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

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та
інформатики
Львівського національного університету
імені Івана Франка
(Протокол № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри

Петро ВЕНГЕРСЬКИЙ

Силабус
з “Навчальної практики та командних проектів”,
що проходить в межах ОПП Кібербезпека
першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека та захист інформації

Львів - 2023

Назва дисципліни	Навчальна практика та командні проекти
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Терлецький Олександр Ігорович, Асистент кафедри кібербезпеки Грицишин Остап Орестович, Асистент кафедри кібербезпеки, В'ячало Михайло Михайлович, Асистент кафедри кібербезпеки
Контактна інформація викладачів	oleksandr.terletskyi@lnu.edu.ua; https://ami.lnu.edu.ua/course/navchalna-obchysliuvalna-praktyka-kb; Ostap.hrytsyshyn@lnu.edu.ua; https://ami.lnu.edu.ua/course/navchalna-obchysliuvalna-praktyka-kb Головний корпус ЛНУ ім. І. Франка, каб. 260. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення практичних занять (а також за розкладом консультацій кафедри).
Сторінка курсу	https://ami.lnu.edu.ua/course/navchalna-obchysliuvalna-praktyka-kb
Інформація про дисципліну	"Навчальна практика та командні проекти" належить до циклу професійної та практичної підготовки з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка проходить у 2-му і 4-му семестрах в обсязі 6-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	"Навчальна практика та командні проекти" передбачає набуття студентами практичних вмінь з процедурного та об'єктно-орієнтованого програмування, а також важливих напрямків кібербезпеки, таких як шифрування, хешування, аутентифікація та авторизація. Студенти навчаться розробляти програмне забезпечення для захисту інформації

	від несанкціонованого доступу, і отримають практичні навички проектування, розробки, налагодження та тестування програм з урахуванням аспектів кібербезпеки - збереження, цілісність, шифрування (захист даних), права доступу до даних. Вміння та знання принципів
Мета та цілі дисципліни	Мета і цілі даної практики – поглиблення і закріплення здобутих теоретичних знань з програмування, роботи з забезпечення цілісності та захисту даних (шифрування даних), конфіденційності і доступу до даних різного типу користувачів, розвитку логічного мислення та набуття професійних та командних навиків.
Література для вивчення дисципліни	*Основна література* 1. Stephen Prata. C++ Primer Plus (Developer's Library). Addison-Wesley Professional; 6th edition (October 18, 2021), – 1440 p. 2. Bruce Brown. Cybersecurity Fundamentals: Best Security Practices (cybersecurity beginner) (May 27, 2023), - 135p 3. Ярошко С.А. Методи розробки алгоритмів. Програмування мовою С++: Навчальний посібник / С.А. Ярошко, О.С. Ярошко – Львів: ЛНУ імені Івана Франка, 2022. – 248 с. [електронна версія: https://lnuittutor.github.io/] 4. Bruce Eckel. Thinking in C++, Vol. 1: Introduction to Standard C++, 2nd Edition. Prentice Hall; (March 25, 2020), 840 p. 5. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посібник. – Запоріжжя : НУ «Зап. пол.», 2020. – 192 с 6. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120с. *Додаткова література* 7. https://www.learncpp.com/ 8. https://en.cppreference.com/w/ 9. https://cplusplus.com/ 10. Nicolai M. Josuttis. C++ Standard Library, The: A Tutorial and Reference. Addison-Wesley Professional; 2nd edition (March 30, 2012) – 1136 p. 11. Ярошко С.А. Методи розробки алгоритмів. Програмування мовою С++: Навчальний посібник / С.А. Ярошко, О.С. Ярошко – Львів: ЛНУ імені Івана Франка, 2022. – 248 с. [електронна версія: https://lnuittutor.github.io/]
Обсяг курсу	Загальний обсяг: 180 годин. З них 180 год. самостійної роботи.
Очікувані результати навчання	• **Після завершення цього курсу студент буде знати:** ○ Основи процедурного та об'єктно-орієнтованого програмування. ○ Стандартну бібліотеку шаблонів. ○ Принципи шифрування, хешування, аутентифікації та авторизації. • **Вміти:** ○ Самостійно розробляти прості алгоритми для доступу, збереження цілісності та конфіденційості даних.

	○ Використовувати програмне середовище MS Visual Studio для розробки безпечних програм. ○ Використовувати набуті знання та навички для створення програм, що захищають інформацію від несанкціонованого доступу. ○ Проектувати, розробляти, налагоджувати та тестувати програми з врахуванням аспектів кібербезпеки. Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 3, КЗ 5, КФ 2, КФ 12; та програмних результатів навчання: ПРН 1-4, ПРН 6, ПРН 10, ПРН 53
Ключові слова	програмування, ООП, C++, стандартна бібліотека шаблонів, кібербезпека
Формат курсу	Очний Виконання практичних робіт та консультації.
Теми	• **Система керування паролями** ○ Реалізація програми, яка зберігає та управляє паролями користувачів. ○ Використання хеш-функції (наприклад, SHA-256) для збереження паролів у безпечному форматі. ○ Генерація випадкових паролів та зміни паролів. ○ Забезпечення шифрування бази даних паролів та безпечну обробку вводу/виводу. ○ (добавити з програмування) • **Система перевірки безпеки мережі:** ○ Розробка програми, яка сканує мережу для виявлення підключених пристроїв. ○ Використання сокетів для встановлення з'єднань та отримання інформації про пристрої у мережі. ○ Аналіз відкритих портів та служб на пристроях для виявлення потенційних вразливостей. ○ Створення звіту про знайдені вразливості та поради щодо забезпечення мережевої безпеки. • **Система аналізу вразливостей файлової системи:** ○ Розробка програми для сканування та аналізу вразливостей файлової системи. ○ Функції управління файлами у C++ для перегляду атрибутів файлів та папок. ○ Аналіз прав доступу до файлів та папок для виявлення потенційних вразливостей. ○ Знаходження вразливостей, таких як недостатні права доступу або небезпечні дії, та поради щодо виправлення.
Підсумковий контроль,	Диференційований залік у кінці 2,4 семестру

форма	
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Практичні роботи, індивідуальні завдання, самостійна робота, консультації Практичні роботи, індивідуальні завдання: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу. Самостійна робота: репродуктивний метод, дослідницький метод.
Необхідне обладнання	Комп'ютер із програмним забезпеченням Visual Studio 2017/2019, Internet. Сервіс Active Directory в операційній системі Windows. Програмне забезпечення для архівування даних.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються наступним чином: • Індивідуальні завдання: максимальна кількість балів 70 • Захист власних проектів: максимальна кількість балів 30 Підсумкова максимальна кількість балів 100. • 10 індивідуальних завдань по 7 балів кожне,. 7 балів – студент виконав завдання вчасно та якісно, 6 балів – студент виконав завдання повністю проте допустив помилки реалізації алгоритму, 4 бали – студент вчасно виконав завдання проте частково, 2 бали – студент частково, неякісно і невчасно виконав завдання, 0 балів – не виконав завдання. • захист проектів – 30 балів: 10 проектів по 3 бали кожний. 3 бали – студент повністю виконав проект, продемонстрував результати та відповів на поставлені запитання, 2 бали – студент частково виконав проект, продемонстрував результати, але не відповів на поставлені запитання, 1 бал – студент частково виконав проект, але не зумів продемонструвати його результати та не відповів на поставлені запитання, 0 балів – студент не захищав проект. Для одержання заліку студент повинен оформити звіт практики, який повинен містити: титульну сторінку та опис виконаних завдань. Для кожного завдання має бути вказано: номер варіанту, формулювання умови, результати роботи програми у вигляді скрін-шотів, текст коду програмної реалізації. **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. **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.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.