Національна металургійна академія України
Кафедра інформаційних технологій та систем

СИЛАБУС
навчальної дисципліни

Назва дисципліни	**Захист та безпека комп'ютерних систем**
Шифр та назва спеціальності	122 – Комп'ютерні науки
Назва освітньої програмии	Комп'ютерні науки
Рівень вищої освіти	Магістерський
Статус дисципліни	Вибіркова навчальна дисципліна циклу загальної підготовки
Обсяг дисципліни	4 кредити ЄКТС (120 академічних годин)
Терміни вичення дисципліни	2 семестр (III – IV чверті)
Назва кафедри, яка викладає дисципліну	Інформаційних технологій і систем (ІТС)
Провідний викладач (лектор)	Деревянко Олександр Іванович, канд. техн. наук, доц., проф. каф. ІТС E-mail: alex_di_46@ukr.net, кімн. 505
Мова викладання	Українська
Передумови вивчення дисципліни	Вивченню дисципліни має передувати вивчення дисциплін: - Вища математика; - Програмування
Мета навчальної дисципліни	Вивчення і освоєння студентами криптографічних методів, алгоритмів побудови процесів захисту інформації від несанкціонованого втручання та застосування протоколів організації технології захисту комп'ютерних систем
Компетентності, формування яких забезпечує навчальна дисципліна	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК13. Здатність оцінювати та забезпечувати якість виконуваних робіт. СК1. Здатність до математичного та логічного мислення, формулювання вимог та досліджування алгоритмів криптографічних методів захисту інформації у комп'ютерних системах, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач, аналізу та інтерпретування їх у галузі комп'ютерних наук. СК4. Здатність оцінити ефективність використання алгоритмів криптографічного захисту інформації (крипостійкість, часові та апаратні ресурси). СК7. Здатність застосовувати теоретичні та практичні методи технології захисту інформації у комп'ютерних системах, розробляти програмні реалізації алгоритмів криптографічного захисту інформації.
Програмні	В результаті вивчення дисципліни студент повинен

результати навчання	***знати:*** - типи і властивості методів криптографічного захисту інформації; - обмеження та можливості використання алгоритмів захисту інформації; - вимоги протоколів до організації технології захисту комп'ютерних систем для забезпечення крипостійкості. ***вміти:*** - проводити порівняльний аналіз властивостей криптографічних методів, алгоритмів захисту інформації від несанкціонованого втручання; - застосування протоколи організації технології захисту комп'ютерних систем. Дисципліна забезпечує досягнення таких програмних результатів навчання: ПР07. Вміти застосовувати методологію криптографічного захисту інформації у комп'ютерних системах від несанкціонованого втручання.
Зміст навчальної дисципліни	Модуль 1. Криптографічний захист методами замін та пістановок Модуль 2. Метод гамірування. Модуль 3. Стандарти шифрування даних ГОСТ 28147-89 та DES. Модуль 4. Методи захисту без обміну ключами - системи з відкритим ключем.
Заходи та методи оцінювання	Оцінювання модулів 1,2,3,4 здійснюється за результатами захисту лабораторних робіт за 12-бальною шкалою. Підсумкова оцінка навчальної дисципліни визначається як середнє арифметичне 4-х модульних оцінок за 12-бальною шкалою або іспит

Види навчальної роботи та її обсяг в акад. годинах

	Усього
Усього годин за навчальним планом	120
у тому числі: **Аудиторні заняття**	32
з них: - лекції	16
- лабораторні роботи	16
- практичні заняття	
- семінарські заняття	-
Самостійна робота	88
у тому числі при : - підготовці до аудиторних занять	8
- підготовці до заходів модульного контролю	4
- виконанні курсових проектів (робіт)	-
- виконанні індивідуальних завдань	-
- опрацюванні розділів програми, які не викладаються на лекціях	76

	Усього
Семестровий контроль	середнє арифметичне 4-х модульних оцінок або іспит

Специфічні засоби навчання	Навчальний процес передбачає використання комп'ютерних робочих місць, програмного забезпечення: С.
Навчально-методичне забезпечення	Основна література: 1. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. «Корнійчук" Киев. 2000. 2. Петраков А.В. Основы практической защиты информации. М. «Радио и связь».2000. 3. Спесивцев А.В. и др. Защита информации в персональных ЭВМ. М. «Радио и связь». 1993. Додаткова література: 4. Шнайдер Б. Прикладная криптография. – М.: Триумф., 2002. -816 с.

Укладач к.т.н., доц. _____ Олександр ДЕРЕВ'ЯНКО

Гарант освітньої програми, д.т.н., проф. _____ Вікторія ГНАТУШЕНКО