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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа
Шабров С.А.

25.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

_Б1.О.03.03 Методы и средства криптографической защиты информации

Код и наименование дисциплины в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

10.05.04 Информационно-аналитические системы безопасности

2. Профиль подготовки/специализация:

Автоматизация информационно-аналитической деятельности

Информационная безопасность финансовых и экономических структур

3. Квалификация выпускника: специалист по защите информации_

4. Форма обучения: очная_____

5. Кафедра, отвечающая за реализацию дисциплины: Кафедра математического анализа

6. Составители программы: Паршин Максим Игоревич, кандидат физико-математических наук

(ФИО, ученая степень, ученое звание)

7. Рекомендована: научно-методическим советом математического факультета, протокол от 25.05.2023, № 0500-06_____

наименование рекомендующей структуры, дата, номер протокола

8. Учебный год: 2025/2026 **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: учебная дисциплина «Методы и средства криптографической защиты информации» относится к части, формируемой участниками образовательных отношений Блока 1.

Дисциплина «Криптографические методы 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 (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Коды	Индикаторы	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 криптографической защиты информации и использовать их при решении задач профессиональной деятельности; Уметь: выбирать методы криптографической защиты информации в соответствии с угрозами безопасности информации и требованиями по защите информации; Владеть: навыками применения средств криптографической защиты информации.
		ОПК-9.2	Способен применять средства криптографической защиты информации	

12 Объем дисциплины в зачетных единицах/часах — 4 / 144**.**

Форма промежуточной аттестации – зачет

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		5 семестр
Аудиторные занятия	68	68
в том числе: лекции	34	34
практические	0	0
лабораторные	34	34
Самостоятельная работа	40	40
Форма промежуточной аттестации *(зачет, экзамен – 36 час.)*	36	36
Итого:	**144**	**144**

13.1. Содержание 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	6		6	8	20
02	Классические криптографические методы	6		6	8	20
03	Совершенная криптостойкость	6		6	8	20
04	Основные криптографические методы	8		8	8	24
05	Примеры систем защиты информации	8		8	8	24
Итого		34		34	40	108

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 *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных), курсовых работ и др.)*

№ 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. Фонд оценочных средств:

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	Устный опрос
2.	Знает задачи, решаемые криптографическими методами защиты информации	ОПК-9	ОПК-9.1	Устный опрос
3.	Умеет программно реализовывать основные алгоритмы криптографической защиты информации	ОПК-9	ОПК-9.2	Устный опрос, Лабораторная работа
4.	Умеет использовать и анализировать фундаментальные знания в области криптографии	ОПК-9	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.

Лабораторная работа №1

Реализовать метод защиты информации на основе блочных шифров

Лабораторная работа №2

Реализовать метод защиты информации на основе потоковых шифров.

Лабораторная работа №3

Реализовать метод защиты информации на основе хеш-функции.

Лабораторная работа №4

Реализовать метод защиты информации на основе асимметричной криптосистемы

Для оценивания результатов каждой лабораторной и контрольной работы используется ***шкала:*** «зачтено», «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения показаны в следующей таблице:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Правильное выполнение лабораторной работы.	Достаточный уровень	Зачтено
Не выполнение лабораторной работы	–	Не зачтено

20.2 Промежуточная аттестация

Промежуточная аттестация в 5 семестре по дисциплине заключается в защите лабораторных работ 1-4 и собеседовании по теоретическим вопросам.

Перечень вопросов к зачету:

№№ п/п	Темы к текущей аттестации (зачету)
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.

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 неверен, отсутствие ориентации в предмете	Ниже порогового уровня	Незачтено

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1. Контроль целостности передаваемых по сетям данных осуществляется посредством …
   электронной цифровой подписи
   аутентификации данных
   аудита событий
   межсетевого экранирования

2. Преобразовательный процесс, в ходе которого исходный текст, который носит также название открытого текста, заменяется измененным текстом, называется
   шифрование
   дешифрование
   преобразование
   искажение
   кодирование
   хеширование

3. Процесс, в ходе которого шифрованный текст преобразуется в исходный, называется …
   шифрование
   дешифрование
   преобразование
   искажение

4. Информация, необходимая для беспрепятственного шифрования и дешифрования текстов, называется …
   ключ
   шифр

код
пароль

5. Характеристика шифра, определяющая его стойкость к шифрованию без знания ключа, называется …
криптостойкостью
пароль
аудентификатор
шифратор

6. Асимметричное шифрование для шифрования и расшифровки использует …
один открытый ключ и один закрытый ключ
один открытый ключ
один закрытый ключ
один и тот же ключ
два открытых ключа
два закрытых ключа

7. Асимметричное шифрование для шифрования использует … ключ.
открытый
закрытый

8. Асимметричное шифрование для расшифровки использует … ключ.
закрытый
открытый

9. При симметричном шифровании для шифрования и расшифровки используются …
два ключа разной длины
два разных по значению ключа
один и тот же ключ
два открытых ключа
два закрытых ключа
один открытый ключ и один закрытый ключ

10. Относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом, называется …
закрытый ключ шифрования
электронная цифровая подпись
вирусная маска
открытый ключ шифрования

11. Криптосистема включает …
алгоритм шифрования
набор ключей, используемых для шифрования
систему управления ключами
антивирусное ПО
межсетевой экран

12. Механизм безопасности, который является сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные

критические ошибки, – …
регистрация и аудит
аутентификация
идентификация
VPN
межсетевой экран

13. Задачи криптосистемы: …
обеспечение конфиденциальности
обеспечение целостности данных
аутентификация данных и их источников
межсетевое экранирование
защита от вирусов

14. Функции управления криптографическими ключами: …
генерация
хранение
распределение
изучение
уничтожение

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания закрытого типа (множественный выбор):

- 2 балла – указаны все верные ответы;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):

- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

5) Задания открытого типа (число):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).