УТВЕРЖДАЮ:
Директор института ИРИТ

_____Мякиньков А.В.
«03» июня 2024 г.

Лист актуализации рабочей программы дисциплины
«Б1.Б.35 Методы и средства криптографической защиты информации»
индекс по учебному плану, наименование

для подготовки **специалистов**
Направление: 10.05.03 «Информационная безопасность автоматизированных систем»
Направленность: Безопасность открытых информационных систем
Форма обучения: очная
Год начала подготовки: 2022
Курс 3
Семестр 5

В рабочую программу 2022 г. вносятся изменения:

1) Таблицу 7.2 читать в следующей редакции:

№	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/

2) Пункт 9 читать в следующей редакции:

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:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом образовательной программы, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес места нахождения помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом образовательной программы
Лаборатория «Программно-аппаратных средств и технической защиты информации» №6039 учебно-лабораторного корпуса №6 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 1.Учебный лабораторный стенд "Блочное кодирование" – 1 шт. 2.Учебный лабораторный стенд "Основы криптографии" – 1 шт. 3.Учебный лабораторный стенд "Биометрическая аутентификация" – 2 шт. 4.Учебный лабораторный стенд "Доверенная загрузка (Соболь)" – 1	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

шт. 5.Учебный лабораторный стенд "Доверенная загрузка (Аккорд)" – 1 шт. 6.Учебный лабораторный стенд "Криптоконтейнеры и ЭЦП" – 2 шт. 7. Для ивалидов и лиц с ОВЗ: переносной радиокласс, клавиатура адаптированная 8. МФУ Brother LC 9. Посадочных мест - 16. **Программное обеспечение:** Распространяемое по свободной лицензии: 1.Операционная система Ubuntu Linux 20 2. GNS3 3. Snort 4. Wareshark 5. OpenVPN 6. Libre Office 7. OpenVPN 8. IP scanner	
Мультимедийная аудитория № 4201 учебного корпуса №4 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** Рабочих мест преподавателя – 1 Рабочих мест студента – 102 1. Моноблок Lenovo ThinkCentre M72z - 1 шт. 2. Проектор Epson - 1 шт. 3. Экран настенный - 1 шт. **Программное обеспечение:** 1.Microsoft Windows 7 (подписка Dream Spark Premium, договор № 0509/КМР от 15.10.18) 2.Р7 Офис (с/н 5260001439) 3. Dr.Web (С/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024, до 30.05.25) 4.Microsoft Office Профессиональный плюс 2010 (лицензия № 49487732)	603155, Нижегородская область, г. Нижний Новгород, ул. Минина, д. 24В
Мультимедийная аудитория №6421 учебно-лабораторного корпуса №6 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 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 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 30 7. Рабочее место для преподавателя – 1 шт. **Программное обеспечение:** 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, до 30.05.25)	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

Программа актуализирована для 2022 г. начала подготовки.

Разработчик (и): __Капранов С.Н., к.т.н., доцент_____
(ФИО, ученая степень, ученое звание)

«_15_»_05___2024г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБВСС протокол № _9___ от «_15_» ___05___2024_г.

И.о. заведующий кафедрой _____Ляхманов Д.А.

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИБВСС _____«03» июня 2024 г.

Методический отдел УМУ:_____ «03» июня 2024 г.

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:
_____ Мякиньков А.В.
подпись ФИО
22 апреля 2023г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.35 Методы и средства криптографической защиты информации
(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 144/4
часов/з.е
Промежуточная аттестация зачет

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 «Информационная безопасность автоматизированных систем», утвержденного приказом МИНОБРНАУКИ РОССИИ от 26 ноября 2020 г. № 1457 на основании учебного плана, принятого УМС НГТУ

протокол от 20.04.2023г № 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-34
Начальник МО _____ Н.Р. Булгакова

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

1. Содержание

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области обеспечения конфиденциальности и целостности информации, основанное на изучении криптографических методов защиты данных.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Методы и средства криптографической защиты информации» способствует подготовке студентов к решению следующих профессиональных задач:

1. Исследование криптографических методов и средств защиты информации
2. Обоснование решений в области использования конкретных криптографических протоколов при проектировании современных защищенных программных комплексов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Методы и средства криптографической защиты информации» Б1.Б.35 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 базируется на дисциплинах блока защиты информации, предшествующими курсами, на которых непосредственно базируется дисциплина «Методы и средства криптографической защиты информации», являются:

– «Теоретико-числовые основы криптологии»

Дисциплина «Методы и средства криптографической защиты информации» является основополагающей для изучения следующих дисциплин: «Программно-аппаратные средства защиты информации» и для прохождения практики: преддипломная.

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

Дисциплина «Методы и средства криптографической защиты информации» формирует компетенции ОПК-5.3, ОПК-10, ОПК-11 совместно с дисциплинами и практиками, указанными в таблице 3.1.

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*
ОПК-5.3 (Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах)											
Методы и средства криптографической защиты информации											
Программно-аппаратные средства защиты информации											
Подготовка и защита ВКР											

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*
ОПК-10 (Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности)											
Методы и средства криптографической защиты информации											
Программно-аппаратные средства защиты информации											
Подготовка и защита ВКР											

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*
ОПК-11 (Способен разрабатывать компоненты систем защиты информации автоматизированных систем)											
Методы и средства криптографической защиты информации											
Защита программ и данных											
Подготовка и защита ВКР											

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-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ИОПК-5.3.1. Применяет криптографические методы защиты информации для обеспечения целостности данных в открытых информационных системах	***Знать:*** - основные подходы к конструированию систем защиты информации с использованием функций хэ-ширования, протоколов цифровой подписи	***Уметь:*** - строить современные защищённые программные комплексы с использованием средств обеспечения целостности и защищенности данных	***Владеть:*** – современными международными стандартами в области криптографических алгоритмов и протоколов для обеспечения целостности информации	Выполнение и сдача 4 лабораторных работ	Зачет – 20 билетов
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИОПК-10.1. Применяет криптографические алгоритмы и протоколы для обеспечения секретности и целостности информации в открытых информационны	***Знать:*** - исторические шифры - основные алгоритмы симметричного шифрования, функции хэширования,	***Уметь:*** - проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов для защиты значимой информации -квалифицированно оценивать	***Владеть:*** – современными международными стандартами в области криптографических алгоритмов и протоколов	Выполнение и сдача 4 лабораторных работ	Зачет – 20 билетов

	х системах	протоколы цифровой подписи, используемые для защиты значимой информации	информационные риски, возникающие при использовании конкретных криптографических протоколов в защищаемой информационной системе	для обеспечения защиты информации – навыками проверки работоспособности применяемых криптографических средств защиты информации		
ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ИОПК-11.1. Применяет криптографические методы для создания компонентов систем защиты информации открытых информационных систем.	***Знать:*** - основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности	***Уметь:*** – строить современные защищённые программные комплексы с использованием криптографических алгоритмов и протоколов	***Владеть:*** – современными и международными стандартами в области криптографических алгоритмов и протоколов для обеспечения защиты информации – навыками проверки работоспособности	Выполнение и сдача 4 лабораторных работ	Зачет – 20 билетов

				применяемых криптографических средств защиты информации		

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 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**
		5 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**72**	**72**
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	**4**	**4**
курсовая работа (проект) (КР/КП) (консультация, защита)		

текущий контроль, консультации по дисциплине	2	2
контактная работа на промежуточном контроле (КРА)	2	2
2. Самостоятельная работа (СРС)	**72**	**72**
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.)	72	72
Подготовка к зачету	-	-

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.2-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					
Раздел 1. Введение										
ОПК-5.3 - ИОПК-5.3.1 ОПК-10 - ИОПК-10.1 ОПК-11 - ИОПК-11.1	**Тема 1.1.** Исторические шифры	2				2				
	Итого по 1 разделу	**2**				**2**				
Раздел 2. Симметричные криптосистемы										
ОПК-5.3 - ИОПК-5.3.1 ОПК-10 - ИОПК-10.1 ОПК-11 - ИОПК-11.1	**Тема 2.1.** Одноразовый блокнот.	2				2	Подготовка к лекциям [6.1.1,6.1.2]	Разбор конкретных ситуаций		
	Тема 2.2. Алгоритм DES и его модификации	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.4]	Разбор конкретных ситуаций		
	Тема 2.3. Алгоритм AES	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.4]	Разбор конкретных ситуаций		
	Тема 2.4. Алгоритмы ГОСТ 34.12-2015 «Магма», «Кузнечик»	4				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.4]	Разбор конкретных ситуаций		
	Тема 2.5. Алгоритмы RC4, RC5, RC6, Salsa20, Chacha	2				2	Подготовка к лекциям [6.1.1, 6.1.2]	Разбор конкретных ситуаций		
	Лабораторная работа. Реализация симметричного алгоритма шифрования		8			10	Подготовка к лабораторной работе.[6.1.1, 6.1.2, 6.1.4]			
	Итого по 2 разделу	**12**	**8**		**1**	**20**				
Раздел 3. Асимметричные криптосистемы										

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					
ОПК-5.3 - ИОПК-5.3.1 ОПК-10 - ИОПК-10.1 ОПК-11 - ИОПК-11.1	**Тема 3.1.** Алгоритм RSA.	2				2	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 3.2. Криптосистема Рабина	2				2	Подготовка к лекциям [6.1.1 – 6.1.3]	Разбор конкретных ситуаций		
	Тема 3.3. Алгоритм Эль-Гамаля	2				2	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 3.4. Алгоритм Меркла-Хеллмана	2				2	Подготовка к лекциям [6.1.1 – 6.1.3]	Разбор конкретных ситуаций		
	Лабораторная работа. Реализация асимметричного алгоритма шифрования		10			10	Подготовка к лабораторной работе.[6.1.1 – 6.1.4]			
	Итого по 3 разделу	**8**	**10**		**1**	**18**				
Раздел 4. Электронные цифровые подписи										
ОПК-5.3 - ИОПК-5.3.1 ОПК-10 - ИОПК-10.1 ОПК-11 - ИОПК-11.1	**Тема 4.1.** Функции хэширования: SHA, MD5, ГОСТ 34.11-94	**2**				**2**	Подготовка к лекциям [6.1.2 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 4.2. Схемы создания ЭЦП: RSA, DSA, Эль-Гамаля	**2**				**2**	Подготовка к лекциям [6.1.2 – 6.1.4]	Разбор конкретных ситуаций		
	Лабораторная работа. Реализация хеш-функции		**8**			**10**	Подготовка к лабораторной работе.[6.1.2 – 6.1.4]			
	Лабораторная работа. Реализация схемы создания электронной цифровой подписи		**8**			**10**	Подготовка к лабораторной работе.[6.1.2 – 6.1.4]			
	Итого по 3 разделу	**4**	**16**		**1**	**24**				
Раздел 5. Идентификация и аутентификация										
ОПК-5.3 - ИОПК-5.3.1	**Тема 5.1.**	**4**				**2**	Подготовка к лекциям	Разбор		

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					
ОПК-10 - ИОПК-10.1 ОПК-11 - ИОПК-11.1	Пароли, использование хеш-функции, шифрование с открытым ключом, сервер аутентификации Kerberos, биометрия, идентификационные карты и электронные ключи.						[6.1.2, 6.1.3]	конкретных ситуаций		
	Итого по 3 разделу	**4**			**0,5**	**2**				
Раздел 6. Управление ключами										
ОПК-5.3 - ИОПК-5.3.1 ОПК-10 - ИОПК-10.1 ОПК-11 - ИОПК-11.1	**Тема 6.1.** Генерация ключей, хранение ключей, распределение ключей	**4**				**2**	Подготовка к лекциям [6.1.1, 6.1.4]	Разбор конкретных ситуаций		
	Итого по 3 разделу	**4**			**0,5**	**2**				
	Подготовка к зачету (контроль)					**4**				
	Итого за семестр	**34**	**34**	**-**	**4**	**72**				

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:

– Как генерируется пара ключей (секретный и публичный ключи) в асимметричных криптосистемах?
– Что такое однонаправленная функция? Как однонаправленные функции используются в криптографических методах?
– Как используется сеть Файстеля в симметричных блочных алгоритмах шифрования?
– Как работают симметричные криптосистемы? Нарисуйте схему работы симметричной криптосистемы?
– Какие вы знаете симметричные алгоритмы шифрования?
– Почему алгоритм DES является недостаточно криптостойким в настоящее время?
– Что такое коллизия?
– Опишите процедуру постановки электронной цифровой подписи?
– Что такое хеш-функция? Как с помощью хэш-функций реализуется контроль целостности данных?
– Как реализуется распределение ключей шифрования?
– Как работают поточные алгоритмы шифрования? Что они отличаются от блочных?
– Почему повторное использование ключевого потока делает алгоритмы шифрования уязвимыми?
– Что такое электронная цифровая подпись?
– Как используется операция сложение по модулю два в криптографических методах?
– Расскажите как работают различные режимы шифрования ECB, CBC, CPB, OFB?

2. Примерный перечень вопросов для зачета:

– Симметричные криптосистемы.
– Алгоритм DES. Разновидности алгоритма DES и атаки на них.
– Алгоритм AES.
– Отечественный стандарт шифрования данных ГОСТ 34.12-2015- «Магма», «Кузнечик»
– Асимметричные криптосистемы.
– Однонаправленные функции.
– Алгоритм RSA.
– Алгоритм Меркла-Хеллмана.
– Криптосистема Рабина.
– Поточные шифры.
– Алгоритмы RC4,RC5, RC6
– Алгоритм Salsa20, алгоритм ChaCha.
– ЭЦП. Основные понятия и функциональность. Процедуры постановки и проверки подписи.
– Хэш-функция. Требования к хэш-функциям.
– Хэш-функция. ГОСТ34.11-2012
– Схемы создания ЭЦП.
– Управление ключами. Генерация ключей. Хранение ключей и распределение ключей.
– Идентификация, аутентификация, авторизация.

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

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 наименовани 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-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ИОПК-5.3.1. Применяет криптографические методы защиты информации для обеспечения целостности данных в открытых информационных системах	Изложение учебного материала бессистемное, неполное, отсутствует понимание принципов функционирования криптографических методов, не способен использовать криптографические протоколы при проектировании защищенных программных комплексов.	Имеет частичное понятие об основных криптографических методах защиты информации, испытывает трудности при использовании криптографических протоколов при проектировании защищенных программных комплексов, не способен анализировать информационные риски в области криптографических протоколов.	Знает основные криптографические методы; применяет на практике криптографические протоколы при проектировании защищенных программных комплексов; испытывает затруднения при анализе информационных рисков в области криптографических протоколов	Имеет глубокие системные знаниякриптографических методов защиты информации,применяет на практике криптографические протоколы при проектировании защищенных программных комплексов; способен анализировать информационных риски в области криптографических протоколов.
ОПК-10. Способен использовать средства криптографической защиты	ИОПК-10.1. Применяет криптографические	Изложение учебного материала бессистемное,	Имеет частичное понятие об основных	Знает основные криптографические методы; применяет	Имеет глубокие системные знания криптографических

информации при решении задач профессиональной деятельности	алгоритмы и протоколы для обеспечения секретности и целостности информации в открытых информационных системах	неполное, отсутствует понимание принципов функционирования криптографических методов, не способен использовать криптографические протоколы при проектировании защищенных программных комплексов.	криптографических методах защиты информации, испытывает трудности при использовании криптографических протоколов при проектировании защищенных программных комплексов, не способен анализировать информационные риски в области криптографических протоколов.	на практике криптографические протоколы при проектировании защищенных программных комплексов; испытывает затруднения при анализе информационных рисков в области криптографических протоколов	методов защиты информации, применяет на практике криптографические протоколы при проектировании защищенных программных комплексов; способен анализировать информационных риски в области криптографических протоколов.
ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ИОПК-11.1. Применяет криптографические методы для создания компонентов систем защиты информации открытых информационных систем.	Изложение учебного материала бессистемное, неполное, отсутствует понимание принципов функционирования криптографических методов, не способен использовать криптографические протоколы при проектировании защищенных программных комплексов.	Имеет частичное понятие об основных криптографических методах защиты информации, испытывает трудности при использовании криптографических протоколов при проектировании защищенных программных комплексов, не способен	Знает основные криптографические методы; применяет на практике криптографические протоколы при проектировании защищенных программных комплексов; испытывает затруднения при анализе информационных рисков в области криптографических	Имеет глубокие системные знания криптографических методов защиты информации, применяет на практике криптографические протоколы при проектировании защищенных программных комплексов; способен анализировать информационных

			анализировать информационные риски в области криптографических протоколов.	протоколов	риски в области криптографических протоколов.

Таблица 5.2 - Критерии оценивания

Оценка	Критерии оценивания
Высокиий 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. Коржик, В. И. Основы криптографии : учебное пособие / В. И. Коржик, В. П. Просихин, В. А. Яковлев. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2014. — 277 с. — ISBN 978-5-89160-097-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181501

6.1.2. 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 (дата обращения: 03.02.2022). — Режим доступа: для авториз. пользователей.

6.1.3. Каширская, Е. Н. Криптографические системы : учебное пособие / Е. Н. Каширская, А. П. Кушнир. — Москва : РТУ МИРЭА, 2021. — 66 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182424

6.1.4. Капранов С.Н. Методы и средства защиты информации. Часть 1. Криптография. Стеганография: учеб. пособие / С.Н. Капранов, Д.А. Ляхманов, П.А. Шагалова; Нижегород. гос. техн. ун-т им. Р.Е. Алексеева. – Нижний Новгород, 2021. - 94 с.

6.2 Справочно-библиографическая литература

6.1.5. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699

6.1.6. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие для вузов / Л. М. Мартынов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-9346-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189446

6.3 Перечень журналов по профилю дисциплины:

Использование журналов не предусмотрено при изучении дисциплины.

6.4 Методические указания, рекомендации и другие материалы к занятиям

6.1.7. Метод. указания для лабораторных работ по дисциплине «Методы и средства криптографической защиты информации», для студентов направления подготовки 10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: П.А. Шагалова, Н.Новгород, 2020

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. Windows 7 32 bit корпоративная VL 49477S2 2. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 3. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 4. Microsoft Windows 7 MSDN (подписка DreamSpark Premium, договор № Tr113003 от 25.09.14)	Adobe Acrobat Reader DC-Russian (беспл.) Свободно распространяемое программное обеспечение: Операционная система Ubuntu Linux 20, GNS3, Snort, Wareshark, OpenVPN, Libre Office, OpenVPN, IP scanner Браузер Google Chrome, Браузер Mozilla Firefox, McAfee Security Scan, Adobe Acrobat

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице7.4указан 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 таблице8.1 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/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 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 № 6421 учебно-лабораторного корпуса № 6 для проведения учебных занятий. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.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 250Ggb,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 GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24)
2	Лаборатория «Программно-аппаратных средств и технической защиты информации» - учебная аудитория № 6039 учебно-лабораторного корпуса № 6 для проведения учебных занятий и практической подготовки обучающихся. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1.Учебный лабораторный стенд "Блочное кодирование" – 1 шт. 2.Учебный лабораторный стенд "Основы криптографии" – 1 шт. 3.Учебный лабораторный стенд "Биометрическая аутентификация" – 2 шт. 4.Учебный лабораторный стенд "Доверенная загрузка (Соболь)" – 1 шт. 5.Учебный лабораторный стенд "Доверенная загрузка (Аккорд)" – 1 шт. 6.Учебный лабораторный стенд "Криптоконтейнеры и ЭЦП" – 2 шт. 7. МФУ Brother LC 8. Посадочных мест - 16.	Распространяемое по свободной лицензии: 1.Операционная система Ubuntu Linux 20 2. GNS3 3. Snort 4. Wareshark 5. OpenVPN 6. Libre Office 7. Splunk 8. Zeek Network Security Monitor 9. Security Onion 10. OpenVPN 11. IP scanner 12. Nemesis 13. Eyercap
3	Помещение для самостоятельной работы обучающихся № 6545 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, оснащенные ПК на базеCore 2 Duo с мониторами – 5 шт. 2. Рабочее место преподавателя, оснащенное ПК на базе Intel Core i5 с монитором – 1 шт. 3. Доска интерактивная ScreenMedia-M. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета. 4. Посадочных мест - 12, шесть оснащены ПК. 5. Принтер Xerox Phaser 3300 MFP	1. Microsoft Windows 7 MSDN реквизиты договора - подписка (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

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 «Методы и средства криптографической защиты 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, Discord.

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

Промежуточная аттестация проводится в форме зачета 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 практическим занятиям и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3Методические указания по освоению дисциплины на лабораторны хработах

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 по дисциплине не предусмотрены

10.5 Методические указания по освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом.

10.6Методические 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

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. Зачет для студентов очной формы обучения в 5 семестре.

Проводится в виде устного собеседования по типовым вопросам.

Типовые вопросы для промежуточной аттестации в форме зачета для студентов очной формы обучения:

Вопросы, направленные на проверку компетенции ОПК-10, ОПК-11:

1. Основные понятия криптографии.
2. Симметричные криптосистемы.
3. Одноразовый блокнот.
4. Алгоритм DES. Разновидности алгоритма DES и атаки на них.
5. Алгоритм AES.
6. Отечественный стандарт шифрования данных ГОСТ 34.12-2015- «Магма», «Кузнечик»
7. Асимметричные криптосистемы.
8. Однонаправленные функции.
9. Алгоритм RSA.
10. Алгоритм Меркла-Хеллмана.
11. Криптосистема Рабина.
12. Поточные шифры.
13. Алгоритмы RC4,RC5, RC6
14. Алгоритм Salsa20, алгоритм ChaCha.
15. ЭЦП. Основные понятия и функциональность. Процедуры постановки и проверки подписи.
16. Хэш-функция. Требования к хэш-функциям.
17. Хэш-функция. SHA.
18. Хэш-функция. MD5.
19. Хэш-функция. ГОСТ34.11-2012
20. Схемы создания ЭЦП. DSA.
21. Схемы создания ЭЦП. RSA.
22. Схемы создания ЭЦП. Алгоритм Эль-Гамаля.
23. Управление ключами. Генерация ключей. Хранение ключей и распределение ключей.
24. Идентификация, аутентификация, авторизация.
25. Способы реализации идентификации и авторизации. Пароли, Хэш-функции.
26. Способы реализации идентификации и авторизации. Шифрование с открытым ключом,

сервер аутентификации Kerberos.

27. Способы реализации идентификации и авторизации. Биометрия.
28. Способы реализации идентификации и авторизации. Идентификационные карты и электронные ключи.
29. Нормативно-правовые акты, обеспечивающие защиту информации

Вопросы, направленные на проверку компетенции ОПК-5.3:

1. ЭЦП. Основные понятия и функциональность. Процедуры постановки и проверки подписи.
2. Хэш-функция. Требования к хэш-функциям.
3. Хэш-функция. SHA.
4. Хэш-функция. MD5.
5. Хэш-функция. ГОСТ34.11-2012
6. Схемы создания ЭЦП. DSA.
7. Схемы создания ЭЦП. RSA.
8. Схемы создания ЭЦП. Алгоритм Эль-Гамаля.
9. Управление ключами. Генерация ключей. Хранение ключей и распределение ключей.
10. Идентификация, аутентификация, авторизация.
11. Способы реализации идентификации и авторизации. Пароли, Хэш-функции.

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