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

ЗАТВЕРДЖУЮ
Декан математичного факультету

_____С.І. Гоменюк
“_____” _____20___р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи захисту електронної інформації

спеціальності 7.04030101 – «Прикладна математика»

факультет математичний

Запоріжжя – 2014

Робоча програма Методи захисту електронної інформації для студентів за напрямом підготовки 7.04030101 – «Прикладна математика», 2014 р. – 7 с.
Розробник: к.т.н., доцент кафедри математичного моделювання С.В. Чопоров
Робоча програма затверджена на засіданні кафедри математичного моделювання
Протокол від “28” серпня 2014 року № 1
Завідувач кафедри _____ С.І. Гоменюк
“_____” _____20___року
Схвалено науково-методичною радою математичного факультету
Протокол від “29” серпня 2014 року № 1
Голова _____ П.Г. Стєганцева

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4,0</td><td>Галузь знань
0403 – «Системні науки та кібернетика»</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність
7.04030101 – «Прикладна математика»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>1-й</td><td>-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання – аналітичний звіт</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 144</td><td>1-й</td><td>-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="8">Тижневих годин для денної форми навчання: аудиторних – 2 самостійної роботи студента – 3</td><td rowspan="8">Освітньо-кваліфікаційний рівень: «спеціаліст»</td><td>18 год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>26 год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>50 год.</td><td>год.</td></tr>
<tr><td colspan="2">Індивідуальне завдання:
50 год.</td></tr>
<tr><td colspan="2">Вид контролю: Екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:
для денної форми навчання – 44 / 50
для заочної форми навчання –

2. Мета та завдання навчальної дисципліни

Мета – вивчення основних методів і засобів захисту автоматизованих інформаційних систем.

Завдання – оволодіння практичними навичками з організації захисту електронної інформації.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні загрози безпеки автоматизованих інформаційних систем;
- принципи криптографічного захисту інформації;
- шифри перестановки;
- шифри простої заміни;
- шифри складної заміни;
- шифри методу гамування;
- алгоритм шифрування DES;
- алгоритми шифрування даних IDEA;
- блокові і потокові шифри;
- методи криптографії з депонуванням ключа;
- асиметричні методи криптографії;
- особливості ідентифікації і перевірки автентичності;
- електронний цифровий підпис;
- методи захисту від дистанційних атак мережею Internet.

вміти:

- програмувати шифри перестановки;
- програмувати шифри простої заміни;
- програмувати шифри складної заміни;
- програмувати шифри методу гамування;
- програмувати алгоритм шифрування DES;
- програмувати алгоритми шифрування даних IDEA;
- програмувати блокові і потокові шифри;
- програмувати криптосисетми з депонуванням ключа;
- програмувати асиметричні криптосистеми;
- розробляти підсистеми ідентифікації та перевірки автентичності;
- розробляти підсистеми генерації та перевірки електронних підписів;
- розробляти підсистеми захисту від атак через мережу Internet.

3. Програма навчальної дисципліни

Змістовий модуль 1. Інформаційна безпека та методи криптографії

Тема 1. Інформаційна безпека комп’ютерних систем

Тема 2. Класичні симетричні методи криптографії

Тема 3. Сучасні симетричні методи криптографії

Тема 4. Асиметричні методи криптографії

Змістовий модуль 2.

Тема 1. Ідентифікація та перевірка автентичності

Тема 2. Електронний цифровий підпис

Тема 3. Управління криптографічними ключами

Тема 4. Методи та засоби захисту від атак мережею Internet

4. Структура навчальної дисципліни

Назви змістовних модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	с/п	лаб	інд	с.р.		л	с/п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Інформаційна безпека та методи криптографії												
Інформаційна безпека комп'ютерних систем	16	2		2	6	6						
Класичні симетричні методи криптографії	16	2		2	6	6						
Сучасні симетричні методи криптографії	18	2		4	6	6						
Асиметричні методи криптографії	18	2		4	6	6						
Разом за змістовим модулем 1	68	8	0	12	24	24						
Змістовий модуль 2. Назва												
Ідентифікація та перевірка автентичності	20	4		4	6	6						
Електронний цифровий підпис	18	2		4	6	6						
Управління криптографічними ключами	18	2		4	6	6						
Методи та засоби захисту від атак мережею Internet	20	2		2	8	8						
Разом за змістовим модулем 2	76	10	0	14	26	26						
Усього годин	144	18	0	26	50	50						

5. Теми лекційних занять

№ з/п	Назва теми	Кількість годин
1	Інформаційна безпека комп'ютерних систем	2
2	Класичні симетричні методи криптографії	2

3	Сучасні симетричні методи криптографії	2
4	Асиметричні методи криптографії	2
5	Ідентифікація та перевірка автентичності	4
6	Електронний цифровий підпис	2
7	Управління криптографічними ключами	2
8	Методи та засоби захисту від атак мережею Internet	2
	Разом	18

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Інформаційна безпека комп’ютерних систем	2
2	Класичні симетричні методи криптографії	2
3	Сучасні симетричні методи криптографії	4
4	Асиметричні методи криптографії	4
5	Ідентифікація та перевірка автентичності	4
6	Електронний цифровий підпис	4
7	Управління криптографічними ключами	4
8	Методи та засоби захисту від атак мережею Internet	2
	Разом	26

7. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Інформаційна безпека комп’ютерних систем	6
2	Класичні симетричні методи криптографії	6
3	Сучасні симетричні методи криптографії	6
4	Асиметричні методи криптографії	6
5	Ідентифікація та перевірка автентичності	6
6	Електронний цифровий підпис	6
7	Управління криптографічними ключами	6
8	Методи та засоби захисту від атак мережею Internet	8
	Разом	50

8. Індивідуальне завдання

Аналітичний звіт

Розробити аналітичний звіт, в якому необхідно розробити рекомендації щодо захисту даних інформаційної системи, що використовує Sqlite для збереження даних. Звіт повинен містите опис криптографічного алгоритму, аналіз його криптостійкості, блок-схеми основних алгоритмів. У додатках до звіту навести програмний код розробленої на базі рекомендацій інформаційної системи.

9. Методи навчання

Під час навчання дисципліни застосовуються наступні методи навчання:

– за джерелом передачі та сприймання навчальної інформації – словесні, наочні, практичні;

– за характером пізнавальної діяльності студентів – пояснювально-ілюстративний, репродуктивний, проблемне викладання, частково-пошуковий, дослідницький;

– залежно від основної дидактичної мети і завдань – методи оволодіння новими знаннями, формування вмінь і навичок, перевірки та оцінювання знань, умінь і навичок; методи усного викладу знань, закріплення навчального матеріалу, самостійної роботи студентів з осмислення й засвоєння нового матеріалу роботи із застосування знань на практиці та вироблення вмінь і навичок, перевірки та оцінювання знань, умінь і навичок;

– з точки зору цілісного підходу до діяльності у процесі навчання – методи організації та здійснення навчально-пізнавальної діяльності; стимулювання й мотивація учіння, контролю, самоконтролю, взаємоконтролю і корекції, самокорекції, взаємокорекції в навчанні.

10. Методи контролю

Тестування, усне та письмове опитування, співбесіда, перевірка лабораторних робіт.

11. Розподіл балів, які отримують студенти

<table>
<tr><td colspan="3">Поточний контроль знань</td><td>Екзамен</td><td>Сума</td></tr>
<tr><td>Контрольний модуль 1</td><td>Контрольний модуль 2</td><td>Індивідуальне завдання</td><td rowspan="3">20</td><td rowspan="3">100</td></tr>
<tr><td>Змістовний модуль 1</td><td>Змістовний модуль 2</td><td rowspan="2">20</td></tr>
<tr><td>30</td><td>30</td></tr>
</table>

Шкала оцінювання: національна та ECTS

<table>
<tr><th rowspan="2">ЗА ШКАЛОЮ ECTS</th><th rowspan="2">За шкалою університету</th><th colspan="2">За національною шкалою</th></tr>
<tr><th>Екзамен</th><th>Залік</th></tr>
<tr><td>A</td><td>90 – 100
(відмінно)</td><td>5 (відмінно)</td><td rowspan="5">Зараховано</td></tr>
<tr><td>B</td><td>85 – 89
(дуже добре)</td><td rowspan="2">4 (добре)</td></tr>
<tr><td>C</td><td>75 – 84
(добре)</td></tr>
<tr><td>D</td><td>70 – 74
(задовільно)</td><td rowspan="2">3 (задовільно)</td></tr>
<tr><td>E</td><td>60 – 69
(достатньо)</td></tr>
<tr><td>FX</td><td>35 – 59
(незадовільно – з можливістю повторного складання)</td><td rowspan="2">2 (незадовільно)</td><td rowspan="2">Не зараховано</td></tr>
<tr><td>F</td><td>1 – 34
(незадовільно – з обов’язковим повторним курсом)</td></tr>
</table>

12. Методичне забезпечення

1. Чопоров С.В. Методи захисту електронної інформації: Методичні рекомендації для самостійної роботи студентів освітньо-кваліфікаційного рівня «спеціаліст» спеціальності

«Прикладна математика» / С.В. Чопоров. – Запоріжжя: ЗНУ, 2014. – 7 с.

13. 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.

14. 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