Приложение 3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ

Декан _____ Буднев Н.М.

«17» апреля 2024 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.О.10 Методы и средства криптографической защиты информации**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №42 от «15» апреля 2024 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8 от «8» апреля 2024 г.

И.О. зав. кафедрой _____ Колесник С.Н.

Иркутск 2024 г.

Содержание

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Учебная дисциплина «Методы и средства криптографической защиты информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует фундаментализации образования, формирование знаний в области криптографии и развитие навыков применения средств криптографической защиты информации.

Цели:

- формирование фундаментальных знаний в области криптографии и способностей, необходимых для решения различных задач шифрования и дешифрирования сообщений;
- овладение современным аппаратом и методами криптографии для защиты информации от угроз раскрытия и нарушения целостности;
- формирование личности обучающегося, развитие его интеллекта и способностей к освоению основополагающих способов защиты информации на базе криптографических методов.
– формирование практических навыков при работе со средствами криптографической защиты информации;
- формирование у будущих специалистов основных понятий и концепций криптографии и криптоанализа, а также в их применении к анализу конкретных систем шифрования.

Задачи:

- изучение математических методов, применяемых для проектирования шифров и анализа криптостойкости алгоритмов;
- изучение криптографических методов защиты информации, передаваемой по каналам связи и обрабатываемой средствами вычислительной техники;
- овладение современным математическим аппаратом для дальнейшего использования при решении задач криптоанализа, аргументации стойкости и синтеза криптосистем;
- изучение концепций построения симметричных и асиммеричных криптографических алгоритмов;
- изучение особенностей применения средств криптографической защиты информации.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина Б1.О.10 Методы и средства криптографической защиты информации относится к обязательной части программы. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами*:*

_Дискретная математика_____

_Математический анализ_____

_Линейная алгебра и аналитическая геометрия_____

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

Программно-аппаратные средства защиты информации

Защита и обработка конфиденциальных документов_____

При подготовке специалистов по разработке и эксплуатации современных средств криптографической защиты информации, необходимо уделять особое внимание изучению современного математического аппарата и методов криптографии.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **10.03.01 Информационная безопасность**.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ИДК$_{ОПК9.1.}$ Использует для решения задач профессиональной деятельности средства криптографической защиты информации	Знать: - методы криптографической защиты информации, - основные характеристики современных криптосистем; - средства криптографической защиты информации; Уметь: - выбирать средства криптографической защиты информации для решения задач профессиональной деятельности; - выбирать средства технической защиты информации для решения задач профессиональной деятельности. Владеть: - методами применения теоретических знаний и практических навыков при оценке характеристик криптографических систем; - навыками применения типовых криптографических и технических средств защиты информации; - навыками использования электронной подписи.
	ИДК$_{ОПК9.2.}$ Использует для решения задач профессиональной деятельности средства технической защиты информации	

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет __4____ зачетных единицы, ____144_____часов,
в том числе _____ зачетных единиц, _____часов на экзамен
Из них ____ часов – практическая подготовка

Форма промежуточной аттестации: __Зачет_____
(экзамен, зачет, зачет с оценкой)

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Раздел 1. Основы криптографии								
2	Тема 1.1. Основные понятия и задачи криптографии	6	7		2	4		4	Устный опрос, письменный опрос на практических занятиях
3	Тема 1.2. Классификация шифров, их основные типы и свойства	6	10		4	4		4	Защита лабораторной

									работы
4	Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.	6	7		2	4		4	Защита лабораторной работы
5	Раздел 2. Криптографическая защита информации на основе симметричных криптосистем	6							
6	Тема 2.1. Одноключевые методы шифрования, элементы теории чисел.	6	7		2	4		4	Устный опрос, письменный опрос на практических занятиях
7	Тема 2.2. Блочные и потоковые шифры.	6	7		2	4		5	Защита лабораторной работы
8	Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.	6	10		4	4		5	Защита лабораторной работы
9	Раздел 3. Криптографическая защита информации на основе асимметричных криптосистем								
10	Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.	6	9		4	4		5	Устный опрос, письменный опрос на практических занятиях
11	Тема 3.2. Современные технологии шифрования.	6	7		2	4		5	Защита лабораторной работы
12	Тема 3.3. Криптоанализ шифров.	6	8		2	4		5	Защита лабораторной работы
13	Раздел 4. Криптографические методы защиты электронного документооборота								
14	Тема 4.1. Хеш-функции и их	6	7		2	4		4	Устный опрос,

	криптографические приложения								письменный опрос на практических занятиях
15	Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты.	6	10		4	4		4	Защита лабораторной работы
16	Тема 4.3. Средства криптографической защиты информации.	6	8		2	4		4	Защита лабораторной работы

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
6	Тема 1.1. Основные понятия и задачи криптографии	Работа с учебником, справочной литературой, первоисточниками, конспектом	1-ая неделя	4	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
6	Тема 1.2. Классификация шифров, их основные типы и свойства	Работа с учебником, справочной литературой, первоисточниками, конспектом	2-ая неделя	4	Защита лабораторной работы	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
6	Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.	Работа с учебником, справочной литературой, первоисточниками, конспектом	3-ая неделя	4	Защита лабораторной работы	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
6	Тема 2.1. Одноключевые алгоритмы шифрования, элементы теории чисел.	Работа с учебником, справочной литературой, первоисточниками, конспектом	5-ая неделя	4	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
6	Тема 2.2. Блочные и потоковые шифры.	Работа с учебником, справочной литературой, первоисточниками, конспектом	6-ая неделя	5	Защита лабораторной работы	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
6	Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.	Работа с учебником, справочной литературой, первоисточниками, конспектом	7-ая неделя	5	Защита лабораторной работы	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
6	Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.	Работа с учебником, справочной литературой, первоисточниками, конспектом	9-ая неделя	5	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
6	Тема 3.2. Современные технологии шифрования.	Работа с учебником, справочной литературой, первоисточниками, конспектом	10-ая неделя	5	Защита лабораторной работы	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
6	Тема 3.3. Криптоанализ шифров.	Работа с учебником, справочной литературой, первоисточниками, конспектом	11-ая неделя	5	Защита лабораторной работы	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
6	Тема 4.1. Хеш-функции и их криптографические приложения	Работа с учебником, справочной литературой, первоисточниками, конспектом	13-ая неделя	4	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
6	Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты.	Работа с учебником, справочной литературой, первоисточниками, конспектом	14-ая неделя	4	Защита лабораторной работы	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
6	Тема 4.3. Средства криптографической защиты информации.	Работа с учебником, справочной литературой, первоисточниками, конспектом	20-ая неделя	4	Защита лабораторной работы	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
Общий объем самостоятельной работы по дисциплине (час)				**53**		

4.3. Содержание учебного материала

Раздел 1. Основы криптографии

Тема 1.1. Основные понятия и задачи криптографии.

Исторический обзор. Основные задачи и понятия криптографии. Требования к криптосистемам.

Тема 1.2. Классификация шифров, их основные типы и свойства.

Шифры перестановки. Шифры замены.

Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.

Принципы построения криптосистем К.Шеннона. Вопросы имитозащиты. Помехоустойчивость шифров. Оценка криптостойкости различных алгоритмов: простых и многомерных подстановок, гаммирования по ключу.

Раздел 2. Криптографическая защита информации на основе симметричных криптосистем

Тема 2.1. Одноключевые алгоритмы шифрования, элементы теории чисел.

Принципы построения криптографических алгоритмов. Режимы выполнения симметричных криптоалгоритмов. Генераторы псевдослучайных последовательностей и их схемная реализация. Элементы алгоритмической теории чисел.

Тема 2.2. Блочные и потоковые шифры.

Основы построения блочных шифров. Потоковые шифры. Комбинированное шифрование. Режимы шифрования. Сеть Фейстеля.

Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.

Алгоритм DES. Усиления DES. Алгоритм IDEA. Алгоритм AES. Алгоритм ГОСТ 28147-89. Российский алгоритм криптографического преобразования. Национальный стандарт РФ по ГОСТ 34.13-2018.

Раздел 3. Криптографическая защита информации на основе симметричных криптосистем

Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.

Требования к асимметричным криптосистемам. Обмен Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля.

Тема 3.2. Современные технологии шифрования.

Криптосистемы на эллиптических кривых. Математические основы. Выбор параметров кривой.

Тема 3.3. Криптоанализ шифров.

Подходы к анализу криптографических алгоритмов. Метод перебора. Частотный анализ. Корреляционный метод анализа поточных шифров. Линейный и дифференциальный методы анализа блочных шифров.

Раздел 4. Криптографические методы защиты электронного документооборота.

Тема 4.1. Хеш-функции и их криптографические приложения.

Целостность данных и аутентификация источника данных. Общие сведения о хеш-функциях. Требования к хэш-функциям. Понятие о стойкости хеш-функции. Ключевые и бесключевые хеш-функции. Российский стандарт 2018.

Тема 4.2. Электронная подпись, зарубежные и отечественные стандарты.

Задачи и назначения электронной подписи. Классификация электронных подписей. Примеры цифровых подписей на основе алгоритмов RSA, Эль-Гамаля. Стандарты подписи ГОСТ 3410 и DSS. Инфраструктура открытых ключей. Правовое обеспечение электронной подписи.

Тема 4.3. Средства криптографической защиты информации.

СКЗИ серии Криптон. СКЗИ КриптоПро CSP. Скремблеры.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	Раздел 1. Основы криптографии Тема 1.1. Основные понятия и задачи криптографии	ПЗ.1. Математические основы криптографии. ПЗ.2. Математические основы шифров.	4		Устный опрос, письменный опрос на практических занятиях	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2.}$
2	Тема 1.2. Классификация шифров, их основные типы и свойства	Лр.1. Шифры замены.	4		Защита лабораторной работы	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
3	Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.	Лр. 2. Шифры перестановки	4		Защита лабораторной работы	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
4	Раздел 2. Криптографическая защита информации на основе симметричных криптосистем Тема 2.1. Одноключевые методы шифрования, элементы теории чисел.	ПЗ 3. Элементы теории чисел. ПЗ 4. Математические основы симметричных шифров.	4		Устный опрос, письменный опрос на практических занятиях	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
5	Тема 2.2. Блочные и поточные шифры.	Лр. 3. Шифры гаммирования.	4		Защита лабораторной работы	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.22}$
6	Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.	Лр. 4. Комбинированные шифры.	4		Защита лабораторной работы	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
7	Раздел 3. Криптографическ	ПЗ 5. Односторонние	4		Устный опрос,	ОПК-9 ИДК$_{ОПК9.1.}$

	ая защита информации на основе асимметричных криптосистем Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.	функции. ПЗ 6. Поля Галуа.			письменный опрос на практических занятиях	ИДК$_{ОПК9.2}$
8	Тема 3.2. Современные технологии шифрования.	Лр.5. Асимметричные шифры.	4		Защита лабораторной работы	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
9	Тема 3.3. Криптоанализ шифров.	Лр. 6. Электронные подписи.	4		Защита лабораторной работы	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
10	Раздел 4. Криптографические методы защиты электронного документооборота. Тема 4.1. Хеш-функции и их криптографические приложения	ПЗ 7. Хэш-функции. ПЗ 8. Схемы электронных подписей на основе криптографических систем.	4		Устный опрос, письменный опрос на практических занятиях	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
11	Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты.	Лр. 7. Установка, настройка и эксплуатация средств электронной подписи	4		Защита лабораторной работы	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
12	Тема 4.3. Средства криптографической защиты информации.	Лр. 8. Установка, настройка и эксплуатация СКЗИ КриптоПро CSP	4		Защита лабораторной работы	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	**2**	**3**	**4**	**5**
1	Раздел 1. Основы криптографии Тема 1.1. Основные понятия и задачи	Повторение и углубленное изучение	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$

	криптографии	учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов		
2	Тема 1.2. Классификация шифров, их основные типы и свойства	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
3	Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
4	Раздел 2. Криптографическая защита информации на основе симметричных криптосистем Тема 2.1. Одноключевые методы шифрования, элементы теории чисел.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
5	Тема 2.2. Блочные и поточные шифры.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$

		конспекта лекций, литературы, Интернет - ресурсов		
6	Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
7	Раздел 3. Криптографическая защита информации на основе асимметричных криптосистем Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
8	Тема 3.2. Современные технологии шифрования.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
9	Тема 3.3. Криптоанализ шифров.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет -	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$

		ресурсов		
10	Раздел 4. Криптографические методы защиты электронного документооборота. Тема 4.1. Хеш-функции и их криптографические приложения	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
11	Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
12	Тема 4.3. Средства криптографической защиты информации.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-9	ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя (научного руководителя (консультанта)), в ходе, которой студент активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи. В процессе проведения самостоятельной работы формируется компетенция ОПК-9.

На самостоятельную работу выносятся следующие вопросы по темам дисциплины:

Тема 1.1. Основные понятия и задачи криптографии (1 ч). Проработка лекционного материала и материала практических занятий (1 ч).

Тема 1.2. Классификация шифров, их основные типы и свойства (2 ч). Проработка лекционного материала (2 ч).

Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров (1 ч). Проработка лекционного материала (1 ч).

Тема 2.1. Одноключевые методы шифрования, элементы теории чисел (1 ч). Проработка лекционного материала и материала практических занятий (1 ч).

Тема 2.2. Блочные и поточные шифры (1 ч). Проработка лекционного материала (1 ч).

Тема 2.3. Алгоритмы и стандарты симметричных криптосистем. (2 ч). Проработка лекционного материала (2 ч).

Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы (1 ч). Проработка лекционного материала и материала практических занятий (1 ч).

Тема 3.2. Современные технологии шифрования (1 ч). Проработка лекционного материала (1 ч).

Тема 3.3. Криптоанализ шифров (2 ч). Проработка лекционного материала (2 ч).

Тема 4.1. Хеш-функции и их криптографические приложения (1 ч). Проработка лекционного материала и материала практических занятий (1 ч).

Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты (2 ч). Проработка лекционного материала и материала практических занятий (2 ч).

Тема 4.3. Средства криптографической защиты информации (2 ч). Проработка лекционного материала (2 ч).

4.5. Примерная тематика курсовых работ

Выполнение курсовых работ не предусмотрено учебным планом

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. Ермакова А. Ю. Криптографические методы защиты информации: Учебно-методическое пособие**.** МИРЭА - Российский технологический университет**,** 2021**,** - 172 с. https://e.lanbook.com/book/176563

2. Овчинников А. А. Криптографические методы защиты информации: учебное пособие. Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2021, - 133 с. https://e.lanbook.com/book/216491

3. Бутакова Н. Г., Федоров Н. В. Криптографические методы и средства защиты информации: Учебное пособие. ИЦ Интермедия**,** 2020, - 380 с. https://e.lanbook.com/book/161347

4. Каширская Е.Н. Криптографический анализ и методы защиты информации: Учебное пособие. МИРЭА - Российский технологический университет, 2020, - 91 с.

б) базы данных, информационно-справочные и поисковые системы

1. Поисковые системы Google, Yandex.

2. Электронные ресурсы доступные по логину и паролю, предоставляемые Научной библиотекой ИГУ.

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Чтение лекций сопровождается демонстрацией информации (мультимедийный проектор, офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материалов).

6.2. Программное обеспечение:

1. Microsoft PowerPoint
2. Microsoft Windows.

6.3. Технические и электронные средства:

В ходе учебного процесса используются технические средства обучения и контроля знаний студентов (презентации, контролирующих программ, демонстрационных установок), использование которых предусмотрено методической концепцией преподавания

VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

На лекциях используются активные методы обучения (компьютерных симуляций, разбор конкретных ситуаций). Практические занятия 1, 2, 5, 6, 9, 10, 13, 14 проводятся в интерактивной форме.

Наименование тем занятий с указанием форм/ методов/ технологий обучения:

№ п/п	Тема занятия	Вид занятия	Форма / Методы//технологии дистанционного, интерактивного обучения	Количество часов
1	**2**	**3**	**4**	**5**
1	Математические основы криптографии.	Практическое занятие	Дисскуссия	2
2	Математические основы шифров.	Практическое занятие	Дисскуссия	2
3	Элементы теории чисел.	Практическое занятие	Дисскуссия	2
4	Математические основы симметричных шифров.	Практическое занятие	Дисскуссия	2
5	Односторонние функции.	Практическое занятие	Мозговой штурм	2
6	Поля Галуа	Практическое занятие	Мозговой штурм	2
7	Хэш-функции.	Практическое занятие	Мозговой штурм	2
8	Схемы электронных подписей на основе криптографических систем.	Практическое занятие	Мозговой штурм	2
Итого часов:				**16**

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

№	Вид контроля	Контролируемые темы (разделы)	Контролируемые компетенции/ индикаторы
1	**2**	**3**	**4**
1	Текущий контроль	Тема 1.1. Основные понятия и задачи	ОПК-9 ИДК$_{ОПК9.1.}$

		криптографии	ИДК$_{ОПК9.22}$
2	Текущий контроль	Тема 1.2. Классификация шифров, их основные типы и свойства	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
3	Текущий контроль	Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
4	Текущий контроль	Тема 2.1. Одноключевые методы шифрования, элементы теории чисел.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
5	Текущий контроль	Тема 2.2. Блочные и поточные шифры.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
6	Текущий контроль	Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
7	Текущий контроль	Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
8	Текущий контроль	Тема 3.2. Современные технологии шифрования.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
9	Текущий контроль	Тема 3.3. Криптоанализ шифров.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
10	Текущий контроль	Тема 4.1. Хеш-функции и их криптографические приложения	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
11	Текущий контроль	Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
12	Текущий контроль	Тема 4.3. Средства криптографической защиты информации.	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
13	Текущий контроль – контрольная работа	Разделы 1-4	ОПК-9 ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$
14	Промежуточный контроль - Зачет	Разделы 1-4	ОПК-9

			ИДК$_{ОПК9.1.}$ ИДК$_{ОПК9.2}$

8.1. Оценочные материалы (ОМ)

8.1.1. Оценочные материалы для входного контроля

Не предусмотрено

8.1.2 Оценочные материалы текущего контроля

Текущий контроль реализуется в виде письменного текущего контроля на ПЗ1-ПЗ16. Текущий контроль направлен на выявление сформированности компетенции ОПК-9. Для реализации текущего контроля используется балльно-рейтинговая система оценки, принятая в университете.

Усвоение студентом изучаемой дисциплины максимально оценивается 100 баллами. Максимальное количество баллов за текущую работу в семестре ограничивается 60-ю баллами, на оценку экзамена максимально предусмотрено 30 баллов. Возможны «премиальные» баллы (от 0 до 10), которые могут быть добавлены студенту за активные формы работы, высокое качество выполненных практических работ и т.д.

За посещение одного вида занятия дается 1.1 балла (23 занятия (Л+Пз+ЛР) * 1.13 балл = 25.99 балла), максимальное количество баллов за письменный контроль на ЛР и Пз – 2.1 балла (10 занятий (ЛР+ПЗ)*2.1 балл = 21 балл).

Параметры оценочного средства для письменного текущего контроля на ПЗ1-ПЗ16.

Критерии оценки	Оценка / баллы			
	Отлично 2.1 балла.	Хорошо 1.4 балла	Удовлетв. 0.7 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и допущено более 3-х ошибок.

ПЗ.1. Математические основы криптографии.
ПЗ.2. Математические основы шифров.
ПЗ. 3. Математические основы шифров замены.
Пз. 4. Математические основы шифров перестановки.
ПЗ 5. Элементы теории чисел.
ПЗ 6. Математические основы симметричных шифров.
ПЗ 7. Математические основы шифров гаммирования.
ПЗ 8. Математические основы комбинированных шифров.
ПЗ 9. Односторонние функции.
ПЗ 10. Поля Галуа.
ПЗ 11. Анализ криптостойкости шифров.
ПЗ 12. Сравнительный анализ шифров.
ПЗ 13. Хэш-функции.
ПЗ 14. Схемы электронных подписей на основе криптографических систем.
ПЗ 15. Стандарты электронной подписи.

ПЗ 16. Принципы построения и функционирования средств криптографической защиты информации.

Вопросы для письменного текущего контроля приведены ниже:

Пз. 1 Найти число x, удовлетворяющее уравнению $3^x = 5(\mathrm{mod} p)$,
где $p - 1 = 2 \cdot 3 \cdot 101 \cdot 103 \cdot 107^2$.
Упрощенный вариант: $p - 1 = 2 \cdot 3 \cdot 101$, или $p - 1 = 2 \cdot 3 \cdot 11 \cdot$

Пз. 2 Используя алгоритм Эвклида и обобщенный алгоритм Эвклида, вычислить наибольшие общие делители *d* для следующей пары чисел (m,n), дать представление вида $d=mk+nl$: (153, 648),(83, 597),(113, 481),(39, 379),(123, 48),(429, 376), (1526, 748),(439, 817),(356, 499),(15439, 379),(1983, 13675).

Пз. 3 Определить ключи шифра Цезаря, если известны следующие пары открытый текст – шифротекст: а) АПЕЛЬСИН-САЦЬНВШЮ б) АБРИКОС - ЫЬЛГЕЙМ.

Пз. 4 Зашифруем, например, указанным способом фразу: ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОЛВКИ используя прямоугольник размера 4X7:

П	Р	И	М	Е	Р	М
Н	Т	У	Р	Ш	Р	А
О	Й	П	Е	Р	Е	С
И	К	В	О	Н	А	Т

Пз. 5 Умножьте сравнения и определите класс вычетов, содержащий результат:
а) $-4 \equiv 10(\mathrm{mod}7)$, $34 \equiv 6(\mathrm{mod}7)$; б) $-3 \equiv 23(\mathrm{mod}13)$, $14 \equiv 79(\mathrm{mod}13)$.

Пз.6 Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

Пз.7 Пусть открытое сообщение (M ={mi}) в двоичной форме имеет вид: M = 10101100. Считаем, что выбран симметричный ключ K1 = K2 = K = 1010. Используется самая простая операция зашифрования: $c_i = m_i \oplus K$, где ci – i-й блок зашифрования; mi – i-я часть сообщения.

Пз. 8 Опишите шифр в общем виде, пронумеровав буквы русского алфавита числами от 0 до 31 (исключив букву Е) по правилу шифрования запишется следующим образом: c = (m + k) mod 32, где m и c — номера букв соответственно сообщения и шифротекста, а k — некоторое целое число, называемое ключом шифра

Пз. 9 Какими свойствами должна обладать односторонняя функция.

Пз. 10 Используя полином $f(x)=x^3+x+1$(неприводимый), $\deg(f(x))=3$, тогда его можно использовать для построения расширенного поля $GF(2^3)=GF(8)$.

Пз. 11 Какие допущения о возможностях криптоаналитика делает криптограф при анализе стойкости системы шифрования?

Пз. 12 1. Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

2. Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA. Пусть хеш-образ Фамилии равен 233, а закрытый ключ алгоритма RSA равен (25, 247).

Пз. 13 Найдите хеш–образ своей Фамилии, используя хеш–функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где n = pq, p, q – заданы.

Пз. 14 Что такое ЭП? Какие схемы ЭП вам известны? Докажите корректность ЭП в схемах RSA и Эль-Гамаля.

Пз. 15 Приведите стандарты ЭП и сравните их характеристики.

Пз. 16 Принципы построения и функционирования современных средств криптографической защиты информации и сравните их характеристики.

Параметры оценочного средства для письменного текущего контроля на ПЗ1-ПЗ16.

Критерии оценки	Оценка / баллы			
	Отлично/ 2.1 балла.	Хорошо/ 1.4 балла	Удовлетв. / 0.7 балла.	Неудовл. / 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и допущено более 3-х ошибок.

8.1.3 Оценочные материалы для промежуточной аттестации

Промежуточная аттестация проводится в форме зачета. Форма проведения зачета – устный по билетам или письменный по билетам. Зачеты проводятся во время экзаменационных сессий в соответствии с расписанием.

Экзаменационный билет состоит из двух теоретических вопросов и одного практического. Экзаменационные задания (билеты) для приема экзаменов выполнены многовариантными, чтобы исключить возможность списывания и обмена информацией в ходе экзамена. Вопросы для самостоятельной подготовки студентов к экзамену приведены в приложении 1.

Студент допускается к экзамену в том случае, если в течение семестра за текущую работу набрано 40 баллов и более. В противном случае выставляется 0 сессионных баллов. Во время экзамена студент может набрать до 30 баллов. Если на экзамене ответ студента оценивается менее чем 10-ю баллами, то экзамен считается не сданным, студенту выставляется 0 баллов, а в ведомость выставляется оценка «неудовлетворительно».

Если на экзамене студент набирает 10 и более баллов, то они прибавляются к сумме баллов за текущую работу и переводятся в академическую оценку, которая фиксируется в ведомости и зачетной книжке студентов.

Итоговый семестровый рейтинг	Академическая оценка
60-70 баллов	«удовлетворительно»
71-85 баллов	«хорошо»
86-100 баллов	«отлично»

Преподаватель имеет право выставить экзаменационную оценку (с согласия студента) без процедуры сдачи экзамена, если сумма баллов, набранная студентом за текущую работу

составит 70 баллов. В этом случае к набранному студентом количеству баллов за текущую работу автоматически добавляется 20 баллов и выставляется соответствующая академическая оценка.

Критерии	Оценка			
	Отлично	Хорошо	Удовлетв.	Неудовлетв.
Знание	Всесторонние глубокие знания **(10 -11 баллов)**	Знание материала в пределах программы **(7 -9 баллов)**	Отмечены пробелы в усвоении программного материала **(4 -6 баллов)**	Не знает основное содержание дисциплины **(0-3 балла)**
Понимание	Полное понимание материала, приводит примеры, дополнительные вопросы не требуются **(8 -10 баллов)**	Понимает материал, приводит примеры, но испытывает затруднения с выводами, однако достаточно полно отвечает на дополнительные вопросы **(6 -8 баллов)**	Суждения поверхностны, содержат ошибки, примеры не приводит, ответы на дополнительные вопросы неуверенные **(4 -6 баллов)**	С трудом формулирует свои мысли, не приводит примеры, не дает ответа на дополнительные вопросы **(0-3 балла)**
Применение проф. терминологии	Дает емкие определения основных понятий, корректно использует профессиональную терминологию**(3-5 баллов)**	Допускает неточности в определении понятий, не в полном объеме использует профессиональную терминологию **(2-3 балла)**	Путает понятия, редко использует профессиональную терминологию **(1-2 балла)**	Затрудняется в определении основных понятий дисциплины, некорректно использует профессиональную терминологию (**0-2 балла**)
Соблюдение норм литературного языка	Соблюдает нормы литературного языка, преобладает научный стиль изложения **(3-4 балла)**	Соблюдает нормы литературного языка, допускает единичные ошибки **(2- 3 балла)**	Допускает множественные речевые ошибки при изложении материала **(1-2 балл)**	Косноязычная речь искажает смысл ответа (**0-1 балл**)

Демонстрационный вариант контрольной работы

1. Какая пара чисел сравнима по mod7 и не сравнима по mod5: (42,47), (–2,12), (19,–6)?

2. Сложите сравнения и определите класс вычетов, содержащий результат:

а) $-9 \equiv 12(\mathrm{mod}7)$, $17 \equiv 3(\mathrm{mod}7)$;

б) $-5 \equiv 12(\mathrm{mod}17)$, $17 \equiv 85(\mathrm{mod}17)$.

3. Какие пары чисел (n,e) можно использовать для построения системы RSA: а) n = 473, e = 289; б) n = 13589, e = 3377; в) n = 38989, e = 4601?

При допустимом наборе определите закрытый ключ d, зашифруйте сообщение x = 128 и затем расшифруйте криптограмму.

4. Докажите, что если $x + k \equiv y \pmod 2$, то $y + k \equiv x \pmod 2$..

5. В алгоритме RSA известно, что $n = p \cdot q = 11102239$, $\phi(n) = 11095560$. Разложите n на множители.

Оценочные средства для текущего контроля в форме тестирования

Тестовые вопросы для проверки сформированности компетенции

ОПК-9. Способность применять соответствующий математический аппарат для решения профессиональных задач.

1. Укажите двухключевую криптосистему:
А) DES
Б) RSA
В) ГОСТ 28147-89

2. Назовите закон об Электронной подписи?
А) ФЗ-16
Б) ФЗ-63
В) ФЗ-32

3. При применении несимметричной криптосистемы, используется:
А) секретный ключ
Б) открытый ключ
В) сначала открытый, а затем секретный ключ

4. Размер хэш-образа по российскому стандарту (ГОСТ-2012) равен:
А) 256 бит или 512 бит
Б) 320 бит или 160 бит
В) 160 бит

5. Двухключевая криптосистема по сравнению с одноключевой имеет более высокую производительность при шифровании данных:
А) ДА
Б) НЕТ
В) ОДИНАКОВУЮ

6. Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и несимметричной:
А) ДА
Б) НЕТ
В) ТОЛЬКО СИММЕТРИЧНОЙ

7. Хэш-функция – криптографическое преобразование информации, переводящее ….
А) из данных фиксированной длины в некоторое значение произвольной длины;
Б) строку битов произвольной длины в строку битов фиксированной длины;
В) из данных произвольной длины некоторое значение произвольной длины.

8. Для проверки целостности информации используется:
А) альфа-функция
Б) бета-функция

В) хэш-функция

9. Размер ЭП по российскому стандарту (ГОСТ-2012) равен:
А) 256 бит 320 бит
Б) 512 бит или 1024 бит
В) 320 бит

10. Программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра это?
А) средства записи и чтения;
Б) средства модуляции и детектирования;
В) средства удостоверяющего центра

11. Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите?
А) шифр Цезаря;
Б) шифр Соломона.
В) шифр Хеопса.

12. Прикладная наука о методах и способах преобразования информации с целью ее защиты от незаконных пользователей – это
А) криптозащита;
Б) криптография
В) криптовставка.

13. Уникальная последовательность символов, предназначенная для создания электронной подписи это?
А) ключ электронной подписи
Б) сертификат
В) синхропреамбула.

14. Хэш-функция не применяется:
А) для удаления информации.
Б) для защиты пароля;
В) при контроле целостности данных;

15. Двухключевая криптосистема применяется в следующих случаях (укажите все правильные варианты ответов):
А) для шифрования небольших по объему данных;
Б) при создании электронной подписи;
В) в задачах аутентификации;+

16. Что называется имитовставкой?:
А) специальный набор символов, который добавляется к сообщению и предназначен для обеспечения его целостности и аутентификации источника данных;
Б) набор символов, в котором для шифрования данных используется гаммирование;
В) шифр, в котором процедура шифрования заключается в перестановках элементов исходного текста или их групп, сами элементы при этом остаются неизменными;

17. Шифр Цезаря – это
а) асимметричный шифр

б) шифр биграммами
в) шифр замены со сдвигом

18. Какой алгоритм не используется при симметричном шифровании:
А) поточное шифрование;
Б) побитовое шифрование;
В) алгоритм Эль-Гамаля.

19. Что может указывать на изменение сообщения?
а) Изменился открытый ключ
б) Изменились дайджест сообщения
в) Изменился закрытый ключ

20. Какова длина блока алгоритма шифрования DES:
А) 64 бита;
Б) 56 бит;
В) 5 байт.

21. Сколько всего циклов выполняется операция зашифровывания в алгоритме DES:
А) 10;
Б) 20;
В) 16;

22. Что в переводе с греческого языка означает слово «криптография»?
А) тайнопись
Б) модуляция.
В) детектирование

23. Какой размер ключа в отечественном стандарте симметричного шифрования:
А) 53бит;
Б) 125 бит;
В) 256 бит.

24. Что из перечисленного ниже описывает разницу между алгоритмами DES и RSA?
а) DES – это алгоритм кодирования, а RSA – алгоритм декодирования
б) DES – это алгоритм записи, а RSA – алгоритм чтения.
в) DES – это симметричный алгоритм, а RSA – асимметричный алгоритм

25. Какое из этих утверждений является верным:
А) у S-блоков ГОСТ 4-битовые входы и 8-битовые выходы;
Б) у S-блоков ГОСТ 4-битовые входы и 4-битовые выходы;
В) у S-блоков ГОСТ 8-битовые входы и 4-битовые выходы;

26. Используется ли в отечественном стандарте симметричного шифрования процедура генерации подключей из ключей, как в DES:
А) да, но эта процедура сравнительно проста;
Б) не используется;
В) используется аналогичная по сложности процедура.

27. В отечественном стандарте симметричного шифрования применяется подстановка, основанная на применении S-блоков. Сколько таких блоков используется в ГОСТ:
А) 8;

Б) 12;
В) 14;

28. Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи это?

А) исходный текст;
Б) ключ проверки электронной подписи
В) открытый текст.

29. Выберите правильное утверждение:

А) в DES нет битовых перестановок шифруемого блока.

Б) в отечественном стандарте симметричного шифрования нет начальной и конечной битовых перестановок шифруемого блока, так как они не влияют на стойкость шифра;

В) в DES нет начальной и конечной битовых перестановок шифруемого блока.

30. Что представляет собой операция XOR?

А) интегрирование;
Б) дифференцирование;
В) сложение по модулю 2.

31. К какому классу преобразований относится шифр Цезаря?

А) подстановки;
Б) суммирования.
В) гаммирование.

32. Что в криптографии называют открытым текстом?

А) электронную цифровую подпись
Б) закрытый ключ шифрования
В) исходное сообщение (сообщение до шифрования)

33. **Какой из перечисленных ниже алгоритмов шифрования не является симметричным?**

А) DES;
Б) RSA;
В) IDEA;

34. **Какую длину имеет секретный ключ в алгоритме DES?**

а) 2 бита;
б) 56 бит;
в) 4 бит;

35. Какая архитектура лежит в основе алгоритма DES?

а) сеть Фейстеля;
б) потоковый шифр;
в) сеть Петри;

36. На чем основана криптостойкость метода Диффи-Хэллмана?

а) на вычислении интегралов;
б) на функции возведения в степень;
в) на трудности вычислений дискретных логарифмов.

37. Какая процедура распределения ключей *не* требует использования защищенного канала для передачи ключа адресату?

а) процедура шифрования по алгоритму DES;

б) продедура Диффи-Хэллмана;

в) процедура шифрования Вижинера.

38. Дайджест сообщения (message digest) – это …

а) результат демодуляции;

б) результат кодирования.

в) результат хэширования.

39. Что такое односторонняя хэш-функция?

а) хэш-функция, трудно вычислимая как в прямом, так и обратном направлениях;

б) хэш-функция, легко вычислимая как в прямом, так и обратном направлениях;

в) хэш-функция, легко вычислимая в прямом и трудно вычисляемая в обратном направлении.

40. Чему равен результат вычисления хэш-функции по алгоритму SHA?

а) 160 бит;

б) 127 бит;

в) 63 бита;

41. Какой шифр является симметричными?

а) RSA (Rivest-Shamir-Alderman);

б) DES (DataEncryptionStandart);

в) Эль-Гамаль (ElGamal).

42. Как называется сообщение, полученное после преобразования с использованием любого шифра?

А) ключом

Б) закрытым текстом

В) текстом

43. Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии

А) односторонней функцией

Б) функцией Соломона.

В) функцией Фурье

44. Какие из перечисленных ниже алгоритмов являются асимметричными? (укажите все правильные ответы)

а) DES;

б) Эль-Гамаль (El-Gamal);

в) RSA+.

45. Что называется ключом электронной подписи?

А) уникальная последовательность символов, предназначенная для создания электронной подписи.

Б) средство, используемые для оказания услуг доверенной третьей стороной;

В) метка доверенного времени.

46. Что называется электронной подписью?

а) характеристика шифра для криптографического преобразования сообщения;

б) присоединенные к сообщению фамилия, имя и отчество отправителя;

в) информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

47. Виды электронной подписи:

А) простая, неквалифицированная, квалифицированная.

Б) быстрая, сложная, простая.

В) оригинальная, неоригинальная,

48. Программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра это?

А) средства записи и чтения;

Б) средства модуляции и детектирования;

В) средства удостоверяющего центра

49. Какие шифры являются симметричными? (укажите все правильные ответы)

а) DES (DataEncryptionStandart);

б) RSA (Rivest-Shamir-Alderman);

в) ГОСТ 28147-89; +

50. Пространством ключей называют

А) множество всех возможных ключей, доступных для использования в алгоритме.

Б) одинаковые ключи;

В) дублированные ключи.

51. Шифрование речевых сообщений

А) модуляция;

Б) манипуляция;

В) аудиоскремблирование.

52. Название одного из алгоритмов блочного шифрования:

А) «Морж»

Б) «Кузнечик»

В) «Цапля»

53. Какое из нижеперечисленных средств используется для формирования электронной подписи?

а) «Бумеранг»

б) «КриптоПро CSP»

в) «Спрут»

54. Что из нижеперечисленного относится к средствам криптографической защиты информации?

а) «Гранит»

б) «Катран»

в) «КриптоПро CSP»

55. Какой математический аппарат используется в криптографии?

А) поля Ширака;

Б) поля Минтона;
В) поля Галуа;

56. Сложность нахождения секретного ключа системы RSA определяется
а) сложностью разложения числа n на простые множители +
б) сложностью интегрирования;
в) сложностью дифференцирования;

57. Кем было выполнено доказательство существования абсолютно стойких криптографических алгоритмов?
А) Б. Соломоном
Б) К. Шенноном
В) Б. Штанмайером

58. Что определяло надежность алгоритма DES?
а) сложностью интегрирования;
б) размер ключа.
в) вычисление корней алгебраических уравнений.

59. Единственный неуязвимый шифр?
А) одноразовый шифровальный блокнот;
Б) шифр Хэмминга.
В) шифр DES.

60. Стеганографией называют
а) науку о раскрытии шифров;
б) наука (и практика ее применения) о методах и способах вскрытия шифров.
в) совокупность методов и средств защиты информации от несанкционированного доступа путем скрытия факта существования тайного сообщения.

Примерный перечень вопросов и заданий к зачету

Раздел 1. Основы криптографии

Тема 1.1. Основные понятия и задачи криптографии.

1. Аспекты безопасности информации.
2. Основные понятия криптографии.
3. Шифры Цезаря, Вижинера.

Тема 1.2. Классификация шифров, их основные типы и свойства.

1. Общая схема шифрования.
2. Основные требования к шифрам.
3. Шифры перестановки.
4. Шифры замены.

Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.

1. Принципы построения криптосистем К.Шеннона.
2. Помехоустойчивость шифров.
3. Надёжность и криптографическая стойкость шифров.

Раздел 2. Криптографическая защита информации на основе симметричных криптосистем

Тема 2.1. Одноключевые методы шифрования, элементы теории чисел.

1. Принципы построения криптографических алгоритмов.
2. Режимы выполнения симметричных криптоалгоритмов.

Тема 2.2. Блочные и поточные шифры.

1. Способы формирования ключей для поточного шифрования.

2. Сеть Фейстеля.
3. Особенности блочных и поточных шифров.

Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.

1. Стандарт криптографической защиты DES.
2. Модификации алгоритма DES.
3. Российский алгоритм криптографического преобразования: режимы шифрования.
4. Российский алгоритм криптографического преобразования: режим имитовставки.
5. Российский алгоритм криптографического преобразования: режим гаммирования.

Раздел 3. Криптографическая защита информации на основе асимметричных криптосистем

Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.

1. Обмен Диффи-Хеллмана. Назначение мастер-ключа.
2. Односторонние функции.
3. Дискретное логарифмирование.
4. Несимметричные системы шифрования.
5. Алгоритм RSA.
6. Криптосистема Эль-Гамаля.
7. Сравнение симметричных и несимметричных криптосистем.

Тема 3.2. Современные технологии шифрования.

1. Криптосистемы на эллиптических кривых.
2. Математические основы криптосистем на эллиптических кривых.
3. Выбор параметров кривой.

Тема 3.3. Криптоанализ шифров.

1. Подходы к анализу криптографических алгоритмов.
2. Криптостойкость симметричных криптосистем.
3. Криптостойкость асимметричных криптосистем.
4. Метод перебора.
5. Частотный анализ.
6. Корреляционный метод анализа поточных шифров.
7. Линейный и дифференциальный методы анализа блочных шифров.

Раздел 4. Криптографические методы защиты электронного документооборота.

Тема 4.1. Хеш-функции и их криптографические приложения.

1. Определение и назначение хэш-функции, российский стандарт.
2. Требования к хэш-функциям.
3. Понятие о стойкости хеш-функции.
4. Ключевые и бесключевые хеш-функции.

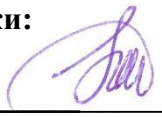
Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты.

1. Классификация электронных подписей.
2. Российский стандарт ЭП: технология создания и проверки.
3. Электронная подпись: определения, назначение, роль в электронном документообороте.
4. Инфраструктура открытых ключей.
5. Правовое обеспечение электронной подписи.
6. Примеры цифровых подписей на основе алгоритмов RSA, Эль-Гамаля.
7. Стандарты подписи ГОСТ 3410 и DSS.

Тема 4.3. Средства криптографической защиты информации.

1. СКЗИ серии Криптон.
2. СКЗИ КриптоПро CSP.
3. Скремблеры.

Разработчики:



_____ _профессор _____ Корольков Ю.Д._____
(подпись) (занимаемая должность) (Ф.И.О.)

_____ ___профессор_____ _Ерохин В.В._____
(подпись) (занимаемая должность) (Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники
«8» апреля 2024 г. протокол № 8

И.О. зав. кафедрой _ _____ Колесник С.Н.

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.