Назва дисципліни: «Прикладна криптологія»
Спеціальність: 122 «Комп'ютерні науки»
Циклова комісія спеціальності «Комп'ютерні науки»
Кількість годин: 120
Кредити ЄКТС: 4
Підсумкова форма контролю: залік

Анотація дисципліни

Курс дисципліни «Прикладна криптологія» спрямований на формування у студентів теоретичних знань і практичних навичок роботи за майбутньою спеціальністю. Оскільки побудова сучасної криптології як науки грунтується на сукупності фундаментальних понять математики, фізики, теорії інформації і складності обчислень. Проте, не дивлячись на органічно властиву їй складність, багато теоретичних досягнень криптології, зараз широко використовуються в нашому насиченому інформаційними технологіями житті. Для глибокого вивчення питань теоретичної криптографії доводиться знайомитися з теорією ймовірності і математичної статистики, вищою алгеброю, теорією чисел та іншими дисциплінами. Прикладна криптографія більше займається питаннями застосування досягнень теоретичної криптографії для потреб конкретних застосувань на практиці, тобто розробкою криптографічних алгоритмів. Також необхідно розрізняти теоретичний і практичний криптоаналіз. Основна мета теоретичного криптоаналізу полягає в оцінці стійкості існуючих криптосистем, що розробляються. Оцінка стійкості криптосистем надається у вигляді кількості операцій, необхідних для злому криптосистеми або у вигляді часу, який потрібний для злому. Основна мета практичного криптоаналізу полягає у зломі криптографічних алгоритмів, досліджуючи нові методи і модифікуючи ті, що існують.

Курс дисципліни «Прикладна криптологія» займається питаннями прикладної криптографії і прикладного криптоаналізу.

Цей етап навчання має допомогти студентам:

– використовувати професійно-профільовані знання і практичні навички методів фундаментальної та прикладної математики під час розв'язання стандартних задач і задач прикладного характеру в галузі комп'ютерних наук (РН03);
– розуміти загальні принципи та моделі побудови комп'ютерних мереж (РН06);
– застосовувати основні механізми та методи безпеки мереж і програмних систем (РН07);
– розробляти супровідну документацію на різних етапах процесу життєвого циклу розробки програмного забезпечення (РН15).

Компетентності, якими повинен оволодіти здобувач

Інтегральні:

– здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій або у процесі навчання, що вимагає застосування положень і методів комп'ютерних наук та може характеризуватися певною невизначеністю умов;

– нести відповідальність за результати своєї діяльності;

здійснювати контроль інших осіб у визначених ситуаціях.

Загальні:

- здатність до абстрактного мислення, аналізу та синтезу (ЗК3);
- здатність застосовувати знання у практичних ситуаціях (ЗК4);
- знання та розуміння предметної області та розуміння професійної діяльності (ЗК5).

Спеціальні (фахові, предметні):

- здатність використовувати теоретичні та фундаментальні знання в галузі комп'ютерних наук та інформаційних технологій для вирішення різноманітних проблем (СК2);
- здатність розробляти, аналізувати та застосовувати ефективні алгоритми для розв'язання конкретних професійних задач залежно від предметного середовища (СК3);
- здатність застосовувати принципи і методи побудови та використання мережевих технологій (СК5);
- здатність застосовувати методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу в умовах супроводження та експлуатації програмних систем і комплексів (СК6).