МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_4_» _сен_____ 2022 г.

# КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Криптографические методы защиты информации» очной формы обучения

Курск 2022

УДК 004.056.55

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *А.Л. Марухленко*

Криптографические методы защиты информации: методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Криптографические методы защиты информации»/ Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2022 – 18 с.

Содержат информацию, необходимую студентам в процессе самостоятельной подготовки к занятиям по дисциплине.

Методические рекомендации соответствуют требованиям программы, утвержденной учебно-методическими объединениями по специальностям.

Предназначены для студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Криптографические методы защиты информации», очной формы обучения.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16
Усл.печ.л. 1,10 Уч.-изд.л. 1,00 Заказ 902 Тираж 100 экз. Бесплатно
Юго-Западный государственный университет
305040, г. Курск, ул. 50 лет Октября, 94

# ПРЕДИСЛОВИЕ

Методические рекомендации разработаны с целью оказания помощи студентам направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Криптографические методы защиты информации», очной форм обучения, при самостоятельной подготовке к занятиям по дисциплине.

Методические рекомендации разработаны в соответствии с Федеральными государственными образовательными стандартами высшего образования соответствующих направлений подготовки.

Предлагаемые методические рекомендации содержат краткое содержание рассматриваемых тем дисциплины и задания для самоконтроля в форме вопросов для собеседования.

Студентам предлагается список учебной литературы по дисциплине и перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для самостоятельной подготовки к занятиям.

## Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы обучающихся являются лекции и практические занятия.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на практическое занятие и указания на самостоятельную работу.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

Практические занятия предполагают свободный обмен мнениями по избранной тематике. Занятие начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, заслушиваются сообщения студентов. Обсуждение сообщения совмещается с рассмотрением намеченных вопросов. Сообщения, предполагающие анализ публикаций по отдельным вопросам семинара, заслушиваются обычно в середине занятия. Поощряется выдвижение и обсуждение альтернативных мнений. В заключительном слове преподаватель подводит итоги обсуждения и объявляет баллы выступавшим студентам. В целях контроля подготовленности студентов и привития им навыков краткого письменного изложения своих мыслей преподаватель в ходе практических занятий может осуществлять текущий контроль знаний в виде тестовых заданий.

При подготовке к занятию студенты имеют возможность воспользоваться консультациями преподавателя. Кроме указанных тем, студенты вправе, по согласованию с преподавателем, избирать и другие интересующие их темы.

Качество учебной работы студентов преподаватель оценивает в конце занятия.

При освоении данного курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой.

В процессе *подготовки к экзамену* студенту следует руководствоваться следующими рекомендациями:

- необходимо стремиться к пониманию всего материала, чтобы еще до экзамена не оставалось непонятных вопросов;
- необходимо строго следить за точностью своих выражений и правильностью употребляемых терминов;
- не следует опасаться дополнительных вопросов – чаще всего преподаватель использует их как один из способов помочь студенту или сэкономить время;
- прежде чем отвечать на вопрос, необходимо сначала правильно его понять.

## Содержание дисциплины, структурированное по темам (разделам)

Таблица 1 – Содержание дисциплины, структурированное по темам (разделам)

| № п/п | Раздел (тема) дисциплины | Содержание |
|---|---|---|
| 1 | 2 | 3 |
| 1 | Введение в криптологию. | Задачи и программа курса. Введение в криптологию. Основные термины и определения. История развития науки. Криптография и криптоанализ. Исторические шифры. |
| 2 | Классификация криптоалгоритмов. | Классификация криптоалгоритмов. Классификация систем шифрования. Симметричное и асимметричное шифрование, достоинства и недостатки систем шифрования относительно друг друга. |
| 3 | Симметричные криптоалгоритмы. | Симметричные криптоалгоритмы. Основы симметричного шифрования. Блочные и поточные системы шифрования. Достоинства и недостатки |

| № п/п | Раздел (тема) дисциплины | Содержание |
|---|---|---|
| | | симметричного шифрования. |
| 4 | Потоковые шифраторы. | Современные поточные шифры. Регистр сдвига с линейной обратной связью. Ассоциированный многочлен.<br>Поточные шифры. Комбинирование РСЛОС. Наиболее распространенные поточные шифры. |
| 5 | Блочные криптоалгоритмы. | Блочные криптоалгоритмы. Блочное шифрование. Режимы блочного шифрования. Обзор наиболее распространенных блочных шифров. |
| 6 | Сеть Фейштеля. | Алгоритмы многократного кодирования. Раунды шифрования. Сеть Фейштеля. Шифр DES. |
| 7 | Ассиметричные криптоалгоритмы. | Ассиметричные криптоалгоритмы. Математические основы шифрования с открытым ключом. Открытый ключ. Секретный ключ. Системы распределения ключей. Достоинства и недостатки систем с открытым ключом. |
| 8 | Системы электронной цифровой подписи. | Хэш функции. Свойства криптографических хэш функций.<br>Схемы цифровой подписи. Схема подписи с приложением.<br>Схема с цифровой подписью с восстановлением сообщения. |
| 9 | Алгоритмы обмена ключами. Разделение секрета. | Система управления симметричными ключами с предварительной частичной установкой. Система управления симметричными ключами без предварительной частичной установки. Схема Диффи-Хеллмана. Схема Шамира. Протокол Диффи-Хеллмана распределения ключей с тремя и более участниками. Система управления ассиметричными ключами. Цифровые сертификаты. Центры сертификации. Депонирование ключей. Encrypted File System |

| № п/п | Раздел (тема) дисциплины | Содержание |
|---|---|---|
| | | (EFS). Схема Шамира разделения секрета. |
| 10 | Применение программных симметричных систем шифрования. | Применение программных криптосистем шифрования. Программная реализация симметричные системы шифрования. Обзор основных программных продуктов на базе симметричных систем шифрования. |
| 11 | Применение программных асимметричных систем шифрования. | Программная реализация асимметричные системы шифрования. Обзор основных программных продуктов на базе асимметричных систем шифрования. Программный продукт PGP. |
| 12 | Стеганография. Основные понятия. | Стеганография. Тайнопись. Основные понятия. Классическая стеганография. Практическое использование. Обзор основных методов использования классической стеганографии. |
| 13 | Компьютерная стеганография. | Компьютерная стеганография. Использование избыточности цифровой информации изображений, звука, видео. Использование компьютерных форматов данных. Применение компьютерной стеганографии. |
| 14 | Криптоанализ и криптостойкость. Основные методы криптоанализа. | Криптоанализ и криптостойкость. Основные методы криптоанализа. Оценка предельных мощностей взлома. Понятие стойкости шифров. Линейный криптоанализ. Дифференциальный криптоанализ. |
| 15 | Анализ безопасности криптографических протоколов. | Безопасность криптографических протоколов. Доказуемая стойкость. Теоретико-информационные оценки стойкости криптосистем. |
| 16 | Способы применения криптосистем для решения специальных | Обзор способов применения криптосистем для решения специальных задач. Аутентификация. Удаленная идентификация пользователей. Контроль целостности сообщений. Невозможность |

| № п/п | Раздел (тема) дисциплины | Содержание |
|---|---|---|
| | задач. | отказа от авторства. |

## Задания для самоконтроля по темам курса

Тема 1. Введение в криптологию.

1. Назовите основные этапы истории развития криптологии как науки.
2. Каковы основные задачи криптологии как науки.
3. Назовите основные термины используемые в криптографии.
4. Исторические сведения о системах и способах составления шифрованных писем.
5. Как были устроены первые криптосистемы.
6. Что такое криптоанализ.
7. Чем криптография отличается от криптоанализа.
8. Какое понятие шире криптография или криптология.

Тема 2. Классификация криптоалгоритмов.

1. Классификация систем шифрования.
2. Симметричное шифрование, достоинства и недостатки.
3. Асимметричное шифрование, достоинства и недостатки
4. Сравнение систем шифрования относительно друг друга.
5. Как происходит использование открытого ключа.

Тема 3. Симметричные криптоалгоритмы.

1. Основы симметричного шифрования.
2. Блочные и поточные системы шифрования.
3. Преимущества использования блочных и поточных систем шифрования
4. Недостатки использования блочных и поточных систем шифрования.
5. Достоинства и недостатки симметричного шифрования.

Тема 4. Потоковые шифраторы.

1. Регистр сдвига с линейной обратной связью.
2. Ассоциированный многочлен.
3. Поточные шифры.
4. Современные поточные шифры.
5. Комбинирование РСЛОС.
6. Наиболее распространенные поточные шифры.
7. Приведите примеры поточных шифров

Тема 5. Блочные криптоалгоритмы.

1. Что такое блочные криптоалгоритмы.
2. Как устроено блочное шифрование.
3. Какие режимы блочного шифрования вы знаете.
4. Как устроены режимы шифрования ECB и CBC, в чем их отличие.
5. Какой режим шифрования блочных шифров более стойкий к атакам удаления и вставки.

6. Сделайте обзор наиболее распространенных блочных шифров.

Тема 6. Сеть Фейштеля.

1. Алгоритмы многократного кодирования.
2. Раунды шифрования.
3. Что такое сеть Фейштеля.
4. Как устроен шифр DES.
5. Сколько раундов шифрования в шифре DES.
6. Как устроен алгоритм разворачивания ключа в шифре DES.

Тема 7. Ассиметричные криптоалгоритмы.

1. Что такое ассиметричные криптоалгоритмы.
2. Математические основы шифрования с открытым ключом.
3. Как используется открытый ключ.
4. Что такое секретный ключ.
5. Системы распределения ключей.
6. Достоинства и недостатки систем с открытым ключом.

Тема 8. Системы электронной цифровой подписи.

1. Что такое хэш функции.
2. Что такое однонаправленные функции.
3. Свойства криптографических хэш функций.
4. Схемы цифровой подписи.

5. Схема подписи с приложением.

6. Схема с цифровой подписью с восстановлением сообщения.

Тема 9. Алгоритмы обмена ключами. Разделение секрета.

1. Система управления симметричными ключами с предварительной частичной установкой.

2. Система управления симметричными ключами без предварительной частичной установки.

3. Схема Диффи-Хеллмана.

4. Схема Шамира.

5. Протокол Диффи-Хеллмана распределения ключей с тремя и более участниками.

6. Система управления ассиметричными ключами.

7. Цифровые сертификаты.

8. Центры сертификации.

9. Депонирование ключей. Encrypted File System (EFS).

10. Схема Шамира разделения секрета.

Тема 10. Применение программных симметричных систем шифрования.

1. Применение программных криптосистем шифрования.

2. Программная реализация симметричные системы шифрования.

3. Обзор основных программных продуктов на базе симметричных систем шифрования.

4. Приведите примеры программных симметричных систем шифрования отечественного производства.

Тема 11. Применение программных асимметричных систем шифрования.

1. Программная реализация асимметричные системы шифрования.

2. Обзор основных программных продуктов на базе асимметричных систем шифрования.

3. Программный продукт PGP.

4. Приведите примеры программных асимметричных систем шифрования отечественного производства

Тема 12. Стеганография. Основные понятия.

1. Что такое стеганография.

2. Дайте основные понятия стеганографии.

3. Что такое тайнопись.

4. Классическая стеганография.

5. Практическое использование стеганографии.

6. Обзор основных методов использования классической стеганографии.

Тема 13. Компьютерная стеганография.

1. Компьютерная стеганография.

2. Использование избыточности цифровой информации изображений.

3. Использование избыточности цифрового звука.

4. Использование избыточности цифрового видео.

5. Использование компьютерных форматов данных.

6. Применение компьютерной стеганографии.

Тема 14. Криптоанализ и криптостойкость. Основные методы криптоанализа.

1. Что такое криптоанализ.

2. Что такое криптостойкость.

3. Основные методы криптоанализа.

4. Оценка предельных мощностей взлома.

5. Понятие стойкости шифров.

6. Линейный криптоанализ.

7. Дифференциальный криптоанализ.

Тема 15. Анализ безопасности криптографических протоколов.

1. На чем основана безопасность криптографических протоколов.

2. Что такое доказуемая стойкость.

3. На чем основана проблема факторизации целых чисел.

4. В чем заключается проблема дискретного логарифма.

5. Теоретико-информационные оценки стойкости криптосистем.

Тема 16. Способы применения криптосистем для решения специальных задач.

1. Обзор способов применения криптосистем для решения специальных задач.

2. Как используются криптосистемы для аутентификация.
3. Удаленная идентификация пользователей.
4. Контроль целостности сообщений.
5. Невозможность отказа от авторства.

## Учебная литература, необходимая для самостоятельной подготовки к занятиям

1. Майстренко, Н. В. Основы теории информации и криптографии: учебное электронное издание / Н. В. Майстренко, А. В. Майстренко. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. : табл., граф., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=570354 (дата обращения: 13.09.2021). – Библиогр. в кн. – ISBN 978-5-8265-1950-9. – Текст : электронный.

2. Усенко, О. А. Приложения теории информации и криптографии в радиотехнических системах : учебное пособие / О. А. Усенко ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 171 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500141 (дата обращения: 13.09.2021). – Библиогр. в кн. – ISBN 978-5-9275-2569-0. – Текст : электронный.

3. Фороузан, Б. А. Математика криптографии и теория шифрования : учебное пособие : [16+] / Б. А. Фороузан. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 511 с. : ил., схем. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428998 (дата

обращения: 13.09.2021). – Библиогр. в кн. – ISBN 978-5-9963-0242-0. – Текст : электронный.

4. Кнауб, Л. В. Теоретико-численные методы в криптографии : учебное пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2011. – 160 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=229582 (дата обращения: 13.09.2021). – ISBN 978-5-7638-2113-7. – Текст : электронный.

5. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. - 2-е изд., перераб. и доп. - М. : Радио и связь, 2001. - 376 с. : ил. - ISBN 5-256-01518-4 : 89.70 р. - Текст : непосредственный. Мельников, В. В. Защита информации в компьютерных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 1997. - 368 с. : ил. - Б. ц.

6. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. - М. : ДМК, 2000. - 448 с. : ил. - ISBN 5-89818-064-8 : Б. ц. - Текст : непосредственный.

7. Левин, М. PGP. Кодирование и шифрование информации с открытым ключом / М. Левин. - М. : Майор, 2001. - 176 с. - ISBN 5-901321-05-7 : 41.80 р. - Текст : непосредственный.

8. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. - М.

: КУДИЦ-ОБРАЗ, 2001. - 368 с. - ISBN 5-93378-021-9 : 165.60 р. - Текст : непосредственный.

а. Основы криптографии : учеб. пособие / А. П. Алферов [и др.]. - М. : Гелиос АРВ, 2001. - 480 с. : ил. - ISBN 5-85438-019-6 : 150.00 р. - Текст : непосредственный.

9. Галатенко, В. А. Основы информационной безопасности. Курс лекций : учебное пособие для студентов вузов / под ред. В. Б. Бетелина. - 2-е изд., испр. - М. : ИНТУИТ. РУ Интернет-университет Информационных Технологий, 2004. - 264 с. - (Основы информационных технологий). - ISBN 5-9556-0015-9 : 184.00 р. - Текст : непосредственный.

10. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко ; Институт проблем информационной безопасности МГУ. - М. : МЦНМО, 2003. - 328 с. - (Информационная безопасность : криптография). - ISBN 5-94057-103-4 : 75.00 р. - Текст : непосредственный.

11. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. - М. : МЦНМО, 2004. - 470 с. - ISBN 5-94057-117-4 : 85.00 р. - Текст : непосредственный.

## Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для самостоятельной подготовки к занятиям по дисциплине

1. http://biblioclub.ru - Электронно-библиотечная система «Университетская библиотека онлайн».
2. www.elibrary.ru/defaultx.asp - научная электронная библиотека.
3. www.edu.ru - федеральный портал «Российское образование».
4. www.consultant.ru - Официальный сайт компании «Консультант Плюс».
5. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/.
6. Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/