# Информационная и компьютерная безопасность

(Афанасьев В.Б., кфмн, доцент, ИППИ РАН)

1. Часть 1. Общая концепция безопасности информации в компьютерных системах.
2. Основные положения конституции РФ о защите и доступе к персональной информации.
3. Общая структура информационных систем. Организационные проблемы обеспечения безопасности.
4. Задачи обеспечения безопасности в подсистемах передачи информации.
5. Задачи обеспечения безопасности в подсистемах хранения и обработки информации.
6. Понятие о защите информации от природных и преднамеренных воздействий.
7. Принципы помехоустойчивого кодирования для защиты от случайных и преднамеренных воздействий.
8. Линейные коды, исправляющие ошибки: построение и основные свойства. Смежные классы линейных кодов.
9. Основные идеи декодирования: синдромное декодирование, декодирование по максимуму правдоподобия, декодирование в ограниченном шаре.
10. Порождающая и проверочная матрицы систематического линейного кода. Циклические коды, исправляющие ошибки: построение и основные свойства (Код Хемминга, коды БЧХ)..
11. Конечные поля Галуа: определения и свойства.
12. Коды Рида-Соломона: построение и основные свойства
13. Декодирование кодов Рида-Соломона: главная идея.
14. Итеративные и каскадные конструкции кодов, идея итеративного декодирования.
15. Многомерные кодовые конструкции для защиты от преднамеренных помех.
16. Скремблирование: применение и реализация. Последовательности максимальной длины.
17. Оценка вероятности отказа и ошибочного декодирования.
18. Часть 2. Псевдослучайные последовательности. Регистры с обратной связью. Комбинирование нескольких регистров с обратной связью: период и эквивалентная линейная сложность.
19. Защита линий связи от несанкционированного чтения информации. Методы определения кодовой конструкции и скремблера по наблюдениям в линии связи.
20. Задачи шифрования информации. Классические шифры: шифр Цезаря, шифр Вернама, одноразовый блокнот, матричные преобразования как шифры.
21. Частотная атака Касиски. Избыточность источника сообщений и расстояние единственности. Определение совершенной криптосистемы.
22. Стандарт шифрования DES – описание и применение, преобразование ключей.
23. Российский стандарт шифрования ГОСТ 28147-89 – описание и применение, преобразование ключей. Комбинирование блочных алгоритмов шифрования.
24. Односторонние функции. Система Диффи-Хелмана распределения секретных ключей. Элементы теории конечного поля.
25. Концепция секретной системы с открытым ключем. Система RSA – описание, свойства и основные атаки.

26. Система Эль Гамаля – описание, свойства и основные атаки.
27. Система МакЭлиса – описание, свойства и основные атаки.
28. Генерация простых чисел. Критерии простоты чисел.
29. Быстрая факторизация целых чисел. Быстрое вычисление дискретного логарифма.
30. Быстрое умножение и деление больших целых чисел.
31. Цифровая подпись и хеш-функции.
32. Аутентификация, сертификация, проблемы распределения ключей.
33. Разделение секрета – пороговые схемы (k,n), k<="" li="">
34. Методы криптографически стойкой генерации псевдослучайных чисел и последовательностей.

## Рекомендуемая литература


1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М. «Мир» 1986.
2. Габидулин Э.М., Афанасьев В.Б. Кодирование в радиоэлектронике. М. «Радио и связь» 1986.
3. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – М. «Мир» 1978.
4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2001.
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002.
6. Чмора А.Л. Современная прикладная криптография: Учебное пособие. – М.: Гелиос АРВ, 2001.


## Список дополнительной литературы


1. Menezes A.J., van Oorshot P.C., Vanstone S.A. Handbook of applied cryptography. – CRC Press, 1997. (Есть Интернет-версия: см., например, http://www.botan.mipt.ru/crypto/.).
2. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. – М.: ГТК 1992.
3. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 1996.
4. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.
5. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2003. – 212 с.
6. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие. – М. «Радио и связь» 2003.
7. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. –МЦНМО, 2003.
8. Введение в криптографию. – Сб. под ред. В.В.Ященко. МЦНМО, 1999.
9. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. – М. «Радио и связь», Веста, 1992.