АНОТАЦІЯ ДИСЦИПЛІНИ

Методи та засоби криптоаналізу

Обсяг дисципліни: 3 кредити / 90 академічних годин, з них: лекцій - 16 годин, практичних занять - 16 годин, самостійної роботи - 58 годин.

Опис дисципліни (мета та завдання): Завданням курсу є формування у студентів на основі системного підходу наукового світогляду, який дозволяє їм вільно орієнтуватись у теоретичних підходах до реалізації сучасних принципів побудови сучасних криптографічних систем і формування знань по визначенню стійкості криптографічних систем до сучасних методів криптоаналізу.

Метою курсу є формування знань та сукупності вмінь щодо розв'язання задач аналізу й оцінки показників стійкості й надійності систем та засобів криптографічного захисту інформації, розуміння теоретичних та практичних принципів щодо впровадження криптоаналітичних атак на шифри, й виявленню каналів їх вразливості.

Результати навчання (знати та вміти):

У результаті вивчення навчальної дисципліни студент повинен:

Знати: математичні моделі шифрів та напрямки їх класифікації; поняття й означення, що використовуються при описі властивостей шифрів та підходи до визначення їх надійності; показники стійкості та надійності шифрів (понятійно-аналітичний); аналітичні методи криптоаналізу блочних симетричних шифрів (продуктивно-синтетичний); статистичні методи криптоаналізу блочних симетричних шифрів (продуктивно-синтетичний); методи криптоаналізу несиметричних алгоритмів шифрування; перспективні напрямки розвитку сучасної криптографії, що стосуються підвищення стійкості та надійності криптографічних методів захисту інформації (ознайомчо-орієнтований).

Уміти: застосовувати отримані знання для оцінки показників практичної стійкості шифрів, виявлення каналів вразливості та оцінки ступеня загрози (виконувати дію, спираючись на постійний розумовий контроль без допомоги матеріальних носіїв інформації; розв'язувати задачі криптоаналізу засобів та систем захисту інформації; обґрунтовувати заходи для підвищення стійкості систем захисту інформації (виконувати дію, спираючись на постійний розумовий контроль без допомоги матеріальних носіїв інформації; оцінювати ступінь захищеності програмних та апаратних засобів захисту інформації (виконувати дію, спираючись на матеріальні носії інформації щодо неї); експлуатувати програмні засоби тестування та криптоаналізу шифрів (виконувати дію автоматично, на рівні навички).

Форми навчання: лекції, практичні заняття, самостійна робота.

Методи навчання: індивідуальні завдання для самостійної роботи.

Форма організації контролю знань: індивідуальні завдання; диференційований залік.

Критерії успішності навчання: до підсумкового контролю допускаються студенти, що успішно виконали індивідуальні завдання та мають позитивні оцінки із семінарських занять.

Лектор: Лагун А.Е. доцент кафедри управління інформаційною безпекою