

Министерство науки и высшего образования  
Российской Федерации

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

Факультет физико-технический  
Кафедра радиоп физики и инфокоммуникационных технологий



УТВЕРЖДАЮ  
проректор

*Маш*  
29 марта 2024 г.  
МП

П.А. Машаров

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
«ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ  
БЕЗОПАСНОСТИ»**

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 **«Информационно-аналитические системы безопасности»** 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:

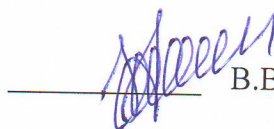
Доцент  
кафедры радиопизики  
и инфокоммуникационных технологий



О.Г. Шелехова

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

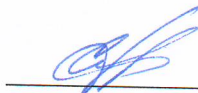
Заведующий кафедрой



В.В. Данилов

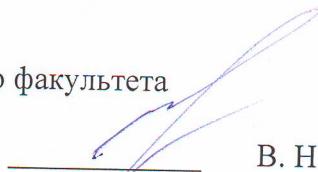
СОГЛАСОВАНО:

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

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

базовая подготовка по математике в объёме программы средней школы; дисциплины программы бакалавриата: «Математика», «Физика», «Информатика» «Основы информационной безопасности», «Программно-аппаратные средства защиты информации», предшествующих и сопутствующих дисциплин программы магистратуры: «Защищенные информационные системы»,

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

«Технологии обеспечения информационной безопасности объектов».

## 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.В.ОД.6. Информационно-аналитические системы безопасности
Часть образовательной программы	Дисциплина по выбору: безальтернативные дисциплины
Количество зачетных единиц / всего часов	4,5/ 162

### 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	2	3	34	34	-	94	162	зачет
Очно-заочная, всего	2	3	8	9	-	145	162	зачет

## 3. ЦЕЛИ ДИСЦИПЛИНЫ

Сформировать систематические знания, представления, умения и навыки в области информационно-аналитических систем безопасности; развить систему знаний, умений и навыков, обучающихся по теоретическим основам их построения, особенностям проектирования и практического применения.

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

### 4.1. Компетенции

Компетенции	Индикаторы	Результаты обучения
ПК-1. Способен разрабатывать программно-	ПК-1.1. Применяет современные математические	ПК-1.1.1. Знает определения и утверждения, методы решения задач, приёмы доказательства утверждений, методы

аппаратные, программно-технические, технические средства и системы защиты информации	методы для решения фундаментальных и прикладных задач, связанных технологией обеспечения безопасности объектов	обеспечения безопасности объектов, применяемые для решения профессиональных задач. ПК-1.1.2. Умеет выбирать и использовать необходимые математические методы и вычислительные средства, решать задачи. ПК-1.1.3. Аргументированно выбирает метод решения задачи, устанавливает свойства математических объектов, закономерности между ними, доводит решение задачи до приемлемого (числового или символического) 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. Сущность, структура и задачи аналитики СБ.	1.1. Понятие и сущность аналитики системы безопасности 1.2. Структура и задачи аналитики систем безопасности. 1.3. Информационно-аналитические технологии системы безопасности, их задачи.
2. Стандарты обеспечения информационной безопасности	2.1. Формирование концепций правового регулирования информационной безопасности за рубежом и в России. 2.2. Системность подхода к построению стратегии кибербезопасности в США 2.3. Национальные стратегии кибербезопасности в странах ЕС и НАТО. 2.4. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом 2.5. Стратегия формирования правовых методов информационной безопасности Российской Федерации
3. Правовые методы обеспечения информационной безопасности	3.1. Характеристика информации, как объекта обеспечения безопасности Российской Федерации 3.2. Гражданско-правовые механизмы обеспечения информационной безопасности 3.3. Значение ноу-хау и режима коммерческой тайны в практической деятельности обеспечения информационной безопасности 3.4. Система уголовно-правового обеспечения информационной безопасности 3.5. Правовое регулирование некоторых сфер информатизации в России и за рубежом 3.6. Защита приватности и персональных данных в законодательстве России и США 3.7. Электронный документ в России и США.
4. Информационно-аналитическое обеспечение системной	4.1. Задачи и определения информационно-аналитического (ИА) обеспечения СБ, 4.2. Организационные формы субъектов ИА работы; 4.3. Описание субъекта информационной безопасности и

безопасности объекта.	<p>выявление среди них критических.</p> <p>4.4. Присвоение категорий значимости.</p> <p>4.5. Анализ угроз безопасности, возможных действий нарушителя.</p> <p>4.6. 4.6. Определение перечня угроз безопасности объекта.</p> <p>4.7. Разработка организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры.</p> <p>4.8. Подготовка сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости</p> <p>4.9. Разработка модели угроз защищаемого объекта</p> <p>4.10. Разработка модели вероятного нарушителя.</p> <p>4.11. Технические каналы утечки информации</p> <p>4.12. Анализ каналов утечки информации. Построение модели угроз с учетом каналов утечки.</p>
5. Синтез информационно-аналитических СБ	<p>5.1. Режимы восприятия информации; средства автоматизации информационно-аналитической работы.</p> <p>5.2. Моделирование и принятие решений в информационно-аналитической системе безопасности объектов.</p> <p>5.3. Аналитические системы поддержки принятия решений</p>

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 6.1. Форма обучения – очная, курс – 2, семестр – 3

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Сущность, структура и задачи аналитики СБ.	6	-	6	18	30
Стандарты обеспечения информационной безопасности	7	-	7	19	33
Правовые методы обеспечения информационной безопасности	7	-	7	19	33
Информационно-аналитическое обеспечение системной безопасности объекта.	7	-	7	19	33
Синтез информационно-аналитических	7	-	7	19	33
ИТОГО ПО КОМПОНЕНТУ ОПОП	34	—	34	94	162

### 6.2. Форма обучения – очно-заочная, курс – 2, семестр – 3

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Основные положения системной концепции обеспечения безопасности объекта.	1,5	-	1,5	30	33
Технические средства охраны объектов	1,5	-	2	30	33,5
Технические каналы утечки информации	1,5	-	2	31	34,5
Методы и средства выявления закладных устройств	1,5	-	2	31	34,5
Применение технических средств наблюдения для контроля территории	2	-	1,5	30	33,5
ИТОГО ПО КОМПОНЕНТУ ОПОП	8	—	9	152	144

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

### 7.1. Контрольные вопросы

1. Основные понятия теории безопасности.
2. Ценность информации.
3. Общий анализ угроз информационной безопасности.
4. Основные виды атак на автоматизированные системы (АС).
5. Понятие политики безопасности.
6. Понятие и сущность аналитики СБ.
7. Структура и задачи аналитики СБ.
8. Информационно-аналитические технологии СБ, их задачи.
9. Основные критерии оценки защищенности АС.
10. Концепция защиты АС и средств вычислительной техники (СВТ) по руководящим документам ФСТЭК РФ.
11. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
12. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
13. Методы структурирования информации.
14. Методы поэтапной структуризации задач и морфологические методы.
15. Методы обработки и анализа числовых данных.
16. Угрозы конфиденциальности, целостности, доступности информации; раскрытие параметров информационной системы.
17. Задачи и определения информационно-аналитического (ИА) обеспечения СБ.
18. Организационные формы субъектов ИА работы.
19. Системы, управляемые потоком событий.
20. Поиск, отбор и анализ данных.
21. Неструктурированные текстовые данные.
22. Структурированные текстовые данные.
23. Резервное копирование данных.
24. Режимы восприятия информации.
25. Средства автоматизации информационно-аналитической работы.
26. Создание информационно-аналитических СБ (ИА СБ).
27. Составные части ИА СБ.
28. Стадии и технология создания ИА СБ.
29. Задачи аутентификации, понятие протокола аутентификации.
30. Основные схемы протоколов аутентификации.
31. Основные принципы построения систем защиты от НСД.
32. Классификация уровней защиты от НСД.
33. Программно-аппаратный состав средств защиты от НСД.
34. Аппаратные устройства для разграничения доступа в сети.
35. Разграничение доступа к ресурсам.
32. Задачи и определения информационно-аналитического (ИА) обеспечения СБ.
33. Организационные формы субъектов ИА работы.
34. Системы, управляемые потоком событий.
35. Поиск, отбор и анализ данных.
36. Неструктурированные текстовые данные.
37. Структурированные текстовые данные.
38. Резервное копирование данных.
39. Режимы восприятия информации.
40. Средства автоматизации информационно-аналитической работы.



41. Создание информационно-аналитических СБ (ИА СБ).
42. Составные части ИА СБ.
43. Стадии и технология создания ИА СБ.
44. Задачи аутентификации, понятие протокола аутентификации.
45. Основные схемы протоколов аутентификации.
46. Основные принципы построения систем защиты от НСД.
47. Классификация уровней защиты от НСД.
48. Программно-аппаратный состав средств защиты от НСД.
38. Аппаратные устройства для разграничения доступа в сети.
39. Разграничение доступа к ресурсам.
40. Роль и место анализа в процессе принятия решения.
41. Этапы аналитического исследования.
42. Классификация источников и методов сбора (получения) информации.
43. Методы анализа и прогнозирования как объект автоматизации.
44. Требования, предъявляемые к информационно-аналитическим системам.
45. Планирование разведывательной деятельности.
46. Модель конкурентной среды М. Портера.
47. Методика сбора информации о юридическом лице.
48. Методика сбора информации о физическом лице.
49. Система конкурентной разведки на предприятии.
50. Основные методы противодействия промышленному шпионажу.
51. Планирование и организация контрразведывательной деятельности.
52. Агенты влияния.
53. Классификация внутренних нарушителей (инсайдеров) и методы борьбы с ними.
54. Принципы работы систем анализа защищенности. Требования к системам.
55. Отечественный рынок информационно-аналитических систем.
56. Подходы к выполнению анализа средствами информационных технологий.
57. Составные части информационно-аналитических систем безопасности.
58. Управление информационно-аналитическими системами безопасности.
59. Интеллектуальный анализ данных
60. Что является исходными данными для проведения оценки и анализа угроз безопасности объектов?

## 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 3

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 работа		40
Общий итог за семестр		100

## 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. Информационно-аналитические системы безопасности объектов [Текст] : учебное пособие для магистров высших учебных заведений, обучающихся по направлению подготовки 10.04.01 Информационная безопасность / [Шелехова О.Г.] ; ДОННУ. – Донецк : Цифровая типография, 2019. – 125 с.

2. Лабораторный практикум по информационно-аналитическим системам безопасности объектов: учебно-методическое пособие [Текст] : учебно-методическое пособие для магистров высших учебных заведений, обучающихся по направлению подготовки 10.04.01 Информационная безопасность / [Шелехова О.Г.] ; ДОННУ. – Донецк : Цифровая типография, 2019. – 83 с.

## 12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

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