Чернівецький національний університет імені Юрія Федьковича
(повне найменування вищого навчального закладу)

Кафедра прикладної математики та інформаційних технологій

"**ЗАТВЕРДЖУЮ**"
Декан
_____
"_____"_____2017 року

(для внутрішньо-факультетських та окремих дисциплін, які читаються на інших факультетах)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Системи захисту інформації

(шифр і назва навчальної дисципліни)

напрям підготовки– Прикладна математика
(шифр і назва напряму підготовки)

спеціальність 113 – Прикладна математика

(шифр і назва спеціальності)

кваліфікація Програміст прикладний
(назва кваліфікації)

Факультет математики та інформатики
(назва інституту, факультету)

Чернівці – 2017 рік

Робоча програма системи захисту інформації (нормативної чи варіативної складової)
(назва навчальної дисципліни)
для студентів 5 –го курсу напряму підготовки (спеціальності) прикладна математика, складена на основі навчальної програми (типової), затвердженої на засіданні кафедри (Протокол №1 від « 27 » серпня 2017 року).

Розробники: Шепетюк Б.Д., доцент,
к.т.н._____
(вказати авторів, їхні посади, наукові ступені, вчені звання)

Робоча програма затверджена на засіданні кафедри прикладної математики та інформаційних технологій

Протокол №1 від « 29 » серпня 2017 року

Схвалено методичною радою інституту, факультету

Протокол №1 від «___ » _____ 2017 року

Голова методичної ради факультету _____ _____
(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 –4</td><td>Галузь знань
(шифр і назва)</td><td colspan="2" rowspan="2">За вибором</td></tr>
<tr><td>Напрям підготовки
_113 прикладна математика
(шифр і назва)</td></tr>
<tr><td>Змістових модулів –2</td><td rowspan="4">Спеціальність (професійне спрямування):
_____</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання _____
(назва)</td><td>1-й</td><td>1-й</td></tr>
<tr><td>Загальна кількість годин - 10</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 2
самостійної роботи студента - 6</td><td>1-й</td><td>1-й</td></tr>
<tr><td rowspan="9">Освітньо-кваліфікаційний рівень:</td><td colspan="2">Лекції</td></tr>
<tr><td>15 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>15 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>90 год.</td><td>110 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:
год.</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

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

для денної форми навчання – 30%;

для заочної форми навчання – 9%.

1. Мета та завдання навчальної дисципліни

1.1. Мета викладання дисципліни **“Системи захисту інформації”** — підготувати майбутніх спеціалістів до ефективного використання сучасних інформаційних технологій в процесі розв’язування фахових завдань,

1.2. Завдання вивчення дисципліни: засвоєння знань, умінь і навичок з основ захисту інформації і набуття навичок практичного їх застосування та навички роботи з сучасним прикладним програмним забезпеченням.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- сучасні стандарти забезпечення інформаційної безпеки;
- сновні компоненти захисту інформації;
- сучасний стан законодавчих норм в області інформаційної безпеки;
- про управління ризиками і системою безпеки;
- теоретичні основи криптозахисту даних;
- предмет, методи та завданнями захисту даних;
- методики захисту важливої інформацію від несанкціонованого доступу;
- механізми шифрування інформації за допомогою існуючих методів шифрування;
- основні методи математичного перетворення інформації та способи її відтворення;
- знати основні напрямки використання криптографічних методів;
- принципи застосування положень теорії захисту інформації в сучасних електронно-обчислювальних системах та мережах.

У результаті вивчення навчальної дисципліни студент повинен

вміти:

- застосовувати математичний апарат теорії захисту інформації для вирішення практичних задач;
- використовувати методи оптимального захисту мереж та баз даних для побудови безпечних інформаційних систем;
- забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;
- здійснювати захист даних в корпоративних розподілених інформаційних системах, застосовувати системи криптографії в професійній діяльності;
- виконувати вибір та застосовувати методи для забезпечення достовірності передачі повідомлень;
- розробляти схеми систем безпечної передачі інформації по незахищених каналах зв'язку.

2. Теоретичний зміст програми навчальної дисципліни

Змістовий модуль 1. Безпека і захист даних

Тема 1. Основні поняття і аспекти комп'ютерної безпеки.

1. Загальні поняття інформаційної безпеки.
2. Історія розвитку інформаційної безпеки.
3. Сучасні стандарти забезпечення інформаційної безпеки
4. Основні компоненти захисту інформації
5. Управління відновленням

Тема 2. **Законодавство в області інформаційної безпеки.**

1. Юридичні питання інформаційної безпеки.
2. Законодавство в даній області низки країн (США, Австралія, Китай і ряд інших).
3. Питання судового переслідування.
4. Конфіденційність особистої інформації.
5. Міжнародні і національні стандарти і специфікації в області інформаційної безпеки
6. Системи ЗІ в провідних світових компаніях
7. Практика компанії IBM в області захисту
8. Практика компанії Cisco Systems в розробці політики розвитку мереж безпеки
9. Практика компанії Microsoft в області інформаційної безпеки

Тема 3. Шифрування даних

1. Основні поняття захисту інформації.
2. Основні терміни і вимоги до криптосистем.
3. Історія розвитку систем шифрування.
4. Симетричні криптосистеми.

Тема 4. Блочне шифрування.

1. Структура шифру Файстеля.
2. Алгоритми традиційного шифрування.
3. Стандарт шифрування даних(DES).

Змістовий модуль 2. Мережева безпека

Тема 5. Аутентифікація повідомлень

1. Методи аутентифікації повідомлень.
2. Код аутентичності повідомлення.
3. Одностороння функція хешування.
4. Захищена функція хешування SHA-1

Тема 6. Криптографія з відкритим ключем.

1. Алгоритми криптографії з відкритим ключем.
2. Алгоритм RSA.
3. Обмін ключами по схемі Діффі-Хеллмана.

Тема 7. Системи захисту інформації та виявлення атак.

1. Вразливості і події безпеки.
2. Вразливі компоненти інформаційної системи.
3. Класифікація вразливостей комп’ютерних систем.
4. Концепція атаки..
5. Сканування мережі

Тема 8. Основні напрями розвитку сучасної криптографії

1. Основні криптографічні примітиви.
2. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри.
3. Основні напрями розвитку асиметричних криптоалгоритмів. Криптографія на еліптичних кривих.
4. Теоретико-чисельні задачі, складність арифметики точок ЕК в різних формах і представленнях.
5. Цифрова стеганографія з відкритим ключем.

3. 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.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Безпека і захист захист даних												
Тема 1. Основні поняття і аспекти комп'ютерної безпеки	16	3		3		10	16	1		1		15
Тема 2. Законодавство в області інформаційної безпеки	20					20	20,5	0,5				20
Тема 3. Шифрування даних	14	2		2		10	12	1		1		10
Тема 4. Блочне шифрування	14	2		2		10	10,5	0,5				10
Разом за змістовим модулем 1	64	7		7		50	60	3		2		55
Змістовий модуль 2. Мережева безпека												
Тема 5. Аутентифікація повідомлень	12	2				10	10					10
Тема 6 Криптографія з відкритим	16	2		4		10	14	2		1		10

ключем												
Тема 7. Системи захисту інформації та виявлення атак	16	2		4		10	17	1		1		15
Тема 8. Основні напрями розвитку сучасної криптографії	12	2				10	10					10
Разом за змістовим модулем 2	56	8		8		40	60	3		2		55
Усього годин	120	15		15		90	120	6		4		110

* ІНДЗ – для змістового модуля, або в цілому для навчальної дисципліни за рішенням кафедри (викладача).

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Побудова резервних копій баз даних з допомогою системних утиліт і додатків	4
2	Адмністрування мережі	2
3	Криптоконтейнер	2
4	Аналіз і програмування алгоритму RSA	4
5	Криптоаналіз	2
6	Сканер мережевої безпеки	1

5. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Інші підходи до визначення аспектів інформаційної безпеки. Кібернетичні війни. Комп'ютерні двійники. Шляхи витоку інформації. Регістрація на WEB – сайтах. Файли КУКІ.	20
2	Криптоаналіз симетричних систем. Криптоаналіз за методом ймовірних слів. Частотний аналіз. Метод Казискі. Криптоаналіз шифросистем на основі простої перестановки та перестановки за шляхами Гамільтона	30
3	Криптозахист файлів, папок і дисків. Додаток PGP	20

	Desktop Security. Захист папок з допомогою програми PGP. Стеганографія.	
4	Одностороння функція хешування. Захищена функція хешування SHA-1. Цифрові підписи. Управління ключами. Цифрові сертифікати. Центр сертифікації.	20
5	Поняття адміністративної безпеки. Рекомендації по організації роботи служби безпеці на підприємстві. Аналіз засобів технічної безпеки. Позитивні і негативні сторони використання стандарту ISO 17799. Типи вірусних атак. Антивірусна система захисту організації. Сучасні антивірусні програми	30
	Разом	120

6. Методи контролю

Контрольні питання до модуля 1.

1. Загальні поняття інформаційної безпеки, історія її розвитку.
2. Сучасні стандарти забезпечення інформаційної безпеки.
3. Категорії атак, визначення і умови для їх здійснення.
4. Розгляд механізму проведення хакреських атакк.
5. Мотивація діяльності хакерів, історія методів злому, різні способи проведення атак
6. Види шкідливого програмного забезпечення.
7. Юридичні питання інформаційної безпеки.
8. Питання судового переслідування, конфіденційність особистої інформації.
9. Міжнародні і національні стандарти і специфікації в області інформаційної безпеки
10. Сучасні аспекти інформаційної безпеки.
11. Порушення, механізми і служби захисту.
12. Класифікація аспектів порушення захисту.
13. Основні функції служби захисту.
14. Модель захисту мережі.
15. Основні кроки по захисту комп’ютера.
16. Адміністрування мережі.
17. Захист документів MS Office XP.
18. Фізична безпека комп’ютера.
19. Утиліти блокування доступу.
20. Загроза електронного шпигунства.
21. Захист жорсткого диску.
22. Резервне копіювання.
23. Архівація даних.
24. Хакінг архівних даних.
25. Моніторинг мережі.
26. Основні поняття захисту інформації.
27. Основні терміни і вимоги до криптосистем.

28. Історія розвитку систем шифрування.
29. Симетричні криптосистеми.
30. Моноалфавітні підстановки. Підстановка Цезаря.
31. Багатоалфавітні підстановки, системи шифрування Віженера.
32. Багатокільцеві поліалфавітні підстановки.
33. Криптоаналіз за методом ймовірних слів.
34. Частотний аналіз.
35. Метод Казискі.
36. Шифросистеми на основі простої перестановки та перестановки за шляхами Гамільтона, табличні перестановки.
37. Блочне шифрування.
38. Структура шифру Файстеля.
39. Алгоритми традиційного шифрування.
40. Стандарт шифрування даних(DES).
41. Криптозахист файлів, папок і дисків. Додаток PGP Desktop Security.
42. Захист папок з допомогою програми PGP.
43. Стеганографія

Контрольні питання до модуль-контролю.

1. Методи аутентифікації повідомлень.
2. Код аутентичності повідомлення.
3. Одностороння функція хешування.
4. Захищена функція хешування SHA-1
5. Принципи криптографії з відкритим ключем.
6. Алгоритми криптографії з відкритим ключем.
7. Алгоритм RSA.
8. Обмін ключами по схемі Діффі-Хеллмана.
9. Цифрові підписи.
10. Управління ключами.
11. Цифрові сертифікати.
12. Вразливості і події безпеки.
13. Вразливі компоненти інформаційної системи.
14. Класифікація вразливостей комп’ютерних систем.
15. Концепція атаки.
16. Сканування мережі.
17. Класифікація атак.
18. Сканери виявлення атак.
19. Управління безпекою.
20. Брандмауери.
21. Шифрування трафіку.
22. Методи захисту баз даних.
23. Мережний сніффінг.
24. Мережі VPN

25.Комп’ютерні віруси.
26.Типи вірусних атак.
27.Антивірусна система захисту організації.
28.Сучасні антивірусні програми

7. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота									Залік	Сума
Змістовий модуль №1					Змістовий модуль № 2					
Т1	Т2	Т3	Т4		Т5	Т6	Т7	Т8	40	100
8	7	8	7		8	7	8	7		

Т1, Т2 ... Т8 – теми змістових модулів.

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	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**		
35-49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

8. Рекомендована література

Базова

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009.-608 с.:іл.
2. Остапов С.Е., Валь Л.О. Основи криптографії: Навчальний посібник. – Чернівці: Книги – XXI, 2008.-188с.
3. Глущаков С.В., Бабенко М,И,., Тесленко Н.С. Секреты хакера. Защита и атака. Учебный курс, -изд.2-е, доп. и перераб. -М.: АСТ: АСТ МОСКВА: ХРАНИТЕЛЬ, 2008.- 544с.
4. Яремчук С.А. Защита вашего компьютера от сбоев, спама, вирусов и хакеров на 1000%. –СПб.: Питер, 2007.-288с.: ил.
5. ДиНиколо Д. Что и как нужно защищать в Windows XP. –М.: НТ Пресс, 2007. – 464с.: ил.

6. Бормотов С.В. Системное администрирование. на 100%. Спб.: Питер, 2006.-256 с.: ил.
7. Столлингс В. Основы защиты сетей. Приложения и стандарты: Пер. с англ.-М.: Изд. Дом “Вильямс”, 2004.-432с.:ил.
8. Фергюсон Н., Шнаер Б. Практическая криптография. : Пер. с анг. – М.: Изд. Дом «Вильямс», 2005. – 424 с.
9. Задірака В., Олексюк О. Комп’ютерна криптологія. Підручник.-Київ: 2002,-504с.
10. Alex JeDaev. Я люблю компьютерную самооборону. Учебное пособие.-М.: Только для взрослых, 2004.-432с.

Допоміжна

1. Ванг Уоллес. Безопасная работа в Интернет. Эффективный самоучитель. Пер с англ.- ООО «ДиаСофтЮП», 2005. - 400 с.
2. Мелтон Г., Пилиган К. Офисный шпионаж. – Ростов н/Д: «Феникс», 2005. – 184 с.
3. Бабан А.В., Шапкин Г.Г. Криптография.-М.: СОЛОН-Р, 2002, 512с. (серия книг “Аспекты защиты”).
4. Мамаев М., Петренко С. Технология защиты информации в Интернете. Специальный справочник.- СПб.: Питер. 2002.- 848с.
5. А.В. Лукацкий. Обнаружение атак. -2-е изд., переб. и доп.- СПб.: "БХВ-Петербург", 2003. - 608 с.: ил.
6. С. Мак-Клар, Д. Скембрей, Д. Курц. Секреты хакеров. Безопасность сетей – готовые решения, 2-е изд.: Пер. с англ. - М.: Издательский дом "Вильяме", 2001.- 656 с.: ил. - Парал. титл. англ.
7. Д.А. Козлов, А.А. Парандовский, А.К. Парандовский "Энциклопедия компьютерных вирусов" - М.: "Солон-Р", 2001. - 457 с.: ил.
8. К. Касперски. Техника сетевых атак. -М.: Солон-Р, 2001. - 396 с.: ил.
9. Донцов Д.А. Самые нужные программы для Windows. Популярный самоучитель. Спб.: Питер, 2006.- 400 с.: ил.

Інформаційні ресурси

1. http://bezopasnost.biz. 20. http://dstszi.gov.ua.
2. Журнал "Информационные технологии. Аналитические материалы" [Електронний ресурс]. – Режим доступа : http://it.ridne.net.
3. Історія розвитку інформаційних технологій в Україні [Електронний ресурс]. – Режим доступу : http://www.icfcst.kiev.ua/ MUSEUM/IT_u.html.
4. Нормативные акты Украины [Електронний ресурс]. – Режим доступа : www.nau.kiev.ua.
5. Центр информационных технологий [Електронний ресурс]. – Режим доступа : http://www.citmgu.ru.

6. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, 1991 [Electronic resource]. – Access mode : www.fbi.gov.
7. www.pgpi.org.
8. linuxpage.ru.
9. www.securityfocus.com.
10. www.sysinternals.com.
11. www.zdnet.ru.
12. www.submarine.ru.
13. www.securitylab.ru.
33. http://www.osp.ru.
34. http://zakon1.rada.gov.ua.
35. http://www.cyberguru.ru.