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

УТВЕРЖДАЮ
декан факультета прикладной
математики, информатики
и механики

_____А. И. Шашкин
подпись, расшифровка подписи
23.05.2020

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.Б.51.04 Криптографические стандарты

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

математические методы защиты информации

3. Квалификация (степень) выпускника:

Специалист по защите информации

4. Форма обучения:

очная

5. Кафедра, отвечающая за реализацию дисциплины:

ERP-систем и бизнес-процессов

6. Составители программы:

Воронков Борис Николаевич, к. т. н., доцент кафедры ERP-систем и бизнес-процессов

7. Рекомендована:

Научно-методическим советом факультета прикладной математики, информатики и механики 23.05.2020 г., протокол № 9

_____
отметки о продлении вносятся вручную)

8. Учебный год: 2024/2025 **Семестр(ы):** 8

9. **Цели и задачи учебной дисциплины:** Цель дисциплины – теоретическая и практическая подготовка специалистов к деятельности, связанной с анализом и использованием криптографических стандартов.

10. Место учебной дисциплины в структуре ООП: Дисциплина «Криптографические стандарты» входит в базовую часть учебного плана, является дисциплиной специализациии и изучается в 8 семестре.

№ п/п	Наименование дисциплин учебного плана, с которым организована взаимосвязь дисциплины рабочей программы
1.	Б1.Б.44 Криптографические методы защиты информации
2.	Б1.Б.43 Криптографические протоколы

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

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-3.	способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знание протоколов: распределения ключей, идентификации, разделения секрета. Умение проводить анализ безопасности криптографических протоколов. Владение навыками программной реализации криптографических протоколов.
ПСК-2.5.	способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учётом современных и перспективных математических методов защиты информации	Знание современных программно-аппаратных средств защиты информации, применяемых в криптографических стандартах. Умение проводить сравнительный анализ используемых криптографических стандартов. Владеть навыками выбора программно-аппаратных средств защиты информации с учётом современных математических методов в области информационной безопасности.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* – 2/72.

Форма промежуточной аттестации*(зачет/экзамен)* зачёт с оценкой.

13. Виды учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
				8		
Аудиторные занятия	32			32		
в том числе: лекции	16			16		
Практические	0			0		
Лабораторные	16			16		
Самостоятельная работа	40			40		
Контроль						
Итого:	72			72		
Форма промежуточной аттестации				ЗаО		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Американский стандарт DES	Шенноновские методы шифрования информации. Схема Фейстеля. Модулярная арифметика.
2	Российский стандарт «Магма»	Модифицированная схема Фейстеля. Нелинейное преобразование. Имитозащита, Гаммирование.
3	Криптосистема RSA	Задача факторизации. Обратные по модулю величины. Функция и теорема Эйлера.
2. Практические занятия не предусмотрены		
3. Лабораторные работы		
3.1	Лабораторная работа №1 Тема: Анализ стандарт DES.	*Теоретические сведения* 1. Перестановки и замены при шифровании. 2. Особенности схемы Фейстеля. 3. Шифрование и расшифрование. *Практическая часть* 1.Освоение стандарта с помощью обучающей программы. 2. Подготовка и защита отчёта по лабораторной работе.
3.2	Лабораторная работа №2 Тема: Российский стандарт «Магма».	*Теоретические сведения* 1. Описание алгоритма. 2. Модифицированная схема Фейстеля. 3. Имитозащита. 4. Режимы работы криптосистемы. *Практическая часть* 1. Освоение стандарта с помощью обучающей программы. 2. Подготовка и защита отчёта по лабораторной работе.
3.3	Лабораторная работа №3 Тема: Криптосистема RSA.	*Теоретические сведения* 1. Вычислительно-трудная задача факторизации. 2. Законы модулярной арифметики. 3. Обратные по модулю величины. 4. Доказательство корректности алгоритма. *Практическая часть* 1. Реализация криптосистемы RSA в виде приложения. 2. Подготовка и защита отчёта по лабораторной работе.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Всего
1	Американский стандарт DES.	4	0	4	12	20
2	Российский стандарт «Магма».	6	0	6	14	26
3	Криптосистема RSA.	6	0	6	14	26
	Итого:	16		16	40	72

14. Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой библиографии, итоговое повторение теоретического материала. Подготовка отчётов по лабораторным работам и подготовка к зачёту с оценкой.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	*Смарт Н. Криптография / Н. Смарт; пер. с англ. С.А. Кулешова; под ред. С. К. Ландо. – М.: Техносфера, 2006. – 525 с.*
2	*1. Салий В. Н. Криптографические методы и средства защиты информации / В. Н. Салий. – 2010. – (URL: http://www.sgu.ru/files/nodes/11017/V.N. Saliy. Kriptograficheskie metody i sredstva zashchity informacii.doc) (дата обращения: 12.05.2019)*

б) дополнительная литература:

№ п/п	Источник
3	*Воронков Б. Н. Криптографические методы защиты информации / Б. Н. Воронков, Ю. А. Крыжановская. – Воронеж: Издательский дом ВГУ, 2018. – 114 с.*

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

№ п/п	Источник
4	https://e.lanbook.com/ - ЭБС «Лань»
5	*www.lib.vsu.ru — Зональная научная библиотека ВГУ*

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Windows7. Мультимедийные лекционные демонстрации. Презентации на базе конспекта лекций.

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-3. Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать: зарубежные и российские криптографические стандарты.	Раздел 1. Американский стандарт DES. Раздел 2. Российский стандарт «Магма». Раздел 3. Криптосистема RSA..	Устный опрос.
	Уметь проводить анализ безопасности криптографических стандартов.	Разделы 1 – 3.	Устный опрос. Лабораторные работы.
	Владеть навыками программной реализации криптографических стандартов.	Разделы 1 – 3.	Устный опрос, защита отчётов по лабораторным работам.
ПСК-2.5. способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учётом современных и перспективных математических методов защиты информации.	Знать: современные программно-аппаратные средства защиты информации, применяемые в криптографических стандартах.	Раздел 1. – 3.	Устный опрос.
	Уметь проводить сравнительный анализ используемых криптографических стандартов.	Разделы 1 – 3.	Устный опрос. Лабораторные работы.
	Владеть навыками выбора программно-аппаратных средств защиты информации с учётом современных математических методов в области информационной безопасности.	Разделы 1 – 3.	Устный опрос, защита отчётов по лабораторным работам.
Промежуточная аттестация			Комплект КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и результаты выполнения лабораторных работ, позволяющие оценить степень сформированности умений и навыков.

Для оценивания результатов обучения на зачёте с оценкой используется – шкала и критерии оценивания в соответствии с таблицей.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Компетенция	Показатель сформированности компетенции	Шкала и критерии оценивания уровня освоения компетенции			
		5	4	3	2
ПК-3.. Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знает: – Основные зарубежные и российские стандарты шифрования.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Умеет: – проводить анализ безопасности криптографических стандартов и разрабатывать модели их безопасности.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеет: – навыками моделирования и программной реализации криптографических стандартов.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
ПСК-2.5. способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учётом современных и перспективных математических методов защиты информации.	Знает: – современные программно-аппаратные средства защиты информации, применяемые в криптографических стандартах.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Умеет: проводить сравнительный анализ используемых криптографических стандартов.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеет: – навыками выбора программно-аппаратных средств защиты информации с учётом современных математических методов в области информационной безопасности.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примеры контрольных вопросов и заданий:

1. Что представляет собой алгоритм шифрования RSA?
2. Какая проблема лежит в основе реализации алгоритма RSA?
3. В чем состоят достоинства и недостатки алгоритма RSA?
4. Докажите корректность алгоритма Эль Гамаля.
5. Докажите корректность алгоритма RSA.
6. Перечислите методы и средства защиты информации.
7. Что такое политика безопасности? Как она реализуется?
8. В чем состоит системно-концептуальный подход при решении задач защиты информации в компьютерных системах?

9. Каковы требования к комплексным системам защиты информации?
10. Какие Вам известны стандарты информационной безопасности? Охарактеризуйте их.
11. Охарактеризуйте атаки на криптосистемы.
12. Что такое идеальная криптосистема? Почему идеальные криптосистемы не находят широкого применения?
13. Что такое однонаправленная функция? Приведите примеры.

19.3.2. Примеры заданий к лабораторной работе

1. Ознакомиться с алгоритмом DES.
2. Пройти обучение по работе с DES с помощью компьютерной программы.
3. Сформулировать основные свойства алгоритма..
4. Ответить на контрольные вопросы.
5. Составить отчёт о проделанной работе.

19.3.3. Пример контрольно-измерительного материала

УТВЕРЖДАЮ

заведующий кафедрой
ERP-систем и бизнес-процессов
_____ Й. Беккер
подпись, расшифровка подписи
_03.06.2019

Направление подготовки / специальность ___10.05.01_Компьютерная безопасность
шифр, наименование
Дисциплина__Криптографические стандарты_____

Вид контроля __зачёт с оценкой_____
промежуточный контроль - экзамен, зачет; текущий контроль с указанием формы

Контрольно-измерительный материал №_1_

1. Сравнение алгоритмов DES и «Магма».

2. Модифицированная схема Фейстеля.

Преподаватель _____ .____
подпись расшифровка подписи

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; лабораторные работы; тестирования. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков по вопросам компьютерной безопасности.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.