Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

СИЛАБУС
Безпекові технології програмування

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю.М._____
(підпис) (прізвище та ініціали)

«26» серпня 2024р.

Розробник (-и): Гребенник. А.Г., старший викладач кафедри кібербезпеки та математичного моделювання _____
(підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від 26 серпня 2024р. № 7

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	Вибіркова
Мова викладання	Українська
Рік навчання та семестр	1 рік, 2 семестр 125 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Гребенник. Алла Григорівна, старший викладач кафедри кібербезпеки та математичного моделювання
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.fi/citations?hl=uk&user=zDx8WrsAAAAJ https://www.scopus.com/authid/detail.uri?authorId=57219054928 https://orcid.org/0000-0002-7464-1412
Контакти викладача	контактний телефон: +380977267613, E-mail: grebennik.alla@gmail.com.

2. Анотація курсу.

Дисципліна є складовою частиною фундаментальної підготовки та відноситься до навчальних дисциплін циклу «Вибіркові компоненти освітньої програми» за спеціальністю «Кібербезпека та захист інформації» (магістр).

Предметом навчальної дисципліни є вивчення вразливостей програмного забезпечення, аналіз помилок програмування, що призводять до таких вразливостей, ознайомлення з технологіями програмування що дозволяють знизити або усунути ризик їх використання зловмисниками при розробці шкідливих сценаріїв їх використання для несанкціонованого доступу до інформації.

Практична спрямованість дисципліни полягає в комплексному розгляді помилок програмування від їх виявлення, аналізу наслідків використання до безпечних альтернатив реалізації.

Посилання на курс в MOODLE: https://eln.stu.cn.ua/course/view.php?id=4618

3. Мета та цілі курсу.

Метою викладання дисципліни є ознайомлення студентів з найбільш розповсюдженими вразливостями програмного забезпечення, методами визначення ризиків та наслідків їх використання, розгляд технологій розробки безпечного програмного забезпечення.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності125 - Кібербезпека та захист інформації:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КФ 1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

4. Результати навчання.

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

У підсумку ЗВО повинен

1) знати:

– теорію та методи безпечного програмування для розв'язування прикладних задач та створення програмного забезпечення систем ІБ;
– лінійні та ієрархічні структури даних та алгоритми їх обробки;
– основи процедурного та об’єктно-орієнтованого програмування із застосуванням принципів безпечного програмування;
– етапи життєвого циклу розробки, методи проектування та реалізації безпечного програмного забезпечення;

2) вміти:

– застосовувати сучасні технології безпечного програмування в системах інформаційної безпеки та кібербезпеки;
– обирати відповідну специфіці задачі технологію програмування, методи зберігання та алгоритми обробки відповідних структур даних для створення захищених програм;
– виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування та вразливостей.

5. Пререквізити.

Передумовою для вивчення дисципліни є наявність базових знань з дисципліни «Стандартизація, сертифікація засобів та комплексів захисту інформації».

6. Обсяг курсу.

Вид заняття	Загальна кількість годин
Лекції	16 / 6
Практичні заняття	16 / 6
Самостійна робота	88 / 108
Всього кредитів	4

Лекційні, практичні заняття, розрахунково-графічна робота, самостійна робота проводяться з використанням системи дистанційного навчання Moodle, Teams, рекомендованих джерел, відеоматеріалів тощо.

7. Тематика курсу.

Лекції (16/6 годин):

1. Проблеми безпеки програмного забезпечення – 2/1 години.
   Предмет та завдання курсу «Безпекові технології програмування». Безпека програмного забезпечення (ПЗ). Концепції, стратегії, недоліки безпеки ПЗ. Вразливості ПЗ та їх використання. Запобігання використанню вразливостей ПЗ.
2. Безпека роботи з текстовими даними – 2/0,5 години.
   Символьні рядки. Розповсюджені помилки при роботі з рядками. Вразливості пов'язані з рядками та їх використання. Переповнення буферу. Порушення стеку. Впровадження коду. Стратегії контрзаходів при роботі з рядками.
3. Управління динамічною пам’яттю – 2/0,5 години.
   Вказівники. Розповсюджені помилки використання вказівників. Запис в довільну ділянку пам’яті. Виділення, вивільнення пам’яті, збір сміття. Некоректна обробка збоїв виділення пам’яті. Подвійне вивільнення пам’яті. Диспетчери пам’яті. Технології протидії.
4. Безпека арифметичних операцій – 2/0,5 години.
   Цілочисельні типи даних. Цілочисельна безпека. Вразливості, пов’язані з цілими числами. Переповнення, помилки перетворення, усічення числа. Технології запобігання: абстрактні типи даних, арифметика довільної точності, перевірка діапазону, виявлення переповнення.
5. Форматований вивід – 2/0,5 години.
   Використання вразливостей функцій форматованого виводу. Переповнення буферу, вихідні потоки, аварійне завершення програми, перезапис пам’яті. Рандомізація стеку. Стратегії протидії.
6. Паралельні обчислення – 2/1 години.
   Вразливості: стан гонки даних, ушкоджені значення, некоректна послідовність звернення до пам’яті. Модель пам’яті. Примітиви синхронізації. Властивості паралельного коду.
7. Файлове введення-виведення – 2/1 години.

Інтерфейси файлового введення-виведення. Управління доступом. Ідентифікація файла. Стратегії виявлення та протидії стану гонки.

8. Інструменти підвищення рівня безпеки програмного забезпечення – 2/1 години.
   Життєвий цикл розробки безпекового програмного забезпечення. Стандарти безпекового програмування. Інжиніринг вимог безпеки. Верифікація. Тестування. Аудит коду.

Практичні роботи (16/6 годин):

1. Безпека обробки рядків – 2/0,5 години.
2. Вказівники, їх модифікація, обробка винятків – 2/0,5 години.
3. Функції роботи з динамічною пам'яттю. Управління пам'яттю – 2/1 години.
4. Безпекові бібліотеки для роботи з цілими числами – 2/0,5 години.
5. Функції та безпека форматованого виводу – 2/0,5 години.
6. Потоки виконання коду. Безпека при багатопоточному програмуванні – 2/1 години.
7. Організація взаємодії потоків, що виконуються паралельно – 2/1 години.
8. Інтерфейси файлового введення-виведення – 2/1 години.

Самостійна робота (88/108 годин):

1. Проблеми безпеки програмного забезпечення.
2. Безпека роботи з текстовими даними.
3. Управління динамічною пам'яттю.
4. Безпека арифметичних операцій.
5. Форматований вивід.
6. Паралельні обчислення.
7. Файлове введення-виведення.
8. Інструменти підвищення рівня безпеки програмного забезпечення.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на накопичувальній системі та включає: поточний контроль (оцінювання практичних занять) – 40 балів, проміжний модульний контроль – 20 балів та підсумковий контроль – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до досягнення навчальних цілей.
Практичні заняття	Оцінка кожного практичного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – 3 бали; 2) аналіз отриманих результатів – 1 бал; 3) належне оформлення звіту – 1 бал.
Умови допуску до підсумкового контролю	1. Виконання та захист не менше 50% практичних робіт. 2. Проходження проміжного модульного контролю. 3. Виконання розрахунково-графічної роботи.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
1	Виконання практичних робіт	**0…40**
2	Проміжний модульний контроль	**0…20**
Усього поточний і проміжний модульний контроль		**60**
Семестровий контроль (Екзамен)		**40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	Оцінка ECTS	Оцінка за національною шкалою (екзамен)	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Політики курсу.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані практичні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ “Чернігівська політехніка”». Повторне складання екзамену з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання екзамену всі набрані протягом семестру бали анулюються, а повторний екзамен складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі практичної роботи оцінюється в 0,5 балу за кожну практичну роботу. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від

вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні практичних робіт (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Базова

1. Robert Seacord. Secure Coding in C and C++. – [Електронний ресурс]. – Режим доступу: https://insights.sei.cmu.edu/documents/1312/2005_009_001_52710.pdf

2. Костюк І.В., Козак Л.І., Стасевич С.П. Основи програмування – Новий світ-2000, 2021р., - 328 с.

3. Васильєв О.М. Програмування на С++ в прикладах та задачах – Ліра К, 2019р., - 382 с.

4. Савченко В., Мнушка О. Сучасні технології безпечного програмування. Практикум : навч.- метод. посіб. – Харків: ФОП Бровін О.В., 2024. —148 с.

5. Коробань О.В. Програмування на мові С. Навчальний посібник. – Умань: Візаві, 2023. 130 с.

Інформаційні ресурси

1. Система дистанційного навчання НУ «Чернігівська політехніка». Курс: Безпекові технології програмування (ВК9). – [Електронний ресурс]. – Режим доступу: https://eln.stu.cn.ua/course/view.php?id=4618

2. Бібліотека та читальний зал НУ «Чернігівська політехніка». – [Електронний ресурс]. – Режим доступу: http://library2.stu.cn.ua

3. Prometheus: Платформа масових відкритих онлайн-курсів [Електронний ресурс]. – Режим доступу: https://prometheus.org.