ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра Компьютерных технологий

УТВЕРЖДАЮ:
Проректор по научно-методической
и учебной работе
_____ Е.И. Скафа
«22» апреля 20
МП

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки: **09.03.01** Информатика и вычислительная техника

Профиль подготовки: Информатика и вычислительная техника

Образовательная программа: бакалавриат

Квалификация: академический бакалавр

Форма обучения: очная, очно-заочная, заочная, в том числе с ускоренным сроком обучения

Донецк 2020

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Защита информации» относится к вариативной части профессионального блока и состоит из четырёх содержательных модулей: модуль 1 – «Понятие Информационной безопасности. Ведение. Законодательный уровень информационной безопасности. Наиболее распространенные угрозы информационной безопасности. Распространение объектно-ориентированного подхода на ИБ», модуль 2 – «Административный уровень информационной безопасности. Процедурный уровень информационной безопасности. Основные программно-технические меры безопасности информации», модуль 3 – «Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись. Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности», модуль 4 – «Криптография: шифрование и обеспечение целостности. Протоколирование и аудит, шифрование, контроль целостности. Антивирусная защита компьютерных систем».

Основывается на базе дисциплин: «Основы программирования», «Информатика и информационно-коммуникационные технологии», «Программирование». Является основой для изучения дисциплин: «Безопасность и защита информации в информационных системах».

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины				
Направление подготовки	09.03.01 Информатика и вычислительная техника			
Профиль	Информатика и вычислительная техника			
Образовательная программа	Бакалавриат			
Квалификация	Академический бакалавр			
Количество содержательных модулей	4			
Дисциплина базовой / вариативной части образовательной программы	Профессиональный блок. Вариативная часть			
Формы контроля (МК, экзамен, зачет)	Два модульных контроля, два диференц. зачета			
Показатели	очная форма обучения		заочная форма обучения	
	нормат. срок	ускор. срок	нормат. срок	ускор. срок
Количество зачётных единиц (кредитов)	3	6	6	6
Год подготовки	4	3	4	3
Семестр	7	5	7	5
Количество часов	108	216	216	216
- лекционных	18	36	36	36
- практических, семинарских	36			
- лабораторных		72	72	72
- самостоятельной работы	54	108	108	108
в т. ч. индивидуальное задание				
Недельное количество часов, т. ч.	7	12	12	12
аудиторных	3	6	1.2	1.2

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи.

умение готовить и проводить доклады с использованием современных компьютерных средств, писать научно-технические отчёты, оформлять результаты исследований в виде статей (ПК-16);

педагогическая деятельность:

готовить конспекты лекций, проводить повышение квалификации сотрудников (ПК-17);

сервисно-эксплуатационная деятельность:

инсталлировать, настраивать и сопровождать программное и аппаратное обеспечение информационных и автоматизированных систем (ПК-21).

В результате изучения учебной дисциплины студент должен

Знать:

– принципы построения и архитектуру вычислительных систем;

– виды контента информационных ресурсов предприятия и Интернет-ресурсов;

– основы безопасности жизнедеятельности в области профессиональной деятельности;

– методы и средства обеспечения информационной безопасности компьютерных систем;

– базовые понятия и определения, используемые в сфере информационной безопасности;

– основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам.

Уметь:

– ставить и решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным);

– проектировать, внедрять и организации эксплуатацию ИС и ИКТ; моделировать, анализировать и совершенствовать бизнес-процессы, разрабатывать конкретные предложения по результатам исследований, готовить справочно-аналитические материалы для ринятия управленческих решений;

– применять на практике собственные и классические алгоритмы криптографической защиты данных.

Владеть:

– методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия;

– основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

– иметь представление о моделях безопасности ИС.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Порядковый номер и тема	**Краткое содержание темы**
	Содержательный модуль 1. **Понятие Информационной безопасности. Ведение. Законодательный уровень информационной безопасности. Наиболее распространенные угрозы информационной безопасности. Распространение объектно-ориентированного**

	подхода на ИБ
Тема 1. Понятие Информационной безопасности. Ведение	Базовые понятия и определения, используемые в сфере информационной безопасности. Роль справочно-аналитических материалов в принятии управленческих решений. Представление о моделях безопасности ИС,
Тема 2. Законодательный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем. Разработка макетов справочно-аналитических материалов для принятия управленческих решений на основе законодательного уровня ИБ. Основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий.
Тема 3. Наиболее распространенные угрозы информационной безопасности	Основы безопасности жизнедеятельности в области профессиональной деятельности. Принципы проектирования, внедрения и эксплуатация в организации ИС и ИКТ. Методы проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия.
Тема 4. Распространение объектно-ориентированного подхода на ИБ	Основные понятия объектно-ориентированного подход. О необходимости объектно-ориентированного подхода к информационной безопасности. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
	Содержательный модуль 2. **Административный уровень информационной безопасности. Процедурный уровень информационной безопасности. Основные программно-технические меры безопасности информации.**
Тема 5. Административный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем на административном уровне ИБ. Обзор справочно-аналитических материалов для принятия управленческих решений на административном уровне. Основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий.
Тема 6. Процедурный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем на процедурном уровне. Проектирование, внедрение и эксплуатация в организации ИС и ИКТ на процедурном уровне.
Тема 7. Основные программно-технические меры безопасности информации	Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам. Постановка и решение схемотехнических задач, связанных с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надлежностным). Знакомство с методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия.
	Содержательный модуль 3. **Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом. Основные программно-технические меры**

шифрование, контроль целостности	контроля целостности(в т.ч. использованием элементов шифрования)
Тема 13. Антивирусная защита компьютерных систем.	Принципы организации антивирусной защиты информационных систем. Типология вирусов. Достоинства и недостатки эвристических алгоритмов поиска вирусов.

Курс дисциплины «ЗАЩИТА ИНФОРМАЦИИ» предусматривает следующие **формы организации учебного процесса**:

1) лекции;
2) практические занятия;
3) самостоятельная работа студента.

Электронные материалы по всем формам организации учебного процесса размещены на сайте (http://donnu.ru/phys/kt/bondarenko или http://donnu.ru/phys/kt/maruga-mihail-mihaylovich).

По источнику передачи и восприятия учебной информации используются словесные (лекция, беседа), наглядные (иллюстрация, демонстрация), практические (исследования, упражнения, практические работы) методы.

По характеру познавательной деятельности студентов используются объяснительно-иллюстративные и репродуктивные методы, проблемное преподавание, частично-поисковый и исследовательский методы.

В зависимости от основной дидактической цели и задач используются методы устного изложения знаний, закрепление учебного материала, самостоятельной работы студентов по осмыслению и усвоению нового материала, работы по применению знаний на практике и выработке умений и навыков, проверки и оценки знаний, умений и навыков.

Используются следующие методы контроля:

1) устный контроль (экспресс-опрос на лекциях);
2) проверка конспектов;
3) проверка практических работ;
4) проверка самостоятельных работ;
5) модульная контрольная работа (дидактическое тестирование).

Тематический план

Названия содержательных модулей и тем	Содержательный модуль 1																						
	Количество часов																						
	Очная форма обучения												Заочная форма обучения										
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения				
	всего	В Т. Ч.					всего	В Т. Ч.					всего	В Т. Ч.					всего	В Т. Ч.			
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные работы	самостоятельная работа
Тема 1. Понятие Информационной безопасности. Ведение	12	2	4		6		12	2	4		6		2,4	0,4	0,8		1,2		2,4	0,4	0,8		1,2
Тема 2. Законодательный уровень информационной безопасности	6	1	2		3		6	1	2		3		1,2	0,2	0,4		0,6		1,2	0,2	0,4		0,6
Тема 3. Наиболее распространенные угрозы информационной безопасности	12	2	4		6		12	2	4		6		2,4	0,4	0,8		1,2		2,4	0,4	0,8		1,2
Тема 4. Распространение объектно-ориентированного подхода на ИБ	12	2	4		6		12	2	4		6		2,4	0,4	0,8		1,2		2,4	0,4	0,8		1,2
Итого по содержательному модулю 1	42	7	14		21		42	7	14		21		8,4	1,4	2,8		4,2		8,4	1,4	2,8		4,2

Названия содержательных модулей и тем	Содержательный модуль 3																					
	Количество часов																					
	Очная форма обучения												Заочная форма обучения									
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения			
	всего	В Т. Ч.					всего	В Т. Ч.					всего	В Т. Ч.					всего	В Т. Ч.		
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные работы	самостоятельная работа
Тема 8. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	12	2	4		6		12	2	4		6		12	0,4	0,8		6		12	0,4	0,8		6
Тема 9. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись.	6	1	2		3		6	1	2		3		6	0,2	0,4		3		6	0,2	0,4		3
Тема 10. Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности.	6	1	2		3		6	1	2		3		6	0,2	0,4		3		6	0,2	0,4		3
Итого по содержательному модулю 3	24	4	8		12		24	4	8		12		24	0,8	1,6		12		24	0,8	1,6		12

Названия содержательных модулей и тем	Содержательный модуль 4																						
	Количество часов																						
	Очная форма обучения												Заочная форма обучения										
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения				
	всего	В Т. Ч.					всего	В Т. Ч.					всего	В Т. Ч.					всего	В Т. Ч.			
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные работы	самостоятельная работа
Тема 11. Криптография: шифрование и обеспечение целостности	12	2	4		6		12	2	4		6		12	0,4	0,8		6		12	0,4	0,8		6
Тема 12. Протоколирование и аудит, шифрование, контроль целостности	6	1	2		3		6	1	2		3		6	0,2	0,4		3		6	0,2	0,4		3
Тема 13. Антивирусная защита компьютерных систем.	6	1	2		3		6	1	2		3		6	0,2	0,4		3		6	0,2	0,4		3
Итого по содержательному модулю 4	24	4	8		12		24	4	8		12		24	0,8	1,6		12		24	0,8	1,6		12
Всего часов	108	18	36		54		108	18	36		54		108	3,6	7,2		54		108	3,6	7,2		54

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий

№ п/п	*Название темы*	*Количество часов*
1.	Понятие Информационной безопасности. Ведение	2
2.	Законодательный уровень информационной безопасности	1
3.	Наиболее распространенные угрозы информационной безопасности	2
4.	Распространение объектно-ориентированного подхода на ИБ	2
5.	Административный уровень информационной безопасности	1
6.	Процедурный уровень информационной безопасности	1
7.	Основные программно-технические меры безопасности информации	1
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	2
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись.	1
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности.	1
11.	Криптография: шифрование и обеспечение целостности	2
12.	Протоколирование и аудит, шифрование, контроль целостности	1
13.	Антивирусная защита компьютерных систем.	1
	ВСЕГО	**18**

Темы практических занятий

№ п/п	*Название темы*	*Количество часов*
1.	Разработка алгоритма и программы шифрования и расшифровки информации методом RSA.	8
2.	Разработка и реализация программы шифрования и дешифрования методом Диффи-Хеллмана и Эль-Гамалля.	7
3.	Разработка и реализация программы шифрования и дешифрования алгоритмом AES.	7
4.	Разработка и реализация программы привязки к биту, разделения секретов схемами Шамира и Блекли.	7
5.	Разработка и реализация электронной цифровой подписи на основе RSA, схемами Шнорра и Фейге-Фиата-Шамира.	7
	ВСЕГО	36

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Организация самостоятельной работы студентов

Самостоятельная работа студентов по курсу «ЗАЩИТА ИНФОРМАЦИИ» предусматривает:

– систематическое ведение конспекта лекций и повседневную проработку лекционного материала;

– изучение дополнительной технической литературы и интернет-источников, рекомендуемых этой программой;

– добросовестную подготовку к лабораторным занятиям;

– самостоятельную разработку алгоритмов и текстов программ лабораторных работ;

– изучение дополнительного инструментария;

– своевременное и качественное оформление отчётов по лабораторным работам.

№ п/п	***Название темы***	***Количество часов***
1.	Понятие Информационной безопасности. Ведение	6
2.	Законодательный уровень информационной безопасности	3
3.	Наиболее распространенные угрозы информационной безопасности	6
4.	Распространение объектно-ориентированного подхода на ИБ	6
5.	Административный уровень информационной безопасности	3
6.	Процедурный уровень информационной безопасности	3
7.	Основные программно-технические меры безопасности информации	3
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	6
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись.	3
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности.	3
11.	Криптография: шифрование и обеспечение целостности	6
12.	Протоколирование и аудит, шифрование, контроль целостности	3
13.	Антивирусная защита компьютерных систем.	3
	ВСЕГО	**54**

7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Индивидуальные задания предусмотрены к каждой теме и полностью приведены в методических указания по выполнению и оформлению лабораторных работ к курсу «ЗАЩИТА ИНФОРМАЦИИ».

Ниже приводится по одному примеру индивидуального задания из каждой темы:

1. Понятие информационной безопасности
2. Что является основными составляющими информационной безопасности?
3. Основные угрозы целостности
4. В чем проявляется «распространение объектно-ориентированного подхода на информационную безопасность»
5. Политика безопасности.
6. В чем заключается и для чего предназначен «процедурный уровень информационной безопасности» ?
7. Что означает и какое место в обеспечении информационной безопасности занимает архитектурная безопасность?

8. Основные программно-технические меры безопасности информации.
9. Для чего предназначена и какую роль в ИБ играет сервис X?
10. Анализ защищенности.
11. Практические рекомендации по использованию шифрования.
12. Что такое активный аудит?
13. Вирусы и средства борьбы с ними.

8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Понятие информационной безопасности. Основные составляющие информационной безопасности.

2. Важность и сложность проблемы информационной безопасности

3. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность.

4. Понятие сервиса информационной безопасности. Идентификация и аутентификация.

5. Понятие сервиса информационной безопасности. Управление доступом.

6. Понятие сервиса информационной безопасности. Протоколирование и аудит.

7. Понятие сервиса информационной безопасности. Управление и анализ защищенности.

8. Понятие сервиса информационной безопасности. Обеспечение высокой доступности и отказоустойчивости.

9. Понятие сервиса информационной безопасности. Экранирование и туннелирование.

10. Понятие сервиса информационной безопасности. Криптография: шифрование.

11. Понятие сервиса информационной безопасности. Криптография: контроль целостности.

12. Криптология: базовые понятия и терминология.

13. Криптографические примитивы и их свойства.

14. Модели основных криптоаналитических атак.

15. Антивирусная защита. История развития вирусов и их классификация. Методы защиты от вредоносных программ

16. Приведите примеры угроз доступности.

17. Как происходит физическая защита информации?

18. Как происходит реагирование на нарушение режима безопасности?

19. Для чего предназначен программно-технический уровень информационной безопасности?

20. Дайте определение идентификации и аутентификации.

21. Дайте определение протоколирование и аудит.

22. Что такое криптографические хэш функции?

9.ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «Донецкий национальный университет»
Физико-технический факультет
Направление подготовки 09.03.01 «Информатика и вычислительная техника»
Программа подготовки бакалавриат
Семестр 3
Учебная дисциплина Защита информации

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА №1
ВАРИАНТ №1

Задание 1

Дайте определение понятия «Защита информации»

Задание 2

Что является основными составляющими информационной безопасности?

Утверждено на заседании кафедры компьютерных технологий, протокол № 12 от «2» апреля 2020 г.

Заведующий кафедрой Ермоленко Т.В.
Преподаватель Бондаренко В.И., Маруга М.М.

Критерии оценивания модульного контроля

Номер задания	***Количество баллов***
1	12
2	12
Всего	**24**

ГОУ ВПО «Донецкий национальный университет»
Физико-технический факультет
Направление подготовки 09.03.01 «Информатика и вычислительная техника»
Программа подготовки бакалавриат
Семестр 3
Учебная дисциплина Защита информации

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА №2
ВАРИАНТ №1

1. Что такое безопасность информации?
2. Дайте письменный ответ на вопрос, что такое ментальная карта понятий?
3. Что такое законодательный уровень информационной безопасности и почему он важен?

Утверждено на заседании кафедры компьютерных технологий, протокол № 12 от «2» апреля 2020 г.

Заведующий кафедрой Ермоленко Т.В.
Преподаватель Бондаренко В.И, Маруга М.М.

Критерии оценивания модульного контроля

Номер задания	*Количество баллов*
1	4
2	4
3	4
Всего	**12**

ГОУ ВПО «Донецкий национальный университет»
Физико-технический факультет
Направление подготовки 09.03.01 «Информатика и вычислительная техника»
Программа подготовки бакалавриат
Семестр 4
Учебная дисциплина Защита информации

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА №3
ВАРИАНТ №1

1. Что такое, как реализуется и где используется электронная цифровая подпись?
2. Как и с какими угрозами позволяет бороться сервис X?
3. Что такое сервис управления доступом?

Утверждено на заседании кафедры компьютерных технологий, протокол № 12 от «2» апреля 2020 г.

Заведующий кафедрой Ермоленко Т.В.
Преподаватель Бондаренко В.И, Маруга М.М..

Критерии оценивания модульного контроля

Номер задания	*Количество баллов*
1	8
2	8
3	8
Всего	**24**

ГОУ ВПО «Донецкий национальный университет»
Физико-технический факультет
Направление подготовки 09.03.01 «Информатика и вычислительная техника»
Программа подготовки бакалавриат
Семестр 4
Учебная дисциплина Защита информации

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА №4

ВАРИАНТ №1

1. Опишите принцип работы криптографических генераторов псевдослучайных чисел.
2. Что такое контроль целостности?
3. Опишите принцип работы инфраструктуры открытых ключей?

Утверждено на заседании кафедры компьютерных технологий, протокол № 12 от «2» апреля 2020 г.

Заведующий кафедрой Ермоленко Т.В.
Преподаватель Бондаренко В.И, Маруга М.М.

Критерии оценивания модульного контроля

Номер задания	***Количество баллов***
1	4
2	10
3	10
Всего	**24**

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Экзамен не предусмотрен программой.

11. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

ГОУ ВПО «Донецкий национальный университет»
Физико-технический факультет
Направление подготовки 09.03.01 «Информатика и вычислительная техника»
Программа подготовки бакалавриат
Семестр 3
Учебная дисциплина Защита информации

Для чего используется VPN?

1) обеспечение безопасности;
2) увеличение пропускной способности канала;
3) уменьшение задержек соединения;
4) блокирования доступа к информации.

ГОУ ВПО «Донецкий национальный университет»
Физико-технический факультет
Направление подготовки 09.03.01 «Информатика и вычислительная техника»
Программа подготовки бакалавриат
Семестр 4
Учебная дисциплина Защита информации

В какой версии HTML появилось нативная поддержка воспроизведения аудио:

1. $HTML5$	**4.** $HTML2$
2. $HTML4$	**5.** $HTML1$
3. $HTML3$	**6.** $HTML6$

12. КРИТЕРИИ ОЦЕНИВАНИЯ

Распределение баллов, которые могут получить студенты в процессе изучения дисциплины

Третий семестр

	Содержательный модуль №1						Содержательный модуль №2						Всего
	Лабораторные работы				Мод. контр. работа	Всего С.М. №1	Лабораторные работы				Мод. контр. работа	Всего С.М. №2	
	№1	№2	№3	№4			№5	№6					
Макс. балл	8	8	8	8	18	50	10	10			30	50	100

Согласно модульному принципу организации учебного процесса содержание дисциплины «Защита информации» включает в себя четыре зачётных модуля. Каждый зачётный модуль состоит из теоретического материала и практических задач, выполнение которых требует овладения теорией в указанном в модуле объёме.

К первому модульному контролю студент должен защитить 6 лабораторных работ. За *первую* лабораторную работу студент может получить 2 балла. За *вторую, третью и четвёртую* лабораторные работы студент может получить по 8 баллов.

На первом модульном контроле студент имеет возможность получить 24 балла, решив 2 практических задания. Первая задача оценивается в 12 баллов, вторая - в 12 баллов.

Ко второму модульному контролю студент должен защитить 4 лабораторные работы. За *пятую*, *шестую* и *седьмую* лабораторные работы студент может получить по 8 баллов. За *восьмую* лабораторную работу студент может получить 14 баллов.

На втором модульном контроле студент имеет возможность получить 12 баллов, ответив правильно на 20 тестовых вопросов, каждый из которых оценивается в 0.5 балла, и

решив 2 практических задачи, каждая из которых оценивается в 1 балл.

Четвертый семестр

	Содержательный модуль №3							Содержательный модуль №4						Всего
	Лабораторные работы				Конс-пект	Мод. контр. работа	Всего С.М. №1	Лабораторные работы			Конс-пект	Мод. контр. работа	Всего С.М. №2	
	№9	№10	№11	№12				№13	№14	№15				
Макс. балл	6	6	6	6	2	24	50	8	8	8	2	24	50	100

К третьему модульному контролю студент должен защитить 4 лабораторные работы. *За девятую, десятую, одиннадцатую и двенадцатую* лабораторные работы студент может получить по 6 баллов. В 2 балла оценивается ведения конспекта лекций.

На третьем модульном контроле студент имеет возможность получить 24 балла, ответив правильно на 12 тестовых вопросов, каждый из которых оценивается в 2 балла.

К четвёртому модульному контролю студент должен защитить 3 лабораторные работы. *За тринадцатую, четырнадцатую и пятнадцатую* лабораторные работы студент может получить по 8 баллов. В 2 балла оценивается ведения конспекта лекций.

На четвёртом модульном контроле студент имеет возможность получить 24 балла, решив правильно 3 практических задания. Первая задача оценивается в 4 балла, вторая - в 10 баллов, третья - в 10 баллов.

Шкала соответствия баллов национальной шкале

Оценка по шкале ECTS	**Оценка по 100-балльной шкале**	**Оценка по государственной шкале (экзамен, дифференцированный зачет)**	**Оценка по государственной шкале (зачет)**
A	90-100	5 (отлично)	зачтено
B	80-89	4 (хорошо)	зачтено
C	75-79	4 (хорошо)	зачтено
D	70-74	3 (удовлетворительно)	зачтено
E	60-69	3 (удовлетворительно)	зачтено
FX	35-59	2 (неудовлетворительно) с возможностью повторной сдачи	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

Оценка за овладение курса выставляется по следующим критериям:

– Оценку «отлично» заслуживает студент, который обнаружил глубокие знания при ответах на теоретические вопросы по темам курса, а также выполнил практические задания в полном объёме и набрал более 90 баллов.

– Оценку «хорошо» заслуживает студент, сделавший ошибки в теоретических или практических ответах, которые могут быть интерпретированы как малосущественные для вопросов, которые рассматривались. Студент должен набрать более 75 баллов.

– Оценку «удовлетворительно» заслуживает студент, который выполнил задания неполно и с ошибками, но при этом набрал более 60 баллов.

– Оценку «неудовлетворительно» заслуживает студент, который не выполнил большинства теоретических и практических задач и набрал менее 60 баллов.

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Лекционные занятия проводятся в аудитории, оснащенной мультимедийной техникой и доской.

Практические занятия проводятся в компьютерном классе, оборудованном компьютерами с лицензионным программным обеспечением, доступом к сети Интернет, столами и доской.

14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	**Наименование**	**Кол-во экземпляров в библиотеке ДонНУ**	**Наличие электронной версии в ЭБС**

Основная литература			
1.	Бондаренко В.И. Обеспечение безопасности в UNIX-подобных операционных системах: лекции и практические работы /	100	Да
2.	Бондаренко В.И. Обеспечение безопасности в UNIX-подобных операционных системах: лекции и практические работы / Бондаренко В.И., Белоусов В.В., Данилов В.В., Каргин А.А., Кожемякин Ю.А. – Донецк: ДонНУ. – 2011 — 50 с.,	100	Да
3.			

15. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Белоусов В.В. Курс лекций по информационной безопасности: Учебное пособие / В.В. Белоусов, В.И. Бондаренко. - Донецк, Юго-Восток 2009. – 124 с.

2. Бондаренко В.И. Обеспечение безопасности в UNIX-подобных операционных системах: лекции и практические работы / Бондаренко В.И., Белоусов В.В., Данилов В.В., Каргин А.А., Кожемякин Ю.А. – Донецк: ДонНУ. – 2011 — 50 с.,

3. Соколова В. В. Вычислительная техника и информационные технологии. Разработка мобильных приложений. – 2018. URL: http://dl.donnu.ru/course/info.php?id=75 (дата обращения 17.03.2020 г.)

4. Бондаренко В.И.. Группа ВКонтакте http://www.donnu.ru/phys/kt/bondarenko (дата обращения 19.03.2020 г.)

5. Маруга М.М. Облако Mail.ru. http://www.donnu.ru/phys/kt/maruga-mihail-mihaylovich (дата обращения 19.03.2020 г.)

6. Прохорова О.В. Информационная безопасность и защита информации: учебник– Самара.: Самарский государственный архитектурно-строительный университет, 2014.– 113с.

7. РуденковН.А., ПролетарскийА.В., СмирноваЕ.В., Суровов А.М. Технологии защитыи нформации в компьютерных сетях– М:Национальный Открытый Университет «ИНТУИТ»,2016-369с.

8. Галатенко В.А. Основы информационной безопасности. -Интернет-университет информационных технологий -ИНТУИТ.ру, 2006

16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Phyton 3 или более старших версий.
2. Программное средство PGP
3. Visual Studio 2015 или более старших версий

Рабочая программа рассмотрена и переутверждена на заседании кафедры компьютерных технологий с изменениями (без изменений) на 2020 год.

Протокол № 12 от «2» апреля 2020 г.

Заведующий кафедрой Ермоленко Т.В.

Рабочая программа рассмотрена и переутверждена на заседании кафедры компьютерных технологий с изменениями (без изменений) на 2021 год.

Протокол № ___ от «_____» _____ 2021 г.

Заведующий кафедрой

Рабочая программа рассмотрена и переутверждена на заседании кафедры компьютерных технологий с изменениями (без изменений) на 2022 год.

Протокол № ___ от «_____» _____ 2022 г.

Заведующий кафедрой

Рабочая программа рассмотрена и переутверждена на заседании кафедры компьютерных технологий с изменениями (без изменений) на 2023 год.

Протокол № ___ от «_____» _____ 2023 г.

Заведующий кафедрой