

МИНОБРНАУКИ РОССИИ

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

Образовательно-научный институт экономики и управления (ИНЭУ)

(Полное и сокращенное название института, реализующего данное направление)

УТВЕРЖДАЮ:
Директор института:

С.Н. Митяков

подпись

ФИО

« 18 » марта

2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ОД 21 Информационная безопасность

для подготовки бакалавров

Направление подготовки: 27.03.03. Системный анализ и управление

Направленность: Цифровая аналитика

Форма обучения: очная

Год начала подготовки 2025

Выпускающая кафедра: Цифровая экономика (ЦЭ)

Кафедра разработчик ЦЭ

Объем дисциплины 180/5

Промежуточная аттестация: экзамен, курсовая работа

Разработчик: Болоничева Т.В., доцент

Нижний Новгород, 2025

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 27.03.03. Системный анализ и управление, утвержденного приказом МИНОБР-НАУКИ РОССИИ от 07 августа 2020 года № 902 на основании учебного плана принятого УМС НГТУ

протокол от 19.12.2025 № 7

Рабочая программа одобрена на заседании кафедры протокол от 18.03.25 №1

Зав. кафедрой д.ф-м.н, профессор _____ С.Н. Митяков
(подпись)

Программа рекомендована к утверждению ученым советом института ИНЭУ, Протокол от 18.03.25 №2

Рабочая программа зарегистрирована в УМУ регистрационный № 27.03.03-я-47
Начальник МО _____ Севрюкова Е.Г.

Заведующая отделом комплектования НТБ _____ Кабанина Н.И.

Рецензент: д.э.н., зав.кафедрой «Менеджмент» Мурашова Н.А.
(ФИО, ученая степень, ученое звание)

_____ (подпись)

«_18.03.2025»_

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	4
4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	7
4.1. Распределение трудоемкости дисциплины по видам работ по семестрам.....	7
4.2. Содержание дисциплины, структурированное по темам	9
5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ	11
6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	13
6.1. Учебная литература, печатные издания библиотечного фонда	13
6.2. Справочно-библиографическая литература	14
6.3. Методические указания, рекомендации и другие материалы к занятиям	14
7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	14
7.1. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины (модуля)	14
7.2. Перечень программного обеспечения и информационных справочных систем	15
8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ	15
9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	16
10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	16
10.1. Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии	16
10.2. Методические указания для занятий лекционного типа	16
10.3. Методические указания по освоению дисциплины на практических занятиях	17
10.4. Методические указания по самостоятельной работе обучающегося	17
11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ	18
11.2. Типовые вопросы для промежуточной аттестации в форме экзамена...	19
11.3. Типовые задания для текущего контроля	20
ПРИЛОЖЕНИЕ	22
Лист актуализации	24

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Целями освоения дисциплины являются:

- обучение использованию, обобщению и анализу информации для решения профессиональных задач,
- ознакомление с основами возможностями шифрования, тенденциями их развития,
- обучение принципам построения криптографических протоколов,
- приобретение навыков шифрования информации,
- ознакомление с основными информационными технологиями, необходимыми для решения профессиональных задач, изучение методов и способов получения, хранения и переработки информации
- применение современных информационных технологий и компьютерной техники в профессиональной деятельности.

В курсе изучаются основные термины и понятия информационной безопасности, технические и программные средства реализации данных процессов.

1.2. Задачи освоения дисциплины (модуля):

- получение и использование навыков работы с техническими и программными средствами для шифрования информации, получение навыков обработки текстовой и числовой информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина Б1. В.ОД21 «Информационная безопасность» включена в обязательный перечень дисциплин вариативной части образовательной программы. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по направлению подготовки 27.03.03. Системный анализ и управление.

Дисциплина базируется на следующих дисциплинах: Анализ и визуализация данных, Аналитика больших данных, Корпоративные информационные системы, Архитектура информационных бизнес-систем.

Дисциплина «Информационная безопасность» является основополагающей для изучения следующих дисциплин: Реинжиниринг бизнес-процессов, Сетевые технологии, Информационные системы обработки данных, Научно-исследовательская практика, Преддипломная практика, выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы.

Рабочая программа дисциплины «Информационная безопасность» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1. Процесс изучения дисциплины (модуля) направлен на формирование элементов следующих общепрофессиональных компетенций в соответствии с ОПОП ВО по

направлению 27.03.03. Системный анализ и управление:

ПК-5 способен применять технологии цифровой аналитики при разработке бизнес-требований к системе, сборе и изучении запросов заинтересованных лиц

Формирование указанных компетенций размещено в таблице 1.

Таблица 1 - Формирование компетенций дисциплинами

Наименование дисциплин, формирующих компетенцию совместно	Семестры формирования дисциплины							
	1	2	3	4	5	6	7	8
ПК-5								
Реинжиниринг бизнес-процессов								
Анализ и визуализация данных								
Аналитика больших данных								
Сетевые технологии								
Информационная безопасность								
Информационные системы обработки данных								
Корпоративные информационные системы								
Архитектура информационных бизнес-систем								
Научно-исследовательская практика								
Преддипломная практика								
Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы								

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы (ОП)

Таблица 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			Код ПС и ТФ	Оценочные средства	
		Планируемые результаты обучения по дисциплине	Текущего контроля	Промежуточной аттестации			
ПК-5 способен применять технологии цифровой аналитики при разработке бизнес-требований к системе, сборе и изучении запросов заинтересованных лиц	ИПК 5.2 Формулирует бизнес-требования к системам с учетом запросов заинтересованных лиц	Знать: - требования к информационной безопасности при применении технологий цифровой аналитики, методы и средства обеспечения информационной безопасности; основные технические средства и методы защиты информации (ИПК-1.3)	Уметь: - проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, применять на практике основные общеметодологические принципы теории информационной безопасности (ИПК-1.3)	Владеть: - навыками применения методов обеспечения информационной безопасности при проектировании концептуальной архитектуры системы на основе разработанных программ и методик (ИПК-1.3)	C/03.6 (06.022) Системный аналитик	Участие в групповых обсуждениях Выполнение практических заданий	Вопросы для устного собеседования

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 и семестрам представлено в таблице 3.

Таблица 3 – Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость в час	
	Всего час.	В т.ч. по семестрам 4 сем
Формат изучения дисциплины		с использованием элементов электронного обучения
Общая трудоёмкость дисциплины по учебному плану	180	180
1. Контактная работа:	76	76
1.1. Аудиторная работа, в том числе:	68	68
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практика, занятия и др.)	34	34
лабораторные работы (ЛР)		
1.2. Внеаудиторная, в том числе	8	8
курсовая работа (проект) (КР/КП) (консультация, защита)	2	2
текущий контроль, консультации по дисциплине	6	6
контактная работа на промежуточном контроле (КРА)		
2. Самостоятельная работа (СРС)	68	68
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.)	68	68
Подготовка к экзамену (контроль)	36	36

4.2. Содержание дисциплины, структурированное по темам

Таблица 4 - Содержание дисциплины, структурированное по темам

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	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа			Самостоятельная работа студентов (час)			
ПК-5 способен применять технологии цифровой аналитики при разработке бизнес-требований к системе, сборе и изучении запросов заинтересованных лиц ИПК 5.2 Формулирует бизнес-требования к системам с учетом запросов заинтересованных лиц	Раздел 1 Основы информационной безопасности и защиты информации	Лекции	Лабораторные работы	Практические занятия	подготовка к лекциям 1.4 (глава 1-2)	Дискуссия		
	Тема 1.1. Основные составляющие информационной безопасности	2			5			
	Тема 1.2. Средства защиты информации	2			5			
	Тема 1.3. Способы передачи конфиденциальной информации на расстоянии	3			7			
	Практическая работа №1. Выполнение индивидуальных заданий по лабораторной работе «Шифрование»			3		подготовка к ПР 3.3 (ст. 5-6); 3.8 (ст. 18-19);		

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	Наименование разработанного Электронного курса (трудоемкость в часах)			
		Контактная работа			Самостоятельная работа студентов (час)						
		Лекции	Лабораторные работы	Практические занятия							
	информации» Защита практической работы			4							
	Итого по 1 разделу	7		7	17						
	Раздел 2 Основные термины и определения. Классификация шифров					подготовка к лекциям 1.4 (глава 1-2)	Дискуссия				
	Тема 2.1. Основные термины и определения	3			5						
	Тема 2.2. Основные требования, предъявляемые к криптосистемам	3			5						
	Тема 2.3. Классификация криптографических систем	3			7						
	Практическая работа №2. Выполнение индивидуальных заданий по лабораторной работе «Шифрование информации» Защита практической работы			8 1		подготовка к ПР 3.3 (ст. 7-9); 3.8 (ст. 27-30);					
	Итого по 2 разделу	9		9	17						

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	Наименование разработанного Электронного курса (трудоемкость в часах)			
		Контактная работа			Самостоятельная работа студентов (час)						
		Лекции	Лабораторные работы	Практические занятия							
Раздел 3 Способы шифрования				подготовка к лекциям 1.4 (глава 3)							
Тема 3.1. Шифры перестановки, замены и гаммирования	3			5							
Тема 3.2. Квантовое шифрование и комбинированные шрифты	3			5							
Тема 3.3. Шифрование с открытым ключом и Хеш-функции	3			7							
Практическая работа №3. Выполнение индивидуальных заданий по лабораторной работе «Шифрование информации» Защита практической работы			8		подготовка к ПР 3.3 (ст. 9-10); 3.8 (ст. 22-24);						
Итого по 3 разделу	9		9	17							
Раздел 4 Криптографические протоколы				подготовка к лекциям 1.4 (глава 4)							
Тема 4.1. Разнообразие криптографических протоколов	3			5							
Тема 4.2. Основы	3			5							

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	Наименование разработанного Электронного курса (трудоемкость в часах)			
		Контактная работа			Самостоятельная работа студентов (час)						
		Лекции	Лабораторные работы	Практические занятия							
	криptoанализы										
	Тема 4.3. Кодирование информации	3			7						
	Практическая работа №4. Выполнение индивидуальных заданий по практической работе «Идентификация и аутентификация. Электронная цифровая подпись» Защита практической работы			8 1		подготовка к ПР 3.3 (ст. 9-10); 3.8 (ст. 22-24);					
	Итого по 4 разделу	9		9	17						
	ИТОГО ЗА СЕМЕСТР	34		34	68						
	ИТОГО по дисциплине	34		34	68						

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

Для осуществления текущего контроля знаний обучающихся сформулированы теоретические вопросы по темам лабораторных работ и примеры заданий для домашних и контрольных работ.

Типовые задания для текущего контроля усвоения знаний, умений и навыков представлены в оценочных материалах по дисциплине «Информационная безопасность», которые хранятся на кафедре «Цифровая экономика».

5.2. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Таблица 5 При текущем контроле (контрольные недели) и оценка выполнения практических работ

Шкала оценивания	Экзамен/ Зачет с оценкой	Зачет
40<R≤50	Отлично	зачет
30<R≤40	Хорошо	
20<R≤30	Удовлетворительно	
0<R≤20	Неудовлетворительно	незачет

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

Таблица 6 - Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код наименование компетенции	Код 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
ПК-5 способен применять технологии цифровой аналитики при разработке бизнес-требований к системе, сборе и изучении запросов заинтересованных лиц	ИПК 5.2 Формулирует бизнес-требования к системам с учетом запросов заинтересованных лиц	Не способен грамотно и логически верно излагать, и использовать теоретический материал. Не способен определять причинно-следственные связи. Не может ответить на уточняющие вопросы преподавателя.	Способен анализировать изученный теоретический материал, однако допускает значительные ошибки. Не способен ответить на уточняющие вопросы. Испытывает затруднения при определении причинно-следственных связей.	Способен анализировать изученный теоретический материал, но допускает незначительные ошибки. Отвечает на уточняющие вопросы неполно/некорректно.	Имеет глубокие знания всего материала дисциплины; изложение полученных знаний полное, системное; допускаются единичные ошибки, самостоятельно исправляемые при собеседовании

Таблица 7 – Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично) – «зачет»	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) – «зачет»	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) – «зачет»	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) – «незачет»	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 Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. - Москва : МИСиС, 2023. - 254 с. - ISBN 978-5-907560-71-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785907560710.html> (дата обращения: 12.05.2025)

6.1.2 Сафиуллина, Л. Х. Информационная безопасность. Практические аспекты : учебник для вузов / Сафиуллина Л. Х. , Касимова А. Р. , Рябов Я. С. , Садыков А. М. , Богомолов В. А. - Санкт-петербург : Интермедиа, 2021. - 240 с. - ISBN 978-5-4383-0205-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785438302056.html> (дата обращения: 12.05.2025).

6.1.3 Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. - 4-е изд. , стер. - Москва : ФЛИНТА, 2022. - 184 с. - ISBN 978-5-9765-1904-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785976519046.html> (дата обращения: 12.05.2025)

6.2 Справочно-библиографическая литература

6.2.1 Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. - 2-е изд. - Москва : ДМК Пресс, 2023. - 451 с. Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10". - ISBN 978-5-89818-453-7. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785898184537.html> (дата обращения: 12.05.2025)..

6.2.2. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. - Москва : Инфра-Инженерия, 2022. - 104 с. - ISBN 978-5-9729-0864-6. - Текст :

электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785972908646.html> (дата обращения: 12.05.2025).

6.2.3. Куковская, А. В. Практикум по профессиональной коммуникации в области информационной безопасности : учебное пособие для бакалавриата направления подготовки 10. 03. 01 "Информационная безопасность" / А. В. Куковская, О. О. Макарова. - Москва : Проспект, 2021. - 240 с. - ISBN 978-5-392-35208-1. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785392352081.html> (дата обращения: 12.05.2025).

6.3. Методические указания, рекомендации и другие материалы к занятиям

Методические указания и рекомендации по проведению конкретных видов учебных занятий по дисциплине «Информационная безопасность» находятся на кафедре «Цифровая экономика».

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

7.1. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Научная электронная библиотека E-LIBRARY.ru. – Режим доступа: <http://elibrary.ru/defaultx.asp>
2. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. – Режим доступа: <http://elib.tolgas.ru/> - Загл. с экрана.
3. Электронно-библиотечная система Znarium.com [Электронный ресурс]. - Режим доступа: <http://znarium.com/>. – Загл. с экрана.
4. Открытое образование [Электронный ресурс]. - Режим доступа: <https://openedu.ru/>. - Загл с экрана.
5. Polpred.com. Обзор СМИ. Полнотекстовая, многоотраслевая база данных (БД) [Электронный ресурс]. - Режим доступа: <http://polpred.com/>. – Загл. с экрана.
6. Базы данных Всероссийского института научной и технической информации (ВИНИТИ РАН) по естественным, точным и техническим наукам Электронный ресурс]. - Режим доступа: <http://www.viniti.ru>. – Загл. с экрана.
7. Университетская информационная система Россия [Электронный ресурс]. - Режим доступа: <http://uisrussia.msu.ru/>. – Загл. с экрана.
8. Научно-техническая библиотека НГТУ <http://www.nntu.ru/RUS/biblioteka/bibl.html>. Электронные библиотечные системы. Электронный каталог книг <http://library.nntu.nnov.ru/>.
9. Электронный каталог периодических изданий <http://library.nntu.nnov.ru/>
10. Гости Нормы, правила, стандарты и законодательство России <http://www.nntu.ru/RUS/biblioteka/resyrs/norma.htm>.

7.2. Перечень программного обеспечения и информационных справочных систем

Таблица 8 – Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка, по которой осуществляется доступ 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/

В таблице 10 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.

Таблица 9 - 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.gost.ru/portal/gost//home/standarts
2	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 10 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/>

На сайте НГТУ размещены в формате PDF материалы, разработанные по курсу
Таблица 10 - 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:

- специализированная аудитория 6130/6131 с проектором и доступом в Интернет для проведения лекций, семинаров самостоятельной работы и презентаций.

Наименование оборудованного учебного кабинета	Оснащенность оборудованного учебного кабинета	Программное обеспечение
Компьютерный класс № 6130 учебно-лабораторного корпуса № 6	<p>1. ПК с процессорами (CPU) IntelCore™ i3 CPU3200@3.7 Ghz, OZU 4 Ggb, Intel HD Graphics integrate, HDD 320Ggb, в составе локальной вычислительной сети, с подключением к интернету. Монитор 17"- 16 шт.</p> <p>2. Доска меловая -1шт.</p> <p>3. Компьютерные столы - 16шт.</p> <p>4. Рабочее место студента - 15</p> <p>5. Рабочее место преподавателя - 1 Для инвалидов и лиц с ОВЗ: переносная клавиатура адаптированная</p>	<p>1. Windows10 Pro для учебных заведений (подписка DreamSpark Premium, договор № 0509/KMP от 15.10.18);</p> <p>2. Adobe Acrobat Reader DC-Russian;(беспл.)</p> <p>3. MsOfficeProPlus 2007 (лицензия № 42470655);</p> <p>4. MathCad 15 M010(PKG-7543-FN, MNT- PKG -7543-FN-T2 договор № 28-13/13-057 от 26.02.13 бессрочное).</p> <p>5. Free Pascal 2.6.4 6. Gimp 2.8.18;</p> <p>6. inkscape: 1.0.2_2021-01-15_e86c870879-x64 free ware</p> <p>7. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24)</p>
Компьютерный класс № 6131 учебно-лабораторного корпуса № 6	<p>1. Моноблоки HP3420 на процессорах Pentium Dual Core 2.81Ghz, OZU 4Ggb,PC3,Hdd 500 Ggb. Video интегрированное Intel Hd Graphic., в составе локальной вычислительной сети, с подключением к интернету 12шт.; Преподавательский ПК AMD Athlon 64X2 Dual Core CPU 4600+, 2 Ggb ОЗУ, HDD 160Ggb.</p> <p>2. Доска меловая - 1 шт.</p> <p>3. Компьютерные столы - 13</p> <p>4. Рабочее место студента - 12</p> <p>5. Рабочее место для преподавателя - 1 Для инвалидов и лиц с ОВЗ: переносная клавиатура адаптированная</p>	<p>1. Windows 8.1 корпоративная 68980858 от 10.10.2017;</p> <p>2. Adobe Acrobat Reader DC-Russian (беспл.)</p> <p>3. MsOfficeProPlus 2007 (лицензия № 42470655);</p> <p>4. MathCad 15 M010(PKG-7543-FN, MNT- PKG -7543-FN-T2 договор № 28-13/13-057 от 26.02.13 бессрочное).</p> <p>5. CorelDraw Graphics suiteX6 LicenseML DR16C22-AFMMDBRT-2HTBNJ3- FQHHS2G (бессрочная)</p> <p>6. Gimp 2.8.18;</p> <p>7. inkscape: 1.0.2_2021-01-15_e86c870879-x64 free ware</p> <p>8. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24)</p>

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.

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;

- разбор конкретных ситуаций.

При преподавании дисциплины «Информационная безопасность», используются

современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы 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, как встреч с студентами, так и современных информационных технологий: чат, электронная почта, ZOOM.

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

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

Промежуточная аттестация проводится в форме экзамена с учетом текущей успеваемости.

Результат обучения считается сформированным на повышенном уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент исчерпывающе, последовательно, четко и логически излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, 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 стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, 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.

Методические указания для занятий лекционного типа, по освоению дисциплины на практических занятиях и по самостоятельной работе находятся в оценочных материалах по дисциплине «Информационная безопасность», которые хранятся на кафедре «Цифровая экономика».

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 (Таблица 4). 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.

В ходе лекционных занятий рекомендуется вести конспектирование учебного материала.

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 и 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 (указано в таблице 11). 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:

- обсуждение теоретических вопросов;
- решение ситуационных задач;
- тестирование;
- экзамен.

Типовые задания по каждому виду текущего контроля представлены в оценочных материалах по дисциплине «Информационная безопасность», которые хранятся на кафедре «Цифровая экономика».

11.2. Типовые вопросы для промежуточной аттестации в форме экзамена

Промежуточный контроль знаний осуществляется преподавателем в форме экзамена, включающего устный ответ на 2 теоретических вопроса.

1. Понятия «информационная безопасность» и «защита информации». Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.
3. Средства защиты информации.
4. Криптография. Основные термины и определения.
5. Классификация криптографических систем.
6. Шифры замены. Классификация и основные методы шифрования.
7. Шифры перестановки. Классификация и основные методы шифрования.
8. Шифры гаммирования. Классификация и основные методы шифрования.
9. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм.
10. Схема режима шифрования DES-ECB.
11. Схема режима шифрования DES-CBC.
12. Схема режима шифрования DES-CPB и DES-OFB.
13. Тройной DES. Сфера применения различных режимов DES.
14. ГОСТ 28147-89. Схема режима шифрования простой замены.
15. AES. Краткая характеристика основных этапов зашифрования/расшифрования.
16. ГОСТ 34.12-2015. Схема шифрования блочного шифра "Кузнецик".
17. Шифрование с открытым ключом. Основные понятия.
18. Алгоритм шифрования RSA.
19. Алгоритм шифрования Эль-Гамаля.
20. Алгоритм шифрования на основе задачи об укладке ранца.
21. Эллиптические кривые. Основные понятия. Сложение и умножение точки.
22. Алгоритм шифрования на основе эллиптических кривых.
23. Хэш-функции. Основные понятия и разновидности.
24. Хэш-функция MD5.
25. Криптографические протоколы. Основные понятия.
26. Протоколы обмена ключами.
27. Протоколы аутентификации. Разновидности и краткая характеристика.
28. Парольная идентификация/аутентификация.
29. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.
30. Сервер аутентификации Kerberos.
31. Идентификация/аутентификация с помощью биометрических данных.
32. Идентификационные карты (ID-cards) и электронные ключи.
33. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
34. ЭЦП на базе алгоритма RSA.
35. Алгоритм цифровой подписи ГОСТ 34.10-94.
36. Алгоритм цифровой подписи ГОСТ 34.10-2001.
37. Протоколы контроля целостности. Разновидности и краткая характеристика.
38. Протоколы контроля целостности. Биты четности, контрольные цифры и числа.
39. Протоколы контроля целостности. Использование ЭЦП и MAC-кодов.
40. Протоколы контроля целостности. Коды Хэмминга и ECC.
41. Электронные платежи. Разновидности и краткая характеристика.
42. Цифровые деньги на базе "слепой" ЭЦП.
43. Биткойн. Блокчейн, сеть и узлы.
44. Биткойн. Адрес.
45. Биткойн. Транзакция.
46. Биткойн. Блок.
47. Биткойн. Дерево Меркля, майнинг и ветвления блокчейна.
48. Классическое («бумажное») голосования.

49. Электронное голосование. Разновидности и краткая характеристика.
50. Российский опыт электронного голосования.
51. Протоколы разбиения и разделения секрета.
52. Тайные многосторонние вычисления.
53. Сложность алгоритмов.
54. Простые числа.
55. Разложение числа на простые сомножители.
56. Нахождение начального списка простых чисел.
57. Тестирование числа на простоту.
58. Определение наибольшего общего делителя.
59. Основные сведения о криптоанализе и атаки на криптосистемы.
60. Классическая стеганография.
61. Компьютерная стеганография.
62. Общие сведения о кодировании.
63. Общедоступные кодовые системы.
64. Представление чисел в двоичном виде.
65. Секретные кодовые системы.

11.3. Типовые задания для текущего контроля

Практическая работа № 1 Шифры перестановки

В необходимо зашифровать свою фамилию (для первых двух шифров) или фамилию и имя (для остальных) с помощью следующих шифров:

- простой одинарной перестановки;
- блочной одинарной перестановки;
- табличной маршрутной перестановки;
- вертикальной перестановки;
- поворотной решетки;
- магический квадрат (размер квадрата - 4x4);
- двойной перестановки.

При оформлении отчета необходимо привести исходное сообщение (фамилию или фамилию и имя), таблицы, ключевые слова (выбираются произвольно), маршруты вписывания и выписывания, повороты решетки и зашифрованное сообщение.

Практическая работа № 2 Шифры перестановки

Зашифровать свою фамилию и имя с помощью шифров:

- шифра «Перекресток»;
- шифры с использованием треугольника.

Практическая работа № 3 Шифры перестановки. Комбинированные шрифты

1. В необходимо зашифровать свою фамилию с помощью следующих шифров:
 - шифра Цезаря;
 - лозунгового шифра;
 - полибианского квадрата;
 - шифрующей системы Трисемуса;
 - шифра Playfair;
 - системы омофонов (допускается для каждой буквы алфавита привести всего по две шифrozамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах);
 - шифра Виженера.

При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифrozамен не является ключом) и зашифрованное сообщение.

2. Зашифровать свою фамилию с помощью шифров:

- шифра масонов;
- биграммного шифра Порты;
- шифра Хилла;
- вариантного шифра;
- шифра Тени;
- совмещенного шифра.

В работе необходимо зашифровать свою фамилию и имя с помощью шифра ADFGVX.

При оформлении отчета необходимо привести исходное сообщение (фамилию и имя), таблицу шифrozамен, ключевое слово, перестановочную таблицу и зашифрованное сообщение.

Практическая работа № 4 Идентификация и аутентификация. Электронная подпись

1. В работе необходимо привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:

- на основе алгоритма RSA;
- по схеме Шнорра;
- по схеме Фейге-Фиата-Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа (k или r) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

2. В работе необходимо привести последовательность выполнения процедур генерации и проверки ЭЦП с использованием следующих способов:

- на базе алгоритма RSA;
- по ГОСТ 34.10-94;
- по ГОСТ 34.10-2001.

При оформлении отчета необходимо привести таблицы генерации ключей, отправки сообщения с ЭЦП и получения сообщения с ЭЦП. В качестве хеш-образа исходного сообщения $h(T)$ принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

РЕЦЕНЗИЯ

на рабочую программу дисциплины «Б.1.ОД.21 «Информационная безопасность»
ОП ВО по направлению: 27.03.03. Системный анализ и управление,
Направленность: Цифровая аналитика

квалификация выпускника – бакалавр

Мурашова наталья Александровна, зав.кафедрой «Менеджмент» НГТУ им. Р.Е. Алексеева, д.э.н. (далее по тексту рецензент), провела рецензию рабочей программы дисциплины «Информационная безопасность» ОП ВО по направлению 27.03.03. Системный анализ и управление, направленность «Цифровая аналитика» (бакалавриат) разработанной в ФГБОУ ВО «Нижегородский государственный технический университет имени Р.Е. Алексеева», на кафедре «Цифровая экономика» (разработчик – Болоничева Татьяна Владимировна, к.э.н.)

Рассмотрев представленные на рецензию материалы, рецензент пришел к следующим выводам:

Программа соответствует требованиям ФГОС ВО по направлению 27.03.03. Системный анализ и управление». Программа содержит все основные разделы, соответствует требованиям к нормативно-методическим документам. Представленная в Программе актуальность учебной дисциплины в рамках реализации ОПОП ВО не подлежит сомнению – дисциплина «Информационная безопасность» является обязательной дисциплиной для профиля «Цифровая аналитика» направления подготовки 27.03.03. Системный анализ и управление.

Представленные в Программе цели дисциплины соответствуют требованиям ФГОС ВО направления 27.03.03. Системный анализ и управление.

В соответствии с Программой за дисциплиной «Информационная безопасность» закреплены ПК-2. Дисциплина и представленная Программа способны реализовать их в объявленных требованиях.

Результаты обучения, представленные в Программе в категориях знать, уметь, владеть соответствуют специфике и содержанию дисциплины и демонстрируют возможность получения заявленных результатов.

Общая трудоёмкость дисциплины «Информационная безопасность» составляет 4 зачётные единицы (144 часа). Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин соответствует действительности. Дисциплина «Информационная безопасность» взаимосвязана с другими дисциплинами ОП ВО и Учебного плана по направлению 27.03.03. Системный анализ и управление, и возможность дублирования в содержании отсутствует.

Представленная Программа предполагает использование современных образовательных технологий, используемых при реализации различных видов учебной работы. Формы образовательных технологий соответствуют специфике дисциплины.

Виды, содержание и трудоёмкость самостоятельной работы студентов, представленные в Программе, соответствуют требованиям к подготовке выпускников, содержащимся во ФГОС ВО направления 27.03.03. Системный анализ и управление.

Представленные и описанные в Программе формы текущей оценки знаний (опрос, как в форме обсуждения отдельных вопросов, так и выступления и участие в дискуссиях, участие в тестировании,) и аудиторных заданиях – решение ситуационных задач), соответствуют специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме экзамена, что соответствует статусу обязательной

дисциплины учебного цикла – Б1ФГОС ВО направления 27.03.03. Системный анализ и управление.

Нормы оценки знаний, представленные в Программе, соответствуют специфике дисциплины и требованиям к выпускникам.

Учебно-методическое обеспечение дисциплины представлено: основной литературой – 3 наименования, дополнительной литературой – 3 наименования, и соответствует требованиям ФГОС ВО направления 27.03.03. Системный анализ и управление.

Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Информационная безопасность» и обеспечивает использование современных образовательных, в том числе интерактивных методов обучения.

ОБЩИЕ ВЫВОДЫ

На основании проведенной рецензии можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Информационная безопасность» ОП ВО по направлению 27.03.03. Системный анализ и управление, направленность «Цифровая аналитика» (бакалавриат), разработанная Болоничевой Т.В., доцентом кафедры «Цифровая экономика», к.э.н., соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Мурашова Наталья Александровна,
Зав. Кафедрой «Менеджмент»
НГТУ им. Р.Е. Алексеева, д.э.н.

Мурашова Н.А.