МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ Федеральное государственное автономное образовательное учреждение высшего образования «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по организации самостоятельной работы
по дисциплине

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	Бакалавр
Форма обучения	Очная
Учебный план	2020 г.

Пятигорск 2020 г.

Методические рекомендации предназначены для студентов направления10.03.01 «Информационная безопасность» очной формы обучения и содержат материалы и задания для самостоятельной работы по дисциплине «Криптографические методы защиты информации».

Составитель: Битюцкая Н.И.

Методические рекомендации рассмотрены и утверждены на заседании кафедры Информационной безопасности, систем и технологий. Протокол № 2 от «04» сентября 2020 г.

1. Методические рекомендации для студентов по изучению дисциплины

1.1. Использование материала учебно-методического комплекса дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций с лабораторными занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

Технологическая карта самостоятельной работы студента

Код реализуемой компетенции	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОПК-2, ОПК-4, ПК-1	Самостоятельное изучение литературы	конспект	Собеседование	4,86	0,54	5,4
	Подготовка к лабораторным работам	отчет	Отчет письменный	7,29	0,81	8,1
			Итого 5 семестр	**12,15**	**1,35**	**13,5**
ОПК-2, ОПК-4, ПК-1	Самостоятельное изучение литературы	конспект	Собеседование	9,72	1,08	10,8
	Подготовка к лабораторным работам	отчет	Отчет письменный, собеседование	6,48	0,72	7,2
	Подготовка к экзамену	экзамен	экзамен	24,3	2,7	27,0
			Итого 6 семестр	**40,5**	**4,5**	**45**
			Итого	**52,65**	**5,85**	**58,5**

1.2. Работа с литературой

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая	Интернет-ресурсы
1	Криптостойкость, иммитостойкость, гаммирование.	1	1-2	1	1-6

2	Открытый и закрытый шифры, сеансовые ключи.	1	1-2	1	1-6
3	Виды генераторов псевдослучайных последовательностей.	1	1-2	1	1-6
4	Подстановки Плэйфера, Виженера.	1	1-2	1	1-6
5	Задача Диффи-Хеллмана и задача дискретного логарифмирования.	1	1-2	1	1-6
6	Способ вероятностного шифрования.	1	1-2	1	1-6
7	Протокол идентификации Шнорра.	1	1-2	1	1-6

2. Типовые контрольные задания для проведения промежуточной аттестации

Вопросы к экзамену (6 семестр)

Базовый уровень

Вопросы (задача, задание) для проверки уровня обученности.

Знать

1. Основные понятия в области криптографии.
2. Классификация классических шифров: шифры замены и перестановки, поточные и блочные шифры, моноалфавитные и многоалфавитные шифры.
3. Классические шифры с симметричным ключом. Шифры замены: аддитивные, мультипликативные, аффинные, автоключевой, Виженера, Плейфера, Хилла, роторный, одноразового блокнота.
4. Классические шифры перестановки: бесключевой шифр, ключевые шифры и шифры с двойной перестановкой.
5. Современные блочные шифры с симметричным ключом. Основные компоненты современного блочного шифра. Шифры Фейстеля и не-Фейстеля.
6. Современные поточные шифры с симметричным ключом. Синхронные и несинхронные шифры потока. Преимущества и проблемы современных шифров потока.
7. Современный стандарт шифрования (DES). Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов.
8. Усовершенствованный стандарт шифрования (AES). Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES.
9. Российский стандарт ГОСТ 2847-89, особенности, принципы

построения, методы шифрования.

10. Алгоритмы шифрования с открытыми ключами. Концепция криптографии с открытым ключом. Криптосистема RSA. Стойкость RSA.

11. Алгоритмы генерации простых чисел. Проверка чисел на простоту. Способы проверки на простое число. Решето Эратосфена. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.

12. Сложность криптографических алгоритмов. Понятие сложности алгоритма. Линейная, полиномиальная и неполиномиальная сложность. Класс NP – полных задач.

13. Криптосистемы с открытым ключом. Криптосистема Рабина. Криптосистема Эль-Гамаля. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистемах Рабина и Эль-Гамаля. Безопасность данных криптосистем.

14. Аутентификация данных. Электронная цифровая подпись. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.

15. Алгоритмы ЭЦП: RSA, Эль-Гамаля, ФиатаШамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ванАнтверпена.

16. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.9.

17. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля. Алгоритм формирования схемы Эль-Гамаля. Алгоритм формирования цифровой подписи. Проверка подписи.

18. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия".

19. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации.

Уметь

1. Шифровать тексты с помощью классических шифров.
2. Шифровать двоичные последовательности с помощью современных шифров.
3. Проверять требования к криптосистемам.
4. Использовать перестановки, подстановки и их комбинации.
5. Реализовывать криптографические методы.

Владеть

1. Методами управления ключами.

2. Методами генерации, накопления и распределения ключей.
3. Основами знаний по порядку разработки схемы ЭЦП Рабина.
4. Основами знаний по порядку разработки схемы ЭЦП Диффи - Хэллмана.
5. Основами знаний по порядку разработки схемы ЭЦП Эль-Гамаля.

Повышенный уровень

Вопросы (задача, задание) для проверки уровня обученности.

Знать
1. Виды атак криптоанализа. Способы противодействия им.
2. Криптоанализ шифров замены.
3. Криптоанализ шифров перестановки.
4. Атаки на современные блочные шифры.
5. Криптоанализ современных шифров потока.
6. Двукратный и трехкратный DES. Криптоанализ шифра DES.
7. Анализ AES.
8. Виды атак на RSA.
9. Способы определения сложности алгоритмов.
10. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.
11. Криптосистемы на основе метода эллиптических кривых.
12. Безопасность криптосистемы с эллиптической кривой.
13. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа.
14. Способы отражения атак на криптографические протоколы.

Уметь
1. Отражать атаки на криптографические протоколы.
2. Выбирать правильно параметры для шифрования наиболее известными шифрами.
3. Оценивать криптостойкость алгоритма шифрования.

Владеть
1. Способами построения криптографических протоколов.
2. Способами отражения атак на криптографические протоколы.

3. Примерная тематика заданий для самостоятельной работы студентов

1) Свойство замкнутости операций кодирования и декодирования в замкнутом конечном пространстве.
2) Теорема Лагранжа и ее следствия.
3) Основные сведения о кольцах и полях.
4) Конечные поля неприводимых полиномов: полиномы над алгебраической структурой, определение неприводимого полинома, конечные поля, построенные с помощью полиноминального базиса.

5) Генерирование равномерно распределенных случайных чисел: линейный конгруэнтный метод (выбор модуля, выбор множителя, потенциал, другие методы).
6) Мультипликативный конгруэнтный метод.
7) Обобщение линейного и конгруэнтного методов на смешанный конгруэнтный метод.
8) Статистические критерии проверки случайных наблюдений: эмпирические, теоретические критерии.
9) Алгоритм возведения в степень по модулю m, его приложения в виде функции усложнения, рандомизация: рандомизация с одной ошибкой.
10) Метод рандомизированного заполнения сообщений.

4. Рекомендуемая литература

4.1 Основная литература:

1. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков; под ред. М.А. Иванова; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». - М.: МИФИ, 2012. - 400 с.: табл., схем. - ISBN 978-5-7262-1676-8; То же [Электронный ресурс]. - URL: //biblioclub.ru /index.php? page=book&id=231673.

4.2 Дополнительная литература:

1. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с.: ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5;То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php? page= book&id=429092.

2. Жуков А.Е. Системы блочного шифрования [Электронный ресурс]: учебное пособие по курсу «Криптографические методы защиты информации»/ Жуков А.Е.— Электрон. текстовые данные.— М.: Московский государственный технический университет имени Н.Э. Баумана, 2013.— 80 с.— Режим доступа: http://www. iprbookshop.ru/31633.— ЭБС «IPRbooks».

4.3 Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Криптографические методы защиты информации» для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения. Пятигорск, 2017.

4.4 Интернет-ресурсы:

1. http://www.intuit.ru – сайт дистанционного образования в области информационных технологий

2. http://www.iqlib.ru - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;

3. http://www.biblioclub.ru - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.

4. http://window.edu.ru – образовательные ресурсы ведущих вузов.

5. http://cryptography.ru – сайт «Математическая криптография».

6. http://algolist.manual.ru - сайт, посвященный алгоритмам и методам.

4.5 Программное обеспечение:

1. Microsoft Visual Studio 2012 / 2015.

5. Материально-техническое обеспечение дисциплины:

Минимально необходимый для реализации ООП бакалавриата перечень материально-технического обеспечения включает в себя лекционную мультимедиа аудиторию, компьютерный класс с выходом в сеть Internet и локальную вычислительную сеть.