

ВЫСШЕЕ ОБРАЗОВАНИЕ

# ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В. В. Лозовецкий  
Е. Г. Комаров  
В. В. Лебедев



E.LANBOOK.COM

**В. В. ЛОЗОВЕЦКИЙ,  
Е. Г. КОМАРОВ,  
В. В. ЛЕБЕДЕВ**

# **ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ**

Под редакцией доктора технических наук, профессора В. В. Лозовецкого

## **ДОПУЩЕНО**

*ФУМО в системе высшего образования по укрупненной группе специальностей и направлений подготовки «Информационная безопасность» в качестве учебного пособия в электронной и печатной формах для студентов, обучающихся по направлениям «Системы управления летательными аппаратами», «Управление в технических системах», «Приборостроение», «Информатика и вычислительная техника», «Автоматизация технологических процессов и производств» по программе подготовки бакалавров, магистров, специалистов*



**ЛАНЬ**

САНКТ-ПЕТЕРБУРГ • МОСКВА • КРАСНОДАР

2023

УДК 654  
ББК 32.97я73

**Л 72**      **В. В. Лозовецкий.** Защита автоматизированных систем обработки информации и телекоммуникационных сетей : учебное пособие для вузов / В. В. Лозовецкий, Е. Г. Комаров, В. В. Лебедев ; под редакцией В. В. Лозовецкого. — Санкт-Петербург : Лань, 2023. — 488 с. : ил. — Текст : непосредственный.

**ISBN 978-5-507-46870-6**

В учебном пособии рассмотрены и проанализированы как классические методы и средства криптографической защиты автоматизированных систем обработки информации и телекоммуникационных систем, так и современные алгоритмы, протоколы и средства защиты информации. Теоретический материал и математические основы решения прикладных задач современной криптографии сопровождаются большим количеством примеров и задач. Большое внимание уделено моделированию систем, обеспечивающих информационную безопасность, и разработке систем управления информационной безопасностью. Представлен материал, позволяющий оценить эффективность средств защиты информации, прогнозирование рисков несанкционированного доступа и обеспечение информационной безопасности в условиях реализации атак на компьютерную сеть, рассмотрены основные методы определения затрат на создание системы обеспечения информационной безопасности с учетом степени ее конфиденциальности. Приведена методика разработки проекта аудита системы защиты информации и конкретный пример ее реализации, которые могут быть использованы при курсовом и дипломном проектировании.

УДК 654  
ББК 32.97я73

**Рецензенты:**

**В. М. АРТЮШЕНКО** — доктор технических наук, профессор, зав. кафедрой информационных технологий и управляющих систем Технологического университета им. дважды Героя Советского Союза, летчика-космонавта А. А. Леонова;

**Ю. Ю. ГРОМОВ** — доктор технических наук, профессор, профессор кафедры информационных систем и защиты информации, директор Института автоматизации и информационных технологий Тамбовского государственного технического университета.

**Обложка**  
**П. И. ПОЛЯКОВА**

© Издательство «Лань», 2023  
© Коллектив авторов, 2023  
© Издательство «Лань», художественное оформление, 2023

# ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ.....	3
Глава 1. ОСНОВНЫЕ ПОНЯТИЯ И ХАРАКТЕРИСТИКА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ.....	5
1.1. Информационная безопасность — цели и средства.....	5
1.2. Состав и классификация информационно-телекоммуникационных сетей (систем) .....	11
1.3. Особенности современных автоматизированных систем.....	21
1.4. Средства информационной безопасности .....	24
Глава 2. ОСНОВЫ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ СИСТЕМ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ИНФОРМАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ .....	71
2.1. Математические основы решения прикладных задач современной криптографии.....	71
2.1.1. Деление с остатком целых чисел. Сравнения .....	71
2.1.2. Простые и составные числа. Разложение составных чисел на множители. Основная теорема арифметики.....	72
2.1.3. Свойство делимости. Наибольший общий делитель (НОД) и наименьшее общее кратное (НОК). Алгоритм Евклида .....	74
2.1.4. Взаимно простые числа .....	77
2.1.5. Линейные целочисленные уравнения .....	77
2.1.6. Сравнения.....	78
2.1.7. Свойства сравнений. Решение сравнений .....	79
2.1.8. Модулярная арифметика .....	80
2.1.9. Решение сравнений первой степени.....	83
2.1.10. Система сравнений первой степени .....	87
2.1.11. Сравнения по модулю как отношение эквивалентности и остаточные классы, или классы вычетов.....	92
2.1.12. Теорема Ферма. Функция Эйлера. Теорема Эйлера.....	96
2.1.13. Решение линейных сравнений с помощью теоремы Эйлера.....	97
2.1.14. Нахождение остатка от деления на модуль больших степеней заданного числа.....	99
2.1.15. Использование малой теоремы Ферма при тестировании простоты целых чисел.....	100
2.1.16. Первообразные корни и индексы .....	100
2.1.17. Свойства индексов, основанием которых является первообразный корень .....	102
2.1.18. Степенные вычеты и невычеты. Применение индексов при решении степенных сравнений .....	103
2.1.19. Квадратичные вычеты и сравнения.....	110
2.1.20. Разрешимость квадратичных сравнений. Критерии существования квадратичного вычета: символы Лежандра и Якоби.....	114

2.1.21. Решение степенных сравнений по составному модулю .....	117
2.1.22. Вычисления в конечных полях вычетов. Определения и свойства групп, колец и полей .....	118
2.1.23. Циклические группы в полях Галуа .....	124
2.2. Принципы и основные положения криптографии .....	126
2.2.1. Цели поддержки безопасности .....	128
2.2.2. Атаки и угрозы безопасности .....	131
2.2.3. Классификация методов шифрования .....	138
2.2.4. Симметричное/асимметричное шифрование .....	140
2.2.5. Поточное/блочное шифрование .....	141
2.2.6. Практическая стойкость шифров .....	142
2.3. Симметричная криптография .....	144
2.3.1. Шифры простой замены .....	147
2.3.2. Аффинная система подстановок Цезаря .....	149
2.3.3. Криптосистема Хилла .....	151
2.3.4. Шифры перестановок .....	156
2.3.5. Шифры сложной замены. Шифр Вижинера .....	158
2.3.6. Шифры гаммирования и атаки на них .....	163
2.3.7. Методы генерации псевдослучайных последовательностей чисел .....	165
2.3.8. Стойкость линейных регистров сдвига .....	175
2.3.9. Поточные и блочные шифры .....	176
2.3.10. Поточные шифры .....	176
2.3.11. Нелинейные поточные шифры .....	180
2.3.12. Блочное шифрование .....	182
2.3.13. Обратимые операции в блочном шифровании .....	185
2.3.14. Необратимые операции в блочном шифровании .....	187
2.3.15. Сети .....	189
2.3.16. Практика блочного шифрования .....	193
2.3.17. Аппаратное шифрование DES. DES: структура .....	193
2.3.18. Анализ алгоритма DES .....	200
2.3.19. Комбинирование блочных алгоритмов .....	201
2.3.20. Структура алгоритма шифрования IDEA .....	204
2.3.21. Анализ алгоритма шифрования IDEA .....	208
2.3.22. Структура алгоритма ГОСТ 28147-89 .....	209
2.3.23. Основы криптоанализа симметричных шифров .....	212
2.3.24. Криптоатаки непосредственно на алгоритмы .....	212
2.3.25. Криптоанализ шифров сдвига (подстановки) .....	217
2.3.26. Статистические атаки .....	217
2.3.27. Криптоанализ аффинного шифра .....	218
2.3.28. Биграммный шифр Плейфейра .....	221
2.3.29. Криптоанализ шифра Вижинера .....	223
2.3.30. Криптоанализ шифров Хилла .....	224
2.3.31. Шифры перестановки .....	226
2.3.32. Общие сведения и классификация хеш-функций .....	227

2.4. Асимметричные криптосистемы .....	229
2.4.1. Основные положения криптосистем с открытым ключом .....	229
2.4.2. Криптосистема шифрования данных RSA .....	234
2.4.3. Безопасность и быстродействие криптосистемы RSA .....	239
2.4.4. Схема шифрования Полига — Хеллмана .....	241
2.4.5. Схема шифрования Эль Гамала .....	241
2.4.6. Комбинированный метод шифрования .....	244
2.4.7. Протоколы электронной цифровой подписи .....	246
<b>Глава 3. МЕТОДЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ</b> <b>ПОЛЬЗОВАТЕЛЯ.....</b>	<b>249</b>
3.1. Идентификации, аутентификация и авторизация .....	249
<b>Глава 4. МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ И УПРАВЛЕНИЯ</b> <b>ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.....</b>	<b>267</b>
4.1. Методы моделирования систем защиты информации .....	267
4.1.1. Математическое моделирование систем защиты информации .....	270
4.1.2. Моделирование как технология решения задач в области разработки и эксплуатации систем защиты автоматизированных информационных систем .....	275
4.1.3. Характеристика задач и методов моделирования систем защиты информации .....	276
4.1.4. Типовые математические схемы и методы моделей СЗИ .....	282
4.1.5. Виды моделей процессов в системах обработки и защиты информации .....	304
4.1.6. Моделирование вероятностных параметров в случайных процессах .....	311
4.1.7. Вероятностные оценки статистической надежности каналов связи .....	312
4.1.8. Вероятностные оценки надежности защиты системы от угроз информационной безопасности .....	313
4.1.9. Вероятностные оценки в моделях риска .....	314
4.1.10. Методы имитационного моделирования .....	316
4.1.11. Алгоритмы имитационного моделирования сценариев развития сетевых атак и процессов противодействия им .....	327
4.1.12. Имитационная дискретно-событийная модель сетевой атаки .....	328
4.1.13. Моделирование динамики случайного процесса противодействия сетевой атаке .....	333
4.1.14. Результаты имитационного моделирования процессов атаки и защиты .....	340
4.2. Система управления информационной безопасностью .....	346
4.2.1. Необходимость управления обеспечением информационной безопасности организации .....	346
4.2.2. Деятельность по обеспечению ИБ организации как процесс .....	347
4.2.3. Определение управления ИБ организации .....	352

4.2.4. Управление ИБ информационно-телекоммуникационных технологий организации .....	356
4.2.5. Система управления ИБ организации .....	360
4.2.6. Область действия СУИБ .....	363
4.2.7. Документальное обеспечение СУИБ .....	365
4.2.8. Политика СУИБ .....	371
4.2.9. Поддержка СУИБ со стороны руководства предприятия .....	373
4.2.10. Планирование СУИБ .....	375
4.2.11. Реализация СУИБ .....	378
4.2.12. Стратегии построения и внедрения СУИБ .....	381
4.2.13. Построение и внедрение СУИБ в целом .....	383
4.2.14. Построение и внедрении процессов СУИБ по отдельности .....	386
<b>Глава 5. МЕТОДОЛОГИЯ АНАЛИЗА ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ .....</b>	<b>389</b>
5.1. Большие системы и их свойства .....	389
5.2. Взаимосвязь эффективности и свойств системы защиты информации .....	391
5.3. Эффективность как свойство достижения цели .....	394
5.4. Методы оценки эффективности СЗИ .....	397
5.4.1. Оценка эффективности в условиях неопределенности .....	399
5.5. Показатели оценки эффективности и методы их определения .....	401
5.6. Способы вычисления сложных показателей эффективности .....	403
5.7. Оценка уровня эффективности СЗИ .....	405
<b>Глава 6. ПРОГНОЗИРОВАНИЕ РИСКОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РЕАЛИЗАЦИИ АТАК НА КОМПЬЮТЕРНУЮ СЕТЬ .....</b>	<b>409</b>
6.1. Методика управления рисками в целом .....	411
6.2. Методики оценки рисков .....	412
6.2.1. Модель качественной оценки .....	412
6.2.2. Количественная модель рисков .....	413
6.2.3. Определение вероятности события .....	414
6.2.4. Определение стоимости активов .....	414
6.3. Модель обобщенного стоимостного результата Миоры (GCC) .....	416
<b>Глава 7. ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ .....</b>	<b>418</b>
7.1. Основные методы определения затрат на информационную безопасность .....	418
7.2. Определение размера целесообразных затрат на обеспечение безопасности информации .....	423
<b>ПРИЛОЖЕНИЯ .....</b>	<b>426</b>
Приложение 1. Поточное шифрование .....	426
Приложение 2. Частота встречаемости букв русского алфавита .....	443

Приложение 3. Процедуры шифрования и дешифрования в криптосистеме RSA .....	444
Приложение 4. Последовательность выполнения процедур генерации и проверки ЭЦП на базе алгоритма RSA.....	451
Приложение 5. Вариант упрощенной методики расчета технико-экономической эффективности автоматизированной обработки информации в АСУ .....	455
Приложение 6. Материалы для разработки курсовой и дипломной работ .....	459
Приложение 7. Скриншот программы на VBA Excel, которая реализует этот алгоритм криптоанализа аффинного шифра.....	476
ЛИТЕРАТУРА .....	477