АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва показників	Характеристика
Повна назва дисципліни	***Основи криптографічного захисту інформації***
Викладацький склад	асистент Стабецька Т.А.
Напрям підготовки	6.170103 «Управління інформаційною безпекою»
Кількість годин	252
Кредити ECTS	7
Опис	Проблеми безпеки інформації за останні роки набули виключної актуальності, при цьому забезпечення захисту інформаційних технологій приймає комплексний характер. Серед різних методів захисту інформації (технічних, правових, організаційних та інших) найважливіше місце займають криптографічні методи. За останні два десятиріччя криптографія сформувалася у самостійну наукову дисципліну, що має свою специфіку постановок задач та методів їхнього дослідження. Знання основних понять криптографії, володіння криптографічними методами захисту інформації за сучасних умов вкрай необхідні будь-якому фахівцю, що займається створенням систем захисту інформації. ***Метою*** викладання дисципліни «Основи криптографічного захисту інформації» є надання студентам знань у галузі теоретичної криптографії та криптоаналізу, а також ознайомлення з основними принципами роботи криптографічних систем, математичними моделями джерел інформації, поняттями теоретичної та практичної секретності. Конкретні типи алгоритмів шифрування та криптографічних перетворень розглядаються у відповідності з їх класифікацією на класичні схеми, системи потокового шифрування, системи блокового шифрування та системи захисту інформації з відкритим ключем. **Завданнями вивчення навчальної дисципліни є:** • розгляд основних етапів історичного розвитку криптографії; • оволодіння теоретичними знаннями про основні методи криптографічного захисту інформації; • розгляд математичних моделей симетричних шифрів та їх властивостей; • оволодіння основними способами шифрування даних; • вивчення методів асиметричної криптографії; • дослідження особливостей криптографічних алгоритмів та криптографічних протоколів; • ознайомлення з основними положеннями нормативно-правового регулювання у галузі КЗІ; • розгляд основних напрямків розвитку сучасних систем КЗІ. *Результати навчання полягають у наступному:* - вміння використовувати сучасні криптографічні

	методи для захисту конфіденційної інформації; - здатність використовувати систему електронного підпису або режиму електронного цифрового підпису; - моделювання (проектування) алгоритмів криптографічних перетворень та елементів криптографічного аналізу на комп'ютері; Методи викладання: поєднання лекційних занять з роботою в комп'ютерній аудиторії. Всі методичні матеріали, завдання лабораторних та контрольних робіт тощо розташовані на персональному комп'ютері комп'ютерної лабораторії навчального закладу та використовуються при навчанні.
Тип дисципліни	Нормативна, цикл дисциплін професійної та практичної підготовки.
Мова	Українська.
Підсумковий контроль	*Іспит* у першому семестрі 3 курсу, *залік* у другому семестрі 3 курсу.
Навчальний рік	2016-2017 н.р.