

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**  
**«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»**

|   |                                      |
|---|--------------------------------------|
| 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 «Управление информационной безопасностью» 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.

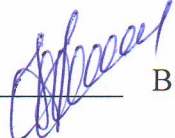
Разработчик:

Доцент  
кафедры радиопизики  
и инфокоммуникационных технологий

  
И.А. Третьяков

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

Заведующий кафедрой


  
В.В. Данилов

СОГЛАСОВАНО:

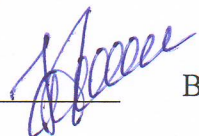
И.о. декана физико-технического факультета  
28.03.2024 г.

  
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:

Дисциплины программы бакалавриата: «Основы управления информационной безопасностью», «Информационные технологии», «Защищенные информационные системы», «Информационно-аналитические системы безопасности», «Модели и методы безопасного информационного обмена».

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

«Технологии обеспечения информационной безопасности объектов», «Информационно-аналитические системы безопасности», «Производственная практика: проектно-технологическая», «Производственная практика: преддипломная», «Подготовка к процедуре защиты и защита выпускной квалификационной работы»

## 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.М2.1 Управление информационной безопасностью  |
| Часть образовательной программы                 | Базовая 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

Знакомство студентов с методами, программными и аппаратными средствами и мерами обеспечения информационной безопасности информационных автоматизированных систем.

Формирование у студентов навыков применения современных методов, программных и аппаратных средств и программных средств, и мер обеспечения информационной безопасности, имеющих распространение в мировой инженерно-технической практике.

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

### 4.1. Компетенции

| Компетенции   | Индикаторы  | Результаты обучения   |
|---|---|---|
| ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание. | ОПК-1.1. Способен использовать методы и средства управления рисками автоматизированных информационных систем. | ОПК-1.1.1. Знает методы управления рисками автоматизированных информационных систем.<br>ОПК-1.1.2. Умеет использовать средства управления рисками автоматизированных информационных систем на объекте защиты.<br>ОПК-1.1.3. Владеет современными методами и средствами управления рисками автоматизированных информационных систем. |
| ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.                          | ОПК-3.1. Способен применять основные принципы анализа информационных рисков организации.                      | ОПК-3.1.1. Знает методы, принципы и технологии управления информационными рисками.<br>ОПК-3.1.2. Умеет анализировать информационные риски организации.<br>ОПК-3.1.3. Владеет современными методами и технологиями управления информационными рисками организации.   |

## 5. ПРОГРАММА ДИСЦИПЛИНЫ

| Название темы   | Краткое содержание темы (вопросы темы)   |
|---|--|
| Тема 1. Введение в методы и технологии управления информационными рисками                                     | 1.1. Задача управления информационными рисками<br>1.2. Международные методики управления рисками<br>1.3. Оценка рисков автоматизированной информационной системы посредством методики анализа и контроля рисков  |
| Тема 2. Основные принципы анализа информационных рисков организации   | 2.1. Задача анализа информационных рисков<br>2.2. Методы анализа информационных рисков и примеры их применения<br>2.3. Методика анализа рисков компании Microsoft  |
| Тема 3. Современные методы и средства управления рисками автоматизированных информационных систем организаций | 3.1. Необходимость анализа и контроля информационных рисков организации<br>3.2. Методика Facilitated Risk Analysis Process<br>3.3. Методика Operationally Critical Threat, Asset, and Vulnerability Evaluation<br>3.4. Методика компании RiskWatch   |
| Тема 4. Правовые меры обеспечения информационной безопасности организации                                     | 4.1. Классификация направлений защиты информации<br>4.2. Законодательная база обеспечения информационной безопасности организации<br>4.3. Нормативно-правовые акты организации по информационной безопасности<br>4.4. Формы правовой защиты информации организации<br>4.5. Внутренняя документация организации для обеспечения информационной безопасности |
| Тема 5. Организационные меры обеспечения  | 5.1. Основные определения организационной защиты<br>5.2. Особенности организационной защиты автоматизированных информационных систем и сетей   |

|   |  |
|---|--|
| безопасности автоматизированных информационных систем   | 5.3. Организационные мероприятия по защите информации в АИС<br>5.4. Структурные подразделения по защите информации организации   |
| Тема 6. Программно-аппаратные меры и средства обеспечения безопасности автоматизированных информационных систем | 6.1. Основные программно-аппаратные меры и средства. Их задачи<br>6.2. Идентификация и аутентификация<br>6.3. Управление доступом<br>6.4. Протоколирование и аудит<br>6.5. Криптографические средства  |
| Тема 7. Управление информационной безопасностью на государственном уровне                                       | 7.1. Введение в управление государственной безопасностью<br>7.2. Необходимость государственного управления в сфере информационной безопасности<br>7.3. Обеспечение информационной безопасности на уровне государства<br>7.4. Доктрина информационной безопасности Российской Федерации<br>7.5. Структура и полномочия органов государственной власти, обеспечивающих информационную безопасность<br>7.6. Государственная граница и ее безопасность |

## 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 |
| Тема 1. Введение в методы и технологии управления информационными рисками                                       | 2                | 0      | -      | 6     | 8     |
| Тема 2. Основные принципы анализа информационных рисков организации   | 2                | 0      | -      | 6     | 8     |
| Тема 3. Современные методы и средства управления рисками автоматизированных информационных систем организаций   | 2                | 8      | -      | 2     | 12    |
| Тема 4. Правовые меры обеспечения информационной безопасности организации                                       | 2                | 6      | -      | 4     | 12    |
| Тема 5. Организационные меры обеспечения безопасности автоматизированных информационных систем                  | 2                | 8      | -      | 2     | 12    |
| Тема 6. Программно-аппаратные меры и средства обеспечения безопасности автоматизированных информационных систем | 2                | 8      | -      | 2     | 12    |
| Тема 7. Управление информационной безопасностью на государственном уровне                                       | 3                | 0      | -      | 5     | 8     |
| 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 |
| Тема 1. Введение в методы и технологии управления информационными рисками                                       | 0,5              | 0      | -      | 7,5   | 8     |
| Тема 2. Основные принципы анализа информационных рисков организации   | 0,5              | 0      | -      | 7,5   | 8     |
| Тема 3. Современные методы и средства управления рисками автоматизированных информационных систем организаций   | 0,5              | 2      | -      | 9,5   | 12    |
| Тема 4. Правовые меры обеспечения информационной безопасности организации                                       | 0,5              | 2      | -      | 9,5   | 12    |
| Тема 5. Организационные меры обеспечения безопасности автоматизированных информационных систем                  | 0,5              | 2      | -      | 9,5   | 12    |
| Тема 6. Программно-аппаратные меры и средства обеспечения безопасности автоматизированных информационных систем | 0,5              | 2      | -      | 9,5   | 12    |
| Тема 7. Управление информационной безопасностью на государственном уровне                                       | 1                | 0      | -      | 7     | 8     |
| ИТОГО ПО КОМПОНЕНТУ ОПОП  | 4                | 8      | -      | 60    | 72    |

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

## 7.1. Контрольные вопросы

1. Какая основная задача управления информационными рисками?
2. Что подразумевает эффективное управление информационными рисками?
3. Качественные методики управления рисками.
4. Количественные методики управления рисками.
5. Основные этапы управления рисками АИС.
6. Что такое контрмеры?
7. Какая основная задача анализа информационных рисков?
8. Какие основные этапы анализа информационных рисков?
9. Какой результат анализа информационных рисков?
10. Перечислите и современные методы анализа рисков.
11. Охарактеризуйте современные методы анализа рисков.
12. Необходимость анализа и контроля информационных рисков организации.
13. Какие основные этапы управления рисками АИС?
14. Назовите основные этапы оценки рисков по методике FRAP.
15. Назовите основные этапы оценки рисков по методике OCTAVE.
16. Назовите основные этапы оценки рисков по методике RiskWatch.
17. Назовите основные направления защиты информации.
18. Какие основные законы в области информационной безопасности?
19. Назовите основные нормативно-правовые акты в области ИБ организации.
20. Перечислите основные формы правовой защиты информации организации.
21. Примеры внутренних документов организации, обеспечивающих ИБ.
22. Что такое организационная защита?



23. Перечислите основные организационные мероприятия по обеспечению ИБ.
24. Назовите нормативные документы, регламентирующие организационные мероприятия по защите информации в АИС.
25. Какие бывают организационные мероприятия по защите информации?
26. Цели и задачи структурных подразделений организации, обеспечивающих безопасность информации.
27. Перечислите современные сервисы безопасности.
28. Какие основные задачи сервисов информационной безопасности?
29. Определения идентификация и аутентификация.
30. Определения протоколирование и аудит.
31. Что включают в себя криптографические сервисы безопасности?
32. Какие документы составляют правовую основу государственной безопасности РФ?
33. Обоснуйте необходимость государственного управления в сфере ИБ.
34. Основные положения Доктрины информационной безопасности РФ.
35. Перечислите государственные органы, обеспечивающих ИБ в РФ.
36. Организация безопасности государственной границы.

## 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

| Номера разделов       | Виды работ                                | Максимальное количество баллов |
|-----------------------|---|--------------------------------|
| 1                     | Организационно-учебная работа в аудитории | 5                              |
|                       | Самостоятельная работа                    | 5                              |
|                       | Лабораторные работы                       | 20                             |
|                       | Модульная контрольная работа              | 20                             |
| ИТОГО                 |   | 50                             |
| Зачет                 |   | 50                             |
| 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 и лабораторных 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 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.405).

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. Третьяков, И. А. Управление информационной безопасностью: методы, средства и меры обеспечения безопасности автоматизированных информационных систем / И. А. Третьяков. – Донецк: ДонНУ, 2023. – 131 с.

### 11.2. Дополнительная литература

2. Шаньгин, В. Ш. Защита информации в компьютерных системах и сетях / В. Ш. Шаньгин. – М.: Изд-во ЛитРес, 2022. – 592 с.

3. Защита информации в компьютерных системах / под ред. д-ра экон. наук Е. В. Стельмашенок, канд. физ.-мат. наук И. Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2017. – 163 с.

4. Краковский, Ю. М. Защита информации: учебное пособие / Ю. М. Краковский. – Изд-во Феникс, 2017. – 348 с.

5. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с.

6. Правовые основы информационной безопасности: учебное пособие / Сост. Т.З. Зульфугарзаде. – М.: ГОУ ВПО «РЭУ им. Г.В. Плеханова», 2010. – 79 с

## 12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. – Москва, 2019- . – URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный, подписка. Необходима установка программного обеспечения. – Текст: электронный.

2. **eLIBRARY.RU:** научная электронная библиотека: сайт. – Москва, 2000- . – URL: <https://elibrary.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. –Текст: электронный.

3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/>. – Режим доступа: свободный. – Текст: электронный.

4. Электронно-библиотечная система **«Лань»:** [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

5. **ЭБС Юрайт:** электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

6. **Электронно-библиотечная система ДонГУ**: сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный. – Текст: электронный.

7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: 01.09.2023). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.

8. **Электронный архив ДонГУ**: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный.

### 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).