

**ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
“ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ”
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ
кафедра економічної кібернетики**

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної
та навчальної роботи
_____ О.І. Гура

«_____» _____ 20__ р.

Інформаційна безпека: загрози та методи захисту

ПРОГРАМА
навчальної дисципліни
підготовки _ бакалаврів _
з напрямку підготовки за вибором студента
Кафедра економічної кібернетики

Статус курсу: спецкурс

Запоріжжя 2016

РОЗРОБЛЕНО ТА ВНЕСЕНО:

кафедра економічної кібернетики,

економічного факультету Запорізького національного
університету

РОЗРОБНИК ПРОГРАМИ

Козін І.В., професор, доктор фіз.-мат. наук

ОБГОВОРЕНО ТА РЕКОМЕНДОВАНО ДО ЗАТВЕРДЖЕННЯ КАФЕДРОЮ
економічної кібернетики «___» _____ року, протокол

№ _____

ЗАВІДУВАЧ КАФЕДРИ

д.е.н., професор _____ Н.К. Максишко

Вступ

Програма з курсу «Інформаційна безпека: загрози та методи захисту» є спеціальним курсом за вибором студента для рівня підготовки бакалавр.

Курс “ **Інформаційна безпека: загрози та методи захисту** ” є загальноосвітнім курсом, який знайомить студентів с сучасними проблемами захисту інформації, що не пов’язана з державною таємницею, та організації захисту інформації на підприємствах,

Предметом вивчення навчальної дисципліни є основні загрози інформації та методи її захисту..

Міждисциплінарні зв’язки:

1. Мета та завдання навчальної дисципліни

1.1 Мета викладання дисципліни.

Основна мета дисципліни – формування у студентів базових знань, необхідних для розуміння широкого кола реальних проблем захисту інформації у комп’ютерних системах та мережах.

1.2 Задачі вивчення дисципліни.

Внаслідок вивчення дисципліни студенти повинні:

ЗНАТИ: загальні принципи організації захисту інформації в комп’ютерних системах та мережах на базі сучасних концепцій.

ВМІТИ: впроваджувати системний підхід к захисту інформації в комп’ютерних системах та мережах, використовувати стандартні криптографічні алгоритми та протоколи, використовувати сучасні засоби та методи криптографічного захисту інформації, виконувати розрахунки характеристик безпечного використання паролів та ключів шифрування .

1.3 Перелік дисциплін, засвоєння яких необхідне для вивчення даної дисципліни.

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль I. Загрози безпеки інформації та методи захисту.

Тема 1 Вступ. Предмет та задачі курсу. Основні визначення та термінологія. Література, що рекомендується.

Тема 2 Загрози безпеки та методи захисту. Основні шляхи витоку інформації та несанкціонованого доступу в каналах телекомунікацій. Політика захисту інформації. Свідомість працівників. Окреслення небезпеки і потенційно можливих атак. Паролі. Firewall.

Тема 3. Організаційні методи захисту. Структура та задачі органів безпеки інформації в інформаційних системах.

Змістовий модуль II. Криптографічні методи захисту інформації.

Тема 4. Криптографічний захист інформації. Основні принципи шифрування.

Тема 5. Криптографічні системи з закритим ключом. Односторонні функції. Хеш-функції. Криптографічні системи з відкритим ключом. Стандарти шифрування.

Тема 6. Електронний цифровий підпис. Протоколи цифрового підпису.

3. Рекомендована література

Основна

1. Дж. Уолрэнд. Телекоммуникационные и компьютерные сети. Вводный курс. Москва: Постмаркет, 2001. – 480с.
2. Вербіцкий О.В. Вступ до криптології. – Видавництво наук.-техн. Літератури. Львів, 1998.

3. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов/ П.Н. Деревянин, О.О.Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.
4. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем: учеб. пособие (спец. 200900, 201000, 060800)/ СПбГУТ. – СПб, 2000. – 134с.
5. Зегжда Д.П., Ивашко А.М. Основы информационной безопасности. – М.: Горячая линия - Телеком, 2000. – 452с.
6. Щербakov А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001, 352с.
7. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
8. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, ПБОЮЛ Н.А. Егоров, 2001. – 264 с.
9. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». – М.: СИНТЕГ, 2000. – 248 с.
10. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.Ж КУДИЦ-ОБРАЗ, 2001 – 386с.

Додаткова література

1. Молдовян А.А., Молдовян Н.А., Советов А.Б. Криптография- Серия «Учебники для вузов. Специальная литература». – СПб.: Изд-во «Лань», 2000.- 224с.
2. Введение в криптографию / Под общ. Ред. В.В. Яценко. – 2-е изд., испр. – М.:МЦНМО: «ЧеРо», 1999. – 272с.
3. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов / Под ред. В.А.Садовниченко – М.: Высш.шк., 1999. – 109с.
4. Петраков А.В., Лагутин В.С. Утечка и защита информации в телефонных каналах. 3-е изд., исправл. и доп. – М.: Энергоатомиздат, 1998. – 320с.
5. М.Н. Аршинов, Л.Е. Садовский. Коды и математика (рассказы о кодировании).- М.: Наука, Главная редакция физико-математической литературы, 1983.- 144с. (Библиотечка «Квант». Выпуск 30).
6. Жельников В. Криптография от компьютера до папируса. – М., АБФ, 1997. – 336с.
7. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов/ П.Ю. Белкин, О.О.Михальский, А.С. Першаков и др. – М.: Радио и связь, 2000. – 168 с.
8. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов/ Проскурин В.Г., Крутов С.В., Маркевич И.В. – М.: Радио и связь, 2000. – 168 с.
9. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов/ П.Н. Деревянин, О.О.Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.
10. Вербицкий О.В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 248.

11. Журнал Захист інформації – Київ: Науково-технічний журнал. Засновано у 1999 році. Засновник - Київський міжнародний університет цивільної авіації.
12. Журнал Проблемы информационной безопасности. Компьютерные системы – С.-Петербург: Санкт-Петербургский государственный технический университет. Осн. в 1999г.
13. Журнал Безопасность информационных технологий – М.: Московский государственный технический университет.
14. Журнал Защита информации. Конфидент –С.-Пб:Информационно-методический журнал. Основан в 1994г., Изд. ООО «Конфидент».
15. Баричев С. Криптография без секретов.
16. Винокуров А. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86.// Монитор. М., 1995. №1,5.
17. Саломаа А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318с.
18. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем: учеб. пособие (спец. 200900, 201000, 060800)/ СПбГУТ. – Спб, 2000. – 134с.
19. Зегжда Д.П., Ивашко А.М. Основы информационной безопасности. – М.: Горячая линия - Телеком, 2000. – 452с.
20. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001, 352с.
21. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
22. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, ПБОЮЛ Н.А. Егоров, 2001. – 264 с.
23. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». – М.: СИНТЕГ, 2000. - 248 с.
24. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.Ж КУДИЦ-ОБРАЗ, 2001 – 386с.
25. Рассказ Эдгара По «Золотой жук».
26. Рассказ Артура Конан Дойля «Пляшущие человечки».

Інформаційні ресурси