

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Физико-технический факультет
Кафедра компьютерных технологий



УТВЕРЖДАЮ
проректор

П.А. Машаров
«29» марта 2024 г.

П.А. Машаров

МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Укрупненная группа направлений
подготовки

Программа высшего образования

Направление подготовки

Профиль подготовки

Квалификация

Форма обучения

09.00.00 Информатика и вычислительная
техника

Программа бакалавриата

09.03.01 Информатика и вычислительная
техника

Информатика и вычислительная техника

Бакалавр

Очная, заочная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «Защита информации» для обучающихся по направлению подготовки 09.03.01 Информатика и вычислительная техника (Профиль подготовки: Информатика и вычислительная техника), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 929 (с изм. и доп.), Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчики:

Старший преподаватель кафедры
компьютерных технологий



И.И. Максименко

Рабочая программа одобрена на заседании кафедры компьютерных технологий.
Протокол от 26.03.2024 г. № 12

Заведующий кафедрой



Г.В. Аверин

СОГЛАСОВАНО:

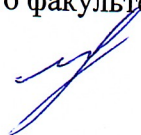
Декан физико-технического факультета
28.03.2024 г.



С.А. Фоменко

Учебно-методическая комиссия физико-технического факультета.
Протокол от 27.03.2024 г. № 2

Председатель



В. Н. Котенко

Руководитель основной профессиональной
образовательной программы,
д-р технических наук, проф.
26.03.2024 г.



Г.В. Аверин

1. МЕСТО ДИСЦИПЛИНЫ / ПРАКТИКИ / КУРСОВОЙ РАБОТЫ / ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

базовая подготовка по математике;

дисциплины программы бакалавриата: «Основы программирования», «Информатика и информационно-коммуникационные технологии», «Программирование», «Математика».

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

«Безопасность и защита информации в информационных системах»; используются при написании выпускной квалификационной работы.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ / ПРАКТИКИ / КУРСОВОЙ РАБОТЫ / ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	09.03.01 Информатика и вычислительная техника
Шифр и название в соответствии с учебным планом	Б1.Б.М4 Защита информации
Часть образовательной программы	Базовая часть Вариативная часть: выбор вуза Вариативная часть: выбор обучающегося
Количество зачетных единиц / всего часов	4 / 144

2.2. Распределение часов по периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы	всего	
Очная	1	1	11	22	-	72,8	105,8	экзамен
Очная, всего								
Заочная	1	1	2	—	4	-	6	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ / ПРАКТИКИ / КУРСОВОЙ РАБОТЫ / ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Целью дисциплины является обзор современных проблем в сфере информационной безопасности в информационных системах, а также обзор направлений развития программы информационной безопасности.

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1. Компетенции

ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности.

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

4.2. Индикаторы компетенций

ОПК-2.1. Применяет современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.

ОПК-3.1. Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

4.3. Результаты обучения

ОПК-2.1.1. Знает: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности

ОПК-2.1.2. Умеет: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности

ОПК-2.1.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-3.1.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.1.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.1.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Компетенции	Индикаторы	Результаты обучения
ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности.	ОПК-2.1. Применяет современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	ОПК-2.1.1. Знает: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.1.2. Умеет: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.1.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.1. Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.1.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.1.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.1.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

5. ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина «Защита информации» предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, самостоятельную работу студентов.

Материал излагается с использованием объяснительно-иллюстративных, эвристических и исследовательских методов преподавания. При проведении лекций используются мультимедийные презентации, специальное оборудование.

В учебном процессе широко применяются активные и интерактивные формы проведения занятий, компьютерные симуляции, внеаудиторная самостоятельная работа, балльно-рейтинговая система оценки успеваемости, личностно-ориентированное обучение, проблемное обучение. В учебном процессе используются интернет-ресурсы по данному курсу; рассматриваются задачи, тесты, самостоятельная работа.

Самостоятельная работа студентов 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, самостоятельное выполнение практических заданий и разработку алгоритмов и текстов программ лабораторных работ, изучение дополнительного инструментария, своевременное и качественное оформление отчётов по лабораторным работам.

Структура дисциплины «Защита информации»

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 подхода. 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.
<p align="center">Содержательный модуль 3.</p> <p align="center">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.</p>	
Тема 8. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	Основы безопасности жизнедеятельности в области профессиональной деятельности. Постановка и решение схемотехнических задач, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надлежностным). Принципы реализации и использования алгоритмов идентификации и аутентификации, управления доступом и процедур анализа защищенности.
Тема 9. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности,	Основные понятия. Описывается протоколирование и аудит, а также криптографические методы защиты. Показывается их место в общей архитектуре безопасности. Методы шифрования. Криптографического контроля целостности. Цифровые сертификаты.

электронная цифровая подпись.	
Тема 10. Основные программно- технические меры безопасности информации: Экранирование, Анализ защищенности.	Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.
Содержательный модуль 4.	
Криптография: шифрование и обеспечение целостности. Протоколирование и аудит, шифрование, контроль целостности. Антивирусная защита компьютерных систем.	
Тема 11. Криптография: шифрование и обеспечение целостности	Основные угрозы безопасности информации и возможные способы их реализации, методы и средства противодействия этим угрозам. Применять на практике собственные и классические алгоритмы криптографической защиты данных. Методы проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия с использованием криптографических систем защиты.
Тема 12. Протоколирование и аудит, шифрование, контроль целостности	Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам в рамках реализации процедур протоколирования и аудита, 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.

Структура дисциплины «Защита информации» по видам учебной деятельности

Названия содержательных модулей и тем	Количество часов									
	Очная форма обучения					Заочная форма обучения				
	всего	в т. ч.				всего	в т. ч.			
		лекции	практические	лабораторные	самостоятель ная работа		лекции	практические	лабораторные	самостоятель ная работа

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	8	1		1	6	8	0		0	7,5
Тема 2. Законодательный уровень информационной безопасности	4,5	1		1	3	4,5	0		0	4,1
Тема 3. Наиболее распространенные угрозы информационной безопасности	8	1		1	6	8	0		0	7,4
Тема 4. Распространение объектно-ориентированного подхода на ИБ	4,5	1		1	3	4,5	0		0	4,2
Итого по содержательному модулю 1	25	3		4	18	25	1		1	23,2
Содержательный модуль 2. Административный уровень информационной безопасности. Процедурный уровень информационной безопасности. Основные программно-технические меры безопасности информации.										
Тема 5. Административный уровень информационной безопасности	9	1		2	6	9	0		0	8,5
Тема 6. Процедурный уровень информационной безопасности	9	1		2	6	9	0		0	8,7
Тема 7. Основные программно-технические меры безопасности информации	9	1		2	6	9	0		0	8,7
Итого по содержательному модулю 2	27	3		6	18	27	0		1	25,9
Содержательный 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.										
Тема 8. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	9	1		2	6	9	0		0	8,4

Тема 9. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись.	9	1		2	6	9	0		0	8,6
Тема 10. Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности.	9	1		2	6	9	0		0	8,6
Итого по содержательному модулю 3	27	3		6	18	27	1		1	25,6
Содержательный модуль 4. Криптография: шифрование и обеспечение целостности. Протоколирование и аудит, шифрование, контроль целостности. Антивирусная защита компьютерных систем.										
Тема 11. Криптография: шифрование и обеспечение целостности	11	1		4	6	11	0		1	10
Тема 12. Протоколирование и аудит, шифрование, контроль целостности	9	1		2	6	9	0		0	8,6
Тема 13. Антивирусная защита компьютерных систем.	9	1		2	6	9	0		0	8,7
Итого по содержательному модулю 4	29	3		8	18	29	1		1	27,3
Всего часов	108	12		24	72	108	2		4	102

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

Темы лекционных занятий

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1.	Понятие Информационной безопасности. Ведение	1	0,1
2.	Законодательный уровень информационной безопасности	0,5	0,2
3.	Наиболее распространенные угрозы информационной безопасности	1	0,2
4.	Распространение объектно-ориентированного подхода на ИБ	0,5	0,1
5.	Административный уровень информационной безопасности	1	0,1
6.	Процедурный уровень информационной безопасности	1	0,1
7.	Основные программно-технические меры безопасности информации	1	0,1

8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	1	0,2
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись.	1	0,2
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности.	1	0,2
11.	Криптография: шифрование и обеспечение целостности	1	0,2
12.	Протоколирование и аудит, шифрование, контроль целостности	1	0,2
13.	Антивирусная защита компьютерных систем.	1	0,1
	ВСЕГО	12	2

Содержание лекций к их выполнению приведены в электронном УМКД кафедры КТ, в электронном репозитории учебных курсов ДонНУ, в материалах учебного курса Cybersecurity Essentials сетевой академии Cisco.

Темы лабораторных занятий

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1.	Разработка алгоритма и программы шифрования и расшифровки информации методом RSA.	6	1
2.	Разработка и реализация программы шифрования и дешифрования методом Диффи-Хеллмана и Эль-Гамалля.	4	0,5
3.	Разработка и реализация программы шифрования и дешифрования алгоритмом AES.	6	1
4.	Разработка и реализация программы привязки к биту, разделения секретов схемами Шамира и Блекли.	4	0,5
5.	Разработка и реализация электронной цифровой подписи на основе RSA, схемами Шнорра и Фейге-Фиата-Шамира.	4	1
	ВСЕГО	24	4

Содержание лабораторных работ и методические рекомендации к их выполнению приведены в электронном УМКД кафедры КТ, в электронном репозитории учебных курсов ДонНУ, в материалах учебного курса Cybersecurity Essentials сетевой академии Cisco.

7. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1.	Понятие Информационной безопасности. Ведение	6	7,5
2.	Законодательный уровень информационной безопасности	3	4,1

3.	Наиболее распространенные угрозы информационной безопасности	6	7,4
4.	Распространение объектно-ориентированного подхода на ИБ	3	4,2
5.	Административный уровень информационной безопасности	6	8,5
6.	Процедурный уровень информационной безопасности	6	8,7
7.	Основные программно-технические меры безопасности информации	6	8,7
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	6	8,4
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись.	6	8,6
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности.	6	8,6
11.	Криптография: шифрование и обеспечение целостности	6	10
12.	Протоколирование и аудит, шифрование, контроль целостности	6	8,6
13.	Антивирусная защита компьютерных систем.	6	8,7
	ВСЕГО	72	102

Содержание самостоятельной работы по темам и методические рекомендации по ее выполнению приведены в электронном УМКД кафедры КТ, в электронном репозитории учебных курсов ДонНУ, в материалах учебного курса Cybersecurity Essentials сетевой академии Cisco.

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 ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «Донецкий национальный университет»

Физико-технический факультет

Направление подготовки 09.03.01 «Информатика и вычислительная техника»

Программа подготовки бакалавриат

Семестр 7

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 № ____ от «__» _____ Г.

Заведующий кафедрой
Преподаватели

Аверин Г.В.
Бондаренко В.И.,
Максименко И.И.

Критерии оценивания модульного контроля

<i>Номер задания</i>	<i>Количество баллов</i>
1	10
2	10
Всего	20

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

11. КРИТЕРИИ ОЦЕНИВАНИЯ ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ

Экзамен не предусмотрен программой.

12. КРИТЕРИИ ОЦЕНИВАНИЯ ОБЩЕЙ УСПЕВАЕМОСТИ

Общая оценка знаний студентов по дисциплине проводится по 100-балльной шкале согласно таким критериям, приведенным в таблице ниже. *Организационно-учебная работа студента* в аудитории оценивается на основе таких критериев как посещаемость занятий, активность во время проведения лекционных и практических занятий (вопросы лектору по теме лекционного материала, участие в обсуждении пройденного материала, и т.п.).

Содержательные модули	Вид работы	Баллы
Содержательный модуль 1,2	Блок лабораторных работ	28
	Организационно-учебная работа студента в аудитории	2
	Модульная контрольная работа	20
	Итого	50
Содержательный модуль 3,4	Блок лабораторных работ	23
	Организационно-учебная работа студента в аудитории	2
	Итоговая контрольная работа	25
	Итого	50
Общий итог		100

Порядок оценивания учебных достижений обучающихся

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

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в 4-м учебном корпусе университета по адресу пр. Театральный 13. Для проведения лекционных и практических занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, компьютер, комплект учебной мебели для студентов, рабочее место преподавателя. Выход в Интернет проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методических кабинетах кафедры компьютерных технологий

В процессе обучения студенты имеют возможность использовать учебные материалы по дисциплине «СУБД Oracle», размещенные на интернет-ресурсах преподавателя, в электронном репозитории учебных курсов ГОУ ВПО «ДонНУ» на платформе Moodle, в материалах учебного курса Cybersecurity Essentials сетевой академии Cisco. С использованием ресурсов платформы дистанционного образования также осуществляется текущий контроль знаний студентов на основе тестирования и проверки результатов самостоятельной работы.

14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
<i>Основная литература</i>			
1.	Бондаренко В.И. Курс лекций по информационной безопасности. Учебное пособие / Бондаренко В.И., Белоусов В.В. – Донецк: Юго-Восток. – 2009 – 124с.	100	Да
2.	Бондаренко В.И. Лабораторные работы по информационной безопасности. Методические указания / Бондаренко В.И., Белоусов В.В. – Донецк: Юго-Восток. – 2009 – 72с.	100	Да
3.	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
<i>Дополнительная литература</i>			
4.	Прохорова О.В. Информационная безопасность и защита информации: учебник– Самара.: Самарский государственный архитектурно-строительный университет, 2014.– 113с.		

15. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Бондаренко В.И. Страница с ресурсами для студентов <http://www.donnu.ru/phys/kt/bondarenko> (дата обращения 19.03.2021 г.)
2. Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М. Технологии защиты информации в компьютерных сетях – М: Национальный Открытый Университет «ИНТУИТ», 2016 – 369 с. (дата обращения 19.03.2021 г.)
3. Галатенко В.А. Основы информационной безопасности. - Интернет-университет информационных технологий - ИНТУИТ.ру, 2006 (дата обращения 19.03.2021 г.)

16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

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