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

Сучасна криптографія

спеціальність 8.05010302 – «Інженерія програмного забезпечення»

факультет математичний

Запоріжжя – 2014

Робоча програма Сучасна криптографія для студентів за напрямом підготовки 8.05010302 – «Інженерія програмного забезпечення», 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
“28” серпня 2014 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 rowspan="2">Кількість кредитів – 5,0</td><td>Галузь знань
0501 – «Інформатика та обчислювальна техніка»</td><td colspan="2" rowspan="2">Нормативна</td></tr>
<tr><td></td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність
8.05010302 – «Інженерія програмного забезпечення»</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 – 180</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 – 4 самостійної роботи студента – 4</td><td rowspan="8">Освітньо-кваліфікаційний рівень: «магістр»</td><td>32 год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>58 год.</td><td>год.</td></tr>
<tr><td colspan="2">Індивідуальне завдання:
58 год.</td></tr>
<tr><td colspan="2">Вид контролю: Залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:
для денної форми навчання – 64/116

2. Мета та завдання навчальної 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.

3. Програма навчальної дисципліни

Змістовий модуль 1. Класифікація алгоритмів шифрування

Тема 1. Загальна структура криптографічних алгоритмів

Тема 2. Режими роботи криптографічних алгоритмів

Тема 3. Атаки на алгоритми шифрування

Тема 4. Атаки на шифратори

Змістовий модуль 2. Основні криптографічні алгоритми

Тема 1. Класичні симетричні методи криптографії

Тема 2. Сучасні симетричні методи криптографії

Тема 3. Асиметричні методи криптографії

Тема 4. Інші алгоритми шифрування

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. Класифікація алгоритмів шифрування												
Загальна структура криптографічних алгоритмів	20	4		4	6	6	0					
Режими роботи криптографічних алгоритмів	20	4		4	6	6	0					
Атаки на алгоритми	24	4		4	8	8	0					

1	2	3	4	5	6	7	8	9	10	11	12	13
шифрування												
Атаки на шифратори	24	4		4	8	8	0					
Разом за змістовим модулем 1	88	16	0	16	28	28	0	0	0	0	0	0
Змістовий модуль 2. Основні криптографічні алгоритми												
Класичні симетричні методи криптографії	20	4		4	6	6	0					
Сучасні симетричні методи криптографії	24	4		4	8	8	0					
Асиметричні методи криптографії	24	4		4	8	8	0					
Інші алгоритми шифрування	24	4		4	8	8	0					
Разом за змістовим модулем 2	92	16	0	16	30	30	0	0	0	0	0	0
Усього годин	**180**	**32**	**0**	**32**	**58**	**58**	**0**	**0**	**0**	**0**	**0**	**0**

5. Теми лекційних занять

№ з/п	Назва теми	Кількість годин
1	Загальна структура криптографічних алгоритмів	4
2	Режими роботи криптографічних алгоритмів	4
3	Атаки на алгоритми шифрування	4
4	Атаки на шифратори	4
5	Класичні симетричні методи криптографії	4
6	Сучасні симетричні методи криптографії	4
7	Асиметричні методи криптографії	4
8	Інші алгоритми шифрування	4
	Разом	32

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Загальна структура криптографічних алгоритмів	4
2	Режими роботи криптографічних алгоритмів	4
3	Атаки на алгоритми шифрування	4

4	Атаки на шифратори	4
5	Класичні симетричні методи криптографії	4
6	Сучасні симетричні методи криптографії	4
7	Асиметричні методи криптографії	4
8	Інші алгоритми шифрування	4
	Разом	32

7. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Загальна структура криптографічних алгоритмів	6
2	Режими роботи криптографічних алгоритмів	6
3	Атаки на алгоритми шифрування	8
4	Атаки на шифратори	8
5	Класичні симетричні методи криптографії	6
6	Сучасні симетричні методи криптографії	8
7	Асиметричні методи криптографії	8
8	Інші алгоритми шифрування	8
	Разом	58

8. Індивідуальне завдання

Аналітичний звіт

Розробити програмний засіб для шифрування та дешифрування файлів алгоритмом ГОСТ 28147-89. За результатом розробки написати аналітичний звіт, який включатиме опис алгоритму шифрування, аналіз криптостійкості цього алгоритму, опис роботи розробленого програмного засобу.

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

Поточний контроль знань			Залік	Сума
Контрольний модуль 1	Контрольний модуль 2	Індивідуальне завдання	20	100
Змістовний модуль 1	Змістовний модуль 2	20		
30	30			

Шкала оцінювання: національна та ECTS

ЗА ШКАЛОЮ ECTS	**За шкалою університету**	**За національною шкалою**	
		Екзамен	**Залік**
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

12. Методичне забезпечення

1. 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.

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