

004:004.056(075.8)

Рекомендовано к изданию методическим советом ПГУТИ,
протокол № _____ от _____ 2014 г.

Рецензенты:

Заведующий кафедрой компьютерных систем и технологий Шуменского университета им. Епископа Константина Преславского (Болгария), д.т.н, профессор
Станев Станимир Стоянов.

Профессор кафедры геоинформатики и информационной безопасности Самарского государственного аэрокосмического университета им. С.П.Королёва (Национального исследовательского университета) д.т.н., профессор, Лауреат Государственной Премии СССР
Мостовой Яков Анатольевич.

Алексеев, А.П.

Информатика для криптоаналитиков: учебное пособие/ Алексеев А. П.- Самара: ИУНЛ ПГУТИ, 2015. – 378 с.

Книга соответствует типовой программе по информатике для высших учебных заведений. Отличительной особенностью публикации является изложение основных принципов, идей, исторического аспекта излагаемых вопросов, обзоров по программным продуктам и аппаратным средствам, толкование терминов. Такой подход позволяет сохранить актуальность изученного материала в течение нескольких лет.

В книге в компактной форме даны основные понятия информатики, рассмотрены арифметические и логические основы работы ЭВМ, принцип действия важнейших устройств ЭВМ. Дано представление о локальных и глобальных сетях, описана организация данных в ЭВМ, методы сжатия информации, помехоустойчивого кодирования. Дано понятие о вирусах и антивирусных программах. Рассмотрены основные понятия криптографии, стеганографии. Заметный акцент в книге сделан на изложение вопросов защиты информации.

Учебное пособие предназначено для студентов специальностей «Информационная безопасность» и «Информационная безопасность в телекоммуникационных системах» (10.03.01, 10.05.02).

Оглавление

Введение.....	3
1. Основные понятия.....	5
1.1. Основные понятия информатики.....	5
1.2. Основные понятия теории информации.....	10
1.3. Этапы развития вычислительной техники.....	16
1.4. Развитие отечественной вычислительной техники.....	22
2. Арифметические и логические основы работы ЭВМ....	25
2.1. Системы счисления.....	25
2.2. Логические основы работы ЭВМ	33
2.3. Арифметические основы работы ЭВМ	37
3. Кодирование информации в ЭВМ.....	43
3.1. Кодовая таблица.....	43
3.2. Представление данных в ЭВМ	45
3.3. Представление команд в ЭВМ.....	49
3.4. Методы сжатия информации без потерь.....	51
3.5. Методы сжатия информации с потерями.....	58
3.6. Помехоустойчивое кодирование.....	66
3.7. QR-коды	74
4. Аппаратные средства ЭВМ.....	85
4.1. Структурная схема ЭВМ.....	85
4.2. Принцип действия основных устройств ЭВМ	91
4.2.1. Принцип действия цифровых устройств.....	91
4.2.2. Арифметико-логическое устройство	98
4.2.3. Память.....	101
4.2.4. Оперативная память	101
4.2.5. Внешние запоминающие устройства	106
4.2.6. Устройства ввода информации	113
4.2.7. Устройства вывода информации	117
4.2.8. Жидкокристаллические мониторы.....	122
4.3. Классификация ЭВМ	124
5. Системное программное обеспечение ЭВМ.....	129
5.1. Понятие об операционной системе.....	129
5.2. Файловая система.....	141
5.3. Вирусы и антивирусные программы	146
5.4. Основные понятия программирования.....	155
5.4.1. Языки программирования.....	155
5.4.2. Основные свойства алгоритма.....	164
5.4.3. Базовые структуры программирования.....	167
6. Прикладное программное обеспечение ЭВМ.....	169
6.1. Текстовые редакторы	169
6.2. Графические редакторы	176
6.3. Средства презентации.....	184
6.4. Электронные таблицы.....	189
6.5. Базы данных	195
6.6. Искусственный интеллект	203
6.7. Экспертные системы	208
6.8. Мультимедиа	213
6.9. Виртуальная реальность	218

7. Основные понятия моделирования	223
7.1. Основные понятия и определения	223
7.1.1. Виды моделей	226
7.1.2. Понятие об имитационном моделировании	229
7.1.3. Понятие о физическом моделировании	231
7.1.4. Уровни моделирования	233
7.2. Системы моделирования РЭУ	235
7.3. Моделирование криптосистем с помощью Multisim.....	240
8. Математические и статистические системы	248
8.1. Обзор математических и статистических систем	248
8.2. Математическая система Mathcad.....	253
8.2.1. Пользовательский интерфейс	253
8.2.2. Компьютерная алгебра	258
8.2.3. Операции с комплексными числами.....	263
8.2.4. Вопросы программирования.....	265
9. Сетевые информационные технологии	272
9.1. Локальные сети	272
9.2. Глобальные сети	277
9.3. Семиуровневая сетевая модель OSI.....	285
9.3.1. Физический уровень.....	285
9.3.2. Канальный уровень	286
9.3.3. Сетевой уровень	286
9.3.4. Транспортный уровень	288
9.3.5. Сеансовый уровень.....	289
9.3.6. Представительный уровень.....	289
9.3.7. Прикладной уровень.....	289
9.4. Электронная почта	290
9.5. Социальные сети.....	302
10. Защита информации.....	307
10.1. Основные понятия криптографии.....	307
10.2. Шифрование сообщений различными методами.....	313
10.3. Гибридная криптосистема.....	323
10.4. Криптографическая система с открытым ключом.....	325
10.5. Криптографическая программа PGP.....	330
10.6. Основные понятия стеганографии.....	337
10.7. Соккрытие информации в рисунках и фотографиях.....	345
10.8. Пространственно-временные методы сокрытия информации	348
11. Перспективы развития информатики.....	356
12. Приложения	361
12.1. Список аббревиатур	361
12.2. Глоссарий.....	362
Заключение.....	370
Список литературы	371
Оглавление.....	373