

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

Учебно-научный институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)

УТВЕРЖДАЮ:
Директор института:
_____ Мякинников А.В.
подпись ФИО
22 апреля 2023г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.Б.32 Основы информационной безопасности
(индекс и наименование дисциплины по учебному плану)
для подготовки специалистов

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

Направленность: Безопасность открытых информационных систем

Форма обучения: очная

Год начала подготовки 2022

Выпускающая кафедра ИБВСС

Кафедра-разработчик ИБВСС

Объем дисциплины 180/5
 часов/з.е

Промежуточная аттестация Экзамен

Разработчик: Капранов С.Н., к.т.н., доцент

Нижний Новгород

2023 г

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденного приказом МИНОБРНАУКИ РОССИИ от 26 ноября 2020 года № 1457 на основании учебного плана принятого УМС НГТУ

протокол от 20.04.2023 № 18.

Рабочая программа одобрена на заседании кафедры протокол от 01.04.2023 № 4
Зав. кафедрой к.т.н, доцент Ляхманов Д.А. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от 21.04.2023 № 4

Рабочая программа зарегистрирована в УМУ, регистрационный № 10.05.03-б-31
Начальник МО _____ Булгакова Н.Р.

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

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	4
1.1 Цель освоения дисциплины.....	4
1.2 Задачи освоения дисциплины (модуля)	4
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....	4
3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	5
4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....	8
4.1 РАСПРЕДЕЛЕНИЕ ТРУДОЁМКОСТИ ДИСЦИПЛИНЫ ПО ВИДАМ РАБОТ ПО СЕМЕСТРАМ	8
4.2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ	9
5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.	16
5.1 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ	16
5.2 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ КОНТРОЛЯ УСПЕВАЕМОСТИ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ	16
6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	19
7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	20
7.1 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ	20
7.2 ПЕРЕЧЕНЬ СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	20
7.3 ПЕРЕЧЕНЬ СОВРЕМЕННЫХ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ	20
8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ	21
9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	21
10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	22
10.1 ОБЩИЕ МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ, ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ.....	22
10.2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ЗАНЯТИЙ ЛЕКЦИОННОГО ТИПА	23
10.3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ НА ЛАБОРАТОРНЫХ РАБОТАХ	23
10.4 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ ОБУЧАЮЩИХСЯ.....	23
11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	24
11.1 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА В ХОДЕ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ.....	24
11.2 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА В ХОДЕ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ	24

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 «Основы информационной безопасности» способствует подготовке студентов к решению следующих профессиональных задач:

1. Анализировать угрозы безопасности информации.
2. Применять программные средства криптографической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Основы информационной безопасности» Б1.Б.32 включена в обязательный перечень дисциплин обязательной части образовательной программы вне зависимости от ее направленности (профиля). Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по направлению подготовки 10.05.03.

Дисциплина «Основы информационной безопасности» является основополагающей для изучения следующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Управление информационной безопасностью», «Экономическая безопасность».

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

Таблица 3.1 - Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	2	3	4	5	6	7	8	9	10	11
<i>ОПК-1 (Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства)</i>											
<i>Основы информационной безопасности</i>											
<i>Государственный экзамен</i>											

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	2	3	4	5	6	7	8	9	10	11
<i>ОПК-6 (Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю)</i>											
<i>Основы информационной безопасности</i>											
<i>Организационное и правовое обеспечение информационной безопасности</i>											
<i>Подготовка и защита ВКР</i>											

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-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1. Оценивает вклад информации и современных информационных технологий для обеспечения информационно-безопасности личности, общества и государства ИОПК-1.2. Оценивает вклад информационных-коммуникативных технологий в обеспечение личной, коммерческой и государственной информационно-безопасности	Знать: - основные понятия и общее содержание проблемы информационной безопасности (ИОПК-1.1) - методы социальной инженерии (ИОПК-1.2); - нормы профессиональной этики (ИОПК-1.2);	Уметь: оценивать методы и средства информационной безопасности, их значение для обеспечения защиты личности, общества и государства (ИОПК -1.1) – осуществлять поиск, изучение, обобщение информации о физических и юридических лицах (ИОПК -1.2); 27 – противодействовать деструктивным психологическим влияниям (ИОПК-1.2);	Владеть: - навыками обработки, интерпретации и обобщения информации (ИОПК-1.1) - методами идентификации и аутентификации пользователей (ИОПК-1.1) - методами противодействия троллингу и черному пиару (ИОПК-1.2); - методами идентификации и снижения рисков безопасности автоматизированных систем, связанных с человеческим фактором (ИОПК-1.2);	Набор индивидуальных заданий (1-5) (лабораторных работ)	Набор билетов для экзамена

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИОПК-6.1. Проводит организационные мероприятия по управлению информационной безопасности на предприятии в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знать: – угрозы и уязвимости информации	Уметь: - оценивать угрозы и уязвимости информации	Владеть: - основными методами защиты информации	Набор индивидуальных заданий (1-5) (лабораторных работ)	Набор билетов для экзамена
---	--	---	---	---	---	----------------------------

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 5 зач. ед. 180 часов, распределение часов по видам работ семестрам представлено в таблице 4.1.

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
		2 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	180	180
1. Контактная работа:	74	74
1.1 Аудиторная работа, в том числе:	68	68
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практ. занятия и др)		
лабораторные работы (ЛР)	34	34
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)	70	70
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.)	70	70
Подготовка к экзамену (контроль)	36	36

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.1 - 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	Наименова ние используем ых активных и интерактив ных образователь ных технологий	Реализация в рамках Практичес кой подготовки (трудоемко сть в часах)	Наименование разработанног о Электронного курса (трудоемкость в часах)	
		Контактная работа									
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР	Самостоятельная работа студентов (час)					
Раздел 1. Введение											
ОПК-1 - ИОПК-1.1 ОПК-6 - ИОПК-6.1	Тема 1.1 Введение в информационную безопасность. Угрозы ИБ	2				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]				
	Итого по 1 разделу	2				2					
Раздел 2. Криптографические методы защиты информации											
ОПК-1 - ИОПК-1.1 ОПК-6 - ИОПК-6.1	Тема 2.1 Введение в криптографию. Исторические шифры	1				2	Подготовка к лекциям [6.1.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций			
	Тема 2.2 Симметричные криптосистемы	4			1	2	Подготовка к лекциям [6.1.2], работа над заданием лабораторной работы	Разбор конкретных ситуаций			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименова ние используем ых активных и интерактив ных образователь ных технологий	Реализация в рамках Практичес кой подготовки (трудоемко сть в часах)	Наименование разработанног о Электронного курса (трудоемкость в часах)
		Контактная работа								
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР	Самостоятельная работа студентов (час)				
	Тема 2.3 Ассиметричные криптосистемы	4				2	Подготовка к лекциям [6.1.2], работа над заданием лабораторной работы			
	Тема 2.4 Алгоритмы ХЭШ-функции и электронной цифровой подписи	2				2	Подготовка к лекциям [6.1.2], работа над заданием лабораторной работы			
	Тема лабораторной работы: «Классические криптосистемы»		6			6	Подготовка к лабораторной работе [6.1.2]			
	Тема лабораторной работы: «Алгоритмы симметричного блочного шифрования»		6			6	Подготовка к лабораторной работе [6.1.2]			
	Тема лабораторной работы:		6			6	Подготовка к лабораторной			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименова ние используем ых активных и интерактив ных образователь ных технологий	Реализация в рамках Практичес кой подготовки (трудоемко сть в часах)	Наименование разработанног о Электронного курса (трудоемкость в часах)
		Контактная работа								
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР	Самостоятельная работа студентов (час)				
	«Алгоритмы симметричного поточного шифрования»						работе [6.1.2]			
	Тема лабораторной работы: «Алгоритмы асимметричного шифрования»		8			6	Подготовка к лабораторной работе [6.1.2]			
	Тема лабораторной работы: «Алгоритмы формирования электронной цифровой подписи»		8			6	Подготовка к лабораторной работе [6.1.2]			
	Итого по 2 разделу	11	34		1	38				
Раздел 3. Правовая защита информации.										
ОПК-1 - ИОПК-1.1 ОПК-6 - ИОПК-6.1	Тема 3.1 Нормативные документы и законы РФ в области информационной безопасности	1				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименова ние используем ых активных и интерактив ных образователь ных технологий	Реализация в рамках Практичес кой подготовки (трудоемко сть в часах)	Наименование разработанног о Электронного курса (трудоемкость в часах)
		Контактная работа								
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР	Самостоятельная работа студентов (час)				
	Тема 3.2 Законодательное регулирование информатизации за рубежом	1				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			
	Тема 3.3 Защита персональных данных	2			1	2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]	Разбор конкретных ситуаций		
	Итого по 3 разделу	4			1	6				
Раздел 4. Политики и модели информационной безопасности										
ОПК-1 - ИОПК-1.1 ОПК-6 - ИОПК-6.1	Тема 4.1. Политики и модели разграничения доступа. Дискреционная политика. Мандатная политика. Ролевая политика	2				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			
	Итого по 4 разделу	2				2				
Раздел 5. Методы аутентификации										
ОПК-1 - ИОПК-1.1 ОПК-6 - ИОПК-	Тема 5.1. Принципы защиты от несанкционированно го доступа. Методы	1				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]	Разбор конкретных ситуаций		

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименова ние используем ых активных и интерактив ных образовател ьных технологий	Реализация в рамках Практичес кой подготовки (трудоемко сть в часах)	Наименование разработанног о Электронного курса (трудоемкость в часах)
		Контактная работа								
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР	Самостоятельная работа студентов (час)				
6.1.	опознавание пользователей									
	Тема 5.2. Механизмы реализации надежных паролей	2			1	2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			
	Итого по 5 разделу	3			1	4				
	Раздел 6. Социальные аспекты защиты информации									
ОПК-1 - ИОПК-1.1 ОПК-6 - ИОПК-6.1	Тема 6.1. Социальная инженерия	2			1	2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]	Разбор конкретных ситуаций		
	Тема 6.2. Информационные войны	2				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]	Разбор конкретных ситуаций		
	Итого по 6 разделу	4			1	4				
Раздел 7. Компьютерные вирусы										
ОПК-1 - ИОПК-1.1 ОПК-6 - ИОПК-6.1	Тема 7.1. Программы-вирусы. История проблемы	1				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			
	Тема 7.2. Типы компьютерных вирусов	2				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			
	Тема 7.3. Средства	1				2	Подготовка к лекциям [6.1.1,			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименова ние используем ых активных и интерактив ных образователь ных технологий	Реализация в рамках Практичес кой подготовки (трудоемко сть в часах)	Наименование разработанног о Электронного курса (трудоемкость в часах)
		Контактная работа								
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР	Самостоятельная работа студентов (час)				
	антивирусной защиты						6.1.3, 6.1.4]			
	Итого по 7 разделу	4				6				
Раздел 8. Инженерная защита информации										
ОПК-1 - ИОПК-1.1 ОПК-6 - ИОПК-6.1	Тема 8.1. Физическая безопасность и безопасность окружения	1				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]	Разбор конкретных ситуаций		
	Тема 8.2. Защищенное проектирование зданий и ландшафта	1				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			
	Тема 8.3. Внутренние системы поддержки и снабжения	1				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			
	Тема 8.4. Обеспечение безопасности периметра	1				2	Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4]			
	Итого по 8 разделу	4			4	8				
	Подготовка к экзамену				2	36				
	Итого за семестр	34	34		6	70				

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) Перечень вопросов, выносимых на промежуточную аттестацию (экзамен)
 1. Определение, основные понятия и общее содержание проблемы информационной безопасности.
 2. Нормативные документы по защите информации
 3. Угрозы информационной безопасности
 4. Уязвимости информационной безопасности
 5. Методы защиты информации от несанкционированного доступа.
 6. Методы идентификации и аутентификации.
 7. Основы криптографических методов защиты информации.
 8. Политика информационной безопасности. Дискреционная модель политики безопасности.
 9. Политика информационной безопасности. Мандатные модели политики безопасности.
 10. Политика безопасности Белла-Лападулы
 11. Технические каналы утечки информации
 12. Вредоносное программное обеспечение (компьютерные вирусы).

Для выполнения процедур оценивания составлен паспорт оценочных средств.

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информационная безопасность вычислительных систем и сетей».

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Таблица 5.4 - При текущем контроле (контрольные недели) и оценке выполнения лабораторных работ

Шкала оценивания	Экзамен (зачет с оценкой)
$40 < R \leq 50$	Отлично
$30 < R \leq 40$	Хорошо
$20 < R \leq 30$	Удовлетворительно
$0 < R \leq 20$	Неудовлетворительно

При промежуточном контроле успеваемость студентов оценивается по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.4 – 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 тах рейтинговой оценки контроля	Оценка «удовлетворительно» / «зачтено» 60-74% от тах рейтинговой оценки контроля	Оценка «хорошо» / «зачтено» 75-89% от тах рейтинговой оценки контроля	Оценка «отлично» / «зачтено» 90-100% от тах рейтинговой оценки контроля
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1. Оценивает вклад информации и современных информационных технологий для обеспечения информационной безопасности личности, общества и государства	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;
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных	ИОПК-6.1. Проводит организационные мероприятия по управлению информационной безопасности на предприятии в	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы защиты информации; не во всех случаях правильно оперирует	Фрагментарные, поверхностные знания базовых принципы защиты информации; не во всех случаях находит правильные ответы на задаваемые вопросы по методам и	Знает методы и средства защиты информации на достаточно хорошем уровне; представляет основные концепции контроля целостности; подтверждает	Имеет глубокие знания по методам и средствам защиты информации; дает развернутые ответы на задаваемые вопросы;

системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	основными понятиями по информационной безопасности; не отвечает на задаваемые вопросы	средствам защиты информации	теоретические знания отдельными практическими примерами; дает ответы на задаваемые вопросы по методам и средствам защиты информации	
---	--	---	-----------------------------	---	--

Таблица 5.5 - 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 сформировал 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/162235>.

6.2 Справочно-библиографическая литература

— учебники и учебные пособия

- 6.1.3. 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
- 6.1.4 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

Методические указания по выполнению лабораторных работ по дисциплине «Основы информационной безопасности» в электронном варианте находятся на кафедре «Информационная безопасность вычислительных систем и сетей». Электронные варианты методических указаний по

выполнению лабораторных работ отправляются на электронные адреса групп.

6.3.1 Методические указания к лабораторным работам по дисциплине «Основы информационной безопасности» [Электронные текстовые данные]: метод. указания к лаб. работе по дисциплине «Основы информационной безопасности» для студентов направления подготовки 10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: С.Н. Капранов. Н. Новгород, 2021, 76 с.

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 - Электронная библиотека технического вуза»	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	«Юрайт» (коллекция «Легендарные книги»)	https://urait.ru/
4	«Техэксперт» - «Нормы, правила, стандарты и законодательство России»	https://www.nntu.ru/frontend/web/ngtu/files/org_structura/library/resurvsy/tehekspert.pdf

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
1. Microsoft Windows 7 (подписка Dream Spark Premium, договор № 0509/KMP от 15.10.18) 2. P7 Офис (с/н 5260001439) 3. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23) 4. Microsoft Office Профессиональный плюс 2010 (лицензия № 49487732) 5. Microsoft Windows 7 MSDN реквизиты договора - подписка DreamSpark Premium, договор № Tr113003 от 25.09.14	Apache OpenOffice, Пакет программ Open Office, Браузер Google Chrome, Браузер Mozilla Firefox, Браузер Opera, McAfee Security Scan, Adobe Acrobat Reader DC, AutoCAD2013

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	2	3
1	База данных издательства Wiley	https://onlinelibrary.wiley.com/
2	База данных Polpred	http://www.polpred.com
3	Научная электронная библиотека ELIBRARY.RU	http://elibrary.ru
4	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
5	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
6	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.nttu.ru/sveden/ovz/>.

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»	Версия для слабовидящих, прослушивание с помощью синтезатора речи
2	ЭБС «Лань»	Версия для слабовидящих, прослушивание с помощью синтезатора речи
3	«Юрайт» (коллекция «Легендарные книги»)	Версия для слабовидящих

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

Учебные аудитории для проведения занятий по дисциплине, оснащены оборудованием и техническими средствами обучения.

В таблице 9.1 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;
- помещения для самостоятельной работы обучающихся, которые должны оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГТУ.

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	Учебная аудитория № 1363-6 учебного корпуса № 1 для проведения учебных занятий. 603950, Нижегородская область, г. Нижний Новгород, ул. Минина, дом 24	1. ПК, с выход. на мультимедийный проектор, на базе Intel CoreDuo 2.66 ГГц, 4 Гб ОЗУ, 300 Гб HDD, монитор 19” – 1 шт. 2. ПК, на базе Intel Core 2Duo 2.93 ГГц, 2 Гб ОЗУ, 300 Гб HDD, монитор 19” – 1 шт. 3. ПК, на базе Intel Core i5-3470 3.2ГГц, 4 Гб ОЗУ, 1 Тб HDD, монитор 19” – 1 шт. 4. Доска меловая – 1 шт. 5. Экран – 1 шт. 6. Мультимедийный проектор Epson – 1 шт. 7. Рабочее место студента – 28 8. Рабочее место преподавателя – 1	Microsoft Windows 7 (подписка Dream Spark Premium, договор № 0509/KMP от 15.10.18) P7 Офис (с/н 5260001439) Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.2023, до 28.05.24) Microsoft Office Профессиональный плюс 2010 (лицензия № 49487732)
2	Лаборатория информационно-аналитического обеспечения автоматизированные системы обработки информации и управления № 4404 учебного корпуса № 4 для проведения учебных занятий и обеспечения практической подготовки обучающихся. 603155, Нижегородская область, г. Нижний Новгород, ул. Минина д.28В	1.Моноблоки Lenovo ThinkCentre M72z - 7 шт. 2.Персональные компьютеры с выходом на Epson X12, Intel Core7-3820/8 Gb RAM/NVIDIA GeForce GTX 560/HDD 500, в составе локальной вычислительной сети, с подключением к интернету - 4 шт. 3. Рабочее место студента - 26.	1. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24) 2. Распространяемое по свободной лицензии: Apache OpenOffice, OC: Windows 7
3	Компьютерный класс № 1 - Помещение для самостоятельной работы обучающихся № 6543 учебно-лабораторного корпуса № 6 для проведения научно-исследовательской работы обучающихся, курсового и дипломного проектирования. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.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/KMP 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 «Основы информационной безопасности», 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, лабораторных 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 лабораторных занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom, Discord.

Иницируется 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 балльно-рейтинговая система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме экзамена с учетом текущей успеваемости.

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 4.4, 4.5, 4.6). 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 работам 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 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 текущего контроля успеваемости

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

- выполнение и защита лабораторных работ для студентов всех форм обучения.

Темы лабораторных работ

1. Исторические шифры
2. Алгоритм шифрования DES
3. Алгоритм шифрования RSA
4. Алгоритм хэширования SHA
5. Алгоритм электронной цифровой подписи DSA

Варианты заданий для лабораторных работ приведены в учебно-методических пособиях 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

Экзамен для студентов очной формы обучения во 2 семестре.

Типовые вопросы для промежуточной аттестации в форме экзамена для студентов очной формы обучения

Вопросы, направленные на проверку компетенции ОПК-1:

1. Основные понятия и общее содержание проблемы информационной безопасности.
2. Методы защиты информации от несанкционированного доступа.
3. Методы идентификации и аутентификации.
4. Симметричные криптосистемы. исторические шифры
5. Симметричные криптосистемы. Сеть Файстеля
6. Симметричные криптосистемы. Режимы шифрования
7. Ассиметричные криптосистемы. Шифрование
8. Ассиметричные криптосистемы. ЭЦП
9. Ассиметричные криптосистемы. Хэш-функции
10. Модель Кларка Вильсона
11. Методы формирования защищенного пароля
12. Методы социальной инженерии
13. Физическая безопасность окружения зданий
14. Физическая безопасность зданий
15. Физическая безопасность. Внутренние системы
16. Вредоносное программное обеспечение (компьютерные вирусы).

Вопросы, направленные на проверку компетенции ОПК-6:

17. Нормативные документы по защите информации
18. Угрозы информационной безопасности
19. Уязвимости информационной безопасности
20. Закон о Персональных данных
21. Политики и модели безопасности информационных систем
22. Технические каналы утечки информации

В полном объеме оценочные средства имеются на кафедре «Информационная безопасность вычислительных систем и сетей». Оценочные средства могут быть получены по требованию.