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

Дзержинский политехнический институт (филиал)

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 056E86B29D369D826C7E310ADEA6E8DA
Владелец: Петровский Александр Михайлович
Действителен: с 03.08.2022 до 27.10.2023

УТВЕРЖДАЮ:
Директор института
_____ А.М. Петровский
«__05_» _____мая_____2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.Б.30 «Информационная безопасность и защита информации»

(индекс и наименование дисциплины по учебному плану)
для подготовки бакалавров

Направление подготовки: 01.03.04 Прикладная математика

Направленность: Математические и компьютерные методы для современных технологий

Форма обучения: очная

Год начала подготовки2022

Выпускающая кафедра Автоматизация, энергетика, математика и информационные системы

Кафедра-разработчик Автоматизация, энергетика, математика и информационные системы

Объем дисциплины 108 / 3
часов / з.е.

Промежуточная аттестациязачет с оценкой

Разработчик: Наумова Е.Г., к.т.н.

Дзержинск 2022

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования(ФГОС ВО 3++) по направлению подготовки 01.03.04 Прикладная математика, утвержденного приказом МИНОБРНАУКИ РОССИИ от 10.01.2018 г. № 11

на основании учебного плана принятого УС ДПИ НГТУ
протокол от 28.04.2022 № 8

Рабочая программа одобрена на заседании кафедры-разработчика РПДАвтоматизация, энергетика, математика и информационные системы
протокол от 05.05.2022 № 6

Заведующийкафедрой АЭМИС, к.т.н., доцент

Л.Ю. Вадова

(подпись) *(расшифровка подписи)*

СОГЛАСОВАНО:

Заведующийвыпускающей кафедрой «Автоматизация, энергетика, математика и информационные системы»,
к.т.н., доцент

Л.Ю. Вадова

(подпись) *(расшифровка подписи)*

Начальник ОУМБО И.В. Старикова

(подпись) *(расшифровка подписи)*

Рабочая программа зарегистрирована в ОУМБО: 01.03.04 - 30

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целью освоения дисциплины является изучение методов практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

1.2. Задачи освоения дисциплины (модуля):

− Понимать сущность информационной безопасности;

− Понимать принципы организации защиты информации на предприятиях;

− Применять программно-аппаратные средства для обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Информационная безопасность и защита информации» включена в обязательный перечень дисциплин в рамках базовой части Блока 1 установленного ФГОС ВО.

Дисциплина базируется на следующих дисциплинах: Информатика, Операционные системы, Банки и базы данных.

Дисциплина Информационная безопасность и защита информации является основополагающей для прохождения преддипломной практики и выполнения выпускной квалификационной работы.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом осо-бенностей психофизического развития, индивидуальных возможностей и состояния здо-ровья таких обучающихся, по их личному заявлению.

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

Таблица 3.1

Формирование компетенции ОПК-3 дисциплинами

Наименование дисциплин, формирующих компетенцию совместно	**Семестры формирования компетенций дисциплинами.**							
Код компетенции ОПК-3.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Информатика	x							
Операционные системы				x				
Информационная безопасность и защита информации								x
Выполнение и защита выпускной квалификационной работы								x

ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОП

Таблица 3.3

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

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной аттестации**
ОПК-3. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	**ИОПК-3.3.** Учитывает основные требования информационной безопасности при решении задач профессиональной деятельности.	**Знать:** возможные угрозы безопасности информации, методы и средства защиты информации, методы разработки внутренней политики безопасности фирмы, программные средства, используемые для обеспечения безопасности информации	**Уметь:** проводить анализ объекта защиты, проектировать, настраивать и эксплуатировать систему защиты информации	**Владеть:** навыками работы в проектировании системы защиты, навыками работы с программными средствами, используемыми для обеспечения безопасности информации.	Тестирование в системе MOODLE (2 тестирования, в базе каждого тестирования около 100 вопросов), собеседование и отчёты при сдаче лабораторных работ	По результатам накопительного рейтинга или в форме компьютерного тестирования

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач.ед. / 108 часов, распределение часов по видам работ и семестрам представлено в таблицах 4.1.

Формат изучения дисциплины: с использованием элементов электронного обучения

Таблица 4.1

Распределение трудоёмкости дисциплины по видам работ по семестрам
для обучающихся очной формы обучения

Вид учебной работы	**Всего часов**	**Семестр**
		8
1. Контактная работа обучающихся с преподавателем (по видам учебных занятий) **(всего),** в том числе:	44	44
1.1. Аудиторные занятия (всего), в том числе:	40	40
- лекции (Л)	20	20
- лабораторные работы (ЛР)	20	20
- практические занятия (ПЗ)		
- практикумы (П)		
1.2. Внеаудиторные занятия (всего), в том числе:	4	4
- групповые консультации по дисциплине	4	4
- групповые консультации по промежуточной аттестации (экзамен)		
- индивидуальная работа преподавателя с обучающимся: - по проектированию: проект (работа) - по выполнению РГР - по выполнению КР - по составлению реферата, доклада, эссе		
2. Самостоятельная работа обучающихся (СРС) (всего)	64	64
Вид промежуточной аттестации зачет с оценкой	**зачет с оценкой**	**зачет с оценкой**
Общая трудоемкость, часы/зачетные единицы	**108/3**	**108/3**

4.2. Содержание дисциплины, структурированное по темам

Содержание дисциплины, структурированное по темам, приведено в таблице 4.2.

Таблица 4.2

Содержание дисциплины, структурированное по темам
для обучающихся очной формы обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				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 обучающихся (СРС), час				
		Лекции, час	Лабораторные работы, час	Практические занятия, час					
8 семестр									
ОПК-3	**Раздел 1** Общие вопросы информационной безопасности					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.1: разделы 2, 3; 6.1.2: разделы 1.1, 1.2, 1.4 6.1.3: тема 1			
	Тема 1.1. Основные понятия	1			2		Тестирование в системе MOODLE (Тест 1)		
	Тема 1.2. Угрозы	1			2				
	Тема 1.3. Классификация средств защиты	1			2				
	Лабораторная работа № 5 Анализ объекта защиты (часть 1)		1		2	Подготовка отчёта по ЛР № 5 (часть 1) и подготовка к собеседованию по отчёту. 6.1.1: разделы 2.2, 3 6.2.3	Собеседование по отчёту		
	Итого по разделу 1	***3***	***1***		***8***				

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				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 обучающихся (СРС),				
		Лекции, час	Лабораторные работы, час	Практические занятия, час					
ОПК-3	**Раздел 2** Правовые средства защиты					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.2: раздел 4.3 6.1.3: тема 3			
	Тема 2.1. Отечественное правовое обеспечение	1			4		Тестирование в системе MOODLE (Тест 1)		
	Тема 2.2. Зарубежная и международная политика безопасности	1			4				
	Лабораторная работа № 5 Анализ объекта защиты (часть 2)		1		2	Подготовка отчёта по ЛР № 5 (часть 2) и подготовка к собеседованию по отчёту 6.1.2: раздел 4.3 6.2.3	Собеседование по отчёту		
	Итого по разделу 2	***2***	***1***		***10***				
ОПК-3	**Раздел 3** Криптографическая защита информации					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.1: разделы 8; 6.1.2: раздел 2			
	Тема 3.1. Криптография, стеганография	1			4		Тестирование в системе MOODLE (Тест 1)		
	Тема 3.2. Симметричные и асимметричные алгоритмы	1			4				
	Тема 3.3. Хэширование	1			2				
	Тема 3.4. Электронная подпись	1			4				

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				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 обучающихся (СРС),				
		Лекции, час	Лабораторные работы, час	Практические занятия, час					
	Лабораторная работа № 1 Криптографическая защита информации. Криптоанализ		2		2	Подготовка отчёта по ЛР № 1 и подготовка к собеседованию по отчёту 6.1.1: разделы 8.2; 6.1.2: раздел 2.2, 2.4 6.2.1	Собеседование по отчёту		
	Лабораторная работа № 2 Криптографическая защита информации. Создание программы шифрования, дешифрования		4		2	Подготовка отчёта по ЛР № 2 и подготовка к собеседованию по отчёту 6.1.1: разделы 8.2; 6.1.2: раздел 2.2, 2.4 6.2.1	Собеседование по отчёту		
	Итого по разделу 3	***4***	***6***		***18***				
ОПК-3	**Раздел 4** Техническая защита информации					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.1: разделы 6, 7, 9; 6.1.2: разделы 1.3, 3 6.1.3: тема 4			
	Тема 4.1. Защита ВС	1			3		Тестирование в системе MOODLE (Тест 2)		
	Тема 4.2. Защита ИС	2			4				
	Тема 4.3. Защита данных	2			4				
	Тема 4.4. Защита в сети	2			4				
	Лабораторная работа № 3 Парольная система защиты		4		2	Подготовка отчёта по ЛР № 3 и подготовка к собеседованию по отчёту 6.1.2: разделы 1.3	Собеседование по отчёту		

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				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 обучающихся (СРС),				
		Лекции, час	Лабораторные работы, час	Практические занятия, час					
						6.2.2			
	Лабораторная работа № 4 Управление доступом		4		2	Подготовка отчёта по ЛР № 4 и подготовка к собеседованию по отчёту 6.1.1: раздел 7.1; 6.1.2: раздел 1.3	Собеседование по отчёту		
	Итого по разделу 4	*7*	***8***		***19***				
ОПК-3	**Раздел 5** Физическая защита информации					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.1: раздел 4, 5; 6.1.3: темы 4, 5			
	Тема 5.1. Организационные средства защиты	2			4		Тестирование в системе MOODLE (Тест 2)		
	Тема 5.2. Программно-технические средства защиты	2			4				
	Лабораторная работа № 5 Анализ объекта защиты (часть 3)		4		2	Подготовка отчёта по ЛР № 5 (часть 3) и подготовка к собеседованию по отчёту 6.1.3: темы 4, 5 6.2.3	Собеседование по отчёту		
	Итого по разделу 5	***4***	***4***		***10***				
	ИТОГО по дисциплине	**20**	**20**		**64**				

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

Тесты для текущего и промежуточного контроля знаний обучающихся

Тесты проводятся на электронной платформе Moodle на сайте ДПИ НГТУ поадресу: http://dpingtu.ru/Moodle. Примеры типовых тестовых заданий приведены в разделе 11.1.1 настоящей рабочей программы.

Вопросы для подготовки к контрольным мероприятиям и защите отчётов по лабораторным работам (текущий контроль)

1. Основные понятия защиты информации и информационной безопасности
2. Модель безопасности информации
3. Угрозы доступности
4. Угрозы конфиденциальности
5. Угрозы доступности
6. Основные направления защиты информации
7. Законодательство РФ в области информационной безопасности
8. Отечественные стандарты безопасности
9. Международные стандарты безопасности
10. Криптографическая защита информации.
11. Симметричные криптосистемы.
12. Система шифрования с открытым ключом.
13. Хэш-функция. Хэширование
14. Электронная цифровая подпись (ЭП). Формирование и получение сообщения с ЭП.
15. Электронная цифровая подпись. Системы сертификации.
16. Процедуры идентификации.
17. Методы аутентификации, использующие пароли и PIN-коды.
18. Методы аутентификации, основанные на владении предметом.
19. Биометрическая аутентификация пользователя.
20. Управление доступом.
21. Защита ОС
22. Безопасное хранение данных.Резервное копирование данных, репликация.
23. Функции межсетевых экранов
24. Фильтрующие маршрутизаторы
25. Шлюзы сетевого и прикладного уровня.
26. Основные схемы сетевой защиты на брандмауэрах.
27. Формирование политики межсетевого взаимодействия
28. Основные понятия и функции виртуальных частных сетей
29. Построение виртуальных частных сетей. Среда передачи данных, оборудование удаленных объектов, протоколы VPN.
30. Компьютерные вирусы. Внешние признаки проявления деятельности вирусов
31. Классификация вирусов.
32. Жизненный цикл вирусов.
33. Методы обнаружения вирусов
34. Виды антивирусных программ
35. Организационные средства защиты
36. Формирование политики безопасности организации
37. Угрозы на инженерно-техническом уровне

38. Программно-технические средства защиты территории, помещений

Перечень вопросов, выносимых на промежуточную аттестацию (зачет с оценкой)

1. Основные понятия защиты информации и информационной безопасности
2. Модель безопасности информации
3. Классификация угроз безопасности компьютерных систем
4. Угрозы доступности
5. Угрозы конфиденциальности
6. Угрозы доступности
7. Основные направления защиты информации
8. Законодательство РФ в области информационной безопасности
9. Отечественные стандарты безопасности
10. Международные стандарты безопасности
11. Политика безопасности РФ
12. Криптографическая защита информации.
13. Симметричные криптосистемы.
14. Система шифрования с открытым ключом.
15. Гибридные технологии шифрования
16. Электронная цифровая подпись (ЭП). Формирование и получение сообщения с ЭП.
17. Хэш-функция. Хэширование
18. Электронная цифровая подпись. Системы сертификации.
19. Процедуры идентификации.
20. Классификация видов аутентификации
21. Методы аутентификации, использующие пароли и PIN-коды.
22. Методы аутентификации, основанные на владении предметом.
23. Биометрическая аутентификация пользователя.
24. Управление доступом.
25. Защита ОС
26. Резервное копирование данных, репликация.
27. Безопасное хранение данных.
28. Функции межсетевых экранов
29. Фильтрующие маршрутизаторы
30. Шлюзы сетевого и прикладного уровня.
31. Основные схемы сетевой защиты на брандмауэрах.
32. Проблемы безопасности межсетевых экранов
33. Формирование политики межсетевого взаимодействия
34. Основные понятия и функции виртуальных частных сетей
35. Построение виртуальных частных сетей. Среда передачи данных, оборудование удаленных объектов, протоколы VPN.
36. Организация VPN-канала. Инкапсуляция и туннелирование.
37. Основные варианты архитектуры VPN.
38. Компьютерные вирусы. Внешние признаки проявления деятельности вирусов
39. Классификация вирусов.
40. Жизненный цикл вирусов.
41. Методы обнаружения вирусов
42. Виды антивирусных программ
43. Организационные средства защиты
44. Формирование политики безопасности организации
45. Угрозы на инженерно-техническом уровне
46. Программно-технические средства защиты территории, помещений

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

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине может применяться балльно-рейтинговая система контроля и оценки успеваемости обучающихся очной формы.Основные требования балльно-рейтинговой системы по дисциплине ишкала оценивания приведены в таблицах 5.1 – 5.3.

Таблица 5.1

Требования балльно-рейтинговой системы по дисциплине

Вид работ	**Количество подвидов работы**	**Макс. баллы за подвид работы**	**Штрафные баллы**	**Макс. количество баллов по виду работ**
1.Тестирование	2	20	0* -1 за повтор (3 попытки)	**40**
2. Выполнение лабораторных работ, в т.ч. на 1 работу	5	8		**40**
- выполнение		*4*	*при наличии ошибок*	*20*
- оформление и защита отчётов		*4*	*отсутствие ответов на вопросы по отчёту*	*20*
3. Посещение занятий	40	0,5		**20**
- лекции	*20*			*10*
- лабораторные работы	*20*			*10*
Итого				**100**

*Если при тестировании верно выполнено менее 55% заданий, то количество баллов за работу приравнивается к «0»

** Освобождение от зачёта с оценкой возможно при условии выполнения всех лабораторных работ, положительных оценок за тестирование, посещения не менее 50 % занятий

Таблица 5.2

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»** 0-54% от max рейтинговой оценки контроля	Оценка **«удовлетворительно»** 55-70% от max рейтинговой оценки контроля	Оценка **«хорошо»** 71-85% от max рейтинговой оценки контроля	Оценка **«отлично»** 86-100% от max рейтинговой оценки контроля
ОПК-3. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	**ИОПК-3.3.** Учитывает основные требования информационной безопасности при решении задач профессиональной деятельности.	Изложение учебного материала бессистемное, неполное, не знает возможные угрозы безопасности информации, методы и средства защиты информации	Фрагментарные, поверхностные знания по анализу объекта защиты. Изложение полученных знаний неполное, но это не препятствует усвоению последующего материала. Допускаются отдельные существенные ошибки, исправленные с помощью преподавателя. Затруднения при формулировании результатов и их решений	Знает материал на достаточно хорошем уровне; представляет основные задачи обеспечения безопасности в рамках постановки целей и выбора оптимальных способов их достижения.	Имеет глубокие знания всего материала структуры дисциплины; освоил новации лекционного курса по сравнению с учебной литературой; изложение полученных знаний полное, системное; допускаются единичные ошибки, самостоятельно исправляемые при собеседовании

Таблица 5.3

Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает обучающийся, 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 обучающийся, 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 обучающийся, 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 обучающийся, 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. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. — Краснодар : КубГАУ, 2020. — 332 с. — ISBN 978-5-907346-50-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254168.

6.1.2. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279.

6.1.3. Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев ; под редакцией В. Н. Ясенева. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2017. — 198 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/153011.

Библиотечный фонд укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных выше на каждого обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль).

6.2. Методические указания, рекомендации и другие материалы к занятиям

6.2.1. **Криптографические методы шифрования данных**: метод. указания к лабораторным работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направлений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова, Н.И. Кечкина.– Дзержинск, 2018. - 24 с.

6.2.2. **Парольная система защиты**: метод. указания к лабораторным работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направ-

лений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова.– Дзержинск, 2018. - 8 с.

6.2.3. **Анализ объекта защиты с целью обеспечения информационной безопасности**: метод. указания к лабораторным работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направлений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова.– Дзержинск, 2018. - 9 с.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

Дисциплина, относится к группе дисциплин, в рамках которых предполагается использование информационных технологий как вспомогательного инструмента для выполнения задач, таких как:

- оформление отчетов по лабораторному занятию;
- использование электронной образовательной среды института;
- использование специализированного программного обеспечения;
- организация взаимодействия с обучающимися посредством электронной почты;
- использование видеоконференцсвязи;
- компьютерное тестирование.

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/

7.2. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства необходимого для освоения дисциплины

Таблица 7.2

Программное обеспечение

№ п/п	Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
1	MicrosoftWindows 10 (подписка MSDN 700593597, подписка DreamSparkPremium, 19.06.19)	Adobe Acrobat Reader https://acrobat.adobe.com/ru/ru/acrobat/pdf-

№ п/п	Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
		reader.html
2	Microsoft VISUAL STUDIO 2008 (подписка MSDN 700593597, подписка DreamSparkPremium, 19.06.19)	Visual Studio Code https://code.visualstudio.-com/download
3	Microsoft office 2010 (Лицензия № 49487295 от 19.12.2011)	OpenOffice https://www.openoffice.org/ru/
4	Консультант Плюс	Python https://www.python.org

7.3. Перечень современных профессиональных баз данных и информационных справочных систем

В таблице7.3указанперечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

Таблица 7.3

Перечень современных профессиональных баз данных
и информационных справочных систем

№ п/п	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки / доступ из локальной сети университета)
1	База данных стандартов и регламентов РОССТАНДАРТ	https://www.gost.ru/portal/gost //home/standarts
2	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
3	Инструменты и веб-ресурсы для веб-разработки – 100+	https://techblog.sdstudio.top/blog/instrumenty-i-veb-resursy-dlia-veb-razrabotki-100-plus
4	Справочная правовая система «КонсультантПлюс»	доступ из локальной сети

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице8.1указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования.

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

Согласно Федеральному Закону об образовании 273-ФЗ от 29.12.2012 г. ст. 79, п.8 «Профессиональное обучение и профессиональное образование обучающихся с ограниченными возможностями здоровья осуществляются на основе образовательных программ, адаптированных при необходимости для обучения указанных обучающихся». АОП разрабатывается по каждой направленности при наличии заявлений от обучающихся, являю-

щихся инвалидами или лицами с ОВЗ и изъявивших желание об обучении по данному типу образовательных программ.

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

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

В таблице 9.1 перечислены:

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

Таблица 9.1

Оснащенность аудиторий и помещений
для самостоятельной работы обучающихся по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенностьаудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	**1448** Учебный кабинет, мультимедийный класс; Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	Оснащён мультимедийным оборудованием: Проектор EPSON EB-FH06 HDMI 1920x1080 Ноутбук Intel Core i3/Ram 4 Gb/ HDD 240 Gb/Intel HD	–
2	**1440** Компьютерный класс; Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	ОснащёнПК, CPU Intel core i5-10400/Ram 16 Gb/SSD 500 Gb/ Intel UHD Graphics 630 – 16 шт.	• Microsoft Windows 10 (подписка DreamSpark Premium) • Apache OpenOffice 4.1.8(свободное ПО); • Mozilla Firefox(свободное ПО); • Adobe Acrobat Reader (свободное ПО); • 7-zip для Windows (свободное ПО); • КонсультантПлюс (ГПД № 0332100025418000079 от 21.12.2018)
3	**1234** Научно-техническая библиотека ДПИ НГТУ, студенческий читальный зал; Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	Комплект демонстрационного оборудования: • ПК, с выходом на мультимедийный проектор, на базе Intel Pentium G4560 3.5 Ггц, 4 Гб ОЗУ, монитор 20’ – 1шт. • Мультимедийный проектор Epson- 1 шт; • Экран – 1 шт.; Набор учебно-наглядных пособий	• MicrosoftWindows 10 Домашняя (поставка с ПК) • LibreOffice 6.1.2.1. (свободное ПО) • Foxit Reader (свободное ПО); • 7-zip для Windows (свободное ПО)
4	**1443а** компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	ПК на базе IntelCeleron 2.67 ГГц, 2 Гб ОЗУ, монитор Acer 17’ – 4 шт. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета	• Microsoft Windows 7 (подписка DreamSpark Premium) • Apache OpenOffice 4.1.8(свободное ПО); • Mozilla Firefox(свободное ПО); • Adobe Acrobat Reader (свободное ПО); • 7-zip для Windows (свободное ПО); • КонсультантПлюс(ГПД № 0332100025418000079 от 21.12.2018)

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.

Контактная работа: аудиторная, внеаудиторная, а также проводиться в электронной информационно-образовательной среде университета (далее - ЭИОС).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;
- текущий контроль знаний в форме тестированияв среде MOODLE.

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

Лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал с обучающимися во время чтения лекций, активировать их деятельность при освоении материала. Материалы лекций в виде слайдов находятся в свободном доступе в системе MOODLE и могут быть получены до чтения лекций и проработаны обучающимися в ходе самостоятельной работы.

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

Все вопросы, возникшие при самостоятельной работе над домашним заданием, подробно разбираются на лабораторных занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием, как встреч с обучающимися, так и современных информационных технологий (электронная почта, Zoom).

Инициируется активность обучающихся, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы обучающегося, 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 обучающихся в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачёта с оценкой с учетом текущей успеваемости.

Результат обучения считается сформированным на повышенном уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях обучающийся 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, обучающийся способен анализировать полученные результаты, проявляет самостоятельность при выполнении зада-

ний.

Результат обучения считается сформированным на пороговом уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях обучающийся 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, обучающийся способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий.

Результат обучения считается несформированным, если обучающийся 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 (Таблица 4.2). Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3. Методические указания по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе обучающийся 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 экспериментально-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 обучающихся к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающихся на занятиях, в качестве выполненных заданий для самостоятельной работы 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 обучающиеся могут работать на компьютере в специализированных аудиториях для самостоятельной работы (указано в таблице 9.1). 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 обучающихся по дисциплине проводится **комплексная оценка знаний,** включающая

- тестирование на сайте преподавателя по различным разделам курса
- проведение лабораторных работ;
- ответы на вопросы для самостоятельной работы для обучающихся очной формы.

Далее для всех форм текущего контроля приведены примеры оценочных средств.

11.1.1. Типовые тестовые задания

Тестирование проводится в системе MOODLE. По приведённым в таблице 4.2 темам проводится два теста. В разделе приведены примеры тестовых заданий для каждого теста по всем темам.

Тест 1

Раздел 1

1. Суть компрометации информации

– внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

– несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

– *внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений*

2. Основные угрозы доступности информации:

– непреднамеренные ошибки пользователей
– злонамеренное изменение данных
– хакерская атака
– *отказ программного и аппаратно обеспечения*
– перехват данных

3. К формам защиты информации не относится…

– *аналитическая*
– правовая
– организационно-техническая
– криптографическая

Раздел 2

1. Изучение стандартов и спецификаций необходимо, поскольку

– создаются условия для разработки безопасных систем
– *они являются формой накопления знаний с целью многократного использования*
– невыполнение их требований преследуется по закону

2. Спецификация TLS близка к

– *SSL*
– SSH
– DNS

3. К правовым методам, обеспечивающим информационную безопасность, относятся:

– Разработка аппаратных средств обеспечения правовых данных

– Разработка и установка во всех компьютерных правовых сетях журналов учета действий

– Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Раздел 3

1. По какой причине удостоверяющий центр отзывает сертификат?

– если открытый ключ пользователя скомпрометирован

– если пользователь переходит на использование модели pem, которая использует сеть доверия

– *если закрытый ключ пользователя скомпрометирован*

– если пользователь переходит работать в другой офис

2. В чем состоит криптографическая задача обеспечения целостности?

– гарантирование невозможности внесения случайных ошибок в процессе передачи по каналам связи;

– *гарантирование невозможности несанкционированного изменения информации;*

– оба ответа верны.

3. Дешифрование – это…

– на основе ключа шифрованный текст преобразуется в исходный

– пароли для доступа к сетевым ресурсам

– сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

Тест 2

Раздел 4

1. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:

– Антивирус

– Замок

– *Брандма́уэр*

– Криптография

– Экспертная система

2. Преимущества эвристического метода антивирусной проверки над методом сравнения с эталоном

– более надежный

– существенно менее требователен к ресурсам

– не требует регулярного обновления антивирусных баз

– *позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы*

3. Запись определенных событий в журнал безопасности сервера называется:

– Идентификацией

– *Аудитом*

– Аутентификацией

– Администрированием

Раздел 5

1. Что не относится к технической радиоэлектронной разведке:

– *фотографическая*

– радиотехническая

– радиолокационная

– разведка ПЭМИН

2. Политика безопасности организации – это комплекс:

– Руководств, требований обеспечения необходимого уровня безопасности

– Инструкций, алгоритмов поведения пользователя в сети

– Нормы информационного права, соблюдаемые в сети

3. Кто в итоге несет ответственность за защищенность данных в компьютерной сети?

– *Владелец сети*

– Администратор сети

– Пользователь сети

11.1.2. Типовые задания для лабораторных работ

Лабораторная работа 1

Теоретические сведения и типовые задания для лабораторных работ приведены в методических указаниях по проведению лабораторных работ (6.2.1).

Типовое задание.

Шифрование выполнено по таблице Вижинера с ключом«билет»:

пъщуфогрдгцнш_срчппюя_рты_зшйщтнюйфьюкбэсищуф

Выполнить дешифрование.

Лабораторная работа 2

Теоретические сведения и типовые задания для лабораторных работ приведены в методических указаниях по проведению лабораторных работ (6.2.1).

Типовое задание.

На одном из языков программирования написать программу шифрования или дешифрования данных одним из методов шифрования, данных на выбор.

Лабораторная работа 3

Типовое задание.

Определить параметры парольной системы. Создать программу для генерации пароля с заданными параметрами.

Лабораторная работа 4

Типовое задание.

Изучить процессы настройки статических и динамических маршрутов. Изучить процесс настройки списков доступа.

Лабораторная работа 5

Типовое задание.

Выполнить анализ объекта защиты.

В качестве объекта защиты могут выступать:почтовый сервер; сеть с выделенным сервером без выхода в Интернет; сеть с выделенным сервером с выходом в Интернет; материалы по недвижимости и другие.

11.1.3. Типовые вопросы для устного и письменного опроса

По завершении лекционных занятий может быть выполнен устный или письменный опрос обучающихся для оценки работы на занятии и для оценки самостоятельной работы обучающихся.

Раздел 1

1. Дать определение термину «защита информации»
2. Дать определение термину«информационная безопасность»
3. Дать определение термину«угроза»
4. Какие данные подлежат защите
5. Привести примеры угроз доступности
6. Привести примеры угроз конфиденциальности
7. Привести примеры угроз доступности
8. Достоинства и недостатки правового направления защиты информации
9. Достоинства и недостатки криптографической защиты информации
10. Достоинства и недостатки технического направления защиты информации
11. Достоинства и недостатки физической защиты информации

Раздел 2

1. На чём основана правовая защита информации
2. Отечественные стандарты безопасности
3. Зарубежные стандарты безопасности
4. Международные стандарты безопасности
5. Основы Доктрины информационной безопасности РФ

Раздел 3

1. Дать определение термину «шифрование».
2. Дать определение термину «дешифрование».
3. Дать определение термину «алфавит».
4. Дать определение термину «ключ».
5. Привести виды симметричных криптосистем.
6. Привести примеры симметричных криптосистем.
7. Привести виды систем шифрования с открытым ключом.
8. Привести примеры систем шифрования с открытым ключом.
9. Свойства хэш-функции.
10. Описать процесс формирования сообщения с электронной подписью.
11. Описать процесс получение сообщения с электронной подписью.
12. Перечислить функции электронной цифровой подписи.
13. Назначение центров сертификации.

Раздел 4

1. Дать определение термину «идентификация».
2. Дать определение термину «аутентификация».
3. Привести примеры методов аутентификации, использующие пароли и PIN-коды.
4. Привести примеры методов аутентификации, основанные на владении предметом.
5. Привести примеры методов биометрическая аутентификация пользователя.
6. Задачи управления доступом.
7. Перечислить способы защиты ОС.
8. Для чего используется резервное копирование данных
9. Дать определение термину «репликация».
10. Перечислить функции межсетевых экранов
11. Привести основные схемы сетевой защиты на брандмауэрах.
12. Проблемы безопасности межсетевых экранов
13. Привести этапы формирования политики межсетевого взаимодействия
14. Основные понятия и функции виртуальных частных сетей
15. Привести протоколы VPN.
16. Дать определение термину «инкапсуляция»
17. Дать определение термину «туннелирование».
18. Основные варианты архитектуры VPN.
19. Дать определение термину «компьютерные вирусы».
20. Внешние признаки проявления деятельности вирусов
21. Классификация вирусов по месту обитания.
22. Классификация вирусов по деструктивным свойствам.
23. Жизненный цикл вирусов.
24. Методы обнаружения вирусов
25. Виды антивирусных программ

Раздел 5

1. Что относится к организационным средствам защиты
2. Формирование политики безопасности организации
3. Угрозы на инженерно-техническом уровне
4. Программно-технические средства защиты территории, помещений

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

Форма проведения промежуточной аттестации по дисциплине: дифференцированный зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Перечень вопросов для подготовки к зачету с оценкой (ОПК-3)

Перечень вопросов, выносимых на промежуточную аттестацию, приведён в разделе 5.1 настоящей рабочей программы.

Примерный тест для итогового тестирования

В итоговом тесте 10 вопросов с выбором ответа. Структура теста:

Раздел 1. Общие вопросы информационной безопасности (ОПК-3)

1. Суть компрометации информации

– внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений
– несанкционированный доступ к передаваемой информации по каналам связи и уничтожение содержания передаваемых сообщений
– внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
– внесение изменений в информационную систему с целью блокировки данных

2. Основные угрозы целостности информации

– непреднамеренные ошибки пользователей
– отказ программного и аппаратного обеспечения
– отказ пользователей
– хакерская атака

Раздел 2. Правовые средства защиты(ОПК-3)

1. К правовым методам, обеспечивающим информационную безопасность, относят:

– внедрение аутентификации, проверки контактных данных пользователей
– разработка и установка во всех компьютерных правовых сетях журналов учета действий
– разработка и конкретизация правовых нормативных актов обеспечения безопасности
– разработка аппаратных средств обеспечения правовых данных

Раздел 3. Криптографическая защита информации (ОПК-3)

1. Пространство ключей – это…

– длина ключа
– набор возможных значений ключа
– набор символов, разрешённых для использования
– область памяти для хранения ключей

2. В методе замены....

– символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
– символы шифруемого текста последовательно складываются с символами некоторой

специальной последовательности
– символы шифруемого текста заменяются другими буквами того же самого или некоторого другого алфавита
– шифруемый текст преобразуется по некоторому аналитическому правилу (формуле)

Раздел 4. Техническая защита информации (ОПК-3)

1. Идентификация - это
– процедура проверки подлинности заявленного пользователя, процесса или устройства
– процедура распознавания пользователя по его идентификатору (имени)
– процедура предоставления субъекту определенных полномочий и ресурсов в данной системе
– процедура регистрации в специальном журнале, называемом журналом аудита или журналом безопасности, событий, которые могут представлять опасность для ИС

2. К какому типу антивирусной защиты можно отнести использование инструкций по работе за компьютером
– практическим
– техническим
– организационным
– теоретическим

3. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
– источник слухов
– фишинг
– черный пиар
– пустые письма

Раздел 5. Физическая защита информации (ОПК-3)

1. Что не относится к технической радиоэлектронной разведке:
– фотографическая
– радиотехническая
– радиолокационная
– разведка ПЭМИН

2. Политика безопасности организации – это комплекс:
– Руководств, требований обеспечения необходимого уровня безопасности
– Инструкций, алгоритмов поведения пользователя в сети
– Нормы информационного права, соблюдаемые в сети

Регламент проведения текущего контроля в форме компьютерного тестирования

Кол-во заданий в банке вопросов	**Кол-во заданий, предъявляемых обучающемуся**	**Время на тестирование, мин.**
не менее 100	**10**	**10**

Полный фонд оценочных средств для проведения промежуточной аттестации в форме компьютерного тестирования размещен в банке вопросов данного курса дисциплины в СДО MOODLE.

В ходе подготовки к текущему контролю обучающимся предоставляется возможность пройти тест самопроверки. Тест для самопроверки по дисциплине размещен в СДО Moodle ДПИ НГТУ в свободном для обучающихся доступе.