

ПРОГРАМА КУРСУ

«Системи захисту інформації»

Напрямок: прикладна математика

Факультет: прикладна математика та інформатика

Форма навчання: денна

Витяг з навчального плану

Курс	Семестр	Кількість кредитів	Загальний обсяг (год.)	Всього аудит. (год.)	у тому числі (год.):			Самостійна робота (год.)	Контрольні (модульні) роботи (шт.)	Розрахунково-графічні роботи (шт.)	Курсові проекти (роботи), (шт.)	Залік (сем.)	Екзамен (сем.)
					Лекції	Лабораторні	Практичні						
5	9	4	144	60	30	30	-	76	1	-	-	-	+

1. Анотація

Даний спеціальний курс є логічним продовженням курсу з основ криптології. До його складу входить цикл лекцій та лабораторних занять. У результаті вивчення дисципліни студенти повинні засвоїти основні практичні методи багаторівневого захисту даних. Студенти знайомляться з практично важливими криптографічними стандартами, протоколами передачі даних, методами аутентифікації користувачів, алгоритмами генерації та узгодження ключової інформації, правилами захисту програмного забезпечення.

2. Зміст програми

2.1. Принципи захисту програмного забезпечення

Тема 1. Предмет дисципліни. Рівні захисту та джерела втрати інформації у комерційних структурах. Поняття про фізичний та електронний захист даних.

Тема 2. Аутентифікація. Слабкі місця комп'ютерних систем та способи підвищення їх надійності. Правила побудови парольного захисту.

Тема 3. Файлові системи. Основні сучасні файлові системи та їх модифікації: FAT, NTFS, Ex2-Ex4 їх структура та принципи функціонування.

Тема 4. Низькорівневе кодування. Асемблер PC; арифметичні операції; умовні та безумовний переходи; зсуви; логічні операції; робота зі стрічками; переривання BIOS та DOS. Асемблерні вставки; роздільна компіляція; виклик підпрограм. Реальний та захищений режими.

Тема 5. Програмний захист. Методи захисту даних та програм від копіювання; програм від трасування і декомпіляції. Стиск виконавчих кодів, відладчики. Приклад використання Debug. Захис Web застосувань.

Тема 6. Арифметика великих чисел. Представлення довгих чисел структурами даних. Класичні алгоритми роботи з довгими числами. Теореми алгоритму ділення.

Тема 7. Методи швидкого множення. Модульна арифметика. Велика Китайська теорема про лишки. Алгоритми переведення довгих чисел у модульне представлення і навпаки. Класичний та узагальнений алгоритми Евкліда. Алгоритми швидкого множення. Метод многочленів та цифровий метод. Дискретне перетворення Фур'є та його застосування для швидкого множення довгих чисел.

2.2. Базові інструменти розробки криптографічного захисту

Тема 8. Стандарти криптування. Криптографія, криптоаналіз, стеганографія. Поняття про класичні методи шифрування та криптографічні системи з відкритим ключем. Стандарти криптування даних.

Тема 9. Хеш функції. Хеш функції, їх призначення, властивості та особливості застосування у криптографії. Теорема про три довжини. Способи побудови хеш функцій. Стандарти MD2, MD4, MD5 та ГОСТ Р34.11-94.

Тема 10. Стандарт ГОСТ 28147-89. Алгоритм криптування ГОСТ 28147-89. Логіка алгоритму. Основний крок криптоперетворення. Базові цикли 32-3, 32-Р, 16-3. Режими алгоритму ГОСТ 28147-89. Режим постої заміни, гамування, гамування з оберненим зв'язком, вироблення імітовставки.

Тема 11. Достовірність даних. Захист, достовірність та аутентичність даних. Електронний підпис та його функції. Вимоги до побудови алгоритмів забезпечення достовірності та авторства даних. Стандарти цифрового підпису.

Тема 12. Електронний підпис. Класичний алгоритм Діффі-Хелмана підпису одного блоку на основі довільного криптоалгоритму, його переваги та недоліки. Функція криптопрокрутки. Модифікований алгоритм Діффі-Хелмана для підпису одного блоку. Правила вибору ключової інформації. Стійкість алгоритму та використання на практиці.

Тема 13. Сертифікаційні центри. Алгоритми керування ключами. Стандарти узгодження ключової інформації. Моделі сертифікації відкритих ключів.

Основна література

1. **Анин Б.Ю.** Защита компьютерной информации / Б.Ю. Анин. – СПб.: ВHV-СПб, 2003. – 400 с.
2. **Берник В.** Математические и компьютерные основы криптологии / В. Берник, С. Матвеев, Ю. Харин. – М.: Новое знание, 2003. – 382 с.
3. **Вербіцький О.В.** Вступ до криптології / О.В. Вербіцький. – Львів, ВНТЛ, 1998. – 248 с.

4. **Гашков С.Б.** Арифметика. Алгоритмы. Сложность вычислений / С.Б. Гашков, В.И. Чубариков. – М.: Высшая школа, 2000.
5. **Девянин П.** Модели безопасности компьютерных систем / П. Девянин. – М.: Academia, 2005. – 144 с.
6. **Кнут Д.** Искусство программирования. Т. 2 / Д. Кнут. – М.: Мир, 1977.
7. **Нечаев В.И.** Элементы криптографии. Основы теории защиты информации / В.И. Нечаев. – М.: Высшая школа, 1999. – 109 с.
8. **Петров А.А.** Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. – М.: ДМК, 2000.
9. **Чмора А.** Современная прикладная криптография / . – М.: Гелиос АРВ, 2001. – 244 с.
10. **Ященко В.В.** Введение в криптографию / В.В. Ященко, Н.В. Варновский, Ю.В. Нестеренко, Г.А. Кабатянский, П.Н. Девянин, В.Г. Проскурин, А.В. Черемушкин, П.А. Гырдымов, А.Ю. Зубов, А.В. Зязин, В.Н. Овчинников. – М.: МЦНМО «ЧеРо», 1999. – 271 с.

Додаткова література

1. **Горбатов В.С.** Основы технологии РКІ / В.С. Горбатов, О.Ю. Полянская. – Харків, Горячая Линия – Телеком, 2004. – 248 с.
2. **Партыка Т.Л.** Информационная безопасность / Т.Л. Партыка, И.И. Попов. – М.: Форум, 2007. – 368 с.
3. **Петраков А.** Основы практической защиты информации / А. Петраков. – М.: Солон, 2005. – 384 с.
4. **Петраков А.** Информационная безопасность и защита информации / А. Петраков, В. Мельников, С. Клейменов. – М.: Academia, 2008. – 336 с.
5. **Пузыренко А.Ю.** Компьютерная стеганография Теория и практика / А.Ю. Пузыренко, Г.Ф. Конахович. – М.: МК-Пресс, 2006. – 288 с.
6. **Хорев П.** Методы и средства защиты информации в компьютерных системах / П. Хорев. – М.: Academia, 2008. – 256 с.
7. **Чекатков А.А.** Методы и средства защиты информации / А.А. Чекатков, В.А. Хорошко. – Харьков, Юниор, 2003. – 504 с.
8. **Шаньгин В.** Защита компьютерной информации / . – М.: ДМК Пресс, 2008. – 544 с.
9. **Шевцов В.А.** Основы защиты информации / В.А. Шевцов, А.В. Сахаров, А.И. Куприянов. – М.: Academia, 2006. – 256 с.
10. **Щеглов А.Ю.** Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – М.: Наука и Техника, 2004. – 384 с.

Програму склав старший викладач Я.С. Гарасим