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_» ___04_____ 2022 г.

ВВЕДЕНИЕ В КРИПТОГРАФИЮ

Методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Введение в криптографию» очной формы обучения

Курск 2022

УДК 004.056.55

Составитель М.А. Ефремов

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

Введение в криптографию: методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Введение в криптографию»/ Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2022. - 14 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 «Введение в криптографию», очной формы обучения.

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 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 «Введение в криптографию», 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.

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 зачету* студенту следует руководствоваться следующими рекомендациями:

- необходимо стремиться к пониманию всего материала, чтобы еще до зачета 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	История криптографии. Первые криптосистемы.	Задачи и программа курса. История криптографии. Первые криптосистемы. Исторические сведения о системах и способах составления шифрованных писем. Сцикалла. Шифр Цезаря. Квадрат Полибия.
2	Криптография как наука. Основные понятия и определения криптографии.	Понятие криптографии как науки. Основные понятия, определения и термины используемые в криптографии. Шифрование. Расшифровка. Шифротекст. Ключ. Криптосистема. Дешифрование сообщений. Криптоанализ. Криптостойкость.
3	Неопределенность сообщения. Совершенные и	Мера неопределенности сообщения. Априорная неопределенность Апостериорная условная неопределенность. Количество информации об

№ п/п	Раздел (тема) дисциплины	Содержание
	несовершенные шифры.	исходном тексте. Условие абсолютной стойкости шифров. Принцип Керкгоффса построения надежных шифров. Функция ненадежности ключа. Расстояние единственности шифра.
4	Источники дискретных сообщений и их вероятностные модели.	Источники дискретных сообщений и их вероятностные модели. Функционал энтропии и его свойства. Определение условной энтропии. Определение удельной энтропии стационарной символьной последовательности. Удельная энтропия для произвольного источника дискретных сообщений.
5	Шенноновские модели криптосистем.	Количество информации по Шеннону и его свойства. Собственная информация о сообщении. Шенноновские модели криптосистем. Подстановка символов алфавита.
6	Классификация систем шифрования.	Классификация систем шифрования. Симметричное и асимметричное шифрование, достоинства и недостатки систем шифрования относительно друг друга.
7	Основы симметричного шифрования.	Основы симметричного шифрования. Блочное шифрование. Режимы блочного шифрования. Поточное шифрование.
8	Криптостойкость. Теоретико-информационные оценки стойкости симметричных криптосистем.	Понятие стойкости шифров. Криптостойкость. Доказуемая стойкость. Совершенные и несовершенные шифры. Теоретико-информационные оценки стойкости симметричных криптосистем.
9	Математические основы шифрования с открытым ключом.	Математические основы шифрования с открытым ключом. Открытый ключ. Секретный ключ. Системы распределения ключей. Сложность алгоритмов. Достоинства и недостатки систем с открытым ключом.

Задания для самоконтроля по темам курса

Тема 1. История криптографии. Первые криптосистемы.

1. Назовите основные этапы истории развития криптографии.
2. Исторические сведения о системах и способах составления шифрованных писем.
3. Как были устроены первые криптосистемы.
4. Что такое сциталла.
5. Как устроен шифр Цезаря.
6. Для чего служит квадрат Полибия.
7. Что такое открытый и закрытый текст.
8. Принципы организации криптографических систем.
9. Для чего используется шифрование и дешифровка.

Тема 2. Криптография как наука. Основные понятия и определения криптографии.

1. Понятие криптографии как науки.
2. Задачи и программа курса.
3. Назначение криптографических методов защиты информации.
4. Назовите основные понятия и определения используемые в криптографии.
5. Как происходит шифрование и расшифровка сообщений.
6. Что такое шифротекст.
7. Как используется криптографический ключ.

8. Как устроена криптосистема.
9. В чем суть дешифрования сообщений.
10. Что такое криптоанализ.

Тема 3. Неопределенность сообщения. Совершенные и несовершенные шифры.

1. Что такое мера неопределенности сообщения.
2. Дайте определение априорная неопределенность.
3. Дайте определение апостериорная условная неопределенность.
4. Количество информации об исходном тексте.
5. В чем заключается условие абсолютной стойкости шифров.
6. Принцип Керкгоффса построения надежных шифров.
7. Что такое функция ненадежности ключа.
8. Как определяется расстояние единственности шифра.

Тема 4. Источники дискретных сообщений и их вероятностные модели.

1. Источники дискретных сообщений и их вероятностные модели.
2. Функционал энтропии и его свойства.
3. Определение условной энтропии.
4. Определение удельной энтропии стационарной символьной последовательности.

5. Удельная энтропия для произвольного источника дискретных сообщений.

Тема 5. Шенноновские модели криптосистем.

1. Что такое количество информации по Шеннону
2. Назовите свойства информации.
3. Собственная информация о сообщении.
4. Шенноновские модели криптосистем.
5. Как осуществляется подстановка символов алфавита.

Тема 6. Классификация систем шифрования.

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 7. Основы симметричного шифрования.

1. Основы симметричного шифрования.
2. Блочное шифрование.
3. Как устроена сеть Фейстеля.
4. Режимы блочного шифрования.
5. Поточное шифрование.
6. Регистры сдвига.
7. Преимущества и недостатки использования блочных и поточных систем шифрования.

Тема 8. Криптостойкость. Теоретико-информационные оценки стойкости симметричных криптосистем.

1. Понятие стойкости шифров.
2. Что такое криптостойкость.
3. Доказуемая стойкость.
4. Совершенные и несовершенные шифры.
5. Теоретико-информационные оценки стойкости симметричных криптосистем.
6. Принципы организации стойких систем шифрования.

Тема 9. Математические основы шифрования с открытым ключом.

1. Математические основы построения систем с открытым ключом.
2. Что такое открытый ключ.
3. Как используется секретный ключ в асимметричных системах шифрования.
4. Системы распределения ключей.
5. В чем заключается сложность асимметричных алгоритмов.
6. Достоинства и недостатки систем шифрования с открытым ключом.

Учебная литература, необходимая для самостоятельной подготовки к занятиям

1. Применко, Э. А. Алгебраические основы криптографии [Текст] : учебное пособие / Э. А. Применко. - Москва : Либроком, 2013. - 288 с. - (Основы защиты информации). - ISBN 978-5-382-014 55-5 : 470.00 р.

2. Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В. Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2011. - 148 с. : ил., табл., схем. - ISBN 978-5-4332-0020-3 // Режим доступа - http://biblioclub.ru/

3. Романец, Ю. В. Защита информации в компьютерных системах и сетях [Текст] / 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.

4. Мельников, В. В. Защита информации в компьютерных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 1997. - 368 с. : ил. - Б. ц.

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

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

7. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / М. А. Иванов, И. Чугунков. - Москва : МИФИ, 2012. - 400 с. - ISBN 978-5-7262-1676-8 : Б. ц.

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

9. Галатенко, В. А. Основы информационной безопасности. Курс лекций [Текст] : 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.

10. Смарт, Н. Криптография [Текст] / перевод с англ. С. А. Кулешова, под ред. С. К. Ландо. - М. : Техносфера, 2006. - 528 с. - (Мир программирования). - ISBN 5-94836-043-1 : 217.26 р.

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

12. Логачев, О. А. Булевы функции в теории кодирования и криптологии [Текст] / О. А. Логачев, А. А. Сальников, В. В.

Ященко. - М. : МЦНМО, 2004. - 470 с. - ISBN 5-94057-117-4 : 85.00 р.

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/