

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


«29» марта 2024 г.

П.А. Машаров

МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Укрупненная группа направлений
подготовки

Программа высшего образования
Направление подготовки

Профиль подготовки

Квалификация
Форма обучения

09.00.00 Информатика и вычислительная
техника

Программа магистратуры

09.04.01 Информатика и вычислительная
техника

Информатика и вычислительная техника

Технологии искусственного интеллекта

Магистр

Очная, заочная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «Безопасность и защита информации в информационных системах» для обучающихся по направлению подготовки 09.04.01 Информатика и вычислительная техника, магистерских программ (Профиль подготовки: Информатика и вычислительная техника, Технологии искусственного интеллекта), составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 918 (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:

Доцент кафедры компьютерных технологий,
канд. техн. наук, доцент



В.И.Бондаренко

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

Заведующий кафедрой



Г.В. Аверин

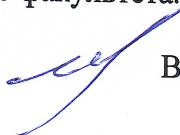
СОГЛАСОВАНО:

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 В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина «Безопасность и защита информации в информационных системах» является практико-ориентированной дисциплиной и относится к базовой части образовательной программы.

Для изучения данной учебной дисциплины необходимы знания и умения, формируемые предшествующими дисциплинами – «Защита информации», «Методы и средства проектирования информационных систем и технологий», «Современные информационные системы и технологии», «Программирование», «Управление проектированием информационных систем». Знания и умения, полученные в ходе изучения дисциплины «Управление проектированием информационных систем», используются при написании магистерской диссертации.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

Наименование показателя	Характеристика дисциплины	
Укрупненная группа направлений подготовки	09.04.00 Информатика и вычислительная техника	
Направление подготовки	09.04.01 Информатика и вычислительная техника	
Программа высшего образования	магистратура	
Магистерская программа	1. Информатика и вычислительная техника 2. Технологии искусственного интеллекта	
Дисциплина базовой / вариативной части образовательной программы	Базовая часть	
	очная форма обучения	заочная форма обучения
Количество зачетных единиц	5	
Общее количество часов	180	
Год подготовки	2	2
Семестр	2	–
Количество содержательных модулей	2	2
Недельное количество часов для очной формы обучения:		
аудиторных	6	–
лекционных	20	4
практических, семинарских	-	-
лабораторных	40	8
самостоятельной работы	120	168
индивидуальные задания		
Форма промежуточной аттестации	экзамен	

3. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Безопасность и защита информации в информационных системах» является изучение основных принципов, методов

и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Основными задачами изучения дисциплины являются усвоение теоретических основ и приобретение практических навыков:

- изучение концепции защиты информации в информационных системах (ИС);
- изучение теоретических основ защиты информации в ИС;
- изучение физических основ инженерно-технической защиты информации;
- изучение технических средств добывания и защиты информации;
- изучение организационных основ защиты информации в ИС;
- изучение методического обеспечения защиты информации в ИС.

4. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Требования к результатам освоения дисциплины. Процесс изучения дисциплины «Безопасность и защита информации в информационных системах» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО РФ по направлению подготовки 09.04.01 Информатика и вычислительная техника и основной профессиональной образовательной программы высшего образования направления подготовки 09.04.01 Информатика и вычислительная техника:

<i>Общепрофессиональные компетенции (ОПК):</i>	
ОПК-5	Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК-6	Способен разрабатывать компоненты программно- аппаратных комплексов обработки информации и автоматизированного проектирования

Индикаторы достижения компетенций и результаты обучения. Достижение компетенций оценивается на основе следующих индикаторов и соответствующих им результатов обучения:

Общепрофессиональные компетенции	Индикаторы	Результаты обучения
ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ОПК-5.1. Знать: современное программное и аппаратное обеспечение информационных и автоматизированных систем	Знает средства и методы предотвращения и обнаружения вторжений.
		Знает возможности технических средств перехвата информации.
		Знает технические каналы утечки информации.
		Знает организацию защиты информации от утечки по техническим каналам на объектах информатизации.

		Знает основные требования к системам криптографической защиты
		Знает основные алгоритмы криптографической защиты и электронной подписи
	ОПК-5.2. Уметь: модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач	Умеет оценивать качество готового программного обеспечения с точки зрения безопасности.
		Умеет ориентироваться в современной системе источников информации.
		Умеет использовать защищенные современные информационные технологии в своей профессиональной деятельности.
		Умеет анализировать информационную безопасность многопользовательских систем.
		Умеет пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа.
		Умеет видеть и формулировать проблему защиты информации.
	ОПК-5.3. Владеть: навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	Владеет методами расчета и инструментального контроля показателей технической защиты информации.
		Владеет навыками разработки инструментов криптографической защиты информации.
		Владеет навыками применения методологии защиты в области информационной безопасности.

ОПК-6. Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования	ОПК-6.1. Знает: аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности	Знает основные подходы для решения задач обеспечения безопасности и защиты информации в информационных системах.
	ОПК-6.2. Умеет: анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования.	Умеет анализировать предметную область, делать обобщения и синтезировать знания о ней.
		Умеет выбрать модель, наиболее адекватную решаемой задаче и обосновать ее эффективность.
	ОПК-6.3. Владеет: навыками составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса.	Владеет основными методами обработки информации

5. ПРОГРАММА ДИСЦИПЛИНЫ

Темы	Вопросы тем
Содержательный модуль 1. Основные положения теории информационной безопасности	
Тема 1. Международные стандарты информационного обмена. Понятие угрозы.	Стандарты в области информационной безопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.
Тема 2. Виды возможных нарушений	Три вида возможных нарушений информационной безопасности. 3 составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз.

информационной системы. Защита.	
Тема 3. Основные положения теории информационной безопасности. Модели безопасности и их применение.	Основные положения теории информационной безопасности. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании. Модели безопасности для домашней информационной системы. Применение методов информационной безопасности
Тема 4. Таксономия нарушений информационной безопасности и причины, обуславливающие их существование.	Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы. Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.
Тема 5. Использование защищенных компьютерных систем.	Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике. Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.
Содержательный модуль 2. Криптографические методы защиты информации.	
Тема 6. Предмет и задачи криптографии.	Основные понятия: задачи, объект, предмет, методы криптографической безопасности. Требования к криптографическим системам защиты информации. Способы реализации криптографических методов. Понятие и виды криптографических атак. Криптографический протокол. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-программные средства защиты информации. Классификация методов шифрования. Требования к современным шифрам.
Тема 7. Методы шифрования с закрытым ключом.	Простейшие методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подстановки. Методы гаммирования. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Режимы работы блочных алгоритмов. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Использование блочных алгоритмов шифрования для формирования хеш-функции. Обзор алгоритмов формирования хеш-функций.
Тема 8.	Основные понятия и классификация средств асимметричной криптографической защиты информации. Основные свойства

Криптографические алгоритмы с открытым ключом.	асимметричных криптосистем. Односторонние функции. Требования к алгоритмам шифрования с открытым ключом. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с открытым ключом. Генерация и хранение ключей. Формирование секретных ключей с использованием асимметричных алгоритмов. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Алгоритм RSA. Алгоритм Эль-Гамала. Криптографические системы на эллиптических кривых. Возможные атаки при использовании алгоритмов асимметричного шифрования.
Тема 9. Электронная цифровая подпись	История развития. Виды электронных подписей в Российской Федерации. Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамала. Стандарты на алгоритмы цифровой подписи. Управление открытыми ключами. Протокол аутентификации Нидхэма-Шредера в случаях симметричной и асимметричной системы шифрования. Модели атак и их возможные результаты.
Тема 10. Совершенно секретные системы.	Основные подходы к измерению информации. Энтропия и неопределенность. Норма языка и избыточность сообщений. Понятие совершенно секретной системы. Расстояние единственности.

6. СТРУКТУРА ДИСЦИПЛИНЫ

Названия содержательных модулей и тем	Количество часов											
	Очная форма обучения						Заочная форма обучения					
	всего	В Т.Ч.					всего	В Т.Ч.				
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа
Содержательный модуль 1. Основные положения теории информационной безопасности												
Тема 1. Международные стандарты информационного обмена. Понятие угрозы.	18	2		4	12		18	0,4		0,8	16,8	

Тема 2. Виды возможных нарушений информационной системы. Защита.	18	2		4	12		18	0,4		0,8	16,8	
Тема 3. Основные положения теории информационной безопасности. Модели безопасности и их применение.	18	2		4	12		18	0,4		0,8	16,8	
Тема 4. Таксономия нарушений информационной безопасности и причины, обуславливающие их существование.	18	2		4	12		18	0,4		0,8	16,8	
Тема 5. Использование защищенных компьютерных систем.	18	2		4	12		18	0,4		0,8	16,8	
Итого по 1-му содержательному модулю	90	10		20	60	0	90	2		4	84	
Содержательный модуль 2. Криптографические методы защиты информации.												
Тема 6. Предмет и задачи криптографии.	18	2		4	12		18	0,4		0,8	16,8	
Тема 7. Методы шифрования с закрытым ключом.	18	2		4	12		18	0,4		0,8	16,8	
Тема 8. Криптографические алгоритмы с открытым ключом.	18	2		4	12		18	0,4		0,8	16,8	
Тема 9. Электронная цифровая подпись.	18	2		4	12		18	0,4		0,8	16,8	
Тема 10. Совершенно секретные системы.	18	2		4	12		18	0,4		0,8	16,8	

<i>Итого по 2-му содержательному модулю</i>	90	10		20	60		90	2		4	84	
<i>Всего часов</i>	180	20		40	120		180	4		8	168	

7. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа имеет особенное значение для креативного (творческого) усвоения основных понятий и категорий основы научной работы обучающихся. Самостоятельная работа обучающегося является важной формой учебного процесса, которая позволяет приобрести, а также закрепить новые знания, навыки и умения, сформировать личные убеждения, использовать полученные знания и умения в практической деятельности. Она осуществляется на протяжении всего процесса обучения и имеет следующие стадии:

1. Первичное ознакомление с материалами лекций и составление конспекта лекций;
2. Изучение и усвоение лекционного материала;
3. Самостоятельная проработка литературных источников и обобщение изученного материала;
4. Подготовка к лабораторным занятиям;
5. Индивидуальная работа по заданию преподавателя.

Контрольными формами самостоятельной работы по дисциплине могут быть следующие: работа с литературными первоисточниками по темам дисциплины; выполнение тестов, подготовка докладов, собственных проектов, тезисов, научных статей.

8. ТЕМАТИКА ЛАБОРАТОРНЫХ ЗАНЯТИЙ

1. Основные технологии построения защищенных систем
2. Симметричные криптосистемы
3. Криптоанализ симметричных криптосистем
4. Криптографические протоколы на основе асимметричных криптосистем
5. Стеганографический метод
6. Тайные многосторонние вычисления и разделение секрета

Содержание лабораторных работ и методические рекомендации к их выполнению приведены в электронном УМКД кафедры КТ и в электронном репозитории учебных курсов ДонГУ.

9. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Основные составляющие информационной безопасности. Категории и носители информации.
2. Объекты и средства защиты информации в информационных системах.

3. Криптография. Основные термины и определения. Классификация криптографических систем.
4. Шифры гаммирования. Классификация и основные методы шифрования.
5. Режимы шифрования DES. Сферы применения различных режимов DES.
6. AES. Краткая характеристика основных этапов зашифрования/расшифрования.
7. Шифрование с открытым ключом. Основные понятия.
8. Алгоритм шифрования RSA.
9. Алгоритм шифрования Эль-Гамала.
10. Алгоритм шифрования на основе эллиптических кривых.
11. Хэш-функции. Основные понятия и разновидности. Хэш-функция. MD5.
12. Криптографические протоколы. Основные понятия.
13. Протоколы обмена ключами.
14. Парольная идентификация/аутентификация.
15. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.
16. Сервер аутентификации Kerberos.
17. Идентификация/аутентификация с помощью биометрических данных.
18. Идентификационные карты (ID-cards) и электронные ключи.
19. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
20. ЭЦП на базе алгоритма RSA и алгоритмы цифровой подписи ГОСТ 34.10-94 и ГОСТ 34.10-2001.
21. Протоколы контроля целостности: Биты четности, контрольные цифры и числа.
22. Протоколы контроля целостности: Использование ЭЦП и MAC-кодов.
23. Протоколы контроля целостности: Коды Хэмминга и ECC.
24. Электронные платежи. Разновидности и краткая характеристика.
25. Протоколы разбиения и разделения секрета.
26. Тайные многосторонние вычисления.
27. Основные сведения о криптоанализе и атаки на криптосистемы.
28. Компьютерная стеганография.
29. Общедоступные кодовые системы.
30. Секретные кодовые системы.

10. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ ОБУЧАЮЩИХСЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ОБРАЗЕЦ ЗАДАНИЯ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

ФГБОУ ВО «ДОНЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Физико-технический факультет

Направление подготовки: **09.04.01 Информатика и вычислительная техника**

Магистерская программа: **Информатика и вычислительная техника**

Программа подготовки: **академическая магистратура**

Семестр **4**

Учебная дисциплина **Безопасность и защита информации в информационных системах**

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА 1

ВАРИАНТ №1

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется
Выберите один ответ.
 - a. Компилятор
 - b. Интернет-черви
 - c. Вирус
2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется
Выберите один ответ.
 - a. Воздействием (влиянием)
 - b. Потерей
 - c. Силой
3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется
Выберите один ответ.
 - a. Троянской программой
 - b. Червем
 - c. Вирусом
4. Уровень риска, который считается доступным для достижения желаемого результата, называется
Выберите один ответ.
 - a. Устойчивостью
 - b. Терпимостью по отношению к риску
 - c. Независимостью
5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд
Выберите один ответ.
 - a. Две
 - b. Одну
 - c. Сколько зададут
6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:
Выберите один ответ.
 - a. Статическими алгоритмами
 - b. Алгоритмы RMS
 - c. Динамическими алгоритмами
7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются: Выберите один ответ.
 - a. Каталоги

- b. Символьные файлы
 c. Регулярные файлы
8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются
 Выберите один ответ.
- a. Вирусами
 b. Руткитами
 c. Червями
9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:
 Выберите один ответ.
- a. Правилами безопасности
 b. Требованием безопасности
 c. Мерами безопасности
10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:
 Выберите один ответ.
- a. Управление риском
 b. Предупреждением рисков
 c. Анализом рисков

Утверждено на заседании кафедры компьютерных технологий,
 протокол № ____ от «____» _____ 20__ г.

Заведующий кафедрой
 Преподаватель

Аверин Г.В.
 Бондаренко В.И.

Критерии оценивания задания модульного контроля

<i>Номер задания</i>	<i>Количество баллов</i>
Задание 1	2
Задание 2	2
Задание 3	2
Задание 4	2
Задание 5	2
Задание 6	2
Задание 7	2
Задание 8	2
Задание 9	2
Задание 10	2
<i>Всего</i>	20

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

ФГБОУ ВО «ДОНЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Физико-технический факультет

Направление подготовки:

09.04.01 Информатика и вычислительная техника

Магистерская программа: **Информатика и вычислительная техника**
 Программа подготовки: **академическая магистратура**
 Семестр **4**
 Учебная дисциплина
Безопасность и защита информации в информационных системах

Экзаменационный билет 1

1. Атаки на систему безопасности и современные методы защиты.
2. Kerberos. Протокол распределения ключей.

Утверждено на заседании кафедры компьютерных технологий,
 протокол № ____ от «__» _____ 20__ г.

Заведующий кафедрой
 Экзаменатор

Аверин Г.В.
 Бондаренко В.И.

Критерии оценивания экзамена

Номер задания	Количество баллов
Задание 1	15
Задание 2	25
Всего	40

Критерии оценивания экзамена

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	Блок лабораторных работ	15
	Организационно-учебная работа студента в аудитории	5
	Модульная контрольная работа	20
	Итого	40
Содержательный модуль 2	Блок лабораторных работ	15
	Организационно-учебная работа студента в аудитории	5
	Экзамен	40
	Итого	60
Общий итог		100

Порядок оценивания учебных достижений обучающихся

Оценка по шкале ECTS	Оценка по 100-балльной шкале	Оценка по государственной шкале	
		экзамен, дифференцированный зачет	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 аттестации	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

11. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

1) для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом.

2) для глухих и слабослышащих:

- лекции оформляются в виде электронного документа;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования;

3) для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ДИСЦИПЛИНЫ

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 «Управление проектированием информационных систем», размещенные на интернет-ресурсах преподавателя, в электронном репозитории учебных курсов ФГБОУ ВО «ДонГУ» на платформе Moodle. С использованием ресурсов платформы дистанционного образования также осуществляется текущий контроль знаний студентов на основе тестирования и проверки результатов самостоятельной работы.

13. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонГУ	Наличие электронной версии в ЭБС
<i>Основная литература</i>			
..	Башлы П. Н. Информационная безопасность [Электронный учебник] : учебное пособие / Башлы П. Н.. - Евразийский открытый институт, 2012. - 311 с.		http://iprbooksh op.ru/10677
..	Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. Учебное пособие - М.: Форум : ИНФРА-М, 2014. – 256 с.		
<i>Дополнительная литература</i>			

8.	Алферов А.П., Зубов А.Ю. и др. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 480 с, ил		
----	---	--	--

14. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Ссылки на электронные материалы курса. URL: <http://donnu.ru/phys/kt/bondarenko> (дата обращения 10.03.2021 г.)
2. Информационная система "Единое окно доступа к образовательным ресурсам" URL: <http://window.edu.ru/> (дата обращения 10.03.2021 г.)
3. Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН) URL: <http://www.vlibrary.ru/> (дата обращения 10.03.2021 г.)

15. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

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