Міністерство освіти і науки України
Львівський національний університет імені Івана Франка
Кафедра РКС

"**ЗАТВЕРДЖУЮ**"

Перший проректор

_____

"__ ____ "_____2014 р.

НАВЧАЛЬНА ПРОГРАМА ДИСЦИПЛІНИ

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

галузі знань **0501 Інформатика та обчислювальна техніка**
напряму підготовки **6.050101 Комп'ютерні науки**
факультету електроніки

Кредитно-модульна система
організації навчального процесу

Львів – 2014

Технології захисту інформації. Навчальна програма дисципліни для студентів за напрямом підготовки **6.050101 Комп'ютерні науки,** — Львів: ЛНУ імені Івана Франка, 2014. — 8 с.

Розробник:
Монастирський Л.С., д. фіз.-мат. наук, професор кафедри РКС

Робоча програма затверджена на засіданні кафедри РКС

Протокол № ___ від. "____"_____2014 р.

Завідувач кафедри РКС Монастирський Л.С.

"_____"_____ 2014р

Схвалено методичною радою факультету електроніки

Протокол № ___ від. "____"_____20___ р.

Голова методичної ради Шувар Р. Я.

"_____"_____ 2014 р

І. ЗАГАЛЬНІ ВІДОМОСТІ

Курс присвячений сучасним проблемам криптографічного та фізико-технічного захисту інформаційних систем.

Мета: виклад основ криптології, криптоаналізу, стенографії та фізико-технічних методів захисту інформації.

Завдання: навчити студентів шифрувати/розшифровувати інформацію з допомогою симетричних/асиметричних криптоалгоритмів та засобів стенографії; освоїти фізичні принципи роботи сенсорних систем та систем відеоспостереження, що застосовуються з метою захисту інформації.

В результаті вивчення даного курсу студент повинен

знати основні поняття (означення) предмету; фундаментальні принципи криптології, криптоаналізу, квантової криптографії та стенографії; фізичні основи роботи сенсорних систем захисту інформації.

вміти: застосовувати крипто- та стено алгоритми для захисту конкретних інформаційних об'єктів; вміти застосовувати сенсори та відеосистеми для захисту об'єктів;

Для вивчення дисципліни необхідні знання з таких розділів математики і фізики: дискретна математика, програмування, електроніка, оптика.

Навчальна програма дисципліни складена на основі освітньо-професійної програми підготовки бакалавра напряму підготовки "Комп'ютерні науки", затвердженої наказом Міністерства освіти і науки № 485 від 26 травня 2010 року .

Форма навчання	*Семестр*	*Всього кредитів/годин*	*Розподіл навчального часу за видами занять* [1]					*Семестрова атестація*
			Лекції	*Практичні заняття*	*Семінарські заняття*	*Лабораторні роботи*	*СРС*	
Денна	5	4/144	36	-	-	36	72	Екзамен

ІІ. ЗМІСТ НАВЧАЛЬНОГО МАТЕРІАЛУ

***1*. Криптологія та криптоаналіз.**

Тема 1. Класична криптографія.

Тема 2. Симетричні криптосистеми та алгоритми.

Тема 3. Асиметричні криптосистеми та алгоритми.

***2*. Фізико-технічні методи захисту інформації.**

Тема 4. Сенсорні системи.

Тема 5. Системи відеоспостереження.

Тема 6. Стенографія та квантова криптографія.

III. ПРИБЛИЗНА ТЕМАТИКА
ПРАКТИЧНИХ (СЕМІНАРСЬКИХ) ЗАНЯТЬ

IV. ПРИБЛИЗНИЙ ПЕРЕЛІК ЛАБОРАТОРНИХ РОБІТ

Мета циклу лабораторних робіт полягає в тому, щоб студенти отримали практичні навички у виборі методу, складанні алгоритму та написанні програми на алгоритмічній мові для розв'язку обчислювальних задач в різноманітних галузях.

№ з/п	Назва теми	Кількість годин
1	Програмна реалізація алгоритмів класичної криптографії на мові Turbo Pascal.	6
2	Системи блочного шифрування DESX, DES100, Krypton.	6
3	Криптографія відкритого ключа. Робота з пакетом PGP-60.	4
4	Захист комп'ютерних ОС та ПК (адміністрування).	4
5	Захист аудіозв'язку (PGP Fone). Телеконференції (Net Meeting).	4
6	Особливості захисту аудіо-відео файлів на CD та CDRW.	4
7	Системи телеспостережень. Web-камери (Win on CD).	4
8	Системи технічного захисту інформаційних об'єктів (інфрачервоні датчики руху).	4
	Разом	**36**

V. ІНДИВІДУАЛЬНІ СЕМЕСТРОВІ ЗАВДАННЯ

№ з/п	Назва теми	Кількість Годин
1	Основи ручного шифрування. Розв'язання критичних задач класичної криптології.	4
2	Основи теорії чисел.	4
3	Алгоритм Евкліда.	2
4	Важкооборотні функції.	2
5	Псевдо випадкові послідовності. Алгоритм BBC.	4
6	Ативірусний захист електронної пошти	2
7	Безпека даних у комп'ютерних мережах.	4
8	Інформаційний захист мережі з використанням брандмауера і сервера посередника.	2
9	Захист інформації в операційних системах.	4
10	Системи охоронної сигналізації.	2
11	Охоронне телебачення.	2
12	Біометричні систем захисту.	4
	Разом	**36**

III. ПРИБЛИЗНА ТЕМАТИКА ПРАКТИЧНИХ (СЕМІНАРСЬКИХ) ЗАНЯТЬ

VI. КОНТРОЛЬНІ РОБОТИ

При вивченні дисципліни СМЗІ для поточного контролю знань студентів передбачається виконання модульної контрольної роботи по закінченню першого модуля.

1. Квантова криптографія.
2. Захист інформація в стільникових мережах.
3. Аналіз можливих загроз в інформаційних системах.
4. Система Райвеста, Шаміра, Адлемана.
5. Класичні шифри. Комп'ютерна реалізація алгоритмів.
6. Бінарний метод піднесення до степення за модулем числа *n*.
7. Система Діффі-Гелмана.
8. Робота з камерами відео спостережень. Пакети Netmeeting та Videoinspector.
9. Стеганографія. Пакет S-tools.
10. Кількаразове шифрування. Суперпозиція шифрів.
11. Криптографічні схеми сучасності.
12. Типи сенсорів, що застосовуються для захисту інформаційних об'єктів.
13. Методи частотного аналізу та прямого перебору.
14. Системи ADFGVX.
15. Технічні засоби охоронної сигналізації..
16. Подання тексту у цифровій формі. Шифр одноразового блокноту.
17. Біомедичні індентифікаційні системи.
18. Елементи теорії чисел. Функція Ойлера.
19. Безпека інформації операційних систем.
20. Детектори вібрацій, розбиття скла та ультразвуку.
21. Алгоритм Евкліда в теорії чисел.
22. Симетричні криптосистеми та системи з відкритим ключем.
23. Комбіновані сенсори охоронної сигналізації.
24. Системи PGP.
25. Системи електронного підпису.
26. Безпека інформації в комп'ютерних мережах.
27. Фотоелектричні сенсори та системи охорони периметра.
28. Принципи сучасної криптології.
29. Елементи і пристрої фізичної та електронної охорони об'єктів.
30. Захист інформації в автоматизованих системах обробки даних.
31. Елементи теорії чисел. Конгруенції та їх властивості.
32. Інформаційний захист ПК.
33. Принципи побудови, структури і задачі служби захисту інформації.
34. Знаходження обернених елементів і в кільці зведених лишків. Елементи теорії чисел.
35. Законодавчі і правові аспекти захисту інформації в Україні.
36. Захист інформації в Internet.
37. Хеш-функції. Вимоги до хеш-функцій. Схема цифрового підпису при застосуванні H(M) для алгоритму RSA.
38. Піднесення великого числа до великого степеня та взяття залишку за модулем третього великого числа.
39. Відкритий розподіл криптографічних ключів. Алгоритм Діффі-Гелмана.
40. Криптосистема Ель-Гамаля.
41. Проблеми генерування випадкових послідовностей та генерування псевдовипадкових чисел операційними системами і мовами програмування. Добування великих простих чисел.

42. Особливості стандарту AES.
43. Потокові шифри, алгоритм потокового шифру RC4. Потоковий шифр на основі генератора BBS. Переваги і недоліки потокових шифрів.
44. Афінні шифри
45. Стеганографія.
46. Що таке криптографія та криптоаналіз?
47. Типи криптографічних систем.
48. Означити крипостійкість та електронний підпис.
49. Описати типову схему криптосистем.
50. Навести приклади класичних криптосистем.
51. Шифр Віженера та програмна реалізація алгоритму на прикладі шифрування за методом Цезаря.
52. Порівняти блочну та асиметричну криптографії.
53. Описати алгоритм DES.
54. Математичні основи асиметричних криптосистем. Важкооборотні функції.
55. Основні означення дискретного аналізу та алгоритм Евкліда.
56. Алгоритм RSA.
57. Електронний підпис на основі асиметричного алгоритму.
58. Описати роботу з пакетом PGP.
59. Прикладні застосування криптографічних методів.
60. Що таке безпека даних у комп'ютерних мережах
61. Способи ідентифікації за персональними фізичними ознаками.
62. Способи з'єднань комп'ютерів в мережу.
63. Програмне та апаратне забезпечення з'єднання комп'ютерів в мережу.
64. Захист мережі з використанням брандмауерів і серверів – посередників.
65. Захист ресурсів в мереженій ОС Novel NetWare.
66. Захист інформації в ОС Windows NT.
67. Адміністративні засоби управління ресурсами домену Windows NT 4.0.
68. Особливості роботи з пакетами Win Snifter та x Intruder.
69. Інформаційна безпека в ОС UNIX.
70. Робота адміністратора в UNIX мережі.
71. Система Kerberos.
72. Робота з ОС Free BSD 3x, BSD 4x.
73. Захист електронної пошти.
74. Види інформацій і актуальність захисту інформацій та інформаційних об'єктів.
75. Потенційні загрози безпеці інформації в інформаційних системах.
76. Обмеження, розмежування і контроль доступу до інформаційних об'єктів.
77. Види систем охоронної сигналізації.
78. Сучасні системи контролю доступу на захищену територію.
79. Види засобів захисту інформації та їх класифікація.
80. Технічні засоби захисту інформаційних об'єктів.
81. Засоби охоронної сигналізації.
82. Охоронне телебачення.
83. Інфрачервоні сенсори охоронної сигналізації. Фізичні основи функціонування.
84. Фотоелектричні сенсори та системи охорони периметру.
85. Детектори вібрацій, розбиття скла, ультразвукові детектори, протипожежні детектори.
86. Охоронні системи телеспостереження.
87. Інтерфейс CRYPTO API Windows XP.
88. Сенсорні пристрої.
89. Голосова ідентифікація.
90. Захист салону автомобіля від зчитування інформації.
91. Автомобільні сигналізації та їх характеристики.
92. Ідентифікація ДНК особи.
93. Біометрія. Відбитки пальців. Розпізнання.

94. Шифрувальна система на основі шифру гамування.
95. Вчені, які зробили великий внесок в криптографію.
96. Елементи теорії криптографічних систем
97. Класичні криптосистеми
98. Програмна реалізація алгоритму шифрування за методом Цезаря
99. Сучасні блочна та асиметрична криптографії. Стандарт шифрування даних ГОСТ 28147 – 89.
100. Блочні криптосистеми типу DES, IDEA,BLOWFISH
101. Криптопакет KRYPTON
102. Асиметричні криптосистеми
103. Прикладні застосування криптографічних методів
104. Комплексне застосування криптографічних перетворень, кодування і стиску інформації.
105. Технології з'єднань комп'ютерів
106. Програмне та апаратне забезпечення з'єднання ПК
107. Реєстрація, розподіл та захист ресурсів у ОС Novel NetWare 3.11
108. Захист інформації в операційній системі Windows N
109. Методи інформаційної безпеки в ОС
110. Антивірусний захист електронної пошти
111. Загальні питання захисту інформації в автоматизованих системах обробки даних (АСОД)
112. Потенційні загрози безпеці інформації в АСОД
113. Обмеження, розмежування і контроль доступу до апаратури
114. Системи охоронної сигналізації (СОС)
115. Сучасні системи контролю доступу на територію, що захищається
116. Архітектура побудови систем контролю доступу
117. Біометрія як засіб ідентифікації особи в охоронних системах
118. Засоби захисту інформації АСОД та їх класифікація
119. Електронні системи захисту автомобілів
120. Інфрачервоні пасивні сенсори охоронної сигналізації
121. Фотоелектричні сенсори та системи охорони периметру
122. Охорона периметру з допомогою оптоелектронної (лазерної) системи
123. Пожежні повідомлювачі
124. Виконавчі пристрої охоронних систем
125. Система захисту, що базується на передачі інформації через стільникові лінії зв'язку
126. Побічні електромагнітні випромінювання (ПЕМВ)
127. Комп'ютерна стеганографія – технологія інформаційної безпеки XXI століття

VII. МЕТОДИЧНІ ВКАЗІВКИ

Л.С.Монастирський . Методичні вказівки з курсу СМЗІ .— Львів, Вид.центр ЛНУ, 2007, -66с.

VIII. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ

Основна література

1. О. В. Вербіцкий Вступ до криптології. ВНТА. Львів.1998 – 247с.
2. Б. Анин Защита компьютерной информации СПБ: БХВ – Санкт-Петербург. 2000. –384с.
3. Б. С.Люцарев, К. В. Ермаков, Е. Б. Рудный, И. Е. Ермаков. Безопасность компьютерных сетей на основе Windows NT. 1998. –340с. «Channel Tr. Ltd»

4. В. В. Домарёв .Защита информации и безопасность компьютерных систем. Diasoft. Киев. 1999. –453с.

Допоміжна

1. В. Ємець, А. Мельник, Р. Попович. Сучасна криптографія. Основні погяття. Львів-2003, “Бак”, -144с.
2. Т. Корнієнко, А. Мельник, В. Мельник. Алгоритм та процеси симетричного блокового шифрування. Львів-2003, “Бак”, -168с.

14. Інформаційні ресурси

1. Eric Weisstein's World of Physics http://scienceworld.wolfram.com/physics/
Wikipedia. http://www.wikipedia.org