

СОДЕРЖАНИЕ

Предисловие редакторов	4
Предисловие авторов	5
Основные обозначения.....	10
 ГЛАВА 1. ИСТОРИЧЕСКИЙ ОЧЕРК РАЗВИТИЯ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ	
Параграф 1.1. Криптографические средства с древнего времени	11
Параграф 1.2. История отечественной криптографии.....	57
Параграф 1.3. Модели шифров по К. Шеннону. Способы представления реализаций шифров	82
Параграф 1.4. Средства защиты информации в переходный период от древности к современности.....	94
Параграф 1.5. Стеганографические средства защиты информации в переходный период от древности к современности	118
Параграф 1.6. Идея открытого ключа- революция в криптографии	122
Параграф 1.7. Недостатки модели шифра Шеннона. Обобщенная модель шифра	130
 ГЛАВА 2. ДЕШИФРОВАНИЕ ИСТОРИЧЕСКИХ ШИФРОВ	
Параграф 2.1. Дешифрование шифра простой замены, перестановки и некоторых шифров гаммирования	134
Параграф 2.2. Дешифрование шифра Виженера	151
 ГЛАВА 3. ИНФОРМАЦИЯ, ЕЕ СВОЙСТВА	
Параграф 3.1. Общее понятие информации. Способы представления информации, подлежащей шифрованию. Дискретизация непрерывных сигналов	186

Параграф 3.2. Открытые сообщения и их характеристики	187
Параграф 3.3. Критерии на осмысленные сообщения	195

ГЛАВА 4. ТЕОРЕТИЧЕСКАЯ СТОЙКОСТЬ ШИФРОВ. ТЕОРЕТИКО-ИНФОРМАЦИОННЫЕ МОДЕЛИ ШИФРОВ

Параграф 4.1. Основные понятия и теоремы математической теории информации.....	201
Параграф 4.2. Стационарные эргодические модели содержательных сообщений.....	211
Параграф 4.3. Энтропии шифртекста и ключей. Расстояния единственности для открытого текста и ключа. Теоретическая стойкость шифров	214

ГЛАВА 5. ПРАКТИЧЕСКАЯ СТОЙКОСТЬ ШИФРОВ

Параграф 5.1. Понятие практической стойкости шифров	228
Параграф 5.2. Принципы построения методов определения ключей шифрсистем	231
Параграф 5.3. Методы опробования	235
Параграф 5.4. Принципы построения статистических методов криптоанализа.....	257
Параграф 5.5. Введение в теорию случайных систем уравнений	271
Параграф 5.6. Аналитические методы криптоанализа.....	294

ГЛАВА 6. ВОПРОСЫ СИНТЕЗА ШИФРОВ И ИХ КРИПТОСХЕМ

Параграф 6.1. Шифры, близкие к совершенным	304
Параграф 6.2. Гомоморфизмы и конгруэнции шифров	310
Параграф 6.3. Групповые шифры. Обратимые групповые шифры.....	313
Параграф 6.4. Инварианты шифров	318
•Параграф 6.5. Введение в вопросы синтеза криптосхем.....	320
Параграф 6.6. Статистическая структура двоичной функции	323
Параграф 6.7. Математические основы синтеза булевых функций с гарантированными	

криптографическими свойствами	328
Параграф 6.8. Регистры сдвига, одноканальные линии задержки.....	358
Параграф 6.9. Вопросы гарантирования периодов выходных последовательностей автоматов при заданной входной последовательности	368
 ГЛАВА 7. ИМИТОСТОЙКОСТЬ ШИФРОВ. ПОМЕХОУСТОЙЧИВОСТЬ ШИФРОВ. СЕТИ ЗАСЕКРЕЧЕННОЙ СВЯЗИ	
Параграф 7.1. Имитостойкость шифров в модели К. Шеннона	380
Параграф 7.2. Примеры имитации и способы имитозащиты.....	388
Параграф 7.3. Помехоустойчивые шифры.....	391
Параграф 7.4. Помехоустойчивые шифрующие автоматы	405
Параграф 7.5. Общие математические задачи, связанные с проблемой построения помехоустойчивых шифров	409
Параграф 7.6. Основные понятия сетей засекреченной связи. Компрометация абонентов	430
Параграф 7.7. Перекрытия в сетях засекреченной связи	437
ЛИТЕРАТУРА	439
ПРИЛОЖЕНИЕ 1	462
ПРИЛОЖЕНИЕ 2	467
ПРИЛОЖЕНИЕ 3	505