ДИСЦИПЛІНА
«МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ»

Анотація. Дисципліна «Математичні основи захисту інформації» належить до вибіркових компонент освітньої програми, блоку дисциплін вільного вибору аспіранта. Вона забезпечує професійний розвиток, спрямована на формування концептуальних та методологічних знань у галузі математики, вміння критично аналізувати, оцінювати і синтезувати нові та комплексні ідеї, аналізувати наукові праці, формулювати методологічну базу власного наукового дослідження, здатність формулювати наукову проблему, робочі гіпотези досліджуваної проблеми. В рамках дисципліни вивчаються основні задачі математичного захисту інформації, криптографічні примітиви для їх розв'язання, способи побудови та аналізу криптографічних компонент, основні криптографічні протоколи.

Мета навчальної дисципліни: Розвиток навичок розв'язання комплексних проблем в галузі математики, використання новітніх інформаційних і комунікаційних технологій, здатності до абстрактного мислення, здатності до пошуку, оброблення та аналізу інформації з різних джерел, вміння генерувати нові ідеї, навички роботи в міжнародному науковому просторі, навички формулювання дослідницьких задач з математики, навички формулювання і строгого доведення математичних тверджень, перевірки правильності їх доведень, навички розв'язання задач математичного захисту інформації, навички аналізу загроз інформаційній безпеці, навички побудови відповідної математичної моделі і конструювання адекватних загрозам математично обґрунтованих засобів захисту інформації.

Попередні вимоги:
Аспірант повинен
1. *Знати*: основні задачі захисту інформації, основні криптографічні примітиви, методи доведення стійкості криптографічних компонент, методи побудови криптосистем з публічним ключем і схем цифрового підпису, протоколи вироблення спільного секрету, розподілу секрету, призначення гомоморфних криптосистем, принцип роботи блокчейну та криптовалют.
2. *Вміти*: проводити критичний аналіз, оцінку і синтез нових ідей і підходів в галузі математичних основ захисту інформації, самостійно застосовувати математичні методи захисту інформації, розробляти та аналізувати криптографічні компоненти.

Змістові модулі:
- Основні задачі і поняття захисту інформації. Криптографічні примітиви;
- Криптографія з публічним ключем;
- Криптографічні протоколи;

Мова викладання: українська.

Рік підготовки, шифр навчальної дисципліни: ВП 1.36, другий рік навчання.

Кількість кредитів: 4.

Форма заключного контролю: іспит.

Структура навчальної дисципліни: загальний обсяг 30 годин, у тому числі 24 години аудиторних занять (18 год. – лекційні заняття, 4 год. – практичні заняття, 2 год. – консульт.), 4 години – консультація, 2 години – іспит.

Викладач: Жук Ярослав Олександрович, чл.-кор. НАН України, д.ф.-м.н, професор, завідувач кафедри теоретичної та прикладної механіки механіко-математичного факультету.

Інформація про викладача:
http://tamd.univ.kiev.ua/about-us/teachers/
http://www.zhuk.com.ua