

Донецк 2024

Рабочая программа дисциплины «Основы управления информационной безопасностью» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 (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:

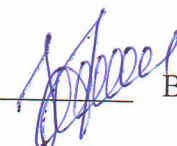
Доцент  
кафедры радиофизики  
и инфокоммуникационных технологий



И.А. Третьяков

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

Заведующий кафедрой



В.В. Данилов

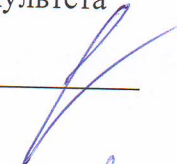
СОГЛАСОВАНО:

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

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

Дисциплины программы бакалавриата: «Организационное и правовое обеспечение информационной безопасности», «Информационные технологии», «Основы информационной безопасности», «Модели и методы безопасного информационного обмена».

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

«Производственная практика: преддипломная», «Подготовка к процедуре защиты и защита выпускной квалификационной работы», дисциплина программы магистратуры «Управление информационной безопасностью»

## 2. ОПИСАНИЕ ДИСЦИПЛИНЫ

### 2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.03.01 Информационная безопасность (Программа бакалавриата: 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем))
Шифр и название в соответствии с учебным планом	Б1.Б.М3.7 Основы управления информационной безопасностью
Часть образовательной программы	Базовая часть
Количество зачетных единиц / всего часов	4,5 / 162

### 2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	Форма контроля
Очная	4	8	30	40	-	92	162	экзамен

## 3. ЦЕЛИ ДИСЦИПЛИНЫ

Знакомство студентов с основными понятиями и определениями в управлении информационной безопасностью, теоретическими аспектами в области угроз информационной безопасности.

Формирование у студентов навыков применения современных методов и моделей оценки рисков информационной безопасности организации, стандартов оценки и управления информационной безопасностью, а также внедрения автоматизированных информационных систем управления информационной безопасностью.

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

### 4.1. Компетенции

Компетенции	Индикаторы	Результаты обучения
-------------	------------	---------------------

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	ОПК-10.1. Способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности.	ОПК-10.1.1. Знает структуру системы политик, процессов и стандартов, обеспечивающих информационную безопасность на объекте защиты. ОПК-10.1.2. Умеет разрабатывать проекты политики информационной безопасности. ОПК-10.1.3. Владеет современными комплексами мер обеспечения информационной безопасности.
ОПК-14. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах.	ОПК-14.1. Знает принципы организации мероприятий по обеспечению безопасности информации в автоматизированных системах.	ОПК-14.1.1. Знает методы и технологии обеспечения информационной безопасности. ОПК-14.1.2. Умеет применять современные методы и технологии защиты информации в автоматизированных информационных системах. ОПК-14.1.3. Владеет современными методами и технологиями организации обеспечения информационной безопасности.

## 5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Тема 1. Введение в управление информационной безопасностью	1.1. Процесс управления информационной безопасностью 1.2. Политика информационной безопасности 1.3. Система управления информационной безопасностью
Тема 2. Основные понятия информационной безопасности	2.1. Понятия: информация, информационная безопасность 2.2. Понятия: объект и предмет защиты, информационная система 2.3. Задачи и основные компоненты информационной безопасности 2.4. Понятия: обеспечение и управление информационной безопасностью 2.5. Важность проблемы информационной безопасности
Тема 3. Угрозы информационной безопасности	3.1. Основные определения. Классификации угроз 3.2. Основные угрозы конфиденциальности 3.3. Основные угрозы целостности 3.4. Основные угрозы доступности 3.5. Вредоносные программы
Тема 4. Стандарты оценки в информационной безопасности	4.1. Функция стандартов в информационной безопасности 4.2. Стандарт «Критерии оценки доверенных компьютерных систем» 4.3. Стандарт «Общие критерии»

Тема 5. Стандарты управления информационной безопасностью	5.1. Стандарт «Практические правила управления информационной безопасностью» 5.2. Стандарт «Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» 5.3. Сертификация СУИБ на соответствие стандарту 27001
Тема 6. Внедрение системы управления информационной безопасностью в организацию	6.1. Этапы разработки системы управления информационной безопасностью 6.2. Инвентаризация активов организации 6.3. Категорирование активов организации 6.4. Оценка защищенности информационной системы организации 6.5. Оценка и обработка информационных рисков 6.6. Внедрение мер обработки рисков и контроль их эффективности
Тема 7. Методы оценки рисков информационной безопасности организации	7.1. Основные понятия управления рисками 7.2. Метод оценки рисков на основе модели информационных потоков 7.3. Расчет риска информационной безопасности на основе модели информационных потоков 7.4. Метод оценки рисков на основе модели угроз и уязвимостей 7.5. Расчет риска информационной безопасности на основе модели угроз и уязвимостей

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 6.1. Форма обучения – очная, курс – 4, семестр – 8

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Тема 1. Введение в управление информационной безопасностью	4	0	-	16	20
Тема 2. Основные понятия информационной безопасности	4	0	-	16	20
Тема 3. Угрозы информационной безопасности	4	0	-	16	20
Тема 4. Стандарты оценки в информационной безопасности	3	10	-	6	19
Тема 5. Стандарты управления информационной безопасностью	3	10	-	6	19
Тема 6. Внедрение системы управления информационной безопасностью в организацию	6	10	-	16	32
Тема 7. Методы оценки рисков информационной безопасности организации	6	10	-	16	32
ИТОГО ПО КОМПОНЕНТУ ОПОП	30	40	-	92	162

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

- 7.1. Контрольные вопросы
  1. Определение «управление информационной безопасностью».
  2. Какова цель управления ИБ?
  3. Какие условия обеспечения ИБ?
  4. Что включает в себя процесс управления ИБ?
  5. Что включает в себя политика ИБ?
  6. Что такое система управления информационной безопасностью?
  7. Примеры метрик производительности процесса управления ИБ?
  8. Понятие «информация» в контексте управления информационной безопасностью.
  9. Термины: защита информации, объект и предмет защиты информации.
  10. Что такое информационная система?
  11. Понятие «информационная система» в контексте управления информационной безопасностью.
  12. Назовите основные задачи информационной безопасности.
  13. Определения основных компонентов ИБ.
  14. Понятие «обеспечение информационной безопасности» в контексте управления информационной безопасностью.
  15. Понятие «угроза» и «уязвимость» в контексте информационной безопасности.
  16. Что такое вероятность и критичность реализации угрозы?
  17. Приведите примеры распространенных угроз современных ИС.
  18. Приведите примеры угроз конфиденциальности.
  19. Приведите примеры угроз целостности.
  20. Приведите примеры угроз доступности.
  21. Приведите классификацию современных вредоносных программ.
  22. Что такое стандарт?
  23. Причины применения стандартизации в области ИБ?
  24. Приведите классификацию стандартов в области ИБ.
  25. Основная идея стандарта «Оранжевая книга».
  26. Основная идея стандарта «Общие критерии».
  27. Назовите основные отличия вышеуказанных стандартов.
  28. Какие задачи разработки стандартов управления информационной безопасностью?
  29. Основная идея Стандарта ISO/IEC 17799.
  30. Основная идея Стандарта ISO/IEC 27001:2005.
  31. Различия стандартов ISO/IEC 17799 и ISO/IEC 27001:2005.
  32. Что подразумевает сертификация системы управления информационной безопасностью?
  33. Какие преимущества внедрения СУИБ по требованиям стандартов?
  34. Какие преимущества внедрения СУИБ?
  35. Назовите основные этапы разработки СУИБ.
  36. В чем заключаются процессы инвентаризации и категорирования активов?
  37. В чем заключается процесс оценки защищенности ИС?
  38. В чем заключается оценка и обработка информационных рисков?
  39. Опишите процесс внедрения и контроля мер обработки рисков.
  40. В чем состоит суть мероприятий по управлению рисками?
  41. Как количественно определяется уровень риска?
  42. Назовите основные этапы процесса управления рисками.

43. Опишите метод оценки рисков на основе модели информационных потоков.
44. Опишите метод оценки рисков на основе модели угроз и уязвимостей.
45. Что такое контрмеры?

7.2. Образец содержания экзаменационного билета (при наличии экзамена по дисциплине)

В случае ведения учебного процесса с использованием электронного обучения и дистанционных образовательных технологий, содержание билета может отличаться от приведенного.

### ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Донецкий государственный университет

Физико-технический факультет

Кафедра радиофизики и инфокоммуникационных технологий

Программа высшего образования	Программа бакалавриата
Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Форма обучения	Очная
Семестр	Восьмой
Дисциплина	Основы управления информационной безопасностью

#### Экзаменационный билет № 1

1. Термины: защита информации, объект и предмет защиты информации.
2. Стандарт ISO/IEC 17799
3. Внедрение системы управления информационной безопасностью.

Утверждено на заседании кафедры радиофизики и инфокоммуникационных технологий,  
протокол № \_\_ от \_\_.\_\_.202\_\_ г.

Заведующий кафедрой

В.В. Данилов

Экзаменатор

И.А. Третьяков

#### 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 8

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
Экзамен	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 автоматизированных информационных систем: основные понятия и определения / И. А. Третьяков. – Донецк: ДонНУ, 2022. – 120 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).