ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА МОДЕЛЮВАННЯ
ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Силабус навчальної дисципліни **«БЕЗПЕКА ПРОГРАМ ТА ДАНИХ»**	
1. Загальна інформація	
Освітня програма (галузь, спеціальність, рівень вищої освіти, форма навчання)	Освітня програма «Інженерія програмного забезпечення» Галузь знань: 12 «Інформаційні технології» Спеціальність: 121 «Інженерія програмного забезпечення» Рівень вищої освіти: Перший (бакалаврський) Форма навчання: Денна, заочна
Тип дисципліни (нормативна/вибіркова)	Нормативна
Кількість кредитів ECTS та кількість годин денна/заочна (лекції / лабораторні / самостійна робота здобувачів) **Форма контролю**	Кредити – 3,0; загальний обсяг годин – 90 год.; Денна: 16 лекц., 16 лаб. роб., 58 сам. роб. Заочна: 8 лекц., 8 лаб. роб., 74 сам. роб. Форма контролю – **іспит**
Викладачі (ПІП, наукові ступені і звання, контактний e-mail)	Гриценко Андрій Миколайович, канд. техн. наук am_hrytsenko@knu.edu.ua
Посилання на матеріали дисципліни (робоча програма, методичні матеріали)	http://mpz.knu.edu.ua/
Мова викладання	Українська
Інформація про розклад занять	http://asu.knu.edu.ua/time-table/chair
Інформація про консультації	Консультацію викладач проводить відповідно до затвердженого графіку
Кафедра: Адреса: Телефон: e-mail: Сайт: QR-code	вул. Віталія Матусевича, 11, корпус 1, каб. 317 м. Кривий Ріг; тел. 056-409-06-07 mpz@knu.edu.ua http://mpz.knu.edu.ua/

2. Коротка анотація до курсу

Дисципліна спрямована на формування у майбутніх фахівців з розробки програмного забезпечення достатнього рівня знань та навичок сучасних стандартів, підходів, методів та засобів захисту програм та даних. Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами основних понять програмно-апаратного захисту інформації, ідентифікації та аутентифікації користувачів комп'ютерних систем, засобів і методів обмеження доступу до програм, методів та засобів криптографічного захисту інформації, захисту програм від несанкціонованого копіювання та дослідження.

3. Мета та цілі курсу

Метою вивчення дисципліни є формування у студентів знань про сучасні стандарти, підходи, методи та засоби захисту програм та даних. Програма дисципліни орієнтована на глибоке та ґрунтовне засвоєння студентами основних понять щодо програмно-апаратного захисту інформації, ідентифікації та аутентифікації користувачів комп'ютерних систем, засобів і методів контролю доступу до програм, методів та засобів криптографічного захисту інформації, написання безпечного коду.

Завдання курсу полягає в надання здобувачам комплексу знань щодо сучасних методів захисту програмного забезпечення та даних від несанкціонованого доступу та дослідження, а також існуючих систем захисту програмного забезпечення та засобів, що застосовуються для зламу існуючих систем захисту. У процесі вивчення дисципліни здобувач має отримати компетентності та програмні результати навчання стосовно безпеки та захисту програм та даних.

4. Програмні компетентності	5. Результати навчання
ЗК02 Здатність застосовувати знання у практичних ситуаціях. **СК02** Здатність брати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування. **СК06** Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). **СК07** Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних. **СК12** Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності програмного забезпечення.	**Програмні результати навчання (ПР)** **ПР05** Знати і застосовувати відповідні математичні поняття, методи доменного, системного і об'єктно-орієнтованого аналізу та математичного моделювання для розробки програмного забезпечення. **ПР12** Застосовувати на практиці ефективні підходи щодо проектування програмного забезпечення. **ПР13** Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань. **ПР18** Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних. **ПР21** Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

6. Матеріально-технічне / інформаційне та навчально-методичне забезпечення

Комп'ютерний клас, проектор, доступ до інтернет.
Програмне забезпечення необхідне для дисципліни: Visual Studio 2022.
Дистанційний курс дисципліни на платформі Google :
https://classroom.google.com/c/NzEwMjYwNDY4ODYy

7. Тематика курсу

Тема 1. Основні поняття безпеки програм та даних. Предмет і задачі захисту програм і даних. Вразливість компютерних систем. Політика безпеки в комп'ютерних системах. Оцінка та механізми захисту програм та даних. Стандарти захисту даних.

Тема 2. Ідентифікація та автентифікація користувачів. Ідентифікація користувачів. Аутентифікація користувачів. Перевірка автентичності користувачів. Протоколи ідентифікації.

Тема 3. Криптографічний захист інформації. Основні поняття та визначання криптографічного захисту інформації. Симетричні алгоритми перетворення даних.

Тема 4. Асиметричні алгоритми шифрування. Основні поняття та визначання криптографічних алгоритмів шифрування з відкритим ключем. Технологія цифрового підпису.

Тема 5. Моделі розповсюдження програмного забезпечення. Моделі безкоштовного ПЗ. Моделі умовно-безоштовного ПЗ. Моделі комерційного ПЗ. Хмарні моделі.

Тема 6. Методи та засоби обмеження доступу до програм та даних. Вразливість комп'ютерних систем. Способи проникнення до комп'ютерних систем. Спостереження за користувачами комп'ютерних систем. Особливості обмеження доступу до програм та даних.

Тема 7. Захист програм від несанкціонованого дослідження. Методи дослідження програмного коду. Засоби дослідження програмного коду. Принципи та підходи щодо захисту програмного коду від несанкціонованого дослідження.

Тема 8. Віртуальні приватні мережі. Поняття про віртуальні захищені (приватні) мережі (VPN). Види віртуальних приватних мереж. Сервіси VPN. Способи утворення захищених тунелів. Рівні реалізації VPN. Протоколи: SSL, SOCKS, IPSec, PPTP, L2F, L2TF.

8. Система оцінювання

Загальна система оцінювання (за 100-бальною шкалою)

Виконання усіх лабораторних робіт – максимум 100 балів

Поточний контроль (за 100-бальною шкалою)

Студент має вчасно, успішно виконати і захистити лабораторні роботи (ЛР) з завданнями різного рівня, набираючи бали.

Вид роботи	Максимальна кількість балів		
	базовий рівень	достатній рівень	Високий рівень
ЛР№1	9	12	15
ЛР№2	14	18	23
ЛР№3	9	12	15
ЛР№4	9	12	15
ЛР№5	8	10	12
ЛР№6	11	16	20
Всього	60	80	100

Підсумковий контроль (відповідно до 100-бальної шкали ECTS)

Студент протягом семестру повинен отримати в сумі не менше 50 балів за виконання лабораторних робіт.

Підсумкова оцінка з дисципліни розраховується як середнє арифметичне суми балів, отриманої за виконання лабораторних робіт протягом семестру та оцінки за екзамен.

9. Політика курсу

Відвідування занять. Регуляція пропусків.

Передбачається систематичне відвідування здобувачами аудиторних занять, за винятком поважних причин. У випадку пропуску лабораторного заняття, студент має виконати та здати лабораторну роботу згідно графіку, наведеного у робочій програмі дисципліни. У випадку пропуску лекції студент опрацьовує матеріал самостійно та може задати питання на консультації.

Політика академічної доброчесності

Як викладач, так і здобувачі вищої освіти мають дотримуватися принципів академічної доброчесності згідно «Положення про академічну доброчесність у Криворізькому національному університеті». Окрім того, викладач повинен дотримуватись вимог Кодексу честі викладача, а здобувач вищої освіти – Кодексу честі студента.

Використання комп'ютерів/телефонів на занятті

На заняттях з курсу допускається використання персональних мобільних пристроїв задля досягнення навчальної мети. Є не припустимим використання персональних мобільних пристроїв задля сторонніх цілей (месенджери та термінові дзвінки за межами аудиторії). Використання комп'ютерів на лабораторних заняттях є обов'язковим задля досягнення навчальної мети.

Розробник силабусу:

Доцент кафедри моделювання та програмного забезпечення
канд. техн. наук Андрій ГРИЦЕНКО _____

Завідувач кафедри моделювання та програмного забезпечення, доцент,
канд. пед. наук Андрій СТРЮК _____

Гарант ОПП, доцент, канд. пед. наук Андрій СТРЮК _____