



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
ФГБОУ ВО «Брянский государственный технический
университет» (БГТУ)

Факультет информационных технологий
(наименование факультета/института)

Кафедра «Системы информационной безопасности»
(наименование кафедры, ответственной за реализацию дисциплины)

УТВЕРЖДАЮ
Первый проректор по учебной
работе

_____ В.А. Шкаберин

«19» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА
учебной дисциплины

«Криптографические методы защиты информации»
(наименование дисциплины)

10.05.04 Информационно-аналитические системы безопасности
(код и наименование специальности или направления подготовки)

Автоматизация информационно-аналитической деятельности
(направленность (профиль)/ специализация образовательной программы)

высшее образование – специалитет
(уровень образования)

специалист
(квалификация, присваиваемая по специальности или направлению подготовки)

очная
(форма обучения)

2018
(год набора)

Брянск 2022

Рабочая программа учебной дисциплины
«Криптографические методы защиты информации»

(наименование дисциплины)

10.05.04 Информационно-аналитические системы безопасности

(код и наименование специальности или направления подготовки)

Автоматизация информационно-аналитической деятельности

(направленность (профиль)/специализация образовательной программы)

Разработал(и):

доцент кафедры «СИБ», к.т.н.

(должность, ученая степень, ученое звание)

(подпись)

С.А. Шпичак

(И.О. Фамилия)

(должность, ученая степень, ученое звание)

(подпись)

(И.О. Фамилия)

Рассмотрена и одобрена на заседании кафедры
«Системы информационной безопасности»

(наименование кафедры, ответственной за реализацию дисциплины)

«25» марта 2022 г., протокол № 7

к.т.н., доцент

(ученая степень, ученое звание)

(подпись)

М.Ю. Рытов

(И.О. Фамилия)

Согласовано:

Заведующий выпускающей кафедрой

«Компьютерные технологии и системы»

(наименование выпускающей кафедры)

д.т.н., доцент

(ученая степень, ученое звание)

(подпись)

Аверченков А.В.

(И.О. Фамилия)

© Шпичак С.А. 2022

© ФГБОУ ВО «Брянский государственный
технический университет», 2022

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ.....	5
1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	Ошибка! Закладка не определена.
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ФГОС	Ошибка! Закладка не определена.
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ	Ошибка! Закладка не определена.
4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ	5
5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	Ошибка! Закладка не определена.
5.1. Структура дисциплины.....	Ошибка! Закладка не определена.
5.2. Распределение формируемых компетенций по разделам (темам) дисциплины.....	Ошибка! Закладка не определена.
5.3. Лекции	Ошибка! Закладка не определена.
5.4. Лабораторные работы	Ошибка! Закладка не определена.
5.5. Практические занятия.....	Ошибка! Закладка не определена.
5.6. Самостоятельная работа обучающихся .	Ошибка! Закладка не определена.
5.7. Организация текущего контроля успеваемости и промежуточной аттестации обучающихся	Ошибка! Закладка не определена.
6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ ...	Ошибка! Закладка не определена.
7. РЕАЛИЗАЦИЯ ДИСЦИПЛИНЫ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И (ИЛИ) ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ.....	Ошибка! Закладка не определена.
8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	Ошибка! Закладка не определена.
8.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся	Ошибка! Закладка не определена.
8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Ошибка! Закладка не определена.
8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при изучении дисциплины	Ошибка! Закладка не определена.
8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и (или) информационных справочных систем ..	Ошибка! Закладка не определена.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ **Ошибка! Закладка не определена.**
10. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ..... **Ошибка! Закладка не определена.**
11. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ..**Ошибка! Закладка не определена.**
- 11.1. Методические материалы для педагогических работников **Ошибка! Закладка не определена.**
- 11.2. Методические материалы для обучающихся **Ошибка! Закладка не определена.**
12. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ**Ошибка! Закладка не определена.**
- 12.1. Виды и средства оценивания результатов освоения дисциплины .. **Ошибка! Закладка не определена.**
- 12.2. Шкала оценивания при текущем контроле успеваемости **Ошибка! Закладка не определена.**
- 12.3. Шкала оценивания при промежуточной аттестации обучающихся **Ошибка! Закладка не определена.**
- 12.4. Оценивание окончательных результатов обучения по дисциплине **Ошибка! Закладка не определена.**
- 12.5. Характеристика результатов обучения **Ошибка! Закладка не определена.**
- 12.6. Контрольно-измерительные материалы для текущего контроля успеваемости и промежуточной аттестации обучающихся ... **Ошибка! Закладка не определена.**
13. ВОСПИТАТЕЛЬНАЯ РАБОТА **Ошибка! Закладка не определена.**

ПРЕДИСЛОВИЕ

Учебная дисциплина «Криптографические методы защиты информации» (далее – дисциплина) ориентирована на формирование у обучающихся компетенций в рамках основной профессиональной образовательной программы высшего образования (ОПОП ВО) по направлению подготовки 10.05.04 Информационно-аналитические системы безопасности, профиль «Автоматизация информационно-аналитической деятельности».

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины – обучение основополагающим принципам защиты информации с помощью криптографических методов, грамотному выбору и применению средств криптографической защиты информации в программной и аппаратной реализации, а также ознакомление с перспективами развития синтеза и анализа современных криптографических систем.

Задачи дисциплины:

- формирование основополагающих знаний о криптографических методах и средствах защиты информации,
- формирование представления об основных подходах к реализации криптографических методов и содержанию спецификаций криптографических стандартов,
- получение обучаемыми теоретических знаний и практических навыков прикладной и программной реализации криптографических методов и алгоритмов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ФГОС

Дисциплина входит в базовую часть учебного плана образовательной программы и реализуется на 4 курсе(-ах) в 7 семестре(-ах).

Предварительно изучаются дисциплины: *«Основы информационной безопасности»*.

Параллельно изучаются дисциплины: *«Безопасность операционных систем»*.

Базируются на изучении дисциплины: *«Безопасность электронного документооборота»*.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Изучение дисциплины направлено на формирование у обучающихся компетенций ОПК-7, представленных в таблице 1.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Таблица 2 – Распределение трудоемкости дисциплины по видам учебной работы и семестрам

[illegible]

Виды учебной работы в соответствии с учебным планом образовательной программы	Трудоемкость, час.												
	Всего	Семестр											
		1	2	3	4	5	6	7	8	9	А	В	С
3.3. Зачет с оценкой, семестр		-											
3.4. Курсовой проект (контроль), семестр		-											
3.5. Курсовая работа (контроль), семестр		-											
3.6. Расчетно-графическая работа (контроль), семестр		-											
3.7. Контрольная работа (контроль), семестр		-											
Общая трудоемкость (3 з.е.)		108											

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Структура дисциплины

Структура дисциплины представлена в виде тематического плана в таблице 3.

Таблица 3 – Тематический план дисциплины

Наименование раздела (темы) дисциплины	Трудоемкость, час.				
	Всего	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа
Тема 1. История криптографии.	8	4	0	0	4
Тема 2. Модели шифров	8	4	0	0	4
Тема 3. Криптографическая стойкость	12	2	3	3	4
Тема 4. Имитостойкость и помехоустойчивость шифров	8	2	2	2	2
Тема 5. Принципы построения криптографических алгоритмов	12	2	4	4	2
Тема 6. Синтез шифров	4	2	0	0	2
Тема 7. Схемы шифрования с открытыми ключами	8	2	2	2	2
Тема 8. Криптографические хэш-функции	8	2	2	2	2
Тема 9. Электронная цифровая подпись	8	2	2	2	2
Тема 10. Ключевые системы, криптографические протоколы	13	2	2	2	3
Тема 11. Особенности использования вычислительной техники в криптографии	6	2	0	0	4
Тема 12. Вопросы организации сетей засекретной связи	8	4	0	0	4
Тема 13. Перспективы развития криптографических систем	8	4	0	0	4
Итого	103	34	17	17	35

5.2. Распределение формируемых компетенций по разделам (темам) дисциплины

Распределение формируемых компетенций по разделам дисциплины представлено в таблице 4.

Таблица 4 – Формирование компетенций по разделам дисциплины

Наименование раздела (темы) дисциплины	Код компетенции						
	ОПК -7
Тема 1. История криптографии.	+	+					
Тема 2. Модели шифров	+	+					
Тема 3. Криптографическая стойкость	+						
Тема 4. Имитостойкость и помехоустойчивость шифров	+						
Тема 5. Принципы построения криптографических алгоритмов	+						
Тема 6. Синтез шифров	+						
Тема 7. Схемы шифрования с открытыми ключами	+						
Тема 8. Криптографические хэш-функции	+						
Тема 9. Электронная цифровая подпись	+						
Тема 10. Ключевые системы, криптографические протоколы	+						
Тема 11. Особенности использования вычислительной техники в криптографии	+						
Тема 12. Вопросы организации сетей засекречной связи	+						
Тема 13. Перспективы развития криптографических систем	+						

5.3. Лекции

Перечень занятий лекционного типа, их содержание и трудоемкость представлены в таблице 5.

Таблица 5 – Тематика и содержание лекций

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
Тема 1. История криптографии.	История криптографии.	История криптографии.	4
Тема 2. Модели шифров	Модели шифров	Модели шифров	4
Тема 3. Криптографическая стойкость	Криптографическая стойкость	Криптографическая стойкость	2
Тема 4. Имитостойкость и помехоустойчивость шифров	Имитостойкость и помехоустойчивость шифров	Имитостойкость и помехоустойчивость шифров	2

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
Тема 5. Принципы построения криптографических алгоритмов	Принципы построения криптографических алгоритмов	Принципы построения криптографических алгоритмов	2
Тема 6. Синтез шифров	Синтез шифров	Синтез шифров	2
Тема 7. Схемы шифрования с открытыми ключами	Схемы шифрования с открытыми ключами	Схемы шифрования с открытыми ключами	2
Тема 8. Криптографические хэш-функции	Криптографические хэш-функции	Криптографические хэш-функции	2
Тема 9. Электронная цифровая подпись	Электронная цифровая подпись	Электронная цифровая подпись	2
Тема 10. Ключевые системы, криптографические протоколы	Ключевые системы, криптографические протоколы	Ключевые системы, криптографические протоколы	2
Тема 11. Особенности использования вычислительной техники в криптографии	Особенности использования вычислительной техники в криптографии	Особенности использования вычислительной техники в криптографии	2
Тема 12. Вопросы организации сетей засекречной связи	Вопросы организации сетей засекречной связи	Вопросы организации сетей засекречной связи	4
Тема 13. Перспективы развития криптографических систем	Перспективы развития криптографических систем	Перспективы развития криптографических систем	4
Итого	—	—	34

5.4. Лабораторные работы

Лабораторные работы по дисциплине предусмотрены учебным планом образовательной программы (таблица 6).

Таблица 6 – Тематика лабораторных работ

Наименование темы дисциплины	Тема лабораторной работы	Трудоемкость, час.
Тема 3. Криптографическая стойкость	Определение и оценка расстояния единственности шифров	1
Тема 3. Криптографическая стойкость	Определение рабочей характеристики шифра	2
Тема 4. Имитостойкость и помехоустойчивость шифров	Сравнительная оценка режимов шифрования в отношении распространения искажений	2
Тема 5. Принципы построения криптографических алгоритмов	Программная реализация генераторов ПСП, ИСП	2
Тема 5. Принципы построения криптографических алгоритмов	Программная реализация блочных криптоалгоритмов	2
Тема 7. Схемы шифрования с открытыми ключами	Программная реализация асимметричного шифрования	2
Тема 8. Криптографические хэш-функции	Программная реализация хэш-функций	2
Тема 9. Электронная цифровая подпись	Программная реализация схем ЭЦП	2
Тема 10. Ключевые системы, криптографические протоколы	Схемы предварительного распределения ключей и разделения секрета	2
Итого	–	17

5.5. Практические занятия

Практические занятия по дисциплине предусмотрены учебным планом образовательной программы.

Перечень практических занятий, их содержание и трудоемкость представлены в таблице 7.

Таблица 7 – Тематика и содержание практических занятий

Наименование темы дисциплины	Тема практического занятия	Содержание практического занятия	Трудоемкость, час.
------------------------------	----------------------------	----------------------------------	--------------------

Наименование темы дисциплины	Тема практического занятия	Содержание практического занятия	Трудоемкость, час.
Тема 3. Криптографическая стойкость	Криптографическая стойкость	Криптографическая стойкость	1
Тема 3. Криптографическая стойкость	Криптографическая стойкость	Криптографическая стойкость	2
Тема 4. Имитостойкость и помехоустойчивость шифров	Имитостойкость и помехоустойчивость шифров	Имитостойкость и помехоустойчивость шифров	2
Тема 5. Принципы построения криптографических алгоритмов	Принципы построения криптографических алгоритмов	Принципы построения криптографических алгоритмов	2
Тема 5. Принципы построения криптографических алгоритмов	Принципы построения криптографических алгоритмов	Принципы построения криптографических алгоритмов	2
Тема 7. Схемы шифрования с открытыми ключами	Схемы шифрования с открытыми ключами	Схемы шифрования с открытыми ключами	2
Тема 8. Криптографические хэш-функции	Криптографические хэш-функции	Криптографические хэш-функции	2
Тема 9. Электронная цифровая подпись	Электронная цифровая подпись	Электронная цифровая подпись	2
Тема 10. Ключевые системы, криптографические протоколы	Ключевые системы, криптографические протоколы	Ключевые системы, криптографические протоколы	2
Итого	—	...	17

5.6. Самостоятельная работа обучающихся

Вопросы, выносимые на самостоятельное изучение, представлены в таблице 8.

Таблица 8 – Вопросы для самостоятельного изучения дисциплины

Наименование темы дисциплины	Вопросы для самостоятельного изучения темы
История криптографии	Изучение дополнительной литературы
Модели шифров	Подготовка к лабораторным работам
Криптографическая стойкость	Подготовка к экзамену
Имитостойкость и помехоустойчивость шифров	Изучение дополнительной литературы
Принципы построения криптографических алгоритмов	Подготовка к лабораторным работам
Синтез шифров	Подготовка к экзамену
Системы шифрования с открытыми ключами	Изучение дополнительной литературы
Криптографические хэш-функции	Подготовка к лабораторным работам
Электронная цифровая подпись	Подготовка к экзамену
Ключевые системы, криптографические протоколы	Изучение дополнительной литературы
Особенности использования вычислительной техники в криптографии	Подготовка к лабораторным работам

Наименование темы дисциплины	Вопросы для самостоятельного изучения темы
Вопросы организации сетей засекреченной связи	Подготовка к экзамену
Перспективы развития криптографических систем.	Изучение дополнительной литературы

В процессе самостоятельной работы обучающиеся должны принимать решение по рассматриваемой проблеме с минимальным участием педагогического работника. Для решения поставленных задач может использоваться дополнительная литература и источники в информационно-коммуникационной сети «Интернет». Для закрепления пройденного материала педагогическим работником могут выдаваться домашние задания.

В таблице 9 указаны виды самостоятельной работы, выполняемые обучающимися при изучении соответствующих тем дисциплины.

Таблица 9 – Виды самостоятельной работы

Наименование темы дисциплины	Виды самостоятельной работы
История криптографии	Изучение дополнительной литературы Подготовка к экзамену
Модели шифров	Изучение дополнительной литературы Подготовка к зачету
Криптографическая стойкость	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Имитостойкость и помехоустойчивость шифров	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Принципы построения криптографических алгоритмов	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Синтез шифров	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Системы шифрования с открытыми ключами	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Криптографические хэш-функции	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Электронная цифровая подпись	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету

Наименование темы дисциплины	Виды самостоятельной работы
Ключевые системы, криптографические протоколы	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Особенности использования вычислительной техники в криптографии	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Вопросы организации сетей засекреченной связи	Изучение дополнительной литературы Подготовка к лабораторным и практическим работам Подготовка к зачету
Перспективы развития криптографических систем.	Изучение дополнительной литературы Подготовка к зачету

Учебным планом в рамках дисциплины не предусмотрено выполнение расчетно-графической работы (РГР)/курсовое проектирование.

5.7. Организация текущего контроля успеваемости и промежуточной аттестации обучающихся

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины. Формы контрольно-оценочных мероприятий, проводимых в рамках текущего контроля успеваемости, представлены в таблице 10.

Таблица 10 – Формы и периодичность текущего контроля успеваемости

Вид учебной работы	Форма текущего контроля успеваемости	Периодичность осуществления
Практические занятия / Лабораторные работы	Устный экспресс-опрос, экспресс-тестирование.	На каждом занятии
Самостоятельная работа обучающихся	- устная (устный опрос, защита письменной работы, доклада по результатам самостоятельной работы, рефератов и т.д.); - письменная (письменный опрос, выполнение конспектов, глоссариев, расчетно-графической работы / курсового проекта / курсовой работы и т.д.); - тестовая (бланочное или компьютерное тестирование)	В течение семестра

Оценивание промежуточных и окончательных результатов обучения по дисциплине (промежуточная аттестация обучающихся) осуществляется в форме зачета, проводимого в устной / письменной форме. Аттестационное испытание может включать в себя прохождение теста с использованием технологии компьютерного тестирования. Для уточнения оценки экзаменатор может проводить короткий опрос-собеседование с обучающимся и (или) выдавать ему дополнительные задания.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины применяются следующие образовательные технологии: личностно-ориентированные, активизации деятельности обучающихся, интеллектуальной направленности, проблемного обучения, диалоговые и профессионально-ориентированные (таблица 11).

Таблица 11 – Образовательные технологии, применяемые в ходе преподавания дисциплины

Вид учебной работы	Применяемые образовательные технологии
Лекции	Проблемная лекция. Лекция-визуализация. Лекция-беседа. Лекция-дискуссия.
Практические занятия / Лабораторные работы	Групповые дискуссии. Решение практических задач. Тестирование. Деловая игра.
Самостоятельная работа обучающихся	Проработка лекционного материала. Изучение рекомендуемой литературы. Подготовка к дискуссии. Выполнение практического задания / лабораторной работы. Выполнение расчетно-графической работы. Выполнение курсовой работы (курсового проекта) Подготовка докладов, рефератов Подготовка к лекциям. Подготовка к практическим занятиям. Изучение дополнительной литературы и самостоятельное формирование конспекта. Подготовка к экзамену/зачету/зачету с оценкой
Консультации	Концентрация внимания на отдельных вопросах. Личностно-ориентированный подход. Диалог.
Промежуточная аттестация обучающихся	Зачет (в устной или письменной форме).

7. РЕАЛИЗАЦИЯ ДИСЦИПЛИНЫ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И (ИЛИ) ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

В электронной информационно-образовательной среде БГТУ размещается электронный курс дисциплины, включающий в себя:

- сведения об авторе курса;
- краткое описание курса;
- рабочую программу дисциплины;
- полный перечень тем дисциплины;
- презентационные материалы для проведения занятий лекционного типа;

- лекции/краткий конспект лекций по каждой теме;
- методические указания по выполнению каждого практического задания;
- материалы и тестовые задания для текущего контроля успеваемости и промежуточной аттестации обучающихся.

Наименование электронного курса в электронной информационно-образовательной среде БГТУ — «Криптографические методы защиты информации – автор Шпчак С.А. РПД для обучающихся по направлению подготовки 10.05.04 Информационно-аналитические системы безопасности, профиль «Автоматизация информационно-аналитической деятельности», форма обучения – очная.

Электронный курс предназначен для обеспечения обучающихся всеми необходимыми учебно-методическими материалами, а также проведения контрольно-оценочных мероприятий в процессе обучения. При необходимости осуществляется файловый обмен отчетами о выполнении обучающимися самостоятельной работы.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Рытов М.Ю., Шпчак С.А. Криптографические методы защиты информации. Основные преобразования и параметры криптографических алгоритмов [Текст] + [Электронный ресурс]: Методические указания к выполнению расчетно-графической работы для студентов очной формы обучения по направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –20с.
2. Шпчак С. А. Криптографические методы защиты информации. Определение и оценка расстояния единственности шифров [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.
3. Шпчак С. А. Криптографические методы защиты информации. Определение рабочей характеристики шифра [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.
4. Шпчак С. А. Криптографические методы защиты информации. Сравнительная оценка режимов шифрования в отношении распространения

- искажений [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.
5. Шпичак С. А. Криптографические методы защиты информации. Программная реализация генераторов ПСП, ИСП [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.
 6. Шпичак С. А. Криптографические методы защиты информации. Программная реализация блочных криптоалгоритмов [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.
 7. Шпичак С. А. Криптографические методы защиты информации. Программная реализация асимметричного шифрования [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.
 8. Шпичак С. А. Криптографические методы защиты информации. Программная реализация хэш-функций [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.
 9. Шпичак С. А. Криптографические методы защиты информации. Программная реализация схем ЭЦП [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.
 10. Шпичак С. А. Криптографические методы защиты информации. Схемы предварительного распределения ключей и Темеания секрета [Текст] + [Электронный ресурс]: методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.04 – «Информационно-аналитические системы безопасности» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2017. –18с.

8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература

1. Аверченков В.И. Криптографические методы защиты информации [Текст] + [Электронный ресурс]: учебное пособие/ В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. – Брянск: БГТУ, 2011. – 216 с. – (Серия «Организация и технология защиты информации»)
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос-АРВ, 2001. – 480 с.
3. Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратных полях [Электронный ресурс]: практическое пособие/ Алешников С.И., Козьминых Е.В.— Электрон. текстовые данные.— Калининград: Балтийский федеральный университет им. Иммануила Канта, 2006.— 97 с.— Режим доступа: <http://www.iprbookshop.ru/23851>.— ЭБС «IPRbooks», по паролю.
4. Алешников С.И. Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых [Электронный ресурс]: практическое пособие/ Алешников С.И., Болтнев Ю.Ф.— Электрон. текстовые данные.— Калининград: Балтийский федеральный университет им. Иммануила Канта, 2007.— 58 с.— Режим доступа: <http://www.iprbookshop.ru/23795>.— ЭБС «IPRbooks», по паролю.
5. Лапониная О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс]/ Лапониная О.Р.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 242 с.— Режим доступа: <http://www.iprbookshop.ru/52217>.— ЭБС «IPRbooks», по паролю.

б) дополнительная литература

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с.
2. Фергюсон, Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Диалектика, 2005. – 424 с.
3. Мао В. Современная криптография. Теория и практика / В. Мао. – М.: Вильямс, 2005. – 768 с.
4. Запечников, С. В., Криптографические протоколы и их применение в финансовой и коммерческой деятельности : учеб. пособие для вузов / С. В. Запечников. — М., Горячая линия - Телеком, 2007, 319 с.

5. Лось, А. Б., Криптографические методы защиты информации: учебник для академического бакалавриата / А.Б. Лось, А.Ю. Нестеренко, М.И. Рожков. – 2-е изд., испр. – М.: Издательство Юрайт, 2016. – 473 с. – Серия: Бакалавр. Академический курс.
6. Фомичев, В. М., Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В.М. Фомичев, Д.А. Мельников. – 2-е изд., испр. – М.: Издательство Юрайт, 2016. – 209 с. – Серия: Бакалавр. Академический курс.
7. Фомичев, В. М., Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В.М. Фомичев, Д.А. Мельников. – 2-е изд., испр. – М.: Издательство Юрайт, 2016. – 245 с. – Серия: Бакалавр. Академический курс.
8. Запечников, С. В., Криптографические методы защиты информации: учеб. пособие для академического бакалавриата / С.В. Запечников, О.В. Казарин, А.А. Тарасов. – М.: Издательство Юрайт, 2017. – 309 с. – Серия: Бакалавр. Академический курс.
9. Васильева, И. Н., Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И.Н. Васильева – М.: Издательство Юрайт, 2016. – 349 с. – Серия: Бакалавр. Академический курс.

в) справочная литература

1. С.П.Панасенко. — СПб.: БХВ-Петербург, 2009. — 576 с.: ил.
2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Стандартинформ, 2012. – 33 с.
3. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2012. – 38 с.
4. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 25 с.
5. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 42 с.

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при изучении дисциплины

- 1). Сайт научной библиотеки (<https://libri.tu-bryansk.ru>)
- 2). Электронно-библиотечная система «Лань» (<https://e.lanbook.com>).
- 3). Электронно-библиотечная система «IPRbooks» (<http://www.iprbookshop.ru>).

- 4). Электронно-библиотечная система ИД «Гребенников» (<https://grebennikon.ru>).
- 5). Единое окно доступа к информационным ресурсам (<http://window.edu.ru>).
- 6). Национальная электронная библиотека (<http://www.elibrary.ru>).
- 7). Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» (<http://school-collection.edu.ru>).
- 8). Федеральный Интернет-портал «Российское образование» (<http://www.edu.ru>).
- 9). Официальный сайт технического комитета по стандартизации «Криптографическая защита информации» (ТК 26)// <http://www.tc26.ru>
- 10). Тема документации в области технической защиты информации официального сайта ФСТЭК России// <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty>

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и (или) информационных справочных систем

Операционная система MS Windows.

1. Программы для открытия файлов форматов PDF, DJVU
2. Архиватор WinRar или аналогичный.
3. Интернет-браузер – любой.
4. MS Visual Studio 2012
5. Пакет LibreOffice.
6. Panda Free Antivirus – бесплатный антивирус.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения обучения необходима следующая материально-техническая база:

- аудитория для проведения лекционных занятий и организации защиты курсовых работ/курсовых проектов, оборудованная персональными компьютерами, мультимедийным компьютерным проектором, средства звуковоспроизведения (по возможности), проекционным экраном, наличием доступа в информационно-коммуникационную сеть Интернет;
- компьютерный класс для проведения лабораторных работ с установленным комплектом программного обеспечения и доступом в информационно-коммуникационную сеть интернет, оборудованный мультимедийным компьютерным проектором, средства звуковоспроизведения (по возможности), проекционным экраном / лаборатория со специализированным оборудованием для проведения лабораторных работ;
- учебная аудитория, оснащенная комплектом мебели и доской, для проведения консультаций, зачета, зачета с оценкой, экзамена;

- компьютерные классы с постоянным доступом к информационно-телекоммуникационной сети «Интернет», а также читальные залы научной библиотеки БГТУ для самостоятельной работы обучающихся.

10. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Изучение дисциплины инвалидами и лицами с ограниченными возможностями здоровья организуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При проведении учебных занятий обеспечивается соблюдение следующих требований:

- учебные занятия проводятся для инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся в ходе учебных занятий;
- присутствие ассистента из числа работников БГТУ или привлеченных лиц, оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитывать и оформить задание, общаться с педагогическим работником и т. п.);
- обучающиеся с учетом их индивидуальных особенностей могут пользоваться необходимыми им техническими средствами;
- материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже; наличие специальных кресел и других приспособлений).

Университетом созданы специальные условия для получения высшего образования обучающимися с ОВЗ:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;
- размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых потребностей) справочной информации о расписании учебных занятий (информация должна быть выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);
- присутствие ассистента, оказывающего обучающемуся необходимую помощь;
- обеспечение выпуска альтернативных форматов печатных материалов

(крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию организации;

2) для лиц с ограниченными возможностями здоровья по слуху:

- дублирование звуковой справочной информации о расписании учебных занятий визуальной (установка мониторов с возможностью трансляции субтитров (мониторы, их размеры и количество необходимо определять с учетом размеров помещения);

- обеспечение надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения Университета, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, локальное понижение стоек-барьеров; наличие специальных кресел и других приспособлений).

11. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

11.1. Методические материалы для педагогических работников

Основными формами организации обучения по дисциплине являются лекции, практические занятия и самостоятельная работа обучающихся.

Организация теоретического обучения предполагает использование инновационных технологий проведения занятий лекционного типа, к которым, в частности, относятся: проблемная лекция, лекция-визуализация, лекция-беседа, лекция-дискуссия, лекция-исследование.

1. *Проблемная лекция* предполагает преимущественно всесторонний анализ исторических и социокультурных, образовательных явлений, научный поиск истины. Проблемная лекция опирается на логику последовательно моделируемых проблемных ситуаций путем постановки проблемных вопросов или предъявления проблемных задач.

2. *Лекция-визуализация* реализует принцип наглядности и учит обучающихся преобразовывать устную и письменную информацию в визуальную форму, что формирует у них профессиональное мышление за счет систематизации и выделения наиболее значимых, существенных элементов содержания обучения.

3. *Лекция-беседа* является наиболее распространенной и сравнительно простой формой активного вовлечения обучающихся в учебный процесс. Такая лекция предполагает непосредственный контакт (диалог) педагогического работника с аудиторией.

4. *Лекция-дискуссия*, в которой в отличие от лекции-беседы педагогиче-

ский работник при изложении лекционного материала не только использует ответы обучающихся на свои вопросы, но и организует свободный обмен мнениями в интервалах между логическими разделами.

Организация практических занятий по дисциплине направлена на углубление научно-теоретических знаний обучающихся, формирование практических умений и овладение определенными методами самостоятельной работы.

Практические занятия представляют собой занятия по решению различных прикладных задач, образцы которых были даны на лекциях.

Задачи практических занятий:

- помочь обучающимся систематизировать, закрепить и углубить знания теоретического характера;
- научить обучающихся приемам решения задач из предметной области дисциплины;
- способствовать овладению навыками и умениями, входящих в структуру формируемых компетенций в результате освоения дисциплины;
- научить их работать с информацией, книгой, пользоваться справочной и научной и методической литературой;
- формировать умение учиться самостоятельно, т.е. овладевать методами, способами и приемами самообучения, саморазвития и самоконтроля.

Содержание практических работ составляют:

- устные экспресс-опросы;
- групповые дискуссии;
- выполнение практических заданий;
- письменное или компьютерное экспресс-тестирование и др.

Цели практических занятий наилучшим образом достигаются в том случае, если студент предварительно проработал тематику практического занятия. Поэтому преподаватель должен информировать студентов о теме следующего практического занятия, чтобы они могли целенаправленно самостоятельно заниматься в домашних условиях.

Организация лабораторных занятий по дисциплине направлена на следующие цели и задачи:

- углубление и закрепление знания теоретического курса путем практического изучения в лабораторных условиях изложенных в лекциях законов и положений;
- приобретение навыков в научном экспериментировании, анализе полученных результатов;
- формирование первичных навыков организации, планирования и проведения научных исследований.

Порядок подготовки лабораторного занятия:

- изучение требований программы дисциплины;
- формулировка цели и задач лабораторного занятия;
- разработка плана проведения лабораторного занятия;
- подбор содержания лабораторного занятия;
- разработка необходимых для лабораторного занятия инструкционных карт;
- моделирование лабораторного занятия;
- проверка специализированной лаборатории на соответствие санитарно-гигиеническим нормам, требованиям по безопасности и технической эстетике;
- проверка количества лабораторных мест, необходимых и достаточных для достижения поставленных целей обучения;
- проверка материально-технического обеспечения лабораторных занятий на соответствие требованиям программы дисциплины.

Формы проведения лабораторных занятий:

- фронтальная;
- по циклам;
- индивидуальная;
- смешанная (комбинированная).

При проведении лабораторных работ используют три подхода к их выполнению:

- на основе рецептурных действий обучающихся, когда они проявляют умение работать преимущественно в стандартных условиях, отраженных в руководстве по лабораторному практикуму;
- на основе частично поисковых действий, когда обучающиеся могут действовать достаточно самостоятельно, решать несложные творческие задачи при подсказке или непосредственном руководстве преподавателя;
- на основе активных творческих действий обучающихся, когда они проявляют способность действовать в условиях, близких к реальным, используя запас приобретенных знаний.

Самостоятельная работа обучающихся предполагает аудиторную и внеаудиторную формы организации.

Основными видами самостоятельной работы обучающихся без участия педагогического работника являются: формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.); подготовка к занятиям; составление аннотированного списка статей из соответствующих журналов по отраслям знаний и т.п.; текущий самоконтроль, выполнение расчетно-графической работы/курсового проекта/курсовой работы.

Основными видами самостоятельной работы обучающихся с участием педагогического работника являются: текущие консультации, прием и разбор домашних заданий и др.

При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, консультации преподавателя и др.

11.2. Методические материалы для обучающихся

Обучающимся, изучающим дисциплину, необходимо знать требования, предъявляемые к их различным видам учебных занятий, в том числе лекционным, практическим, индивидуальным и др. (таблица 12).

Таблица 12 – Методические рекомендации обучающимся по освоению дисциплины

Вид учебной работы	Организация деятельности обучающегося
Лекции	Изучение дисциплины следует начинать с прослушивания и конспектирования лекций, перечитывать конспект перед выполнением домашних заданий и практическими занятиями. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать педагогическому работнику на консультации, на практическом занятии. Над конспектами лекций надо работать систематически: первый просмотр рекомендуется сделать вечером того же дня, когда была прочитана лекция, затем просмотреть через 3-4 дня, и сделать это еще раз накануне практического занятия.
Практические занятия	Ознакомление с целью и задачами занятия. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Прослушивание аудио- и видеозаписей по заданной теме. Выполнение (решение) практических заданий и задач по алгоритму, на основе частично поисковой и или исследовательской деятельности и др.
Лабораторные работы	Подготовка к эксперименту (ознакомление с целью и задачами, ходом лабораторной работы, работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, подготовка таблиц для фиксирования хода и результатов опытно-экспериментальной работы и др.). Проведение измерений (вводный и текущий инструктаж, проведение опытов и экспериментов). Обработка полученных результатов; формулировка выводов и написание отчета. Защита отчета по лабораторной работе.
Изучение дополнительной литературы и самостоятельное формирование конспекта	Ознакомление с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в конкретной теме. Составление аннотаций к прочитанным источникам и др. Рефлексия собственных достижений
Подготовка к зачету / зачету с оценкой / экзамену	При подготовке к зачету/зачету с оценкой/экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую

Вид учебной работы	Организация деятельности обучающегося
	литературу, шкалу оценивания и др.

12. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

12.1. Виды и средства оценивания результатов освоения дисциплины

Виды и средства оценивания результатов освоения дисциплины представлены в таблице 13.

Таблица 13 – Виды и средства оценивания результатов освоения дисциплины

Код индикатора достижения компетенции	Оценочные средства текущего контроля успеваемости	Оценочные средства промежуточной аттестации обучающихся
ОПК-7.	1. Устные экспресс-опросы (представлены в ФОС по дисциплине). 2. Экспресс-тестирование (комплекты тестов по темам представлены в ФОС по дисциплине).	Вопросы к экзамену представлены в ФОС по дисциплине.

12.2. Шкала оценивания при текущем контроле успеваемости

Оценивание отдельных видов работ в процессе изучения дисциплины рекомендуется осуществлять с использованием следующей шкалы:

– обучающийся ответил правильно на более, чем 90 % заданных вопросов или вопросов-тестов, выполнил и успешно защитил практические работы, показал отличное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «отлично» (максимальный уровень освоения компетенций);

– обучающийся ответил правильно на 75-89% заданных вопросов или вопросов-тестов, выполнил и защитил практические работы с незначительными замечаниями, показал хорошее владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «хорошо» (средний уровень освоения компетенций);

– обучающийся ответил правильно на 60-74% заданных вопросов или вопросов-тестов, выполнил и защитил практические работы со значительными замечаниями, показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «удовлетворительно» (минимальный уровень освоения компетенций);

– обучающийся ответил правильно на менее, чем 60% заданных вопросов или вопросов-тестов, не выполнил все или выполнил часть практических работ, не защитил или защитил их со значительными замечаниями, при выполнении задания обучающийся не продемонстрировал уровень самостоятельного владения умениями и навыками при решении профессиональных задач в рамках

усвоенного учебного материала и т.д. – «неудовлетворительно» (минимальный уровень освоения компетенций не достигнут).

Критерии и шкала оценки доклада (реферата), его презентации по дисциплине представлены в таблице 14.

Таблица 14 – Критерии и шкала оценки доклада (реферата), его презентации по дисциплине

Оценка	Оцениваемые параметры
«отлично»	Теоретический вопрос раскрыт полностью без смысловых и логических ошибок. Задание решено верно. На защите ответ обучающегося полный и правильный. Обучающийся способен изложить решение задания, сделать собственные выводы, проанализировать основные показатели. В полном объеме представлен соответствующий графический материал.
«хорошо»	Теоретический вопрос раскрыт на достаточно высоком уровне без смысловых и логических ошибок. Задание решено верно. Имеются незначительные недочеты в определении единиц измерения, точности вычислений и т.п. На защите ответ обучающегося в целом полный и правильный. Обучающийся способен изложить решение задания, сделать собственные выводы, проанализировать основные показатели. В полном объеме представлен соответствующий графический материал.
«удовлетворительно»	Теоретический вопрос раскрыт на достаточном уровне, без существенных смысловых и логических ошибок. Задание решено верно, но имеются значительные недочеты в его решении, связанные с неполнотой ответа, с правильным исчислением одних данных и неверным – других и пр. На защите ответ неполный. Обучающийся способен четко изложить решение задания, но допускает неточности в формулировке собственных выводов и анализе основных показателей. В неполном объеме представлен графический материал.
«неудовлетворительно»	Теоретический вопрос не раскрыт или раскрыт не полностью при наличии разного рода неточностей и ошибок. Задание решено со значительными недочетами, с неполными ответами, с неправильным исчислением данных. На защите ответ обучающегося неполный. Обучающийся не способен четко изложить решение задания, допускает неточности в формулировке собственных выводов, не способен проанализировать основные показатели. Графический материал не представлен или представлен не в полном объеме.

В процесс преподавания дисциплины педагогическим работником формируется оценка, характеризующая текущую успеваемость обучающегося.

12.3. Шкала оценивания при промежуточной аттестации обучающихся

При проведении промежуточной аттестации обучающихся в форме зачета используется шкала оценивания, представленная в таблице 15.

Таблица 15 – Шкала оценивания при промежуточной аттестации обучающихся

Уровень освоения (оценка)	Планируемые результаты освоения дисциплины
Высокий (зачтено)	Обучающийся глубоко и прочно усвоил теоретический и практический материал, уверенно это демонстрирует в ходе промежуточной аттестации. Исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе.
Повышенный (зачтено)	Обучающийся знает теоретический и практический материал, грамотно и по существу излагает его в ходе промежуточной аттестации, не допуская существенных неточностей. Правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе.
Базовый (зачтено)	Обучающийся знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине.
Низкий (не зачтено)	Обучающийся не знает на пороговом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине.

12.4. Оценивание окончательных результатов обучения по дисциплине

Итоговая оценка по дисциплине определяется с учетом результатов промежуточной аттестации обучающегося (зачета / экзамена) и оценок, полученных обучающимся в ходе текущего контроля успеваемости в семестре.

12.5. Характеристика результатов обучения

Характеристики результатов обучения по дисциплине в зависимости от полученной обучающимся оценки приведены в таблице 18.

Таблица 18 – Характеристика результатов обучения по дисциплине

Оценка	Характеристика результатов обучения
Зачтено (высокий уровень)	Содержание дисциплины освоено полностью, все цели до-

Оценка	Характеристика результатов обучения
освоения всех индикаторов достижения компетенций в дисциплине)	стигнуты, все предусмотренные программой обучения учебные задания выполнены
Зачтено (повышенный уровень освоения всех индикаторов достижения компетенций в дисциплине)	Содержание дисциплины освоено полностью, все предусмотренные программой обучения учебные задания выполнены с незначительными замечаниями
Зачтено (базовый уровень освоения всех индикаторов достижения компетенций в дисциплине)	Содержание дисциплины освоено частично, большинство предусмотренных программой обучения учебных заданий выполнено, в них имеются ошибки
Не зачтено (низкий уровень освоения всех индикаторов достижения компетенций в дисциплине)	Содержание дисциплины не освоено, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий

12.6. Контрольно-измерительные материалы для текущего контроля успеваемости и промежуточной аттестации обучающихся

Контрольно-измерительные материалы для текущего контроля успеваемости и промежуточной аттестации обучающихся представлены в электронном курсе «Криптографические методы защиты информации», размещенном в системе электронной поддержки учебных курсов на базе программного обеспечения Moodle со встроенной подсистемой тестирования (edu.tu-bryansk.ru), входящей в состав электронной информационно-образовательной среды БГТУ (<http://edu.tu-bryansk.ru>) и «Фонд оценочных средств по дисциплине «Криптографические методы защиты информации».

13. ВОСПИТАТЕЛЬНАЯ РАБОТА

В соответствии с Федеральным законом «Об образовании в Российской Федерации» воспитание - «деятельность, направленная на развитие личности, создание условий для самоопределения и социализации обучающихся на основе социокультурных, духовно-нравственных ценностей и принятых в российском обществе правил и норм поведения в интересах человека, семьи, общества и государства, формирование у обучающихся чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению, взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации, природе и окружающей среде».

В учебном процессе воспитательная работа с обучающимися реализуется средствами учебных дисциплин.

Воспитательная деятельность в ходе преподавания дисциплины направлена на формирование у обучающегося системы убеждений, нравственных

норм и общекультурных качеств, на оказание им помощи в жизненном самоопределении, нравственном, гражданском и профессиональном становлении, на создание условий для самореализации личности. Воспитательная работа также ориентирует обучающихся на будущую профессиональную деятельность, формируя не только личностные, но и профессионально значимые качества.

Воспитательные задачи во время учебных занятий выполняются в скрытой (контекстной) и открытой (целенаправленной) формах. Скрытая форма воспитательной работы представляет собой воздействие всего хода педагогического процесса на становление личностных качеств обучающихся. Например, соблюдение педагогическим работником трудовой дисциплины, демонстрация преданности науке, заинтересованность в успехе обучающихся, правильная речь, хорошие манеры и т.п. имеют положительное воспитательное значение и формируют у обучающихся добросовестность, исполнительность, трудолюбие, ответственность и другие положительные качества. Обучающиеся неосознанно перенимают данные черты у педагогического работника.

Воспитание в открытой форме – это целенаправленное воздействие содержанием учебной дисциплины на становление личности обучающегося. Например, решение проблем и исследовательская работа формируют у обучающихся умение аргументировать, самостоятельно мыслить, стремление к научному поиску, развивают творчество, профессиональные умения.