ДИСЦИПЛІНА «ПРОБЛЕМИ КОДУВАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Анотація. Дисципліна «Проблеми кодування та захисту інформації» належить до переліку вибіркових дисциплін. Вона забезпечує формування у аспірантів знань щодо теоретичних основ та сучасних методів кодування інформації, криптографічного захисту даних та забезпечення інформаційної безпеки програмних систем. Розглядаються теорія інформації Шеннона, завадостійке кодування, симетрична та асиметрична криптографія, криптографічні протоколи, цифрові підписи, хеш-функції, а також постквантова криптографія. Вивчаються сучасні загрози інформаційній безпеці та методи побудови захищених програмних архітектур.

Мета навчальної дисципліни: формування у аспірантів здатності аналізувати та розробляти системи захисту інформації з використанням сучасних криптографічних методів та протоколів, що передбачає опанування математичних засад криптографії, теорії кодування, уміння оцінювати криптографічну стійкість систем, а також здатність проєктувати комплексні рішення для забезпечення конфіденційності, цілісності та доступності інформації.

Попередні вимоги: Аспірант повинен мати знання з дискретної математики, теорії чисел, алгебраїчних структур, теорії ймовірностей, а також базові знання з комп'ютерних мереж та операційних систем. Бажаним є досвід програмування та знайомство з основними концепціями інформаційної безпеки.

Змістовні модулі:

- Теорія інформації: ентропія, канали зв'язку, теореми Шеннона.
- Завадостійке кодування: коди Хеммінга, БЧХ, Ріда–Соломона, турбо-коди, LDPC.
- Симетрична криптографія: блокові та потокові шифри, AES, режими шифрування.
- Асиметрична криптографія: RSA, еліптичні криві, протокол Діффі–Гелмана.
- Хеш-функції та коди автентифікації повідомлень (MAC, HMAC).
- Цифрові підписи та інфраструктура відкритих ключів (PKI).
- Криптографічні протоколи: TLS, SSH, протоколи з нульовим розголошенням.
- Постквантова криптографія: решіткова криптографія, кодова криптографія.
- Аналіз вразливостей та атак на криптографічні системи.

Мова викладання: українська

Рік підготовки, шифр навчальної дисципліни: перше півріччя першого року навчання

Кількість кредитів: 4

Форма заключного контролю: іспит

Структура навчальної дисципліни: загальний обсяг 120 годин.

Викладач: Бичков Олексій Сергійович, д.т.н., проф., професор кафедри програмних систем і технологій факультету інформаційних технологій.

Інформація про викладача: https://fit.knu.ua/archives/189