МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
И.о. заведующего кафедрой
математического анализа
Шабров С.А.

01.07.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.03.03 Методы и средства криптографической защиты информации

1. Код и наименование направления подготовки/специальности: 10.05.04 Информационно-аналитические системы безопасности

2. Профиль подготовки/специализация: Применение математических методов к решению инженерных и экономических задач

3. Квалификация выпускника: Специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: математического анализа

6. Составители программы:
Паршин Максим Игоревич, канд. физ.-мат. наук, преподаватель кафедры математического анализа

7. **Рекомендована:** Научно-методическим Советом математического факультета, протокол **№0500-07 от 29.06.2021**

8. Учебный год: 2023/2024 **Семестр(ы): 5**

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:

- получение базовых знаний о методах защиты информации и областях применения этих методов;
- изучение методов криптографической защиты, формирования секретных ключей, протоколов ограничения доступа;
- изучение типовых уязвимостей операционных и информационно-вычислительных систем;
- приобретение базовых умений в решении основных задач защиты информации.

Задачи учебной дисциплины:

- получение знаний о методах защиты информации;
- приобретение навыков практической реализации методов криптографической защиты информации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Методы и средства криптографической защиты информации» относится к учебным дисциплинам Обязательной части Блока 1, группа учебных дисциплин «Методы и средства обеспечения информационной безопасности»

Дисциплина «Методы и средства криптографической защиты информации» базируется на знаниях, полученных по основным математическим дисциплинам и программирования.

Приобретенные в результате обучения знания, умения и навыки могут использоваться в областях, связанных с защитой информации, представленной как в текстовом, так и в электронном виде, а также для сохранения целостности данных.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-9	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-9.1	Способен выбирать методы криптографической защиты информации в соответствии с угрозами безопасности информации и требованиями по защите информации	знать: - основные методы и основные области применения криптографической защиты информации; уметь: - программно реализовывать основные алгоритмы криптографической защиты информации
		ОПК-9.2	Способен применять средства	знать: - задачи, решаемые криптографическими методами

			криптографической защиты информации	защиты информации; - вопросы реализации алгоритмов криптографических методов защиты информации с помощью ЭВМ; уметь: - использовать и анализировать фундаментальные знания в области криптографии; владеть: - использовать методы, позволяющие решить задачи защиты информации

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 4/144.

Форма промежуточной аттестации зачёт с оценкой.

13. Виды учебной работы:

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			Семестр №5
Контактная работа		68	68
в том числе:	лекции	34	16
	практические		
	лабораторные	34	16
	курсовая работа		
	др. виды		
Самостоятельная работа		40	40
Промежуточная аттестация		36	36
Итого:		144	144

13.1 Содержание разделов дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Введение в криптографические методы защиты информации	Краткая история. Модели систем передачи информации. Классификация. Методы криптоанализа и типы атак.	–

1.2	Классические криптографические методы	Моноалфавитные шифры. Биграммные шифры замены. Полиграммный шифр замены Хилла. Шифр гаммирования Виженера. Криптоанализ полиалфавитных шифров.	–
1.3	Совершенная криптостойкость	Определение. Криптосистема Вернона. Расстояние единственности.	–
1.4	Основные криптографические методы	Блочные шифры. Генераторы псевдослучайных чисел. Потоковые шифры. Хеш-функции. Асимметрические криптосистемы. Криптографические протоколы. Распространение ключей.	–
1.5	Примеры систем защиты информации	Примеры систем защиты информации. Аутентификация пользователя. Программные уязвимости.	–
2. Практические занятия			
3. Лабораторные занятия			
3.1	Классические криптографические методы	Моноалфавитные шифры. Биграммные шифры замены. Полиграммный шифр замены Хилла. Шифр гаммирования Виженера. Криптоанализ полиалфавитных шифров.	–
3.2	Основные криптографические методы	Блочные шифры. Генераторы псевдослучайных чисел. Потоковые шифры. Хеш-функции. Асимметрические криптосистемы. Криптографические протоколы. Распространение ключей.	–

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Введение в криптографические методы защиты информации	4		4	8	
02	Классические криптографические методы	6		6	8	
03	Совершенная криптостойкость	6		6	8	
04	Основные криптографические методы	6		6	8	
05	Примеры систем защиты информации	6		6	8	

Итого	34		34	40	

14. Методические указания для обучающихся по освоению дисциплины

В процессе освоения дисциплины студенты должны посетить лекционные и лабораторные занятия и сдать зачёт.

Указания для освоения теоретического материала и материала для лабораторных работ:

1. Обязательное посещение лекционных и лабораторных занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.
2. Получение в библиотеке рекомендованной учебной литературы и электронное копирование рабочей программы с методическими рекомендациями, конспекта лекций.
3. Копирование (электронное) перечня вопросов к зачёту по дисциплине, а также списка рекомендованной литературы из рабочей программы дисциплины.
4. При подготовке к лабораторным занятиям по дисциплине необходимо изучить рекомендованный лектором материал, иметь при себе конспекты соответствующих тем и необходимый справочный материал.
5. Рекомендуется следовать советам лектора, связанным с освоением предлагаемого материала, провести самостоятельный Интернет – поиск информации (видеофайлов, файлов-презентаций, файлов с учебными пособиями) по ключевым словам курса и ознакомиться с найденной информацией при подготовке к лабораторным занятиям.

Студент допускается к сдаче зачёта, если имеет на руках конспект основного теоретического материала с разбором основных типовых задач, имеется зачёт по контрольной работе.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины:

а) основная литература:

№ п/п	Источник
1	***Владимиров, Сергей Михайлович***. Криптографические методы защиты информации / Э.М. Габидулин, А.И. Колыбельников, А.С. Кшевецкий.— Москва: Издательский центр "Академия", 2013.— 191 с.

б) дополнительная литература:

№ п/п	Источник
2	***Ахо А., Ульман Д., Хопкрофт Д.*** Построение и анализ вычислительных алгоритмов / под ред. Ю. В. Матиясевича ; пер. А. О. Слисенко. — М. : Мир, 1979.
3	***Гультяева Т. А.***. Основы теории информации и криптографии. — Новосибирск : Издательство НГТУ, 2010. — 88 с. — ISBN 978-5-7782-1425-5.
4	***Крэндалл Р., Померанс К.***. Простые числа: Криптографические и вычислительные аспекты / под ред. В. Н. Чубарикова ; пер. А. В. Бегунца [и др.]. — М. : УРСС: Книжный дом «ЛИБРОКОМ», 2011. — 664 с

5	***Алферов А.П.*** Основы криптографии. Учебное пособие / А. П. Алферов [и др.]. — М. : Гелиос АРВ, 2001. — 480 с. — ISBN 5-85438-137-0.
6	***Шеннон К.*** Работы по теории информации и кибернетике / под ред. Р. Л. Добрушина, О. Б. Лупанова. — М. : Издательство иностранной литературы, 1963. — 830 с.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
12	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
13	*Электронно-библиотечная система "Консультант студента". – (http://www.studentlibrary.ru/)*
14	*Электронно-библиотечная система «Издательства Лань». – (https://e.lanbook.com/)*
15	*Электронно-библиотечная система "РУКОНТ". – (https://rucont.ru/)*

16. Перечень учебно-методического обеспечения для самостоятельной работы:

Самостоятельная работа студента-бакалавра, прежде всего, заключатся в изучении литературы, дополняющей материал, излагаемый на лекции и в ходе лабораторных работ. Необходимо овладеть навыками библиографического поиска, уметь находить подходящие источники, творчески и критически перерабатывать информацию, научиться определять методы исследований.

№ п/п	Источник
1	*Защита информации. Основные термины и определения [текст] : ГОСТ Р 50922-2006. — Введ. 27.12.2007. — М. : Стандартинформ, 2008. — 12 с. — (Государственный стандарт Российской Федерации). — URL: http://protect.gost. ru/document.aspx?control=8&id=120843.*
2	*Информационная технология. Криптографическая защита информации. Блочные шифры [текст] : ГОСТ Р 34.12-2015. — Введ. 01.01.2016. — М. : Стандартинформ, 2015. — 25 с. — (Национальный стандарт Российской Федерации). — URL: http://protect.gost.ru/document.aspx?control=7&id= 200990*
3	*Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров [текст] : ГОСТ Р 34.13-2015. — Введ. 01.01.2016. — М. : Стандартинформ, 2015. — 38 с. — (Национальный стандарт Российской Федерации). — URL: http://protect.gost.ru/document.aspx? control=7&id=200971.*
4	*Информационная технология. Криптографическая защита информации. Функция хэширования [текст] : ГОСТ Р 34.11-2012. — Введ. 01.01.2013. — М. : Стандартинформ, 2013. — 24 с. — (Национальный стандарт Российской Федерации). — URL: http://protect.gost.ru/document.aspx?control=7&id= 180209.*
5	*Информационная технология. Методы и средства обеспечения*

	безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [текст] : ГОСТ Р ИСО/МЭК 13335-1-2006. — Введ. 01.06.2007. — М. : Стандартинформ, 2007. — 19 с. — (Государственный стандарт Российской Федерации). — URL: http://protect.gost.ru/document.aspx?control=8&id=120843.
6	*Информационная технология. Техническая защита информации. Основные термины и определения [текст] : ГОСТ Р 50.1.056-2005. — Введ. 01.01.2006. — М. : Стандартинформ, 2005. — 13 с. — (Государственный стандарт Российской Федерации).*
7	*Киви Б. О процессе принятия AES // Компьютерра. — 1999. — дек. — № 49. — ISSN 1815-2198. — URL: http : / / kiwibyrd.chat.ru/aes/aes2.htm.*

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Осуществляется интерактивная связь с преподавателем через сеть интернет, проводятся индивидуальные онлайн консультации и проверка контрольной работы через email.

Лабораторные работы осуществляются с использованием ЭВМ и прикладного ПО: MS VS.

18. Материально-техническое обеспечение дисциплины:

Учебные аудитории для проведения лекционных и практических занятий. Компьютерные классы для выполнения индивидуальных заданий, оснащённые лицензионным и свободно распространяемым программным обеспечением: Windows 7 или 10, MS VS.

---

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Знает основные методы и основные области применения криптографической защиты информации	ОПК-9	ОПК-9.1 ОПК-9.2	Устный опрос
2.	Знает задачи, решаемые криптографическими методами	ОПК-9	ОПК-9.1 ОПК-9.2	Устный опрос

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	защиты информации			
3.	Умеет программно реализовывать основные алгоритмы криптографической защиты информации	ОПК-9	ОПК-9.1 ОПК-9.2	Устный опрос, Контрольная работа
4.	Умеет использовать и анализировать фундаментальные знания в области криптографии	ОПК-9	ОПК-9.1 ОПК-9.2	Устный опрос
Промежуточная аттестация форма контроля - зачёт				*Перечень вопросов* *Практическое задание*

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- выполнение лабораторных работ;
- зачёт.

Требования к выполнению заданий (или шкалы и критерии оценивания)

Для оценивания результатов обучения на зачёте используются следующие показатели:

- Знание основных методов и основных областей применения криптографической защиты информации; задач, решаемых криптографическими методами защиты информации.
- Умение программно реализовывать основные алгоритмы криптографической защиты информации; использовать и анализировать фундаментальные знания в области криптографии.
- Владение навыками, позволяющими решить задачи защиты информации.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Достаточное владение материалом: правильные и конкретные, без грубых ошибок ответы на основные вопросы, с возможными неточностями в отдельных ответах;	Пороговый уровень и/или выше порогового	Зачтено
Плохое владение материалом: ответ	Ниже порогового	Незачтено

неверен, отсутствие ориентации в предмете	уровня	

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

- устный опрос;
- контрольная работа.

Примерный перечень вопросов и заданий проверки практических навыков

1. Реализовать метод защиты информации на основе блочных шифров.
2. Реализовать метод защиты информации на основе потоковых шифров.
3. Реализовать метод защиты информации на основе хеш-функции.
4. Реализовать метод защиты информации на основе асимметричной криптосистемы.

Примерный перечень вопросов к зачёту

1. Основные модели систем передачи информации, классификация, методы криптоанализа и типы атак.
2. Моноалфавитные шифры.
3. Биграммные шифры замены.
4. Полиграммный шифр замены Хилла. Шифр гаммирования Виженера.
5. Криптоанализ полиалфавитных шифров.
6. Определение. Криптосистема Вернона. Расстояние единственности.
7. Блочные шифры.
8. Генераторы псевдослучайных чисел.
9. Потоковые шифры.
10. Хеш-функции.
11. Асимметрические криптосистемы.
12. Криптографические протоколы. Распространение ключей.
13. Примеры систем защиты информации.
14. Аутентификация пользователя.
15. Программные уязвимости.