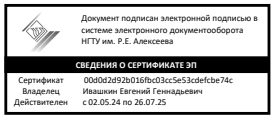
МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева» (НГТУ)

Институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)



УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
“_22___”_____04_____2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.14 Защита информации
(индекс и наименование дисциплины по учебному плану)
для подготовки бакалавров

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность: Вычислительные машины, комплексы, системы и сети, Программное обеспечение средств вычислительной техники и автоматизированных систем

Форма обучения: очная, очно-заочная, заочная

Год начала подготовки 2024, 2025

Выпускающая кафедра ВСТ

Кафедра-разработчик ИСУ

Объем дисциплины 144/4
часов/з.е

Промежуточная аттестация экзамен

Разработчик: Андреева А.Д.., ассистент

Нижний Новгород, 2025

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденного приказом МИНОБРНАУКИ РОССИИ от 19 сентября 2017 года № 929 на основании учебного плана принятого УМС НГТУ, протокол №17 от 28.05.2024 г., протокол №6 от 17.12.2024 г.

Рабочая программа одобрена на заседании кафедры разработчика протокол от 30.03.2025 №9
Зав. кафедрой к.т.н, доцент Тимофеева О.П. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, протокол от 22.04.2025 №3

Рабочая программа зарегистрирована в УМУ, регистрационный № 09.03.01-п-14
Начальник МО _____ Е.Г. Севрюкова

Заведующая отделом комплектования НТБ _____ Н.И. Кабанина
(подпись)

Содержание

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является освоение дисциплинарных компетенций в области методов и средств защиты информации для решения задач профессиональной деятельности.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Защита информации» способствует подготовке студентов к решению следующих профессиональных задач:

1. Анализировать угрозы безопасности информации.
2. Применять программных средств криптографической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Защита информации» Б1.Б.14 включена в обязательный перечень дисци направлению подготовки.

Дисциплина базируется на дисциплинах математического блока и блока программирования программы бакалавриата по направлению «Информатика и вычислительная техника»:

- Информатика,
- Программирование,
- Алгоритмы и структуры данных.

Дисциплина «Защита информации» является основополагающей для преддипломной практики и выполнения выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Защита информации» формирует компетенции ОПК-3 и УК-2 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Наименование дисциплин, формирующих компетенцию совместно	Семестры формирования дисциплины							
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности								
Информатика								
Защита информации								
Выполнение и защита ВКР								
УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений								
Защита информации								
Правоведение								
Преддипломная								
Выполнение и защита ВКР								

Таблица 3.1 – Формирование компетенций дисциплинам

Таблица 3.2 – Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной аттестации**
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИОПК-3.2. Решает стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	***Знать:*** - угрозы информационной безопасности; - методы обеспечения целостности данных; - модели информационной безопасности	***Уметь:*** - защищать информацию от компьютерных вирусов	***Владеть:*** - криптографическими методами защиты информации; - основами правовой защиты информации; - организационными методами защиты информации	Выполнение и сдача 5 лабораторных работ	Вопросы для аттестации – 30 билетов
УК-2.Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИУК-2.3. Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм.	***Знать:*** - правовые нормы в области защиты информации; - закон о защите персональных данных; - отечественный и зарубежный опыт законодательного регулирования информатизации		***Владеть:*** - основами правовой защиты информации; - организационными методами защиты информации.	Выполнение и сдача 5 лабораторных работ	Вопросы для аттестации – 30 билетов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач. ед. 144 часа, распределение часов по видам работ и семестрам представлено в таблицах 4.1, 4.2, 4.3.

Таблица 4.1 – Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очного обучения

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		4 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**57**	**57**
1.1 Аудиторная работа, в том числе:	**51**	**51**
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практ. занятия и др)	-	-
лабораторные работы (ЛР)	17	17
1.2 Внеаудиторная, в том числе	**6**	**6**
курсовая работа (проект) (КР/КП) (консультация, защита)	-	-
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)	2	2
2. Самостоятельная работа (СРС)	**60**	**60**
реферат/эссе (подготовка)	-	-
расчётно-графическая работа (РГР) (подготовка)	-	-
контрольная работа	-	-
курсовая работа/проект (КР/КП) (подготовка)	-	-
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	60	60
Подготовка к экзамену	27	27

Таблица 4.2 – Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очно-заочного обучения

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		4 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**40**	**40**
1.1 Аудиторная работа, в том числе:	**34**	**34**
занятия лекционного типа (Л)	17	17
занятия семинарского типа (ПЗ-семинары, практ. занятия и др)	-	-
лабораторные работы (ЛР)	17	17
1.2 Внеаудиторная, в том числе	**6**	**6**
курсовая работа (проект) (КР/КП) (консультация, защита)	-	-
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)	2	2
2. Самостоятельная работа (СРС)	**77**	**77**
реферат/эссе (подготовка)	-	-

расчётно-графическая работа (РГР) (подготовка)	-	-
контрольная работа	-	-
курсовая работа/проект (КР/КП) (подготовка)	-	-
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	77	77
Подготовка к экзамену	27	27

Таблица 4.3 – Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов заочного обучения

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		8 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**24**	**24**
1.1 Аудиторная работа, в том числе:	**18**	**18**
занятия лекционного типа (Л)	6	6
занятия семинарского типа (ПЗ-семинары, практ. занятия и др)	6	6
лабораторные работы (ЛР)	6	6
1.2 Внеаудиторная, в том числе	**6**	**6**
курсовая работа (проект) (КР/КП) (консультация, защита)	-	-
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)	2	2
2. Самостоятельная работа (СРС)	**111**	**111**
реферат/эссе (подготовка)	-	-
расчётно-графическая работа (РГР) (подготовка)	-	-
контрольная работа	-	-
курсовая работа/проект (КР/КП) (подготовка)	-	-
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	111	111
Подготовка к экзамену	9	9

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.3 – Содержание дисциплины, структурированное по темам для студентов очного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
4 семестр										
Раздел 1. Введение										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 1.1.** Введение в информационную безопасность. Угрозы ИБ.	2				2	Подготовка к лекциям [6.1.1, 6.2.1]			
	Тема 1.2. Введение в криптографию. Исторические шифры.	1				1	Подготовка к лекциям [6.1.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		
	Лабораторная работа. Классические криптосистемы.		2			6	Подготовка к лабораторной работе [6.3.1]			
	Итого по 1 разделу	**3**	**2**	**-**	**-**	**9**				
Раздел 2. Криптографические методы защиты информации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 2.1.** Симметричные криптосистемы.	4			1	2	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		
	Тема 2.2. Ассиметричные криптосистемы.	4			0,5	2	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы			
	Тема 2.3. Алгоритмы ХЭШ-функции и электронной цифровой подписи.	2			1	2	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы			

	Лабораторная работа. Алгоритмы симметричного шифрования.		4			6	Подготовка к лабораторной работе [6.3.1]			
	Лабораторная работа. Алгоритмы асимметричного шифрования.		4			8	Подготовка к лабораторной работе [6.3.1]			
	Лабораторная работа. Алгоритмы хэширования.		3			2	Подготовка к лабораторной работе [6.3.1]			
	Итого по 2 разделу	**10**	**11**	**-**	**2,5**	**22**				
Раздел 3. Правовая защита информации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 3.1.** Нормативные документы и законы РФ в области информационной безопасности.	1				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 3.2. Законодательное регулирование информатизации за рубежом.	1				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 3.3. Защита персональных данных.	2			0,5	1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 3 разделу	**4**	**-**	**-**	**0,5**	**3**				
Раздел 4. Политики и модели информационной безопасности										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 4.1.** Политики и модели разграничения доступа. Дискреционная политика. Мандатная политика. Ролевая политика.	2				2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 4 разделу	**2**	**-**	**-**	**-**	**2**				
Раздел 5. Методы аутентификации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 5.1.** Принципы защиты от несанкционированного доступа. Методы опознавание пользователей.	1				1	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		

	Тема 5.2. Механизмы реализации надежных паролей.	2			0,5	2	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы			
	Лабораторная работа. Алгоритмы формирования электронной цифровой подписи.		4			8	Подготовка к лабораторной работе [6.3.1]			
	Итого по 5 разделу	**3**	**4**	**-**	**0,5**	**11**				
Раздел 6. Социальные аспекты защиты информации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 6.1.** Социальная инженерия	2			0,5	2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Тема 6.2. Информационные войны	2				2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 6 разделу	**4**	**-**	**-**	**0,5**	**4**				
Раздел 7. Компьютерные вирусы										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 7.1.** Программы-вирусы. История проблемы	1				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 7.2. Типы компьютерных вирусов	2				2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 7.3. Средства антивирусной защиты	1				2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Итого по 7 разделу	**4**	**-**	**-**	**-**	**5**				
Раздел 8. Политики и модели информационной безопасности										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 8.1.** Физическая безопасность и безопасность окружения	1				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 8.2. Защищенное проектирование зданий и ландшафта	1				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 8.3. Внутренние системы поддержки и снабжения	1				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 8.4.	1				1	Подготовка к лекциям			

	Обеспечение безопасности периметра						[6.1.2, 6.2.1, 6.2.2]			
	Итого по 8 разделу	**4**	**-**	**-**	**-**	**4**				
	Подготовка к экзамену (контроль)	-	-	-	**2**	**27**				
	Итого	**34**	**17**	**-**	**6**	**60**				

Таблица 4.4 – Содержание дисциплины, структурированное по темам для студентов очно-заочного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	**Наименование разделов, тем**	**Виды учебной работы (час)**					**Вид СРС**	**Наименование используемых активных и интерактивных образовательных технологий**	**Реализация в рамках Практической подготовки (трудоемкость в часах)**	**Наименование разработанного Электронного курса (трудоемкость в часах)**
		Контактная работа				**Самостоятельная работа студентов (час)**				
		Лекции (час)	**Лабораторные работы (час)**	**Практические занятия (час)**	**КСР**					
4 семестр										
Раздел 1. Введение										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 1.1.** Введение в информационную безопасность. Угрозы ИБ.	1				2	Подготовка к лекциям [6.1.1, 6.2.1]			
	Тема 1.2. Введение в криптографию. Исторические шифры.	0,5				4	Подготовка к лекциям [6.1.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		
	Лабораторная работа. Классические криптосистемы.		2			6	Подготовка к лабораторной работе [6.3.1]			
	Итого по 1 разделу	**1,5**	**2**	**-**	**-**	**12**				
Раздел 2. Криптографические методы защиты информации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 2.1.** Симметричные криптосистемы.	2			1	2	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		
	Тема 2.2. Ассиметричные криптосистемы.	2			0,5	2	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной			

							работы			
	Тема 2.3. Алгоритмы ХЭШ-функции и электронной цифровой подписи.	1			1	2	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы			
	Лабораторная работа. Алгоритмы симметричного шифрования.		4			6	Подготовка к лабораторной работе [6.3.1]			
	Лабораторная работа. Алгоритмы асимметричного шифрования.		4			8	Подготовка к лабораторной работе [6.3.1]			
	Лабораторная работа. Алгоритмы хэширования.		3			2	Подготовка к лабораторной работе [6.3.1]			
	Итого по 2 разделу	**5**	**11**	**-**	**2,5**	**22**				
Раздел 3. Правовая защита информации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 3.1.** Нормативные документы и законы РФ в области информационной безопасности.	0,5				2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 3.2. Законодательное регулирование информатизации за рубежом.	0,5				2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 3.3. Защита персональных данных.	1			0,5	2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 3 разделу	**2**	**-**	**-**	**0,5**	**6**				
Раздел 4. Политики и модели информационной безопасности										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 4.1.** Политики и модели разграничения доступа. Дискреционная политика. Мандатная политика. Ролевая политика.	1				6	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 4 разделу	**1**	**-**	**-**	**-**	**6**				
Раздел 5. Методы аутентификации										

ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 5.1.** Принципы защиты от несанкционированного доступа. Методы опознавание пользователей.	0,5				3	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		
	Тема 5.2. Механизмы реализации надежных паролей.	1			0,5	5	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы			
	Лабораторная работа. Алгоритмы формирования электронной цифровой подписи.		4			8	Подготовка к лабораторной работе [6.3.1]			
	Итого по 5 разделу	**1,5**	**4**	**-**	**0,5**	**16**				
Раздел 6. Социальные аспекты защиты информации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 6.1.** Социальная инженерия	1			0,5	4	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Тема 6.2. Информационные войны	1				4	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 6 разделу	**2**	**-**	**-**	**0,5**	**8**				
Раздел 7. Компьютерные вирусы										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 7.1.** Программы-вирусы. История проблемы	0,5				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 7.2. Типы компьютерных вирусов	1				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 7.3. Средства антивирусной защиты	0,5				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Итого по 7 разделу	**2**	**-**	**-**	**-**	**3**				
Раздел 8. Политики и модели информационной безопасности										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 8.1.** Физическая безопасность и безопасность окружения	0,5				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 8.2. Защищенное проектирование зданий и	0,5				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			

	ландшафта									
	Тема 8.3. Внутренние системы поддержки и снабжения	0,5				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 8.4. Обеспечение безопасности периметра	0,5				1	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Итого по 8 разделу	**2**	**-**	**-**	**-**	**4**				
	Подготовка к экзамену	-	-	-	**2**	**27**				
	Итого	**17**	**17**	**-**	**6**	**77**				

Таблица 4.5 – Содержание дисциплины, структурированное по темам для студентов заочного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	**Наименование разделов, тем**	**Виды учебной работы (час)**					**Вид СРС**	**Наименование используемых активных и интерактивных образовательных технологий**	**Реализация в рамках Практической подготовки (трудоемкость в часах)**	**Наименование разработанного Электронного курса (трудоемкость в часах)**
		Контактная работа				**Самостоятельная работа студентов (час)**				
		Лекции (час)	**Лабораторные работы (час)**	**Практические занятия (час)**	**КСР**					
8 семестр										
Раздел 1. Введение										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 1.1.** Введение в информационную безопасность. Угрозы ИБ.	0,5				4	Подготовка к лекциям [6.1.1, 6.2.1]			
	Тема 1.2. Введение в криптографию. Исторические шифры.	0,5		0,5		2	Подготовка к лекциям [6.1.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		
	Лабораторная работа. Классические криптосистемы.		1			8	Подготовка к лабораторной работе [6.3.1]			
	Итого по 1 разделу	**1**	**1**	**0,5**	**-**	**14**				
Раздел 2. Криптографические методы защиты информации										

ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 2.1.** Симметричные криптосистемы.	1		0,5	1	6	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		
	Тема 2.2. Ассиметричные криптосистемы.	1		0,5		6	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы			
	Тема 2.3. Алгоритмы ХЭШ-функции и электронной цифровой подписи.			0,5		4	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы			
	Лабораторная работа. Алгоритмы симметричного шифрования.		1			6	Подготовка к лабораторной работе [6.3.1]			
	Лабораторная работа. Алгоритмы асимметричного шифрования.		2			6	Подготовка к лабораторной работе [6.3.1]			
	Лабораторная работа. Алгоритмы хэширования.		2			4	Подготовка к лабораторной работе [6.3.1]			
	Итого по 2 разделу	**2**	**5**	**1,5**	**1**	**32**				
Раздел 3. Правовая защита информации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 3.1.** Нормативные документы и законы РФ в области информационной безопасности.	0,25				4	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 3.2. Законодательное регулирование информатизации за рубежом.	0,25				2	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 3.3. Защита персональных данных.			0,5	1	6	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 3 разделу	**0,5**	**-**	**0,5**	**1**	**12**				
Раздел 4. Политики и модели информационной безопасности										

ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 4.1.** Политики и модели разграничения доступа. Дискреционная политика. Мандатная политика. Ролевая политика.			0,5		7	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 4 разделу	**-**	**-**	**0,5**	**-**	**7**				
Раздел 5. Методы аутентификации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 5.1.** Принципы защиты от несанкционированного доступа. Методы опознавание пользователей.			0,5		4	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций		
	Тема 5.2. Механизмы реализации надежных паролей.			0,5	1	6	Подготовка к лекциям [6.1.2, 6.2.2], работа над заданием лабораторной работы			
	Итого по 5 разделу	**-**	**-**	**1**	**1**	**10**				
Раздел 6. Социальные аспекты защиты информации										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 6.1.** Социальная инженерия	0,5			1	6	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Тема 6.2. Информационные войны	0,5				6	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]	Разбор конкретных ситуаций		
	Итого по 6 разделу	**1**	**-**	**-**	**1**	**12**				
Раздел 7. Компьютерные вирусы										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 7.1.** Программы-вирусы. История проблемы	0,5				4	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 7.2. Типы компьютерных вирусов			**1**		4	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 7.3. Средства антивирусной защиты			**1**		4	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Итого по 7 разделу	**0,5**	**-**	**2**	**-**	**12**				
Раздел 8. Политики и модели информационной безопасности										
ОПК-3 - ИОПК-3.2 УК-2 - ИУК-2.3	**Тема 8.1.** Физическая безопасность и	0,25				3	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			

	безопасность окружения									
	Тема 8.2. Защищенное проектирование зданий и ландшафта	0,25				3	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 8.3. Внутренние системы поддержки и снабжения	0,25				3	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Тема 8.4. Обеспечение безопасности периметра	0,25				3	Подготовка к лекциям [6.1.2, 6.2.1, 6.2.2]			
	Итого по 8 разделу	**1**	**-**	**-**	**-**	**12**				
	Подготовка к экзамену (контроль)	-	-	-	**2**	**9**				
	Итого	**6**	**6**	**6**	**6**	**111**				

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

1. Примерный перечень вопросов при защите лабораторных работ:

- Что такое шифр замены? Приведите примеры.
- В чем разница между моноалфавитными и полиалфавитными шифрами замены?
- Как работает шифр Цезаря? Каков его ключ?
- Какие уязвимости есть у шифров замены? Как их можно взломать?
- Как можно усилить стойкость шифра замены?
- Опишите структуру алгоритма DES. Каков размер блока и ключа?
- Какие основные этапы выполняются в одном раунде DES?
- Что такое S-блоки и как они работают в DES?
- Какие режимы работы DES вы знаете? Чем отличается ECB от CBC?
- Почему DES считается устаревшим? Какие его модификации существуют?
- Каковы основные характеристики шифра «Кузнечик» (размер блока, ключа)?
- В чем отличие «Кузнечика» от DES и AES?
- Как устроен раунд шифрования в «Кузнечике»?
- Какие преимущества у «Кузнечика» перед другими алгоритмами?
- Где применяется шифр «Кузнечик» в российской криптографии?
- В чем суть алгоритма RSA? Как происходит шифрование и расшифрование?
- Как выбираются параметры RSA (простые числа, открытый и закрытый ключи)?
- Какие атаки возможны на RSA и как от них защититься?
- Как используется RSA в электронной цифровой подписи (ЭЦП)?
- В чем отличие RSA от алгоритмов симметричного шифрования?
- Какие криптографические алгоритмы лежат в основе ГОСТ Р 34.10-2018?
- Как формируется подпись в ГОСТ Р 34.10-2018?
- В чем отличие ГОСТ Р 34.10-2018 от предыдущих версий (например, ГОСТ Р 34.10-2012)?
- Какие преимущества у российской ЭЦП перед RSA?
- Где применяется ГОСТ Р 34.10-2018 в государственных и коммерческих системах?

2. Примерный перечень вопросов для экзамена:

- Что такое политика информационной безопасности?
- Какие существуют уровни защиты информации?
- Что регулирует Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации"?
- Какие требования к защите информации содержит ГОСТ Р 57580?
- Какие организации в России отвечают за регулирование ИБ?
- Что такое APT-атаки и чем они опасны?
- Как классифицируются угрозы по источнику возникновения?
- Что такое Zero-day уязвимость?
- Какие методы устранения уязвимостей вы знаете?
- Как уязвимости связаны с атаками на информационные системы?
- Как применяется шифрование для защиты от НСД?
- Какие существуют системы обнаружения вторжений (IDS/IPS)?

- Как работают одноразовые пароли (TOTP, HOTP)?
- Что такое OAuth и OpenID Connect?
- Какие уязвимости есть у парольной аутентификации?
- Какие атаки возможны на моноалфавитные шифры?
- В чем отличие между перестановочными и заменяющими шифрами?
- Какие алгоритмы используют сеть Фейстеля (DES, ГОСТ 28147-89)?
- В чем преимущества и недостатки сети Фейстеля?
- Как обеспечивается обратимость шифрования в сети Фейстеля?
- Какие режимы обеспечивают не только шифрование, но и аутентификацию (GCM)?
- В каких случаях применяется режим OFB?
- Что такое алгоритм Диффи-Хеллмана и для чего он применяется?
- Какие преимущества и недостатки у асимметричного шифрования?
- Как применяется гибридное шифрование (SSL/TLS)?
- В чем отличие между ЭЦП и MAC (Message Authentication Code)?
- Какие атаки возможны на системы ЭЦП?
- Что такое "коллизия" в хеш-функциях?
- Где применяются хеш-функции в криптографии?
- Какие российские стандарты хеширования вы знаете (ГОСТ Р 34.11)?

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информатика и системы управления».

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется **традиционная** система, при которой успеваемость студентов оценивается по четырехбалльной шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.1 – Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Критерии оценивания результатов обучения**			
		Оценка **«неудовлетворительно»** / «не зачтено» 0-59% от max рейтинговой оценки контроля	Оценка **«удовлетворительно»** / «зачтено» 60-74% от max рейтинговой оценки контроля	Оценка **«хорошо» /** «зачтено» 75-89% от max рейтинговой оценки контроля	Оценка **«отлично» /** «зачтено» 90-100% от max рейтинговой оценки контроля
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИОПК-3.2. Решает стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы защиты информации; не во всех случаях правильно оперирует основными понятиями по информационной безопасности; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципы защиты информации; не во всех случаях находит правильные ответы на задаваемые вопросы по методам и средствам защиты информации	Знает методы и средства защиты информации на достаточно хорошем уровне; представляет основные концепции контроля целостности; подтверждает теоретические знания отдельными практическими примерами; дает ответы на задаваемые вопросы по методам и средствам защиты информации	Имеет глубокие знания по методам и средствам защиты информации; дает развернутые ответы на задаваемые вопросы
УК-2.Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИУК-2.3. Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм.	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы защиты информации; не во всех случаях правильно оперирует основными понятиями по информационной безопасности; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципы защиты информации; не во всех случаях находит правильные ответы на задаваемые вопросы по методам и средствам защиты информации	Знает методы и средства защиты информации на достаточно хорошем уровне; представляет основные концепции контроля целостности; подтверждает теоретические знания отдельными практическими примерами; дает ответы на задаваемые вопросы по методам и средствам защиты информации	Имеет глубокие знания по методам и средствам защиты информации; дает развернутые ответы на задаваемые вопросы

Таблица 5.2 – Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформулировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «**неудовлетворительно»** заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401. — Режим доступа: для авториз. пользователей.

6.1.2. Борисова, С. Н. Криптографические методы защиты информации: классическая криптография : учебное пособие / С. Н. Борисова. — Пенза : ПГУ, 2018. — 186 с. — ISBN 978-5-907102-51-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/162235Волкова, С. С. Введение в машинное обучение. Линейные модели: учебное пособие / С. С. Волкова. — Вологда: Вологод, 2023. — 76 с. — ISBN 978-5-907606-46-3. — URL: https://elibrary.ru/item.asp?id=50732254

6.2 Справочно-библиографическая литература

6.2.1. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184. — Режим доступа: для авториз. пользователей

6.2.2. Прохорова, О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 124 с. — ISBN 978-5-8114-8924-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/185333

6.3 Методические указания, рекомендации и другие материалы к занятиям

6.3.1. Методические указания к лабораторным работам по дисциплине «Защита информации» [Электронные текстовые данные]: метод. указания к лаб. работе по дисциплине «Защита информации» для студентов направления подготовки бакалавра 09.03.01 «Информатика и вычислительная техника» дневной формы обучения / НГТУ; Сост.: С. Н. Капранов. Н.Новгород, 2021, 76 с.

Электронные варианты всех методических указаний отправляются на электронные адреса групп.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебный процесс по дисциплине обеспечен необходимым комплектом свободно распространяемого программного обеспечения (состав по дисциплине определен в настоящей РПД и подлежит обновлению при необходимости).

7.1 Перечень информационных справочных систем

Таблица 7.1 – Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	Консультант студента	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	Юрайт	https://biblio-online.ru/
4	TNT-ebook	https://www.tnt-ebook.ru/

7.2 Перечень свободно распространяемого программного обеспечения

Таблица 7.2 – Программное обеспечение, используемое студентами очного обучения

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
-	Adobe Acrobat Reader (https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html)
	Linux (https://www.linux.com/)
	OpenOffice (FreeWare) https://www.openoffice.org/ru/
	JDK 8 и выше (https://adoptopenjdk.net/)
	Фреймворк Java Spring 5 (https://spring.io/projects/spring-framework)
	Eclipse (https://www.eclipse.org/) Intellij Idea (https://www.jetbrains.com/ru-ru/idea/)
	git (https://git-scm.com/), github (https://github.com/)
	Maven (https://maven.apache.org/), Gradle (https://gradle.org/)
	Редактор блок-схем (https://app.diagrams.net/)

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 7.4 указан перечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

В данном разделе могут быть приведены ресурсы (ссылки на сайты), на которых можно найти полезную для курса информацию, в т.ч. статистические или справочные данные, учебные материалы, онлайн курсы и т.д.

Таблица 7.4 – Перечень современных профессиональных баз данных и информационных справочных систем

№	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета)

1	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
2	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
3	Каталог паттернов проектирования	https://refactoring.guru/ru/design-patterns/catalog

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть использована информация, размещенная в подразделе «Доступная среда» специализированного раздела сайта НГТУ «Сведения об образовательной организации» https://www.nntu.ru/sveden/accenv/

Таблица 8.1 – Образовательные ресурсы для инвалидов и лиц с ОВЗ

№	Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
1	ЭБС «Консультант студента»	озвучка книг и увеличение шрифта
2	ЭБС «Лань»	специальное мобильное приложение - синтезатор речи, который воспроизводит тексты книг и меню навигации
3	ЭБС «Юрайт»	версия для слабовидящих

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Для контактной и самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

- зал электронно-информационных ресурсов (ауд. 2210 – 11 компьютеров, ауд. 6119 – 9 компьютеров);
- читальный зал открытого доступа (ауд. 6162 – 2 компьютера);
- ауд. 2303, 2202, оборудованные Wi-Fi.

Перечень материально-технического обеспечения, необходимого для реализации программы бакалавриата для студентов очного обучения, включает в себя компьютерные классы.

1. Ауд. 4408 кафедры «Информатика и системы управления» – лаборатория Информационных технологий

Компьютеры, оснащенные необходимым оборудованием, техническими и электронными средствами обучения и контроля знаний студентов:

- 8 рабочих мест на базе тонких клиентов DellWise,
- мультимедийный проектор BenQ PB6240,
- ноутбук Lenovo V130-151KB,
- стенд для изучения автоматических систем управления на базе блока MyRio с FPGA под управлением LabView.

Пакеты ПО (лицензионное):

- Dr.Web (с/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024).

Пакеты ПО (распространяемое по свободной лицензии):

- Apache OpenOffice;
- Linux Ubuntu 20.04 (https://releases.ubuntu.com/20.04/)
- git (https://git-scm.com/)
- Microsoft Visual Studio 2017 Community Edition (https://visualstudio.microsoft.com/ru/vs/community/)

Также, для самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

Таблица 9.1 – Оснащенность аудиторий и помещений для самостоятельной работы студентов по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	**6421** учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации; г. Нижний Новгород, Казанское ш., 12	1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250 Ggb, SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента – 74 7. Рабочее место для преподавателя – 1 шт.	1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (с/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024)
2	**6543** компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), г. Нижний Новгород, Казанское ш., 12)	1. Рабочие места студента, оснащенные ПК на базе Intel Core i5 с мониторами – 8 шт. 2. Рабочие места студента, оснащенные ПК на базеCore 2 Duo с мониторами – 2 шт. 3. Рабочее место преподавателя, оснащенное ПК на базе Intel Core i5 с монитором – 1 шт. 4. Проектор Accer, проекционный экран – 1 шт. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета 5. Принтер HP LaserJet 1200 – 1 шт.	1. Microsoft Windows 7 MSDN реквизиты договора - подписка DreamSpark Premium, договор № 0509/КМР от 15.10.18 2. Бесплатное ПО: Пакет программ Open Office, True Conf, Браузер Google Chrome, Браузер Mozilla Firefox, Браузер Opera, McAfee Security Scan, Adobe Acrobat Reader DC, AutoCAD2013

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При преподавании дисциплины «Защита информации», используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Весь лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала. Электронные материалы лекций в период дистанционного обучения отправляются по электронной почте на адреса групп и могут быть получены до чтения лекций и проработаны студентами в ходе самостоятельной работы.

На лекциях, практических занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием, подробно разбираются на практических занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom.

Инициируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента, рекомендуются методы успешного самостоятельного усвоения материала в зависимости от уровня его базовой подготовки.

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется традиционная система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме экзамена с учетом текущей успеваемости.

Результат обучения считается сформированным на повышенном уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент исчерпывающе, последовательно, четко и логически излагает учебный материал; свободно справляется с заданиями, вопросами, использует в ответе дополнительный материал. Все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты, проявляет самостоятельность при выполнении заданий.

Результат обучения считается сформированным на пороговом уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент последовательно, четко и логически излагает учебный материал; справляется с заданиями, вопросами, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже трех по оценочной системе, что соответствует пороговому уровню.

10.2 Методические указания для занятий лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины (Таблицы 4.3, 4.4, 4.5). Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным занятиям и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3 Методические указания по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом подлежит защите у преподавателя.

При оценивании лабораторных работ учитывается следующее:

- качество выполнения практической части работы и степень соответствия результатов работы заданным требованиям;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

10.4 Методические указания по освоению дисциплины на практических занятиях

Практические занятия представляют собой перечень заданий, которые охватывают основные разделы дисциплины, изложенные в тематическом плане. Цель практических занятий − углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать освоению необходимых компетенций.

10.5 Методические указания по освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом.

10.6 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных в Разделе 9. В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

11.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе контроля текущей успеваемости

Для текущего контроля знаний студентов по дисциплине проводится комплексная оценка знаний, включающая

- защиту лабораторных работ.

11.1.1. Типовые задания для лабораторных работ

Типовые задания для лабораторных работ приведены в учебно-методических указаниях по проведению лабораторных работ.

11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине

11.2.1. Защита курсового проекта/ работы

Курсовая работа не предусмотрена учебным планом.

11.2.2. Экзамен для студентов очной и очно-заочной формы обучения в 4 семестре, для студентов заочной формы – в 8 семестре. Проводится в виде устного собеседования по типовым вопросам.

Типовые вопросы для промежуточной аттестации в форме экзамена для студентов всех форм обучения:

1. Что такое политика информационной безопасности?
2. Какие существуют уровни защиты информации?
3. Что регулирует Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации"?
4. Какие требования к защите информации содержит ГОСТ Р 57580?
5. Какие организации в России отвечают за регулирование ИБ?
6. Что такое APT-атаки и чем они опасны?
7. Как классифицируются угрозы по источнику возникновения?
8. Что такое Zero-day уязвимость?
9. Какие методы устранения уязвимостей вы знаете?
10. Как уязвимости связаны с атаками на информационные системы?
11. Как применяется шифрование для защиты от НСД?
12. Какие существуют системы обнаружения вторжений (IDS/IPS)?
13. Как работают одноразовые пароли (TOTP, HOTP)?
14. Что такое OAuth и OpenID Connect?
15. Какие уязвимости есть у парольной аутентификации?
16. Какие атаки возможны на моноалфавитные шифры?
17. В чем отличие между перестановочными и заменяющими шифрами?
18. Какие алгоритмы используют сеть Фейстеля (DES, ГОСТ 28147-89)?
19. В чем преимущества и недостатки сети Фейстеля?
20. Как обеспечивается обратимость шифрования в сети Фейстеля?
21. Какие режимы обеспечивают не только шифрование, но и аутентификацию (GCM)?
22. В каких случаях применяется режим OFB?
23. Что такое алгоритм Диффи-Хеллмана и для чего он применяется?
24. Какие преимущества и недостатки у асимметричного шифрования?
25. Как применяется гибридное шифрование (SSL/TLS)?
26. В чем отличие между ЭЦП и MAC (Message Authentication Code)?
27. Какие атаки возможны на системы ЭЦП?

28. Что такое "коллизия" в хеш-функциях?
29. Где применяются хеш-функции в криптографии?
30. Какие российские стандарты хеширования вы знаете (ГОСТ Р 34.11)?

В полном объеме оценочные средства имеются на кафедре «Информатика и системы управления». Оценочные средства могут быть получены по требованию.