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

УТВЕРЖДАЮ

Заведующий кафедрой
цифровых технологий

С.Д.Кургалин
30.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

1. Код и наименование направления подготовки/специальности:

02.03.01 Математика и компьютерные науки

2. Профиль подготовки/специализация: для всех профилей

3. Квалификация (степень) выпускника: бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: цифровых технологий

6. Составители программы: Кургалин Сергей Дмитриевич, доктор физико-математических наук, профессор

7. Рекомендована: Научно-методическим советом факультета компьютерных наук (протокол № 6 от 25.06.2018)

8. Учебный год: 2020-2021 **Семестр(ы):** 5

9.Цели и задачи учебной дисциплины: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

10. Место учебной дисциплины в структуре ООП: дисциплина относится к вариативной части блока Б1. Для успешного освоения дисциплины требуется предварительное изучение математического анализа и основ программирования.

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	
ОПК-2	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	знать: проблемы обеспечения безопасности информации, решаемые методами и средствами ЗИ от утечки по техническим каналам; принципы и способы использования существующих средств ЗИ от утечки по техническим каналам; принципы построения перспективных средств ЗИ от утечки по техническим каналам; уметь: применять на практике теоретические знания для обеспечения безопасности информации и для моделирования процессов защиты информации; практически реализовывать защиту информации от утечки по техническим каналам; работать со средствами защиты информации; владеть: техническими средствами защиты информации на объектах информатизации.

12. Объем дисциплины в зачетных единицах/час — 4/144.

Форма промежуточной аттестации: 5 семестр – зачёт с оценкой.

13. Виды учебной работы

Вид учебной работы		Трудоемкость (часы)	
		Всего	По семестрам
			5 сем.
Аудиторные занятия		66	66
в том числе:	лекции	34	34
	практические	16	16
	лабораторные	16	16
Самостоятельная работа		78	78
Экзамен			
Итого:		144	144

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Введение.	Основные понятия и определения. Организационно-правовые аспекты защиты информации. Политика безопасности. Стандартизация в сфере ИТ-безопасности.
1.2	Математические методы и модели в задачах защиты информации.	Криптография. Классификация криптоалгоритмов. Симметричные криптоалгоритмы и криптосистемы. Асимметричные криптоалгоритмы и криптосистемы.
1.3	Многоуровневая защита информации в компьютерных системах и сетях.	Проблемы обеспечения безопасности при удаленном доступе. Методы и средства идентификации и аутентификации. Виртуальные частные сети (VPN). Безопасность сетевых ОС. Виды и классификации атак.
1.4	Квантовые криптографические системы.	Принципы квантовой криптографии. Алгоритмы квантовой криптографии. Алгоритм Беннетта. Квантовый криптоанализ.
2. Лабораторные и практические занятия		
2.1	Введение.	Основные понятия и определения. Организационно-правовые аспекты защиты информации. Политика безопасности. Стандартизация в сфере ИТ-безопасности.
2.2	Математические методы и модели в задачах защиты информации.	Криптография. Классификация криптоалгоритмов. Симметричные криптоалгоритмы и криптосистемы. Асимметричные криптоалгоритмы и криптосистемы.
2.3	Многоуровневая защита информации в компьютерных системах и сетях.	Проблемы обеспечения безопасности при удаленном доступе. Методы и средства идентификации и аутентификации. Виртуальные частные сети (VPN). Безопасность сетевых ОС. Виды и классификации атак.
2.4	Квантовые криптографические системы.	Принципы квантовой криптографии. Алгоритмы квантовой криптографии. Алгоритм Беннетта. Квантовый криптоанализ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Введение.	4	0	0	18	22
2	Математические методы и модели в задачах защиты информации.	10	6	6	20	42
3	Многоуровневая защита информации в компьютерных системах и сетях.	10	6	6	20	42
4	Квантовые криптографические системы.	10	4	4	20	38
	Итого:	34	16	16	78	144

14. Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения практических работ.

Форма организации самостоятельной работы: подготовка к аудиторным занятиям; выполнение домашних заданий; выполнение контрольных работ.

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

а) основная литература:

№ п/п	Источник
1	Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин .— Москва : ДМК Пресс, 2012. — 592 с. URL:http://biblioclub.ru/index.php?page=book&id=231889
2	Башлы, П. Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы ; Е.К. Баранова ; А.В. Бабаш. — Москва : Евразийский открытый институт, 2011. — 375 с. — URL: http://biblioclub.ru/index.php?page=book&id=90539

б) дополнительная литература:

№ п/п	Источник
3	Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков ; Рытов М. Ю. — 3-е изд., стер. — Москва : Флинта, 2011. — 184 с. URL:http://biblioclub.ru/index.php?page=book&id=93343
4	Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. — Москва : ДМК Пресс, 2010. — 544 с. *URL:http://biblioclub.ru/index.php?page=book&id=86475*

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

№ п/п	Источник
5	www.lib.vsu.ru –ЗНБ ВГУ

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

№ п/п	Источник
1	Башлы, П. Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы ; Е.К. Баранова ; А.В. Бабаш. — Москва : Евразийский открытый институт, 2011. — 375 с. — URL: http://biblioclub.ru/index.php?page=book&id=90539

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

18. Материально-техническое обеспечение дисциплины: лекционная аудитория, компьютерный класс с необходимым программным обеспечением.

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)
ОПК-2	Знать: проблемы обеспечения безопасности информации, решаемые методами и средствами ЗИ от утечки по техническим каналам; принципы и способы использования существующих средств ЗИ от утечки по техническим каналам; принципы построения перспективных средств ЗИ от утечки по техническим каналам.	Разделы 1-4	Письменный опрос
	Уметь: применять на практике теоретические знания для обеспечения безопасности информации и для моделирования процессов защиты информации; практически реализовывать защиту информации от утечки по техническим каналам; работать со средствами защиты информации.	Разделы 1-4	Лабораторные работы 1-3
	Владеть: техническими средствами защиты информации на объектах информатизации.	Разделы 1-4	Лабораторные работы 1-3
Промежуточная аттестация			По результатам текущих аттестаций

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

Для оценивания результатов обучения на экзамене используются следующие показатели:

1) знание проблем обеспечения безопасности информации, решаемые методами и средствами ЗИ от утечки по техническим каналам; принципов и способов использования существующих средств ЗИ от утечки по техническим каналам; принципов построения перспективных средств ЗИ от утечки по техническим каналам;

2) умение применять на практике теоретические знания для обеспечения безопасности информации и для моделирования процессов защиты информации; практически реализовывать защиту информации от утечки по техническим каналам; работать со средствами защиты информации;

3) владение техническими средствами защиты информации на объектах информатизации.

Для оценивания результатов обучения на зачёте с оценкой используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Полное соответствие ответа обучающегося всем перечисленным критериям. Обучающийся демонстрирует высокий уровень владения материалом, ориентируется в предметной области, верно отвечает на все дополнительные вопросы.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не соответствует одному или двум из перечисленных показателей, но обучающийся дает правильные ответы на дополнительные вопросы. Допускаются ошибки при воспроизведении части теоретических положений.	Базовый уровень	Хорошо
Ответ на контрольно-измерительный материал не соответствует любым трём из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы. Сформированные знания основных понятий, определений и теорем, изучаемых в курсе, не всегда полное их понимание с затруднениями при воспроизведении.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым четырём из перечисленных показателей. Обучающийся демонстрирует отрывочные знания (либо их отсутствие) основных понятий, определений и теорем, используемых в курсе.	–	Неудовлетворительно

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 Перечень вопросов для письменного опроса

1. Организационно-правовые аспекты защиты информации.
2. Политика безопасности.
3. Стандартизация в сфере ИТ-безопасности.
4. Классификация криптоалгоритмов.
5. Симметричные криптоалгоритмы и криптосистемы.
6. Асимметричные криптоалгоритмы и криптосистемы.
7. Проблемы обеспечения безопасности при удаленном доступе.
8. Методы и средства идентификации и аутентификации.
9. Виртуальные частные сети (VPN).
10. Безопасность сетевых ОС.
11. Виды и классификации атак.
12. Принципы квантовой криптографии.
13. Алгоритмы квантовой криптографии.
14. Алгоритм Беннетта.
15. Квантовый криптоанализ.

19.3.2 Перечень лабораторных работ

1. Алгоритмы симметричного шифрования. Алгоритм DES.
2. Алгоритмы шифрования с открытым ключом. Алгоритм RSA.
3. Квантовые алгоритмы. Алгоритм Гровера GSA.

Типовые задания для лабораторных работ

Лабораторная работа № 1
«Алгоритмы шифрования с открытым ключом. Алгоритм RSA»

Цель работы: изучение принципов работы криптографической системы с открытым ключом на примере алгоритме RSA.
Требования к выполнению работы: выполнение лабораторной работы предусматривает написание программы, реализующей алгоритм RSA, и проверку её работы на контрольном примере. Должен быть разработан интерфейс, удобный для эксплуатации программы, в интерфейсе необходимо предусмотреть режим задания параметров системы по умолчанию и режим генерирования параметров системы.
Отчёт о работе состоит из двух частей. Проводится демонстрация работы программы и объясняется принцип работы алгоритма. По результатам устной защиты требуется написать письменный отчет о лабораторной работе.
Критерии оценки: для получении оценки «зачтено» необходимо показать высокий уровень владения теоретическим материалом, уметь объяснить принцип работы написанной программы, верно ответить на дополнительные вопросы.

Задание: Написать программу, реализующую алгоритм RSA шифрования входного сообщения. Входной файл содержит одну строку текста, который необходимо зашифровать. Выходной файл должен содержать исходный текст, его зашифрованную и вновь расшифрованную версии. В программу включить простейший алгоритм формирования простых чисел и проверки чисел на простоту.

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: письменного опроса и контрольных работ. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования, а также в соответствии с Положением о балльно-рейтинговой системе контроля знаний на факультете компьютерных наук ВГУ.

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