програмування - Практичні навички програмування
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, модульний контроль. Індивідуальні завдання
Необхідне обладнання	Комп'ютер із програмним забезпеченням: мова програмування на вибір студента, інтегроване середовище розробки(IDE – Integrated Development Environment).

Критерії оцінювання (окремо для кожного виду навчальної діяльності)

Оцінювання проводиться за 100-бальною шкалою.

Оцінка за шкалою ECTS		Оцінка в балах	Оцінка за національною шкалою		
			Екзамен, диференційований залік		залік
A	Відмінно	100 - 90	Відмінно	5	зараховано
B	Дуже добре	81- 89	Добре	4	
C	Добре	71 -80			
D	Задовільно	61 - 70	Задовільно	3	
E	Достатньо	51- 60			
FX (F)	Незадовільно	0 - 50	Незадовільно	2	не зараховано

Бали нараховуються за наступним співвідношенням:

• індивідуальні завдання : 80% семестрової оцінки; максимальна кількість балів 80 (3 завдання: 25, 25 та 30 балів);

№ 1 (25 балів)	№ 2 (25 балів)	№ 3 (30 балів)	Критерії оцінювання
25 балів	**25 балів**	**30 балів**	студент повністю виконав умови завдання, алгоритм реалізовано правильно, відповідає на всі запитання, пов'язані з тематикою завдання, проводить чіткий аналіз та порівняння отриманих результатів, пропонує інші підходи до вирішення поставленого завдання;
17-24 балів	**17-24 балів**	**20-29 балів**	студент повністю виконав умови завдання, на деякі запитання, алгоритм реалізовано правильно, пов'язані з тематикою завдання, відповідає з незначними неточностями, проводить аналіз отриманих результатів з незначними неточностями;
10-16 балів	**10-16 балів**	**13-19 балів**	студент виконав завдання з незначними помилками, але самостійно їх виправляє, якщо на них вкаже викладач, на деякі запитання, пов'язані з тематикою завдання, відповідає з неточностями, проводить аналіз отриманих результатів з неточностями;
6-9 балів	**6-9 балів**	**8-12 балів**	студент виконав завдання частково, алгоритм реалізовано з помилками, які частково може виправити, якщо на них вкаже викладач, на запитання відповідає з помилками, проводить аналіз отриманих результатів з помилками;
4-5 бали	**4-5 бали**	**4-7 бали**	студент виконав завдання частково, алгоритм реалізовано з помилками, які самостійно не може виправити, переважно не відповідає на запитання;
1-3 бал			студент виконав завдання частково або з грубими помилками, які самостійно не може виправити, демонструє незнання матеріалу;
0 балів			студент не виконав завдання.

• контрольні заміри (модулі): 20% семестрової оцінки; максимальна кількість балів 20 (4 тестові модулі в середовищі MS Teams по 5 балів);

	Критерії оцінювання тестових завдань (модулі): **1 бал:** відповідь на завдання правильна; **0 балів:** відповідь на завдання неправильна. Загалом протягом семестру 100 балів. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними 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. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання домашніх 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 набрані за індивідуальні завдання та контрольні заміри. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного 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 контрольних замірів	1. Алгоритми шифрування та дешифрування. 2. Криптографія
Опитування	Оцінювання якості курсу буде доступне у системі "Dekanat' після завершенню курсу. Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу ***"Захист інформації"***

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література, Ресурси в інтернеті	Завдання, год	Термін виконання
1	**Тема 1.** Вступ. Концепції	Лекція (2 год)		Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 1. Формулювання процесу роботи над індивідуальними завданнями, процедури здачі	Лабораторне заняття (2 год)		Налаштування локального середовища (3 год.)	2 тижні

2	**Тема 2.** Шаблони безпеки розробки програмного забезпечення. Шаблон Атрибути дизайну. Шаблон Мінімізація експозиції.	Лекція (2 год)	[1, 2]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 2. Шаблони безпеки розробки програмного забезпечення 1.	Лабораторне заняття (2 год)	[1, 2]	Використання шаблонів безпеки розробки програмного забезпеченн(5 годин)	1 тиждень
3	**Тема 3.** Шаблони безпеки розробки програмного забезпечення. Шаблон Строгого правозастосування. Шаблон Надмірність. Шаблон Довіра та відповідальність	Лекція (2 год)	[1, 2]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 3. Шаблони безпеки розробки програмного забезпечення 2.	Лабораторне заняття (2 год)	[1, 2]	Використання шаблонів безпеки розробки програмного забезпеченн (3годин)	2 тижні
4	**Тема 4.** Антишаблони безпеки розробки програмного забезпечення.	Лекція (2 год)	[1, 2]	Опрацювання лекційного матеріалу (2 год)	1 тиждень
	Тема 4. Шаблони безпеки розробки програмного забезпечення 3.	Лабораторне заняття (2 год)	[1, 2]	Використання шаблонів безпеки розробки програмного забезпеченн(5 год)	2 тижні
5	**Тема 5.** Криптографія. Випадкові числа. Коди автентифікації повідомлень.	Лекція (2 год)	[3, 4, 5]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 5. Розробка алгоритмів з випадковими числами та кодами автентифікації повідомлень	Лабораторне заняття (2 год)	[3, 4, 5]	Розробка алгоритмів з випадковими числами та кодами автентифікації повідомлень(4 год)	2 тижні
6	**Тема 6.** Криптографія. Симетричне шифрування.	Лекція (2 год)	[3, 4, 5]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 6. Розробка алгоритмів симетричного шифрування та дешифрування	Лабораторне заняття (2 год)	[3, 4, 5]	Розробка алгоритмів симетричного шифрування та дешифрування	2 тижні

7	**Тема 7.** Криптографія. Асисиметричне шифрування.	Лекція (4 год)	[3, 4, 5, 6]	Опрацювання лекційного матеріалу (3 год.)	1 тиждень
	Тема 7. Розробка алгоритмів асиметричного шифрування та дешифрування	Лабораторне заняття (2 год)	[3, 4, 5, 6]	Розробка алгоритмів асиметричного шифрування та дешифрування (4год)	2 тижні
8	**Тема 8.** Презентації та оцінювання індивідуального завдання №1	Лабораторне заняття (2 год)		Захист індивідуального завдання	
9	**Тема 9.** Безпечне програмування. Кращі практики	Лекція (2 год)	[13, 14]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 9. Використання кращих практик безпечного програмування	Лабораторне заняття (2 год)	[13, 14]	Розробка функцій роботи з вхідними даними згідно безпечного програмування (4 год)	2 тижні
10	**Тема 10.** Безпека мікросервісної архітектури	Лекція (4 год)	[7, 8, 9]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 10. Розробка мікросервісу з підтримкою OAuth 2.0 та шлюзом API.	Лабораторне заняття (2 год)	[7, 8, 9]	Розробка мікросервісів (3 год)	2 тижні
11	**Тема 11.** Презентації та оцінювання індивідуального завдання №2	Лабораторне заняття (2 год)		Захист індивідуального завдання	
12	**Тема 12.** Безпека ВЕБ-додатків.	Лекція (2 год)	[10, 11, 12]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 12. Розробка ВЕБ-додатку згідно безпеки	Лабораторне (2 год)	[10, 11, 12]	Розробка ВЕБ-додатку(5 год)	2 тижні
13	**Тема 13.** Тестування безпеки.	Лекція (4 год)	[10, 11, 12]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 13. Розробка скриптів тестування безпеки.	Лабораторне заняття (2 год)	[10, 11, 12]	Розробка скриптів тестування безпеки (5год.)	1 тиждень
14	**Тема 14.** Презентації та оцінювання індивідуального завдання №3	Лабораторне заняття (2 год)		Захист індивідуального завдання	