Державний вищий навчальний заклад
«Прикарпатський національний університет імені Василя Стефаника »

Кафедра інформаційних технологій

"**ЗАТВЕРДЖУЮ**"
Проректор з науково-
педагогічної роботи

_____ Михайлишин Г.Й.

"___" вересня 2015 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека програм та даних

(назва навчальної дисципліни)

напрям підготовки **6.050103 Програмна інженерія**
(шифр і назва напряму підготовки)

факультет **математики та інформатики**
(назва інституту, факультету)

Івано-Франківськ – 2015 рік

Робоча програма дисципліни “Безпека програм та даних” для студентів напряму підготовки 6.050103 Програмна інженерія, «31» серпня 2015р. – __ с.

Розробники: к.ф.-м.н, доцент Ткачук В.М., к.т.н., доцент Іщеряков С.М.

Робоча програма затверджена на засіданні кафедри інформаційних технологій

Протокол від “31” серпня 2015 р. № 1

Завідувач кафедри інформаційних технологій _____ (Філевич П.В.)
(підпис) (прізвище та ініціали)

“31” серпня 2015 р.

Схвалено методичною комісією факультету математики та інформатики.
Протокол від “04” вересня 2015р. № 1

“04” вересня 2015р.

Голова _____ (Соломко А.В.)
(підпис) (прізвище та ініціали)

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 – 3</td><td>Галузь знань
0501 - Інформатика та обчислювальна техніка
(шифр і назва)</td><td colspan="2" rowspan="2">Нормативна</td></tr>
<tr><td>Напрям підготовки
6.050103 Програмна інженерія
(шифр і назва)</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність (професійне спрямування):</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</td><td>4-й</td><td>4-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання
-
(назва)</td><td colspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин - 90</td><td>8-й</td><td>8-й</td></tr>
<tr><td></td><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 6</td><td rowspan="9">Освітньо-кваліфікаційний рівень:
бакалавр</td><td>12 год.</td><td></td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>18</td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>60</td><td></td></tr>
<tr><td colspan="2">Індивідуальні завдання:
0 год.</td></tr>
<tr><td colspan="2">Вид контролю:
Екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

для денної форми навчання – 33,3% : 66,6%

2. Мета та завдання навчальної дисципліни

Мета:

Метою навчальної дисципліни є навчання студентів принципам побудови ситем захисту інформації на основі використання алгоритмів симетричної та несиметричної криптографії, MAC-кодів та хеш-функцій щодо забезпечення аутентичності, цілісності та конфіденціальності інформації в інформаційних системах.

Завдання:

1. Одержання знань з основоположних принципів побудови механізмів захисту інфор-мації на основі алгоритмів симетричної та несиметричної криптографії;
2. Одержання знань про основні криптографічні процедури для забезпечення аутентичності, цілісності та конфіденційності інформації.

У результаті вивчення дисципліни студенти повинні:

знати:

- особливості стеку мережевих протоколів та їх вразливі місця з точки зору безпеки даних,
- використання брандмауерів та пов’язаних з цим проблем, основи криптографії, загальні відомості що до криптоаналізу;
- основні міжнародні та національні стандарти з захисту інформації.
- основні принципи організації захисту інформації в інформаційних системах.
- механізми та протоколи забезпечення конфіденціальності інформації.
- механізми й протоколи забезпечення аутентичності інформації в інформаційних системах.
- механізми та протоколи цілісності даних в інформаційних системах.

вміти:

- аналізувати інформаційні систем безпеки даних, використовувати криптографічні системи при необхідності збереження конфіденційності даних.
- визначати механізми та протоколи для забезпечення аутентичності інформації.
- визначати криптографічні системи для забезпечення конфіденціальності даних в інформаційних системах.
- вибирати механізми та протоколи для забезпечення цілісності даних, проводити розрахунки їх потрібних показників.
- забезпечувати грамотний підбір програмно-апаратних і програмних засобів для забезпечення необхідного рівня захисту інформації.

3. Програма дисципліни “ Безпека програм та даних ”

Змістовний модуль 1. Основи захисту інформації та життєвий цикл розробки систем безпеки.

Тема 1.1 Роль інформації в сучасному світі.

Основні поняття та визначення. Конфіденційна інформація. Законодавство в галузі захисту інформації.

Тема 1.2 Архітектура безпеки.

Послуги безпеки. Принципи проектування систем захисту інформації.

Тема 1.3 Критерії захищеності інформації в інформаційних системах.

Профіль захищеності. Методи захисту даних.

Змістовний модуль 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС.

Тема 1. Міжнародні стандарти криптографічних методів захисту інформації.

Стандарти ISO. Сучасні методи збереження та передачі даних.

Тема 2. Державні стандарти України з методів захисту інформації.

Криптографічні стандарти. Шифрування даних. Кодування сигналів.

Тема 3. Стандарти науково-дослідницьких і промислових організацій.

Напрямки дослідження систем шифрування інформації. Перспективи розвитку закритих систем.

Змістовний модуль 3.

Криптографічні механізми захисту інформації в інформаційних системах.

Тема 1. Симетричні криптографічні системи шифрування.

Конфіденційність інформації. Класифікація симетричних шифрів. Вимоги до симетричних шифрів. Структура блочних симетричних шифрів. Національний стандарт блочного шифру.

Тема 2. Сучасні асиметричні шифри.

Схема асиметричного шифрування. Компоненти асиметричної криптосистеми.

Криптосистема RSA. Національний стандарт асиметричного шифрування.

Тема 3. Аутентифікація інформації.

Вимоги аутентифікації. Односпрямовані геш-функції. MAC-коди. Характеристика алгоритмів MD5, SHA-1, HMAC. Цифровий підпис. Вимоги до цифрового підпису. Правові аспе-кти використання цифрового підпису. Національній стандарт цифрового підпису.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		п	п	лаб	інд	с.р
1	2	3	4	5	6	7	8	9		11	12	13
Змістовий модуль 1 Основи захисту інформації та життєвий цикл розробки систем безпеки.												
Тема 1 Роль інформації в сучасному світі.	2	1				1						
Тема 2 Архітектура безпеки.	4	1				3						
Тема 3 Критерії захищеності інформації в інформаційних системах.	10	2		2		6						
Разом за змістовим модулем **1**	**16**	**4**		**2**		**10**						
Змістовий модуль 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС.												
Тема 1 Міжнародні стандарти криптографічних методів захисту інформації.	12	2		2		8						
Тема 2 Державні стандарти України з методів захисту інформації.	9	1		2		6						
Тема 3 . Стандарти науково-дослідницьких і промислових організацій.	9	1		2		6						
Разом за змістовим	**30**	**4**		**6**		**20**						

модулем **2**												
Змістовий модуль 3. Криптографічні механізми захисту інформації в інформаційних системах.												
Тема 1 Симетричні криптографічні системи шифрування.	15	1		4		10						
Тема 2 Сучасні асиметричні шифри.	15	1		4		10						
Тема 3 Аутентифікація інформації.	14	2		2		10						
Разом за змістовим модулем **3**	**44**	**4**		**10**		**30**						
Усього годин	**90**	**12**		**18**		**60**						

5. Теми лабораторних занять

5.1 Теми лабораторних занять для денної форми навчання

№ з/п	Назва теми	Кількість годин
Змістовий модуль 1. Основи захисту інформації та життєвий цикл розробки систем безпеки		
1	Безпека Інтернет-застосувань. Налаштування брандмауерів	2
Змістовий модуль 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС		
1	Дослідження електроного цифрового підпису. ЦП Ель Гамаля, ДСТУ-4145, ECDSA	2
2	Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-3.	2
3	Безпечність персональних конфіденціальних даних на базі секретного диску та захищеної електронної пошти PGP	2
Змістовий модуль 3. Криптографічні механізми захисту інформації в інформаційних системах.		
1	Аудит парольного захисту інформації	2
2	Класичні симетричні системи.	2
3	Дослідження крипостійкості простих симетричних шифрів	2
4	Розгортання та управління інфраструктурою відкритих ключів.	2
5	Криптографія з несимметричним ключем.	2
	Всього:	**18**

6. Самостійна робота

№ з/п	Назва теми	Кількість годин, денна ф.н.	Кількість годин, заочна ф.н.
1	Канали витоку інформації при експлуатації ЕОМ	6	
2	Класифікація комп’ютерних вірусів	8	
3	Система шифрування Цезаря. Система шифрування Віжінера. Шифр "подвійний квадрат" Уїтстона.	8	
4	Одноразова система шифрування. Шифрування методом Вернама.	6	
5	Сучасні симетричні криптосистеми. Американський стандарт шифрування даних DES. Основні режими роботи. Режим "Електронна кодова книга". Режим "Зчеплення блоків шифру". Режим "Зворотний зв’язок по шифру". Режим "Зворотний зв’язок по виходу". Області застосування алгоритму DES.	8	
6	Сучасні симетричні криптосистеми. Комбінування блокових алгоритмів. Алгоритм шифрування даних IDEA. Криптоаналіз.	6	
7	Сучасні симетричні криптосистеми. Стандарт шифрування даних ГОСТ 28147-89. Режим простої заміни. Режим вибірки гами. Режим шифрування зі зворотним зв’язком. Режим вироблення імітовставки.	6	
8	Сучасні симетричні криптосистеми. Алгоритм RC-4. Опис криптосхеми.	6	
9	Криптосистема шифрування даних RSA. Процедури шифрування і розшифрування в криптосистемі RSA. Безпека і швидкодія криптосистеми RSA.	6	
	Разом	60	

7. Індивідуальні завдання

8. Методи навчання

При вивченні дисципліни використовуються наступні методи навчання:

- мультимедійні лекції;
- навчальні відео та презентаційні матеріали;
- індивідуальних завдань для виконання на лабораторних заняттях.

9. Методи контролю

Загальна кількість балів, що може бути набрана студентом на протязі семестру складається із оцінок за 10 лабораторних робіт, тестових опитувань та самостійних робіт.

Оцінювання знань, умінь і навичок студентів з навчальної дисципліни при підсумковому контролі необхідно проводити, виходячи з таких загальних рекомендацій:

“відмінно” – студент демонструє повні і глибокі знання навчального матеріалу, достовірний рівень розвитку умінь та навичок, правильне й обґрунтоване формулювання практичних висновків, уміння приймати необхідні рішення в нестандартних ситуаціях, вільне володіння науковими термінами, аналізує причинно-наслідкові зв’язки;

“добре” – студент демонструє повні знання навчального матеріалу, але допускає незначні пропуски фактичного матеріалу, вміє застосувати його щодо конкретно поставлених завдань, у деяких випадках нечітко формулює загалом правильні відповіді, допускає окремі несуттєві помилки та неточності;

“задовільно” – студент володіє більшою частиною фактичного матеріалу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, не завжди вміє інтегровано застосувати набуті знання для аналізу конкретних ситуацій, нечітко, а інколи й невірно формулює основні теоретичні положення та причинно-наслідкові зв’язки;

“незадовільно” – студент не володіє достатнім рівнем необхідних знань, умінь, навичок, науковими термінами.

10. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота					Сума
Змістовий модуль №1		Змістовий модуль № 2		Інд. робота	
Т1.1	Сума	Т2.1	Сума		100
54	54	46	46	0	

Т1.1, Т1.2 ... Т3.2 – теми змістових модулів.

11. Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
80 – 89	**B**	добре	
70 – 79	**C**		
60 – 69	**D**	задовільно	
50 – 59	**E**		
26 – 49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-25	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

12. Методичне забезпечення

1.	Конспект опорних лекцій темах курсу.
2.	Електронні презентації до лекційного матеріалу
3.	Варіанти завдань для виконання на практичній роботі.
4.	Варіанти індивідуальних завдань для виконання на самостійній роботі.
5.	Варіанти теоретичних питань для самостійного вивчення.
6.	Тестові завдання для поточного контролю
7.	Теоретичні питання для заліку

13. Рекомендована література

№ з/п	Назва	Кількість примірників у бібліотеці
Основна література		
1.	Остапов С. Е., Валь Л. О. Основи криптографії навч. посіб.Чернівці: Книги-ХХІ, 2008	6
2.	Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформаціїЧернівці: Видавничий дім «РОДОВІД», 2014.	1
3.	Галицький А. В. Защита информации в сети-анализ технологий и синтез решенийМ.: ДМК Пресс, 2004.	2
4.	Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа СПб.: Наука и техника, 2004	2
5.	Вернер М. Основы кодирования. Учебник для ВУЗов. М.: Техносфера, 2006	3
6.	Галатенко В. А. Основы информационной безопасности. Курс лекций: учеб. пособ.-изд. 3-е. М.: ИНТУИТ. РУ "Интернет-университет Информационных Технологий, 2006	3
7.	ред. Голубев В. А. Компьютерная преступность и кибертерроризм. Исследования по программе малых грантов: сборник научных работ Вып. 1. Запоріжжя: Центр исследов. компьтерн. преступности, 2004.	1
8.	Коркішко Т., Мельник А., Мельник В. Алгоритми та процесори симетричного блокового шифруванняЛьвів: БаК, 2003.	1
9.	Бетелина В. Б., Галатенко В. А. Основы информационной безопасности. Курс лекций: учеб. пособ.-изд. 3-е. М.: ИНТУИТ. РУ "Интернет-университет Информационных Технологий, 2006.	3
10.	Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2001. — 688 с.	
11.	Герасименко В.А. Защита информации в автоматизированных	
12.	Шнайдер Брюс. Прикладная криптография . Диасофт, 1998.	
13.	Хорошко В.А и др. Методы и средства защиты информацию- Юниор, 1999	
14.	Емельянов С. П. Основы информационной безопасности: Кон-спект лекций. – Одесса: Юридична література, 2003. – 200 с.	

Додаткова література

1.Столлингс В. Криптография и защита сетей: принципы и практика / Пер. с англ. – 2-е изд. – М.: Издательский дом "Вильямс", 2001. – 672 с.

2. Щеглов А. Ю. Защита компьютерной информации от несанкцио-нированного доступа. – СПб.: Наука и Техника, 2004. – 384 с.

3. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.

4. Вербіцький О. В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 248 с.

5. Пономаренко В. С. Основи захисту інформації. Навчальний посібник / В. С. Пономаренко, І. В Журавльова. – Харків: Вид. ХДЕУ, 2003. – 176 с.

6. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М.: СОЛОН-Прес, 2002. – 272 с. (Серия "Аспекты защиты")

7. Горбатов В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. По-лянская. – М.: Горячая линия – Телеком, 2004. – 248 с.

14. Інформаційні ресурси

1. http://bezopasnost.biz.
2. http://dstszi.gov.ua.
3. Журнал "Информационные технологии. Аналитические мате-риалы" // http://it.ridne.net
4. Центр информационных технологий. // http://www.citmgu.ru
5. Нормативные акты Украины // www.nau.kiev.ua
6. Information Technology Security Evaluation Criteria, v.1.2. -Office for Official publications of the European Communities, 1991.
7. www.fbi.gov.
8. www.pgpi.org.
9. www.rootshell.com.
10. www.securityfocus.com.
11. www.sysinternals.com.
12. www.zdnet.ru.
13 www.submarine.ru.
14. www.securitylab.ru.