Назва Практичні застосунки у криптографії
Тип. Вибіркова
Рік навчання. 2019-2020
Семестр. II
Кількість кредитів ЄКТС. 5
ПІБ лектора, науковий ступінь, посада. Євсеєв Сергій Петрович, д.т.н., с.н.с., завідувач кафедри кібербезпеки та інформаційних технологій

Результати навчання.

В результаті навчання студенти отримують навички дослідження криптографічних алгоритмів, які застосовуються в сучасних протоколах інформаційно-комунікаційних систем щодо забезпечення основних послуг конфіденційності, цілісності та автентичності даних. Формування ключових даних в алгоритмах симетричної та несиметричної криптографії, формування MAC і MDC-кодів, генераторів ПВП. Основами аналізу стійкості криптоалгоритмів, визначенню переваг та недоліків в умовах постквантової криптографії.

Обов'язкові попередні навчальні дисципліни

"Вища математика"

Зміст.

Основні напрямки застосування криптографії в сучасних інформаційно-комунікаційних системах та мережах. Сучасні практичні алгоритми симетричної криптографії. Сучасні практичні алгоритми несиметричної криптографії. Алгоритми формування геш-кодів. Використання генераторів ПВП в сучасних мережах. Алгоритми цифрового підпису, їх використання в системах відкритих ключів (PKI). Основи криптографії на еліптичних кривих. Основи дослідження криптостійкості сучасних криптосистем і алгоритмів.

Рекомендовані джерела.

1. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6

2. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом "Родовід", 2014. – 428 с.

3. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

4. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

5 Хорошко В. А. Методы и средства зашиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

Методи навчання.
Лекції, лабораторні.
Комунікативні методи навчання на лабораторних заняттях

Методи оцінювання
Поточний контроль (опитування)
Модульний контроль (контрольна робота)
Підсумковий контроль (екзамен)

Мова навчання Українська