О.Г. ШВЕЧКОВА, А.Н. ПЫЛЬКИН, Д.В. МАРЧЕВ

КУРС

БАЗОВЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УЧЕБНОЕ ПОСОБИЕ

О.Г. Швечкова
А.Н. Пылькин
Д.В. Марчев

БАЗОВЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УЧЕБНОЕ ПОСОБИЕ

Рекомендовано Научно-методическим советом Федерального государственного бюджетного образовательного учреждения высшего образования «Рязанский государственный радиотехнический университет» в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям подготовки 2.09.03.04 «Программная инженерия» и 2.09.03.03. «Прикладная информатика»

Москва
КУРС
2021

УДК 004.056.55(075.8)
ББК 32.973.2я73
Ш35

ФЗ № 436-ФЗ	Издание не подлежит маркировке в соответствии с п. 1 ч. 4 ст. 11

Рецензенты:
Минаев В.А. — д-р техн. наук, профессор кафедры «Защита информации» МГТУ им. Н.Э. Баумана;
Кузнецов А.Е. — д-р техн. наук, зам. директора НИИ обработки аэрокосмических изображений «Фотон» (г. Рязань)

Швечкова О.Г.,

Ш35 Базовые криптографические алгоритмы защиты информации: учебное пособие / О.Г. Швечкова, А.Н. Пылькин, Д.В. Марчев. — Москва: КУРС, 2021. — 168 с.

ISBN 978-5-906923-83-7

В учебном пособии рассмотрены вопросы решения проблем информационной безопасности методами криптографической защиты информации. Исследованы и проанализированы цели защиты информации в свете существующей Доктрины информационной безопасности Российской Федерации. Изложены теоретические основы базовой криптографии, формализации и программной реализации классических криптографических алгоритмов. Представлены механизмы контроля и тестирования знаний и приемов практической реализации рассмотренных методов (в форме оценочных материалов).

Учебное пособие предназначено для подготовки специалистов по образо-вательным программам направлений 2.09.03.04 «Программная инженерия» и 2.09.03.03 «Прикладная информатика.

УДК 004.056.55(075.8)
ББК 32.973.2я73

КУРС INTERACTIVE ON-LINE

ISBN 978-5-906923-83-7

© Швечкова О.Г., Пылькин А.Н., Марчев Д.В., 2018, 2019, 2020
© КУРС, 2018, 2019, 2020

Подписано в печать 05.03.2021.
Формат 60×90/16. Бумага офсетная. Гарнитура Newton.
Печать цифровая. Усл. печ. л. 10,5.
Доп.тираж 100 экз. Заказ № 1503.

ТК 683039-961731-100118

ООО Издательство «КУРС»
127273, Москва, ул. Олонецкая, д. 17А, офис 104.
Тел.: (495) 203-57-83. E-mail: kursizdat@gmail.com http://kursizdat.ru

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ ... 3

Основные положения Доктрины информационной безопасности РФ ... 4

Тема 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ... 9

1.1. Понятие информационной безопасности. Задачи обеспечения информационной безопасности ... 9

1.2. Угрозы информационной безопасности ... 12

1.2.1. Основные угрозы конфиденциальности ... 13

1.2.2. Основные угрозы целостности ... 14

1.2.3. Основные угрозы доступности ... 15

1.3. Роль криптографических протоколов в задаче обеспечения информационной безопасности ... 15

1.4. Общие сведения классической криптографии ... 17

1.4.1. Основные понятия и определения классической криптографии ... 17

1.4.2. Стойкость алгоритмов шифрования ... 19

1.4.3. Основные методы криптографической защиты информации ... 22

1.4.4. Классификация криптографических алгоритмов ... 24

1.5. Аппаратная и программная реализация алгоритмов шифрования ... 33

1.5.1. Аппаратная реализация криптографических алгоритмов ... 34

1.5.2. Программная реализация криптографических алгоритмов ... 35

1.5.3. Программно-аппаратная реализация криптографических алгоритмов ... 35

Контрольные вопросы ... 36

Тема 2. ШИФРЫ ЗАМЕНЫ ... 38

2.1. Шифры простой замены ... 39

2.1.1. Система шифрования Цезаря ... 39

2.1.2. Аффинная система подстановок Цезаря ... 40

2.1.3. Лозунговый шифр ... 42

2.1.4. Полибианский квадрат ... 44

2.1.5. Шифрующая таблица Трисемуса ... 45

2.1.6. Биграммный шифр Плейфера ... 46

2.1.7. Система омофонов ... 49

2.1.9. Тесты по теме «Алгоритмы простой замены» ... 51

2.2. Шифры сложной замены ... 55

2.2.1. Шифр Гронсфельда ... 56

2.2.2. Система шифрования Вижинера ... 57

2.2.3. Шифр Вижинера с автоключом ... 58

2.2.4. Шифр Вижинера с перемешанным алфавитом ... 60

2.2.5. Двойной квадрат Уитстона ... 61

2.2.7. Тесты по теме «Алгоритмы сложной замены» ... 62

2.2.8. Задание для самостоятельной работы по практической реализации алгоритмов шифрования методами замены ... 66

Тема 3. ШИФРЫ ПЕРЕСТАНОВКИ 68

3.1. Шифр простейшей перестановки 68
3.2. Шифр маршрутной перестановки 69
3.3. Шифр перестановки «Сцитала» 72
3.4. Шифр «Поворотная решетка» 74
3.5. Шифр вертикальной перестановки 78
3.6. Шифр на основе магических квадратов 80
3.7. Контрольные вопросы 81
3.8. Тесты по теме «Шифры перестановки» 82
3.9. Задание для самостоятельной работы по практической реализации алгоритмов шифрования методами перестановки 87

Тема 4. ШИФРОВАНИЕ МЕТОДОМ ГАММИРОВАНИЯ 89

4.1. Методы генерации псевдослучайных последовательных чисел 89
4.1.1. Аддитивный генератор 91
4.1.2. Линейный конгруэнтный генератор 92
4.1.3. Мультипликативный генератор 93
4.1.4. Смешанный генератор 94
4.2. Описание алгоритмов шифрования и дешифрования методом гаммирования 95
4.2.1. Алгоритм шифрования 95
4.2.2. Алгоритм дешифрования 96
4.3. Контрольные вопросы 96
4.4. Тесты по теме «Шифрование методом гаммирования» 96
4.5. Задание для самостоятельной работы по практической реализации алгоритмов шифрования методами гаммирования 100

Тема 5. СИСТЕМА СИММЕТРИЧНОГО ШИФРОВАНИЯ 102

5.1. Моделирование кодера и декодера 103
5.2. Контрольные вопросы 108
5.3. Тесты по теме «Шифрование методом гаммирования» 108
5.4. Задание для самостоятельной работы по практической реализации алгоритмов шифрования методом Вернама 111

Тема 6. РЕЗУЛЬТИРУЮЩИЕ ТЕСТЫ ПО ВСЕМ РАЗДЕЛАМ ДИСЦИПЛИНЫ 113

СЛОВАРЬ КРИПТОГРАФИЧЕСКИХ ТЕРМИНОВ 120

СПИСОК ЛИТЕРАТУРЫ 161