

Министерство науки и высшего образования
Российской Федерации

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

Факультет физико-технический
Кафедра радиофизики и инфокоммуникационных технологий



УТВЕРЖДАЮ

проректор

П.А. Машаров

«29» марта 2024 г.

МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

Укрупненная группа направлений подготовки	10.00.00 Информационная безопасность
Программа высшего образования	Программа магистратуры
Направление подготовки	10.04.01 Информационная безопасность
Магистерская программа	Информационная безопасность
Квалификация	Магистр
Форма обучения	очная; очно-заочная


Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «**Защищенные информационные системы**» для обучающихся по направлению подготовки 10.04.01 Информационная безопасность (Магистерская программа: Информационная безопасность), составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации Приказ от 26 ноября 2020 г. № 1455(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.

Разработчик:

Доцент
кафедры радиофизики
и инфокоммуникационных технологий

 О.Г. Шелехова

Рабочая программа утверждена на заседании кафедры радиофизики и
инфокоммуникационных технологий
Протокол от 26.03.2024 г. № 16

Заведующий кафедрой

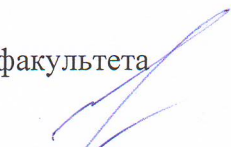
 В.В. Данилов

СОГЛАСОВАНО:

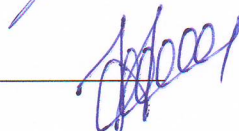
И.о. декана физико-технического факультета
28.03.2024 г.

 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 тех. наук, проф.
26.03.2024 г.

 В.В. Данилов

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

базовая подготовка по математике в объеме программы средней школы; дисциплины программы бакалавриата: «Математика», «Физика», «Информатика» «Основы информационной безопасности», «Надежность автоматизированных систем», «Программно-аппаратные средства защиты информации», «Моделирование и системы принятия решений»;

предшествующих и сопутствующих дисциплин программы магистратуры: «Защищенные информационные системы», «Технологии обеспечения информационной безопасности объектов».

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

«Автоматизированные системы радиомониторинга».

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1.Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.04.01. Информационная безопасность (Магистерская программа: Информационная безопасность)
Шифр и название в соответствии с учебным планом	Б1.Б.М2.2. Защищенные информационные системы
Часть образовательной программы	Базовая обязательная часть
Количество зачетных единиц / всего часов	2/ 72

2.2.Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная, всего	1	2	15	30	-	27	72	зачет
Очно-заочная, всего	1	2	4	8	-	60	72	зачет

3. ЦЕЛИ ДИСЦИПЛИНЫ

Изучение особенностей и строения, а также функциональных возможностей и областей применения современных операционных систем на базе Windows и Linux, с целью применения данных знаний в контексте задач информационной безопасности.

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

4.1.Компетенции

Компетенции	Индикаторы	Результаты обучения
ОПК-2. Владеет	ОПК-2.1. Применяет	ОПК-2.1.1. Знает определения и утверждения,

навыками и технологиями разработки приложений для решения задач информационной безопасности	современные математические методы для разработки приложений для решения задач информационной безопасности	современные математические методы решения задач, приёмы доказательства утверждений, методы обеспечения безопасности объектов, применяемые для решения профессиональных задач. ОПК-2.1.2. Умеет выбирать и использовать необходимые математические методы и вычислительные средства, решать задачи. ОПК-2.1.3. Аргументированно выбирает метод решения задачи, устанавливает свойства математических объектов, закономерности между ними, доводит решение задачи до приемлемого (числового или символьного) результата, оценивает и анализирует полученный результат, строит математические модели обеспечения безопасности объектов для решения профессиональных
---	---	--

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1.Состояние и перспективы развития методического обеспечения защиты информации в информационных системах	1.1. Оценка состояния и перспективы развития методического обеспечения категорирования информационных систем и обрабатываемой в них информации. 1.2. Оценка состояния и перспективы развития методического обеспечения прогнозирования возникновения уязвимостей программного обеспечения и угроз безопасности информации в информационных системах. 1.3. Оценка состояния и перспективы развития методического обеспечения оценки рисков реализации угроз безопасности информации.
2. Анализ моделей и методов построения систем, атак и угроз безопасности информации, оценки эффективности систем защиты информации	2.1.Анализ моделей и методов построения информационных систем 2.2.Анализ ИТ - архитектуры и систем защиты информации 2.3 Анализ моделей угроз безопасности информации и атак на информационные системы. 2.4 Анализ международных стандартов в области обеспечения безопасности информации. 2.5 Анализ требований по защите информации регуляторов Российской Федерации 2.6 Анализ методов и методик оценки эффективности систем защиты информации
3.Методика определения актуальных угроз безопасности информации	3.1 Типы угроз безопасности информации 3.2 Определение источников угроз безопасности информации 3.3 Перечень возможных угроз безопасности информации 3.4 Методика определения актуальных угроз безопасности информации
4. Вопросы управления рисками информационной безопасности	4.1.Методики анализа и оценки рисков информационной безопасности. 4.2. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартом ГОСТ Р ИСО/МЭК

	27005-2010. 4.3. Особенности подхода к анализу рисков информационной безопасности для малого и среднего бизнеса 4.4. Анализ безопасности информационных систем методом тестирования на проникновение.
5. Управление инцидентами информационной безопасности	5.1. Особенности управления инцидентами информационной безопасности 5.2. Современные DDoS атаки как угроза для бизнеса в Интернете

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 1, семестр – 2

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Состояние и перспективы развития методического обеспечения защиты информации в информационных системах	3	6	-	5	14
Анализ моделей и методов построения систем, атак и угроз безопасности информации, оценки эффективности систем защиты информации	3	6	-	6	15
Методика определения актуальных угроз безопасности информации	3	6	-	5	14
Вопросы управления рисками информационной безопасности	3	6	-	6	15
Управление инцидентами информационной безопасности	3	6	-	5	14
ИТОГО ПО КОМПОНЕНТУ ОПОП	15	30	-	27	72

6.2. Форма обучения – очно-заочная, курс – 1, семестр – 2

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Состояние и перспективы развития методического обеспечения защиты информации в информационных системах	0,5	1	-	12	13,5
Анализ моделей и методов построения систем, атак и угроз безопасности информации, оценки эффективности систем защиты информации	1	2	-	12	15
Методика определения актуальных угроз безопасности информации	1	2	-	12	15
Вопросы управления рисками информационной безопасности	1	2	-	12	15
Управление инцидентами информационной безопасности	0,5	1	-	12	13,5
ИТОГО ПО КОМПОНЕНТУ ОПОП	4	8	-	60	72

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

1. Оцените состояние и перспективы развития методического обеспечения категорирования информационных систем и обрабатываемой в них информации.
2. Оцените состояние и перспективы развития методического обеспечения прогнозирования возникновения уязвимостей программного обеспечения и угроз безопасности информации в информационных системах.
3. Оцените состояние и перспективы развития методического обеспечения оценки рисков реализации угроз безопасности информации.
4. Проанализируйте модели и методы построения информационных систем
5. Выполните анализ ИТ - архитектуры и систем защиты информации
6. Проанализируйте модели угроз безопасности информации и атак на информационные системы.
7. Проанализируйте международные стандарты в области обеспечения безопасности информации.
8. Выполните анализ требований по защите информации регуляторов Российской Федерации
9. Проанализируйте методы и методики оценки эффективности систем защиты информации
10. Типы угроз безопасности информации
11. Определение источников угроз безопасности информации
12. Перечень возможных угроз безопасности информации
13. Методика определения актуальных угроз безопасности информации
14. Методики анализа и оценки рисков информационной безопасности.
15. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартом ГОСТ Р ИСО/МЭК 27005-2010.
16. Особенности подхода к анализу рисков информационной безопасности для малого и среднего бизнеса
17. Анализ безопасности информационных систем методом тестирования на проникновение.
17. Особенности управления инцидентами информационной безопасности
19. Современные DDoS атаки как угроза для бизнеса в Интернете

7.2. Темы докладов

1. Обзор руководящих документов Федеральной службы технического и экспортного контроля (ФСТЭК России).
2. Какие вызовы могут возникнуть при составлении и использовании модели угроз безопасности информационной системы?
3. Каким образом составленная модель угроз может быть использована для планирования мер по обеспечению безопасности информационной системы?

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

8.1. Семестр 2, курс 1

Номера разделов	Виды работ	Максимальное количество баллов
1-8	Организационно-учебная работа обучающегося в аудитории	30
	Самостоятельная работа	20
	Модульная контрольная работа	10
ИТОГО		60
Зачетная работв		40
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. 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.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в корпусе №4 ДонГУ (г. Донецк, пр. Театральный, 13). Для проведения лекционных занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для проведения лабораторных занятий требуется оборудованная персональными компьютерами аудитория.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.312).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Бабаш А.В., Баранова Е.К. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. – М. : РИОР : ИНФРА-М, 2017. – 111 с. (Научная мысль). – https://doi.org/10.12737/monography_58dbc380a_a3a4.

2. Бабаян Б.И. Защищенные информационный системы – http://www.mcst.ru/files/521c577c6487/1a361c/000000/secure_information_system_v5_2r.pdf

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Научная электронная библиотека elibrary.ru : информ.-аналит. портал / ООО Научная электронная библиотека. – Москва : ООО Науч. электрон. б-ка, cop. 2000–2022. –

URL: <https://elibrary.ru> (дата обращения: 01.03.2024). – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. Электронный каталог Научной библиотеки Донецкого государственного университета. – Донецк : НБ ДонГУ, 1999– . – URL: <http://catalog.donnu.education> (дата обращения: 01.01.2024). – Текст : электронный;

3. Учебники и другие книги по математике URL: <http://eqworld.ipmnet.ru/ru/library/mathematics.htm> (дата обращения: 31.03.2024). – Режим доступа: свободный. – Текст : электронный

4. Интернет-библиотека Виталия Арнольда URL: <http://ilib.mccme.ru/> (дата обращения: 31.03.2024). – Режим доступа: свободный. – Текст : электронный;

5. Техническая библиотека URL: <http://techlibrary.ru/> (дата обращения: 31.03.2024). – Режим доступа: свободный. – Текст : электронный;

6. Научные журналы ФГБОУ ВО «ДонГУ» URL: <http://donnu.ru/science/journals> (дата обращения: 31.03.2024). – Режим доступа: свободный. – Текст : электронный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).
5. Федеральный портал «Российское образование» <http://www.edu.ru>