Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Кургалин Сергей Дмитриевич

Кафедра цифровых технологий

25.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.02.02 Методы и средства защиты информации

1. Код и наименование направления подготовки/специальности:

02.03.01 Математика и компьютерные науки

2. Профиль подготовки/специализация:

Квантовая теория информации, Распределенные системы и искусственный интелллект

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра цифровых технологий

6. Составители программы:

Кургалин Сергей Дмитриевич, доктор физико-математических наук, профессор

7. Рекомендована:

протокол НМС ФКН № 5 от 10.03.2021

8. Учебный год:

2023-2024

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 части учебного плана, формируемой участниками образовательных отношений, блок Б1. Для успешного освоения дисциплины необходимо 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) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий.	ПК-1.1 Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий	Знает 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.
ПК-5 Способен участвовать в разработке технической документации программных продуктов и программных комплексов	ПК-5.1 Знает основные стандарты, нормы и правила разработки технической документации программных продуктов и программных комплексов	Знает основные стандарты, нормы и правила разработки технической документации программных продуктов и программных комплексов в области защиты информации.
ПК-5 Способен участвовать в разработке технической документации программных продуктов и программных комплексов	ПК-5.2 Умеет использовать их при подготовке технической документации программных продуктов	Умеет использовать стандарты, нормы и правила при подготовке технической документации программных продуктов для защиты информации.
ПК-5 Способен участвовать в разработке технической документации программных продуктов и программных комплексов	ПК-5.3 Имеет практический опыт подготовки технической документации	Владеет навыками подготовки технической документации в области защиты информации.

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий.	ПК-1.2 Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике	Умеет 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.
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий.	ПК-1.3 Имеет практический опыт научно-исследовательской деятельности в математике и информатике	Владеет техническими средствами защиты информации на объектах информатизации.

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой,Контрольная работа

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 5	Всего
Аудиторные занятия	66	66
Лекционные занятия	34	34
Практические занятия	16	16
Лабораторные занятия	16	16
Самостоятельная работа	42	42
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль		0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Введение.	Основные понятия и определения. Организационно-правовые аспекты защиты информации. Политика безопасности. Стандартизация в сфере ИТ-безопасности.	
2	Математические методы и модели в задачах защиты информации.	Криптография. Классификация криптоалгоритмов. Симметричные криптоалгоритмы и криптосистемы. Асимметричные криптоалгоритмы и криптосистемы.	
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.	
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)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Введение.	4	0	0	6	10
2	Математические методы и модели в задачах защиты информации.	10	6	6	14	36

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
3	Многоуровневая защита информации в компьютерных системах и сетях.	10	6	6	12	34
4	Квантовые криптографические системы.	10	4	4	10	28
		34	16	16	42	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины складывается из аудиторной работы (учебной деятельности, выполняемой под руководством преподавателя) и внеаудиторной работы (учебной деятельности, реализуемой обучающимся самостоятельно).
Аудиторная работа состоит из работы на лекциях и выполнения практических (или лабораторных) заданий в объёме, предусмотренном учебным планом. Лекция представляет собой последовательное и систематическое изложение учебного материала, направленное на знакомство обучающихся с основными понятиями и теоретическими положениями изучаемой дисциплины. Лекционные занятия формируют базу для практических (или лабораторных) занятий, на которых полученные теоретические знания применяются для решения конкретных практических задач. Обучающимся для успешного освоения дисциплины рекомендуется вести конспект лекций и практических (лабораторных) занятий.
Самостоятельная работа предполагает углублённое изучение отдельных разделов дисциплины с использованием литературы, рекомендованной преподавателем, а также конспектов лекций, презентационным материалом (при наличии) и конспектов практических (лабораторных) занятий. В качестве плана для самостоятельной работы может быть использован раздел 13.1 настоящей рабочей программы, в котором зафиксированы разделы дисциплины и их содержание. В разделе 13.2 рабочей программы определяется количество часов, отводимое на самостоятельную работу по каждому разделу дисциплины. Большее количество часов на самостоятельную работу отводится на наиболее трудные разделы дисциплины. Для самостоятельного изучения отдельных разделов дисциплины используется перечень литературы и других ресурсов, перечисленных в пунктах 15 и 16 настоящей рабочей программы.
Успешность освоения дисциплины определяется систематичностью и глубиной аудиторной и внеаудиторной работы обучающегося.
При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

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

№ п/п	Источник
1	Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков ; Министерство образования и науки Российской Федерации ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет» .— Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2017 .— 194 с. : ил. — Библиогр.: с. 190. — http://biblioclub.ru/ .— ISBN 978-5-8265-1737-6 .— <URL:http://biblioclub.ru/index.php?page=book&id=499013>.
2	**Смирнов, В. И.** Защита информации : лабораторный практикум / В.И. Смирнов ; Поволжский государственный технологический университет .— Йошкар-Ола : ПГТУ, 2017 .— 67 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-8158-1866-8 .— <URL:http://biblioclub.ru/index.php?page=book&id=476512>.
3	**Бирюков, А. А.** Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А. А. — 2-е .— Москва : ДМК Пресс, 2017 .— 434 с. — Книга из коллекции ДМК Пресс - Информатика .— ISBN 978-5-97060-435-9 .— <URL:https://e.lanbook.com/book/93278>.

б) дополнительная литература:

№ п/п	Источник
1	**Кирпичников, А. П.** Криптографические методы защиты компьютерной информации : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина ; Министерство образования и науки России ; Казанский национальный исследовательский технологический университет .— Казань : Казанский научно-исследовательский технологический университет, 2016 .— 100 с. : табл., схем. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-7882-2052-9 .— <URL:http://biblioclub.ru/index.php?page=book&id=560536>.
2	**Ищукова, Е. А.** Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова ; Министерство образования и науки РФ ; Южный федеральный университет ; Инженерно-технологическая академия .— Таганрог : Издательство Южного федерального университета, 2016 .— 80 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-9275-2066-4 .— <URL:http://biblioclub.ru/index.php?page=book&id=493059>.
3	**Комаров, С. А.** Правовое регулирование обеспечения информационной безопасности и защиты персональных данных : монография / С.А. Комаров, Е.В. Мицкая ; под ред. С. А. Комарова .— Санкт-Петербург, 2018 .— 169 с. — Библиогр.: с. 129-140. — http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=564652>.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	ЗНБ ВГУ: https://lib.vsu.ru/

№ п/п	Источник
2	Электронно-библиотечная система "Университетская библиотека online": http://biblioclub.ru/
3	Электронно-библиотечная система "Лань": https://e.lanbook.com/
4	Электронно-библиотечная система "Консультант студента": http://www.studmedlib.ru
5	Электронный университет ВГУ: https://edu.vsu.ru/

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков ; Министерство образования и науки Российской Федерации ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет» .— Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2017 .— 194 с. : ил. — Библиогр.: с. 190. — http://biblioclub.ru/ .— ISBN 978-5-8265-1737-6 .— <URL:http://biblioclub.ru/index.php?page=book&id=499013>.

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

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 477

Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 479

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19», мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 505п

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 297

Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 380

Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 290

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27» (12 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 291

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-3220-3,3ГГц, мониторы ЖК 19» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 293

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-8100-3,6ГГц, мониторы ЖК 22» (17 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 295

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 24» (14 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 382

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 383

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i7-9700F-3ГГц, мониторы ЖК 27» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 384

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 22» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 385

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 19» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 301п

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 17» (15 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 303п

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-8100-3,9ГГц, мониторы ЖК 24» (13 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 314п

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-7100-3,6ГГц, мониторы ЖК 19» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7,

Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 316п

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 19» (30 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Разделы 1-4	ПК-1	ПК-1.1	Лабораторная работа
2	Разделы 1-4	ПК-5	ПК-5.1	Лабораторная работа
3	Разделы 1-4	ПК-5	ПК-5.2	Лабораторная работа
4	Разделы 1-4	ПК-5	ПК-5.3	Лабораторная работа
5	Разделы 1-4	ПК-1	ПК-1.2	Лабораторная работа
6	Разделы 1-4	ПК-1	ПК-1.3	Лабораторная работа

Промежуточная аттестация

Форма контроля - Зачет с оценкой

Оценочные средства для промежуточной аттестации

Перечень вопросов для письменного опроса

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:
– лабораторные работы

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.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

– письменный опрос

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.

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