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 2023р.)

Зав. кафедри П.С.Венгерський

Силабус з навчальної дисципліни "Безпека ігрових додатків", що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека та захист інформації

Львів - 2023

Назва дисципліни	Безпека ігрових додатків
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	Грицишин Остап Орестович, Асистент кафедри кібербезпеки,
Контактна інформація викладачів	ostap.hrytsyshyn@lnu.edu.ua; https://ami.lnu.edu.ua/employee/hrytsyshyn-o-o 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 (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/course/navchalna-obchysliuvalna-praktyka-kb
Інформація про дисципліну	Дисципліна “Безпека ігрових додатків” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека яка викладається в 8-му семестрах в обсязі 6 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).

Коротка анотація дисципліни	Дисципліна "Безпека ігрових додатків" передбачає навчання студентів основам створення ігрових застосунків в середовищі Unity із використанням мови програмування C#. Водночас, курс поглиблено зосереджується на важливості і методах забезпечення кібербезпеки в розробці ігрових додатків. Студенти дізнаються про сучасні підходи до захисту даних і коду, а також про техніки обфускації і методи аутентифікації, що є ключовими для забезпечення безпеки ігрових продуктів. Курс має на меті не лише надати теоретичні знання, а й розвинути практичні навички у сфері кібербезпеки, критично необхідні для сучасного розробника ігрових застосунків.
Мета та цілі дисципліни	Метою дисципліни "Безпека ігрових додатків" є надання студентам глибокого розуміння та практичних навичок у розробці ігрових застосунків з використанням середовища Unity та мови програмування C#, з особливим акцентом на застосуванні принципів та методів кібербезпеки. Курс має на меті ознайомити студентів з викликами, які стоять перед розробниками ігрових застосунків у контексті забезпечення безпеки додатків, та навчити їх ефективно вирішувати ці виклики за допомогою сучасних технологій і підходів.
Література для вивчення дисципліни	*Основна література* 1. C# 9.0 in a Nutshell: The Definitive Reference by Joseph Albahari, Ben Albahari. O'Reilly Media; 1st edition February 21, 2021. 2. Unity 2021 Cookbook: Over 140 recipes to take your Unity game development skills to the next level by Matthew Smith, Shaun Ferns; Fourth Edition September 2021. 3. Bruce Brown. Cybersecurity Fundamentals: Best Security Practices (cybersecurity beginner); May 27, 2023 4. Cybersecurity A Complete Guide, Gerardus Blokdyk , 2021 *Додаткова література* 5. https://docs.unity3d.com/Manual/index.html 6. https://docs.unity3d.com/ScriptReference/index.html 7. https://dotnet.microsoft.com/en-us/learn/cshar
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 70 год., з них 28 год. лекцій та 42 год. лабораторних робіт. Самостійної роботи: 110 год.

Очікувані результати навчання	• **Після завершення цього курсу студент буде знати:** ○ Основи розробки ігрових застосунків у середовищі Unity і програмування на мові C#. ○ Принципи обфускації коду та даних, що застосовуються для підвищення безпеки ігрових додатків. ○ Основні аспекти та методи кібербезпеки, включаючи шифрування, аутентифікацію та авторизацію, специфічні для ігрових застосунків. ○ Найкращі практики та стратегії захисту ігрових додатків від потенційних кіберзагроз. • **Після завершення цього курсу студент буде вміти:** ○ Розробляти ігрові застосунки з використанням Unity та C#, враховуючи вимоги та рекомендації забезпечення безпеки. ○ Застосовувати методи обфускації та шифрування для захисту коду та даних в ігрових проектах. ○ Ідентифікувати потенційні вразливості в ігрових застосунках та розробляти ефективні стратегії їх усунення. Курс забезпечує набуття таких компетентностей: КІ, ЗК 1, ЗК 3, ЗК 5, ФК 2, ФК 12; та програмних результатів навчання: ПРН 1-4, ПРН 6, ПРН 10, ПРН 53
Ключові слова	розробка ігрових застосунків, Unity, C#, кібербезпека, обфускація коду, шифрування даних, аутентифікація
Формат курсу	Очний
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці семестру
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	● Лабораторні роботи ● Індивідуальні завдання ● Самостійна робота ● Консультації

Необхідне обладнання	● Комп'ютер із встановленим Unity Personal Edition (безкоштовна версія). ● Visual Studio Community Edition (безкоштовна версія) для програмування на C#. ● Доступ до Інтернету для завантаження необхідного програмного забезпечення та доступу до ресурсів та документації. ● Програмне забезпечення для архівування даних, наприклад, 7-Zip або WinRAR (безкоштовні версії). ● Git для контролю версій та співпраці в команді (безкоштовна версія). ● Firebase для баз даних, аутентифікації користувачів та інших бекенд-сервісів (безкоштовний тарифний план).

Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються наступним чином: ● Лабораторні роботи: 20% семестрової оцінки; максимальна кількість балів – 20. ● Індивідуальний проект: 30% семестрової оцінки; максимальна кількість балів – 30. ● Підсумкове тестування: 50% семестрової оцінки; максимальна кількість балів – 50. Підсумкова максимальна кількість балів 100. **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 незарахуванння 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 всіх видів письмових 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 набрані на лабораторних заняттях, 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 контролю	1. Представити звіт індивідуального проєкту, який міститиме: a. Титульну сторінку. b. Опис проекту, включаючи його мету та завдання. c. Детальний опис реалізованих ігрових механік та елементів кібербезпеки (обфускація коду, шифрування даних, аутентифікація та авторизація). d. Скріншоти з ключовими елементами ігрового процесу та імплементованими функціями безпеки. e. Вихідний код основних компонентів проекту з коментарями. 2. Пройти підсумкове тестування, яке оцінює знання теоретичного матеріалу за курс, включно з основами розробки в Unity, програмування на C#, а також принципи та методики забезпечення кібербезпеки в ігрових додатках. Захист індивідуального проєкту відбудеться в кінці семестру.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

№	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Термін виконання
1	Вступ до курсу "Безпека ігрових додатків". Основні цілі, значення курсу та введення в ігрову безпеку.	лекція – 2 год самостійна робота – 6 год	[1-7]	2 тижні
2 -3	Основи розробки в Unity. Перший погляд на Unity та його можливості для створення ігор.	лекція – 4 год лабораторна – 4 год самостійна робота – 16 год	[1-2, 5-7]	2 тижні
4	Програмування на C# в Unity. Основи мови C# і як вона використовується в Unity для розробки ігрової логіки.	лекція – 2 год лабораторна – 4 год самостійна робота – 8 год	[1-2, 5-7]	2 тижні
5	Робота з асетами та сценами в Unity. Як управляти ресурсами і створювати ігрові світи.	лекція – 2 год лабораторна – 2 год самостійна робота – 8 год	[1-2, 5-7]	2 тижні
6	Фізика та анімація в Unity. Використання Unity Physics та	лекція – 2 год лабораторна – 4 год самостійна робота – 8 год	[1-2, 5-7]	2 тижні

	Animator для додавання реалістичності іграм.			
7	Скриптинг та обробка подій: Розгляд подій та їх обробки в контексті ігрової логіки.	лекція – 2 год лабораторна – 4 год самостійна робота – 8 год	[1-2, 5-7]	2 тижні
8-9	Шифрування даних та безпека зберігання: Застосування методів шифрування для захисту ігрових даних.	лекція – 4 год лабораторна – 4 год самостійна робота – 16 год	[1-7]	1 тиждень
10	Системи аутентифікації в іграх. Реалізація надійних систем аутентифікації та авторизації.	лекція – 2 год лабораторна – 4 год самостійна робота – 8 год	[1-7]	2 тижні
11	Безпека мережі для онлайн-ігор. Принципи захисту мережевих ігрових проектів від загроз.	лекція – 2 год лабораторна – 4 год самостійна робота – 8 год	[1-7]	1 тиждень
12	Тестування безпеки ігрових застосунків. Підходи та інструменти для аудиту безпеки ігор.	лекція – 2 год лабораторна – 2 год самостійна робота – 8 год	[1-7]	2 тижні
13	Адаптація заходів безпеки для ігор на різних платформах. Особливості забезпечення безпеки ігрових застосунків на платформах iOS, Android та інших, з урахуванням їх специфіки.	лекція – 4 год лабораторна – 4 год самостійна робота – 16 год	[1-7]	1 тижні
14	Здача курсового проекту. Процес представлення та обговорення курсових проектів, оцінювання їх якості, повноти реалізації поставлених завдань та відповідності критеріям безпеки.	лабораторна – 6год		1 тиждень

	Підсумкове тестуванн. Оцінювання здобутих знань та навичок в кінці курсу.			