ДИСЦИПЛІНА «МЕТОДИ ПОБУДОВИ СУЧАСНИХ КРИПТОСИСТЕМ»

Анотація. Дисципліна «**Методи побудови сучасних криптосистем»** забезпечує особистісний і професійний розвиток аспіранта та спрямована на формування ефективного дослідника і викладача вищої школи, здатного до використання сучасних методів дослідження кіберпростору та передачі знань. В курсі розглядається методологія побудови криптосистем. Окремо приділена увага новим тенденціям розподілу ключової інформації, як одному із важливих етапів при функціонуванні сучасних криптографічних систем.

Мета навчальної дисципліни: формування у здобувачів системи теоретичних знань та практичних умінь про сучасні наукові концепції, поняття, методи та технології криптографічного захисту інформації, їх відповідність до вимог найбільш поширених міжнародних стандартів.

Попередні вимоги: *аспірант повинен знати:* архітектуру комп'ютерних систем; основні операційні системи; основи побудови інформаційних систем та мереж; технології забезпечення кібербезпеки; криптографічні системи захисту інформації; основи технологій підтримки та прийняття рішень; основи аудиту інформаційних систем.

Змістовні модулі:

- криптографічна стійкість шифрів;
- сучасні симетричні криптосистеми;
- мережі Фейстеля, SP-мережі, поля Галуа GF(pn), побудова полів Галуа GF(2n);
- криптосистеми з відкритим ключем;
- алгоритм шифрування RSA;
- еліптична криптографія;
- поняття електронного цифрового підпису (ЕЦП); схеми використання;
- система ЕЦП Ель-Гамаля (EGSA);
- хешування. Вимоги до хешфункцій; схема Меркеля–Дамгарда; алгоритми сімейства MD і SHA.

Мова викладання: українська

Кількість кредитів: 4

Рік підготовки, шифр навчальної дисципліни: другий рік навчання, входить до переліку вільного вибору аспіранта, ДВА. 2.02.04.

Структура навчальної дисципліни: загальний обсяг 120 годин, у тому числі 24 години навчальних занять (10 год. - лекційні заняття, 12 год. - практичні заняття), 2 год. консультація, 96 годин самостійної роботи.

Викладач: Бучик Сергій Степанович, д.т.н., професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій.

Інформація про викладача: http://fit.univ.kiev.ua/archives/18833