ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра математичного моделювання

Чопоров С.В.

СУЧАСНА КРИПТОГРАФІЯ

методичні рекомендації
для самостійної роботи студентів освітньо-кваліфікаційного рівня «магістр»
спеціальності «Інженерія програмного забезпечення»

Запоріжжя – 2014

Чопоров С.В. Сучасна криптографія: Методичні рекомендації для самостійної роботи студентів освітньо-кваліфікаційного рівня «магістр» спеціальності «Інженерія програмного забезпечення» / С.В. Чопоров. – Запоріжжя: ЗНУ, 2014. – 7 с.

ВСТУП

Самостійна робота студентів протягом усього періоду навчання в університеті є найважливішою ланкою формування фахівця.

Навчальні плани за курсом передбачають наступні основні види самостійної роботи:

1. Робота з підручником по змісту лекційного матеріалу;
2. Підготовка до виконання лабораторних робіт і складанню по них звіту;
3. Підготовка до контрольних робіт та підсумкового контролю (заліку або екзамену).

Вивчення теоретичного матеріалу рекомендується проводити в день прослуховування відповідної лекції . У процесі пророоблення необхідно з'ясувати все неясне і сформулювати питання, які варто задати викладачу на консультації. Для поглиблення знань та їх конкретизації потрібно самостійно відповідати на конкретні питання і вирішувати контрольні задачі з підручників.

Відведений на самостійну роботу час варто використовувати раціонально протягом усього семестру. Систематична робота над теоретичним матеріалом зменшує час, що вимагається на підготовку до лабораторних робіт і підсумкового контролю.

Підготовка до лабораторних робіт поряд з вивченням теорії пропонує аналіз конкретного змісту роботи послідовності її виконання, а також готування звіту з по результатам її виконання. При підготовці звітів по лабораторних роботах необхідно прагнути до точних систематизованих записів. Малюнки повинні бути простими і наглядними, для графіків потрібно вибирати зручний масштаб.

Основними формами контролю самостійної роботи студентів є співбесіда й опитування лабораторних занять, а також виконання індивідуальних завдань. За необхідності призначаються додаткові консультації.

Усі ці форми самостійної роботи переслідують загальні цілі та задачі: освоєння і поглиблення теоретичних знань курсу, розвиток навичок розв'язання прикладних задач, придбання досвіду правильного оформлення науково-технічної документації та інші.

Самостійна робота студентів в обов'язковому порядку підлягає контролю. Тим самим переслідуються наступні цілі:

- спонукання студента до глибокого регулярного вивчення курсу протягом усього семестру;
- допомога студенту об'єктивною оцінкою його роботи;
- установлення «зворотного зв'язку» між викладачем і студентами;
- представлення деканам, кафедрам важливої інформації для представлення стану навчального процесу і своєчасного вживання заходів по його поліпшенню .

Система контролю самостійної роботи повинна передбачати перевірку фізичного виконання студентом видаваних йому навчальних доручень, так і з'ясування рівня глибини його знань.

МЕТА ТА ЗАВДАННЯ ДИСЦИПЛІНИ

Мета – оволодіння основними методами і засобами використання криптографічних методів для захисту інформації.

Завдання – формування практичних навичок, необхідних для використання методів і засобів сучасної криптографії у професійній діяльності.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- криптографічні алгоритми;
- категорії алгоритмів шифрування;
- структуру алгоритмів симетричного шифрування;
- режими роботи алгоритмів шифрування;
- можливі атаки на алгоритми шифрування;
- можливі атаки на шифратори.

вміти:

- використовувати бібліотеки криптографічних алгоритмів;
- програмувати методи криптографії;
- визначити структуру алгоритмів симетричного шифрування;
- використовувати режими алгоритмів шифрування;
- розрізняти атаки на алгоритми шифрування та шифратори.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Тема самостійної роботи	Рекомендована література	Форми контролю та звітності
Змістовий модуль 1		
Загальна структура криптографічних алгоритмів	1-5	Конспект
Режими роботи криптографічних алгоритмів	1-5	Конспект
Атаки на алгоритми шифрування	1-5	Конспект
Атаки на шифратори	1-5	Конспект
Змістовий модуль 2		
Класичні симетричні методи криптографії	1-5	Конспект
Сучасні симетричні методи криптографії	1-5	Конспект
Асиметричні методи криптографії	1-5	Конспект
Інші алгоритми шифрування	1-5	Конспект

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгиню – М.: Радио и связь, 2001. – 376 с.

2. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия, 2006. – 544 с.

3. Завгородний В.И. Комплексная защита информации в компьютерных системах / В.И. Завгородний. – М.: Логос, 2001. – 264 с.

4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. – М.: Форум, 2008. – 416 с.

5. Панасенко С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 576 с.

Додаткова

1. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

2. Вельшенбах М. Криптография на Си и С++ в действии. Учебное пособие / М. Вельшенбах. – М.: Триумф, 2004. – 464 с.

3. Щеглов А.Ю. Защита информации от несанкционированного доступа / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384 с.

4. Мельников В.П. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. – М.: Академия, 2008. – 336 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Защита информации от несанкционированного доступа [Електронний ресурс] – Режим доступу: http://ru.wikibooks.org/wiki/

2. Введение в криптографию [Електронний ресурс] – Режим доступу: http://algolist.manual.ru/defence/intro.php

3. Математическая криптография [Електронний ресурс] – Режим доступу: http://cryptography.ru/

4. Основы криптографии [Електронний ресурс] – Режим доступу: http://www.intuit.ru/studies/courses/691/547/info

5. Криптографические методы защиты в языках программирования [Електронний ресурс] – Режим доступу: http://compress.ru/article.aspx?id=10153