

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Циклова комісія, яка забезпечує викладання ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА АВТОМАТИЗАЦІЇ

Викладач	<u>Боюн Неоніла Олександрівна</u>
Семестр	<u>6-й</u>
Освітньо-професійний ступінь	<u>Фаховий молодший бакалавр</u>
Кількість кредитів ЄКТС	<u>4</u>
Форма контролю	<u>Диференційований залік</u>

ЗАГАЛЬНИЙ ОПИС ДИСЦИПЛІН

Мета вивчення освітнього компонента «Безпека програм та даних» - є навчання здобувачів освіти принципам захисту програмного забезпечення на всьому циклі його існування, дослідженню та використанню сучасних процедур забезпечення основних послуг безпеки інформації в інформаційно-комунікаційних ресурсах Інтернет-технологій та кіберпросторі, що засновані на використанні алгоритмів симетричної та несиметричної криптографії, цифровому підписі та протоколів інфраструктури відкритих ключів (ІВК)

Компетентнісний потенціал освітнього компонента (навчальної дисципліни) та результати навчання:

Інтегральна компетентність:

ІК1. Здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій в процесі професійної діяльності або навчання, що вимагає застосування методів і технологій комп'ютерної інженерії та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності, здійснювати контроль інших осіб у визначених ситуаціях.

Загальна компетентність:

ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК4. Здатність застосовувати знання у практичних ситуаціях.

ЗК7. Здатність працювати в команді.

ЗК8. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальна компетентність:

СК2. Здатність застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування апаратних, програмних та інструментальних засобів комп'ютерної інженерії.

СК3. Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями, прикладними та спеціалізованими комп'ютерно інтегрованими середовищами для розробки, впровадження та обслуговування апаратних та програмних засобів комп'ютерної інженерії.

СК4. Здатність брати участь у розробці системного та прикладного програмного забезпечення засобів комп'ютерної інженерії з використанням ефективних алгоритмів, сучасних методів і мов програмування.

СК5. Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

СК6. Здатність брати участь у модернізації апаратних та програмних засобів комп'ютерної інженерії.

СК7. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

СК10. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення.

Результати навчання (програмні результати навчання):

РН2. Знати і розуміти теоретичні положення, що лежать в основі функціонування апаратних та програмних засобів комп'ютерної інженерії.

РН3. Знати сучасні методи та технології для розв'язання прикладних задач комп'ютерної інженерії.

РН4. Застосовувати правові норми, норми з охорони праці, безпеки життєдіяльності у професійній діяльності.

РН6. Тестувати, діагностувати та обслуговувати апаратні та програмні засоби комп'ютерної інженерії.

РН9. Розробляти, тестувати, впроваджувати, експлуатувати програмне забезпечення для вбудованих і розподілених систем.

РН10. Здійснювати пошук інформації з різних джерел для розв'язання задач комп'ютерної інженерії.

РН11. Ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів комп'ютерної інженерії.

РН12. Поєднувати теорію і практику, знаходити та обґрунтовувати шляхи рішення типових задач у професійній діяльності з урахуванням виробничих інтересів.

РН15. Проводити інсталяцію та налаштування системного та прикладного програмного забезпечення, у тому числі програмних засобів захисту інформації з метою реалізації встановленої політики інформаційної безпеки.

Теми лекцій:

1. Механізми і політики розподілу прав доступу
2. Механізми шифрування. Симетричні та несиметричні криптосистеми
3. Протоколи автентифікації. Цифрові підписи
4. Комплексні системи захисту даних
5. Основні види атак на програмне забезпечення. Основи криптоаналізу Тема 6. Основи цифрової стеганографії
7. Основи технології відкритих ключів (PKI)
8. Захист програмного забезпечення в Інтернет-технологіях
9. Захист персональних даних

Теми лабораторних занять

1. Поняття захисту інформації та інформаційної безпеки. Критерії оцінки інформаційної безпеки. Аспекти захисту інформації
2. Засоби резервного копіювання та відновлення даних. Пристрої відновлення даних
3. Захист інформації засобами операційних систем
4. Управління паролями. Засоби збереження та доступу до паролів. Правила роботи з паролями.
5. Криптографічний вид захисту інформації.
6. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації
7. Поняття шкідливого програмного забезпечення. Основні типи та загальний огляд сучасних комп'ютерних вірусів

8. Захист комп'ютерних мереж та персональних комп'ютерів за допомогою брандмауера (Firewall)
9. Інформаційна безпека держави. Потенційні загрози, засоби їх попередження та ліквідації
10. Основи безпеки інформації в комп'ютерних мережах Харківський національний економічний університет імені Семена Кузнеця
11. Поняття авторського права. Захист авторських прав. Поняття комп'ютерного піратства
12. Поняття плагіату. Загальний огляд програмного забезпечення призначеного для виявлення плагіат