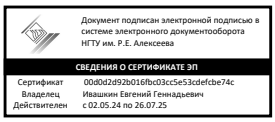
МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева» (НГТУ)

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



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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ОД.5 Основы криптографических методов
(индекс и наименование дисциплины по учебному плану)
для подготовки бакалавров

Направление подготовки: 09.03.02Информационные системы и технологии

Направленность: Безопасность информационных систем

Форма обучения: очная
Год начала подготовки 2025

Выпускающая кафедра ИСУ

Кафедра-разработчик ИСУ

Объем дисциплины 144/4
часов/з.е
Промежуточная аттестация экзамен

Разработчик: Шагалова П.А., к.т.н., доцент

Нижний Новгород

2025

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки09.03.02Информационные системы и технологии, утвержденного приказом МИНОБРНАУКИ РОССИИ от 19 сентября 2017 года № 926на основании учебного плана принятого УМС НГТУ

протокол от 12.12.24 № 5

Рабочая программа одобрена на заседании кафедры 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 № 09.03.02-б-38
Начальник МО _____Е.Г. Севрюкова_

Заведующая отделом комплектования НТБ _____ Н.И. Кабанина

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 «Основы криптографических методов» 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 «Основы криптографических методов»Б1.В.ОД.5 включена в обязательный перечень дисциплин вариативной части (формируемой участниками образовательных отношений), определяющий направленность образовательной программы. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по данному направлению подготовки.

Дисциплина базируется на дисциплинах математического блокапрограммы бакалавриатапо направлению «Информационные системы и технологии». Предшествующими курсами, на которых непосредственно базируется дисциплина «Основы криптографических методов», являются:

- «Алгоритмы и структуры данных»
- «Теоретико-числовые основы криптологии»

Дисциплина «Основы криптографических методов» является основополагающей для изучения следующих дисциплин: «Инструментальные средства информационных систем защиты информации», «Теория и методология информационной безопасности».

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

Дисциплина «Основы криптографических методов» формирует компетенцию ПКС-3 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Дисциплинарная часть компетенции ПКС-3 «Способен обеспечивать безопасность и целостность данных информационных систем»: способен понимать и применять на практике криптографические методы, на которых базируются алгоритмы, обеспечивающие защиту и целостность данных информационных систем.

Таблица 3.1- Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра»							
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
ПКС-3: Способен обеспечивать безопасность и целостность данных информационных систем								
Основы криптографических методов								
Защита программного обеспечения								
Теоретико-числовые основы криптологии								
Безопасность сетевых протоколов								
Защита информационных процессов в компьютерных системах и сетях								
Теория и методология информационной безопасности								
Безопасность информационных технологий								
Техническая защита информации								
Интеллектуальные системы защиты информации								
Защита информации в сетях передачи данных								
Основы построения масштабируемых сетей передачи данных								
Практика по получению профессиональных умений и опыта профессиональной деятельности								
Преддипломная практика								
Выполнение 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**
ПКС-3 Способен обеспечивать безопасность и целостность данных информационных систем	ИПКС-3.2.Способен обеспечивать защиту информации при передаче данных в информационных системах	***Знать:*** – исторические шифры, основные алгоритмы симметричного шифрования, функции хэширования, протоколы цифровой подписи, базовые протоколы проверки подлинности и обмена ключами, – основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности	***Уметь:*** – обосновывать решения в области использовании конкретных криптографических протоколов при проектировании современные защищенных программных комплексов, – проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов – на основе международного опыта квалифицированно анализировать информационные риски в области криптографических протоколов,	***Владеть:*** – современными международными стандартами в области криптографических алгоритмов и протоколовкриптографической защиты информации	Выполнение и сдача 4 лабораторных работ	Экзамен – 20 билетов

Освоение дисциплины причастно к ТФ B/03.6 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу исследования принципов функционирования программных средств криптографической защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работпо семестрам

Общая трудоёмкость дисциплины составляет 4 зач.ед. 144 часов, распределение часов по видам работ семестрам представлено в таблице 4.1.

Таблица 4.1 - Распределение трудоёмкости дисциплины по видам работ по семестрамдля 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:	**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)	**43**	**43**
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.)	43	43
Подготовка к экзамену (контроль)	27	27

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					
5 семестр										
Раздел 1. Введение										
ПКС-3 - ИПКС-3.2	**Тема 1.1.** Исторические шифры	1								
	Итого по 1 разделу	**1**				-				
Раздел 2. Симметричные криптосистемы										
ПКС-3 - ИПКС-3.2	**Тема 2.1.** Одноразовый блокнот.	1				1	Подготовка к лекциям [6.1.1,6.1.2]	Разбор конкретных ситуаций		
	Тема 2.2. Алгоритм DES и его модификации	1				1	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.4]	Разбор конкретных ситуаций		
	Тема 2.3. Алгоритм AES	2				1	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»	2				4	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.4]	Разбор конкретных ситуаций		
	Тема 2.5. Алгоритмы RC4, RC5, RC6, Salsa20, Chacha	3				4	Подготовка к лекциям [6.1.1, 6.1.2]	Разбор конкретных ситуаций		
	Лабораторная работа. Реализация симметричного алгоритма шифрования		8				Подготовка к лабораторной работе.[6.1.1, 6.1.2, 6.1.4]			

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					
	Итого по 2 разделу	**9**	**8**		**1**	**11**				
Раздел 3. Асимметричные криптосистемы										
ПКС-3 - ИПКС-3.2	**Тема 3.1.** Алгоритм RSA.	2				1	Подготовка к лекциям [6.1.1– 6.1.4]	Разбор конкретных ситуаций		
	Тема 3.2. Криптосистема Рабина	2				1	Подготовка к лекциям [6.1.1–6.1.3]	Разбор конкретных ситуаций		
	Тема 3.3. Алгоритм Эль-Гамаля	2				1	Подготовка к лекциям [6.1.1– 6.1.4]	Разбор конкретных ситуаций		
	Тема 3.4. Алгоритм Меркла-Хеллмана	2				1	Подготовка к лекциям [6.1.1–6.1.3]	Разбор конкретных ситуаций		
	Лабораторная работа. Реализация асимметричного алгоритма шифрования		9			5	Подготовка к лабораторной работе.[6.1.1 – 6.1.4]			
	Итого по 3 разделу	**8**	**9**		**1**	**9**				
Раздел 4. Электронные цифровые подписи										
ПКС-3 - ИПКС-3.2	**Тема 4.1.** Функции хэширования: SHA, MD5, ГОСТ 34.11-94	**4**				**2**	Подготовка к лекциям [6.1.2– 6.1.4]	Разбор конкретных ситуаций		
	Тема 4.2. Схемы создания ЭЦП: RSA, DSA, Эль-Гамаля	**4**				**2**	Подготовка к лекциям [6.1.2– 6.1.4]	Разбор конкретных ситуаций		
	Лабораторная работа. Реализация хеш-функции		**9**			**5**	Подготовка к лабораторной работе.[6.1.2 – 6.1.4]			
	Лабораторная работа. Реализация схемы создания электронной цифро-		**8**			**4**	Подготовка к лабораторной работе.[6.1.2 – 6.1.4]			

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					
	вой подписи									
	Итого по 3 разделу	**8**	**17**		**1**	**13**				
Раздел 5. Идентификация и аутентификация										
ПКС-3 - ИПКС-3.2	**Тема 5.1.** Пароли, использование хеш-функции, шифрование с открытым ключом, сервер аутентификации Kerberos, биометрия, идентификационные карты и электронные ключи.	**5**				**6**	Подготовка к лекциям [6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Итого по 3 разделу	**5**			**0,5**	**6**				
Раздел 6. Управление ключами										
ПКС-3 - ИПКС-3.2	**Тема 6.1.** Генерация ключей, хранение ключей, распределение ключей	**3**				**4**	Подготовка к лекциям [6.1.1, 6.1.4]	Разбор конкретных ситуаций		
	Итого по 3 разделу	**3**			**0,5**	**4**				
	Подготовка к экзамену (контроль)				**2**	**27**				
	Итого за семестр	**34**	**34**	**-**	**6**	**43**				

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 экзамена:

– 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 «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 которойуспеваемость студентовоценивается 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
ПКС-3. Способен проводить разработку и анализ объектов информационной безопасности	ИПКС-3.2. Разрабатывает объекты информационной безопасности	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.

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 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 (дата обращения: 30.11.2021)

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 (дата обращения: 30.11.2021)

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 (дата обращения: 30.11.2021)

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 (дата обращения: 30.11.2021)

6.3 Перечень журналов по профилю дисциплины:

Использование журналов не предусмотрено при изучении дисциплины.

6.4 Методические указания, рекомендации и другие материалы к занятиям

Методические указания по выполнению практических работ по дисциплине «Основы криптографических методов» отправляются на электронные адреса групп.

6.1.7. Метод. указания для лабораторных работ по дисциплине «Основы криптографических методов», для студентов направления подготовки 09.03.02 «Информационные системы и технологии» 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	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 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 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 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/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 бакалавриатадля 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	Оснащенностьаудиторий 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 +GeFORCE 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 ZNFC-CR5D-5U3U-JKGP от 20.05.2024)
	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 «Основы криптографических методов», 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 сформированностикомпетенции применяетсябалльно-рейтинговаясистема контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачета с оценкой 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 допороговому 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 4.4, 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 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 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 вРазделе 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. Экзамен для студентов очной формы обучения в 5 семестре.

Проводится в виде устного собеседования по типовым вопросам.

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

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

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