



Силабус курсу ПРОГРАМУВАННЯ ДЛЯ КІБЕРБЕЗПЕКИ

Ступінь вищої освіти – бакалавр

Галузь знань – F Інформаційні технології

Спеціальність - F5 Кібербезпека та захист інформації

Освітньо-професійна програма – «Кібербезпека»

Рік навчання: 1

Семестр: 2

Кількість кредитів: 5

Мова викладання: українська

Керівник курсу

ППП

Степан ІВАСЬЄВ

Контактна інформація

isv@wunu.edu.ua

Опис дисципліни

Курс «Програмування для кібербезпеки» орієнтований на вивчення основ програмування з метою застосування навиків в сфері кібербезпеки. Метою дисципліни є вивчення науково-практичного інструментарію технологій структурного та об'єктно-орієнтованого підходів при проектуванні комп'ютерних програм та його використанні при реалізації програмних додатків. Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами систематичних знань та практичних навичок для створення програмних продуктів з ефективним використанням сучасних технологій

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/2	Основи ООП в C++. C++ в кібербезпеці	Організовувати власну професійну діяльність, обирати й використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	Поточне опитування
2/2	Конструктори.	Вміти створювати та застосовувати різні типи конструкторів для безпечної ініціалізації об'єктів і контролю доступу до ресурсів. Вміти проектувати класи так, щоб конструктори запобігали некоректному стану об'єкта та забезпечували цілісність і безпеку даних.	Поточне опитування
2/2	Можливості використання класів.	Знати призначення та основні можливості використання класів у C++, включно з інкапсуляцією, спадкуванням і поліморфізмом. Створювати класи для моделювання об'єктів безпечних систем, реалізовувати методи для контролю доступу й перевірки даних;	Поточне опитування
2/2	Перевантаження операторів в C++.	Вміти безпечно перевантажувати оператори для власних типів даних, забезпечуючи передбачувану та контрольовану поведінку. Знати потенційні ризики безпеки, що можуть	Поточне опитування

		виникати через неправильне перевантаження операторів (наприклад, порушення цілісності даних або неочікувані побічні ефекти).	
2/2	Конструктор копіювання.	Реалізовувати конструктор копіювання для безпечного дублювання об'єктів, що містять динамічні ресурси або критичні дані. Контролювати копіювання об'єктів у програмах, пов'язаних із безпекою, щоб запобігти несанкціонованому розповсюдженню або зміні інформації.	Поточне опитування
2/2	Зв'язки між об'єктами в C++.	Проектувати зв'язки між об'єктами з урахуванням принципів безпеки, запобігаючи витокам пам'яті та некоректним посиланням. Реалізовувати взаємодію об'єктів так, щоб забезпечити контроль доступу, цілісність даних і надійність програмного коду.	Поточне опитування
2/2	Спадкування в C++. Безпечне використання спадкування і вразливості пам'яті	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	
2/2	Спадкування і специфікатори доступу.	Спадкування в C++ і вплив специфікаторів доступу (public, protected, private) на видимість членів базового класу у похідних класах. Правильно застосовувати спадкування та специфікатори доступу для контролю доступу до критичних ресурсів і методів класу	Поточне опитування
2/2	Віртуальні функції в C++.	Принципи роботи віртуальних функцій у C++, їх роль у реалізації поліморфізму та динамічного зв'язування. Можливі проблеми безпеки, пов'язані з неправильним використанням віртуальних функцій, зокрема переписування vtable і некоректне звільнення ресурсів.	Поточне опитування
2/2	Чисті віртуальні функції. VTABLE і атаки на таблиці віртуальних функцій	Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.	Поточне опитування
2/2	Динамічне приведення типів.	Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.	Поточне опитування
2/2	Шаблони в C++.	Створювати безпечні функціональні та класові шаблони, які коректно працюють з різними типами даних.	Поточне опитування
2/2	Винятки в C++.	Механізм обробки винятків у C++ (try,	Поточне

		catch, throw) та його роль у безпечному управлінні помилками й ресурсами.	опитування
2/2	Розумні вказівники. Семантика переміщення в C++.	Потенційні ризики безпеки, пов'язані з неправильним використанням вказівників і переміщенням об'єктів, зокрема використання вищих показників або подвійне звільнення пам'яті.	Поточне опитування
2/2	Потоки вводу і виводу. Буферизація та переповнення буфера.	Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.	Поточне опитування

Літературні джерела

1. Куліков В.М., Рябцев В.В., Паршуков С.С. Об'єктно-орієнтоване програмування для фахівців з кібербезпеки: навч. посіб. / ІСЗІ КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, 2023. 365 с.
2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
3. Вступ до програмування мовою C++. Організація обчислень : навч. посіб. / Ю. А. Белов, Т. О. Карнаух, Ю. В. Коваль, А. Б. Ставровський. – К. : Видавничо-поліграфічний центр "Київський університет", 2012. – 175 с.
4. Трофименко О. Г. C++. Алгоритмізація та програмування : підручник / О. Г. Трофименко, Ю. В. Прокоп, Н. І. Логінова, О. В. Задерейко. 2-ге вид. перероб. і доповн. – Одеса : Фенікс, 2019. – 477 с.
5. «Об'єктно-орієнтоване програмування. Практикум»: навч. посіб. для студентів спеціальності 163 «Біомедична інженерія» / КПІ ім. Ігоря Сікорського; уклад. В.А. Данілова.– КПІ ім. Ігоря Сікорського.- 2021. – 121 с
6. BDM. C++ & Python Complete Manual. 11th Edition. - Papercut Limited, 2022. - 148 p.
7. Kirk Dorothy R. Demystified Object-Oriented Programming with C++: Implement proven object-oriented design principles to write better code and create robust software. Packt Publishing, 2021. — 568 p.
8. Bouras Aristides. C++ and Algorithmic Thinking for the Complete Beginner: Learn to Think Like a Programmer/2nd edition. - Independently published, 2021. - 1056 p.
9. Briggs W. C++20 for Lazy Programmers: Quick, Easy, and Fun C++ for Beginners. 2nd.ed. - Apress, 2020. - 706p.
10. Browning J. Burton, Sutherland Bruce. C++20 Recipes: A Problem-Solution Approach. 2nd edition. - Apress, 2020. - 657 p.
11. Cyganek B. Introduction to Programming with C++ for Engineers. Hoboken: Wiley, 2021. – 649 p.
12. Mueller J.P. C++ All-in-One For Dummies. 4th ed. - Wiley, 2021. — 915 p.
13. Davidson J. Guy, Gregory Kate. Beautiful C++: 30 Core Guidelines for Writing Clean, Safe, and Fast Code (Final). Addison-Wesley Professional, 2022. - 352 p.
14. Deitel P., Deitel H. C How to Program. 9th ed. - Pearson, 2022. - 838 p.
15. Singer Adam B. Practical C++ Design: From Programming to Architecture. 2nd Edition. - Apress Media LLC, 2022. - 303 p.
16. Fertig A. Programming with C++20: Conceptes, Coroutines, Ranges, and more. Fertig Publications, 2021. - 344 p.
17. Gladstone Adam. C++ Software Interoperability for Windows Programmers. Apress Media LLC, 2022. - 235 p.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-10 балів). Перескладання

модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Здобувач зобов'язаний виконувати усі роботи та завдання самостійно. Під час контрольного заходу він може користуватися лише дозволеними допоміжними матеріалами або засобами; йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, а також використовувати, розповсюджувати або збирати варіанти чужих робіт чи контрольних завдань.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, карантин, воєнний стан, міжнародне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу та з дозволу дирекції факультету.

Оцінювання

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-6.	Підсумкове модульне тестування за темами №1-8.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №7-12.	Підсумкове модульне тестування за темами № 9-15.	Визначається як середнє арифметичне з оцінок за виконання та презентацію одного завдання тренінгу.	Підсумкове тестування за результатами опрацювання теоретичного матеріалу. Теоретичні питання: 25 питань по 4 бали - мах 100 балів	Теоретичні питання: у вигляді тестів - мах 60 балів. Практичне завдання - мах 40 балів

Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

Виконання лабораторних робіт:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав усі кроки в рамках лабораторної роботи, правильно задокументував етапи та вільно оперує поняттями та принципами, що відносяться до теми дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання лабораторної роботи, проте в процесі виконання допустив кілька дрібних помилок, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), в процесі роботи виникали додаткові запитання.

60-74 балів (Задовільно) - здобувач освіти виконав завдання лабораторної роботи, але з суттєвими помилками, наприклад, не з першого разу чи не до кінця. Розуміння поставлених у лабораторній роботі завдань є поверхневим та неповним.

1-59 балів (Незадовільно) - здобувач освіти не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з програмним

забезпеченням.

Підсумкове модульне тестування:

90–100 балів – правильно виконано 90–100% завдань тесту.

75–89 балів – правильно виконано 75–89% завдань тесту.

60–74 бали – правильно виконано 60–74% завдань тесту.

1–59 балів – правильно виконано менше 60% завдань тесту.

Тренінг:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат, в процесі роботи виникали додаткові запитання.

60-74 балів (Задовільно) - здобувач освіти виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених у тренінгу завдань є поверхневим.

1-59 балів (Незадовільно) - здобувач освіти не зміг виконати завдання або результати були повністю невірними. Не продемонстрував достатній рівень навичок роботи з апаратним та програмним забезпеченням.

Самостійна робота: оцінюється у вигляді тестування за результатами опрацювання теоретичного матеріалу. Теоретичні питання: 25 питань по 4 бали, Максимальна оцінка 100 балів.

Підсумковий екзамен - вид підсумкового контролю, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу з дисципліни «Програмування для кібербезпеки». Екзаменаційний білет складається з двох блоків.

Перший блок містить теоретичні питання і вигляді тестів, за кожну правильну відповідь тестування здобувач освіти отримує 4 бали, максимум 60 балів. Виконання практичних завдань передбачається у текстовому вигляді (засобами системи дистанційного навчання) та можуть бути прокоментовані усно для пояснення шляху реалізації поставленого практичного завдання. Максимальна кількість балів за виконання практичного завдання 40 балів.