

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

*Машаров*

П.А. Машаров

«29» марта 2024 г.

МП

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Увеличенная группа направлений подготовки	10.00.00 Информационная безопасность
Программа высшего образования	Программа бакалавриат
Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Квалификация	Бакалавр
Форма обучения	очная

Рабочая программа адаптирована для лиц  
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «**Основы информационной безопасности**» 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 радиопизики  
и инфокоммуникационных технологий

 М.В. Бабичева

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

Заведующий кафедрой

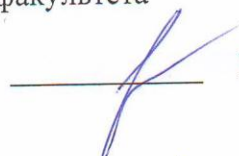
 В.В. Данилов

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:

Информатика, Информационные технологии, Технологии и методы программирования, Языки программирования, Теория информации, Архитектура компьютерных систем, Пакеты прикладных программ для обработки изображений, Модели и методы безопасного информационного обмена.

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

Web-программирование, Программно-аппаратные средства защиты информации, Методы и средства криптографической защиты информации.

Используются при написании выпускной квалификационной работы, Производственная практика: научно-исследовательская работа (обязательная). Производственная практика: преддипломная практика (обязательная).

## 2. ОПИСАНИЕ ДИСЦИПЛИНЫ

### 2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.03.01 Информационная безопасность (Программа бакалавриата Информационная безопасность)
Шифр и название в соответствии с учебным планом	Б1.Б.М3.6 Основы информационной безопасности
Часть образовательной программы	Базовая часть (Профессионально-ориентированный блок)
Количество зачетных единиц / всего часов	3 / 108

### 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	4	30	30	-	48	108	зачет

## 3. ЦЕЛИ ДИСЦИПЛИНЫ

Знакомство с понятиями национальной безопасности; видами безопасности; ИБ в системе национальной безопасности; основными понятиями, общеметодологическими принципами теории ИБ; анализом угроз ИБ, проблемами информационной войны; государственной информационной политикой; видами информации; методами и средствами обеспечения ИБ; методами нарушения конфиденциальности, целостности и доступности информации; причинами, видами, каналами утечки и искажения информации.

## 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 оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 Умеет применять современные информационные технологии для сбора, передачи, обработки и накопления информации	Знает методы обработки информации с использованием современных технических средств коммуникации и связи Умеет использовать современные информационно-коммуникационные технологии для решения задач информационной безопасности
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1 Выбирает нормативные и правовые акты, методические документы и использует в профессиональной деятельности	Знает и умеет применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 Способен применять современные технологии для защиты информации в соответствии с соответствующими нормативными документами	Знает о необходимости защиты совокупности объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации. Умеет применять современные программные средства системного и прикладного назначения отечественного и российского производства

## 5. ПРОГРАММА ДИСЦИПЛИНЫ

Темы	Вопросы темы
1. Основные понятия Программа дисциплины и составляющие информационно й безопасности.	1. Основные понятия информационной безопасности. 2. Правовые основы ИБ и законодательство ДНР об информации. 3. Информация, информационная система, владелец информации. 4. Виды информации. Конфиденциальная информация, государственная тайна. 5. Нормативные документы РФ по ИБ. 6. Конфиденциальность, целостность, доступность.
2. Структура файлов и hex-редактор.	1. Понятие файла. 2. Hex-редактор, структура и предназначение. 3. Форматы файлов. 4. Структура некоторых текстовых и графических файлов. 5. Сигнатуры файлов. 6. Определение формата файла в различных ОС.

3. Криптография и криптоанализ.	<ol style="list-style-type: none"> <li>1. Историческая справка, примитивные шифры. Шифр хог, Цезаря, Винежера.</li> <li>2. Симметричные и ассиметричные криптосистемы.</li> <li>3. Суть ассиметричного шифрования.</li> <li>4. Алгоритм RSA и Эль-Гамала.</li> <li>5. Симметричное шифрование. Гаммирование. AES.</li> <li>6. Квантовая криптография.</li> </ol>
4. Хеш-функции.	<ol style="list-style-type: none"> <li>1. Понятие хеш-функции.</li> <li>2. Криптографические и не криптографические хеш-функции.</li> <li>3. Свойства хеш-функции.</li> <li>4. CRC –суммы.</li> <li>5. Хеш-функции MD5 и SHA1.</li> <li>6. Коллизии хеш-функций.</li> <li>7. Криптоанализ хеш-функций.</li> </ol>
5. Аутентификация по паролю	<ol style="list-style-type: none"> <li>1. Авторизация, аутентификация и идентификация.</li> <li>2. Системы аутентификации.</li> <li>3. Парольная защита.</li> <li>4. Уязвимости парольной защиты.</li> <li>5. Методы хранения пароля.</li> <li>6. Определение криптостойкости пароля. Формула Шеннона.</li> <li>7. Метода взлома пароля.</li> <li>8. Программы для взлома пароля.</li> <li>9. Организация безопасной парольной защиты.</li> </ol>
6. Другие методы аутентификации	<ol style="list-style-type: none"> <li>1. Электронные методы аутентификации.</li> <li>2. Аппаратная аутентификация.</li> <li>3. Биометрические методы аутентификации.</li> <li>4. Аутентификация по отпечатку пальца, аутентификация по лицу.</li> <li>5. Распространенность методов аутентификации.</li> <li>6. Уязвимости биометрической аутентификации.</li> <li>7. Федеральная аутентификация.</li> </ol>
7. Вирусы	<ol style="list-style-type: none"> <li>1. История создания вирусов.</li> <li>2. Классификация вирусов.</li> <li>3. Загрузочные, файловые, макросы, скрипт-вирусы.</li> <li>4. Вирусы для Linux, Android, iOSm</li> <li>5. Трояны, черви, собственно вирусы.</li> <li>6. Хакеры.</li> </ol>
8. Антивирусы	<ol style="list-style-type: none"> <li>1. Принцип работы антивирусных программ.</li> <li>2. Сигнатуры вирусов.</li> <li>3. Возможности антивирусного ПО. Написание антивирусной программы.</li> <li>4. Платные и бесплатные антивирусы.</li> <li>5. Международные рейтинги антивирусных программ.</li> <li>6. Обзор наиболее популярных антивирусных программ.</li> </ol>
9. Web-безопасность.	<ol style="list-style-type: none"> <li>1. Основные понятия web. HTML, CSS и JS.</li> <li>2. Цели злоумышленников, атакующих сайты.</li> <li>3. Куки и их роль в безопасности сайтов.</li> <li>4. Атаки на сайты. XSS, CSRF, SQL-инъекции и методы защиты от них.</li> <li>5. Программы для анализа сайтов на уязвимости.</li> <li>6. Уязвимости методов аутентификации.</li> <li>7. Уязвимости прикладного уровня.</li> </ol>
10. Защита информации в	<ol style="list-style-type: none"> <li>1. Уязвимости компьютерных сетей.</li> <li>2. Основные виды атак при передаче информации.</li> </ol>

компьютерных сетях.	3. Снифферы. 4. Ответвления трафика. 5. Анализ электромагнитных излучений. 6. Атаки на канальном и сетевом уровне. 7. Спуфинг. 8. Виды сканирования. DOS и DDOS атаки. 9. Подмена IP адреса. 10. Меры противодействия атакам. 11. Виртуальные сети.
11. Техническая защита информации	1. Каналы утечки информации. 2. Радиозакладки. Пассивные, активные и полуактивные РЗ. 3. Детектирование радиозакладок. 4. Нелинейные локаторы. 5. Акустические и лазерные микрофоны. 6. Утечка по виброканалу. 7. Стетоскопы. 8. Генераторы шума, скремблеры, постановщики помех. IP шифраторы и токены. 9. Электронные замки.
12. Защита документов	1. Методы подделки документов. 2. Методы подделки цифровых документов. 3. Методы определения подлинности документов. 4. Получение дополнительной информации из EXIF. 5. Методы ELA и PCA и их ограничения. 6. Методы защиты документов.
13. Электронно-цифровая подпись	1. Понятие электронно-цифровой подписи. 2. История развития ЭЦП. 3. Основные схемы ЭЦП. 4. Построение ЭЦП. 5. Протокол подписания документа. 6. Центры сертификации. 7. Удостоверяющие центры. 8. Криптостойкость схем ЭЦП.
14. Методы стеганографии.	1. Стеганография, как средство защиты файлов. 2. Цифровые водяные знаки. 3. Слияние файлов, LSB. 4. Соккрытие информации в аудио и видео файлах. 5. Методы обнаружения скрытых сообщений.
15. Социальная инженерия.	1. История развития социальной инженерии. 2. Человек, как самое уязвимое звено любой системы. 3. Психологические основы социальной инженерии. 4. Методы социальной инженерии.

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 6.1. Форма обучения – очная, курс – 2, семестр – 4

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор	Практ.	СРС+К	Всего
Основные понятия и составляющие информационной безопасности.	2	2		4	8
Структура файлов и hex-редактор.	2	2		4	8



Криптография и криптоанализ.	2	2		4	8
Хеш-функции.	2	2		4	8
Аутентификация по паролю	2	2		4	8
Другие методы аутентификации	2	2		4	8
Вирусы	2	2		4	8
Антивирусы	2	2		4	8
Web- безопасность.	2	2		4	8
Защита информации в компьютерных сетях.	2	2		4	8
Техническая защита информации	2	2		4	8
Защита документов	2	2		5	9
Электронно-цифровая подпись	2	2		5	9
Методы стеганографии.	2	2		4,8	8,8
Социальная инженерия.	2	2		4,2	8,2
ИТОГО ЗА СЕМЕСТР / ЗА КУРС / ПО КОМПОНЕНТУ ОПОП	30	30		60,2+2,8	<b>108</b>
ИТОГО ПО КОМПОНЕНТУ ОПОП	30	30		63	<b>108</b>

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

### 7.1. Контрольные вопросы

1. Что такое информация? Свойства информации. Информационные технологии.
2. Составляющие информационной безопасности.
3. Правовые основы защиты информации.
4. Информация с точки зрения возможности ее распространения.
5. Какая информация относится к конфиденциальной?
6. Какая информация относится к государственной тайне?
7. Три категории стандартной модели безопасности.
8. Уровни защиты информации.
9. Что такое криптография и криптоанализ?
10. Шифр Цезаря и частотный анализ.
11. Шифр хог.
12. Симметричные и асимметричные криптосистемы.
13. Симметричные шифры. Примеры.
14. Симметричные шифры. Достоинства и недостатки.
15. Принцип ассиметричного шифрования.
16. Асимметричные шифры. Примеры.
17. Асимметричные шифры. Достоинства и недостатки.
18. Квантовая криптография.
19. Два основных алгоритма квантовой криптографии.
20. Что такое авторизация, аутентификация и идентификация? Что такое хэш и зачем он нужен?
21. Какие хеш-функции вы знаете?
22. Для чего используются хеш-функции?
23. Чем отличаются криптографические хеш-функции от некриптографических?
24. Что такое коллизия хеш-функции?
25. Что такое парадокс дней рождения и как он связан со взломом хешей?
26. Методы взлома хеш-функций.
27. Что такое «радужные таблицы»?
28. Какие виды паролей существуют?
29. Что такое динамические пароли?

30. Аппаратная и программная защита флешки.
31. Программы для защиты паролем папок, файлов и носителей информации.
32. Что такое «правильный пароль» и как его запомнить?
33. Методы взлома паролей.
34. Что такое «радужные таблицы»?
35. Системы аутентификации и идентификации. Классификация.
36. Используемый фактор аутентификации. Приоритет использования. Степень автоматизации.
37. Недостатки парольной аутентификации.
38. Аппаратная аутентификация, ее виды, достоинства и недостатки.
39. Биометрическая аутентификация.
40. Достоинства и недостатки аутентификации по отпечаткам пальцев.
41. Аутентификация по геометрии лица 2 вида.
42. Аутентификация по голосу.
43. Биометрические технологии будущего.
44. Распространенность методов биометрической аутентификации.

## 7.2. ВАРИАНТЫ ИНДИВИДУАЛЬНЫХ ЗАДАНИЙ

1. История криптографии.
2. Современная криптография
3. Квантовая криптография
4. Атаки на сайты.
4. XSS -атаки.
5. SQL-атаки.
6. Методы взлома wi-fi.
7. Современная стеганография.
8. Поисковик Shodan.
9. Форензика.
10. Стеганография.
11. Google Hacking
12. DOS и DDOS атаки.
13. Honey Pots.
14. Аутентификация на сайтах.
15. Куки.
16. Хакеры. Субкультура хакеров.
17. Боты. Угрозы, исходящие от ботов.
18. Системы аутентификации.
19. Электронно-цифровая подпись.
20. Фишинговые сайты.
21. Вирусные атаки.
22. Прослушивающие устройства.
23. Скремблеры.
24. Направленные микрофоны.
25. Спуфинг.
26. Эвристический анализ для антивирусов.
27. Сниферы.
28. Охранные системы.
29. Видеонаблюдение.
30. Безопасность интернета вещей.
31. Методы криптоанализа.
32. Кейлогеры.



33. Методы социальной инженерии.
34. Антивирусные программы. Есть ли смысл?
35. Взлом мобильных телефонов.
36. Применение нейронных сетей в информационной безопасности.

## 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.).

Номера разделов	Виды работ	Максимальное количество баллов
тема 1-17	Текущий контроль	10
	Индивидуальное задание	10
	Лабораторные работы	60
ИТОГО		80
зачет		20
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 практических 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 лаборатория, оснащенная компьютерами с установленным специальным программным обеспечением, указанным в пункте 13.

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. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов по специальности "Компьютерная безопасность и др. / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. – М. : Радио и связь, 2000. - 192 с

2. Корт, С. С. Теоретические основы защиты информации : Учеб. пособие для студентов вузов, обучающихся по группе спец. в обл. информ. безопасности / С. С. Корт. - М. : Гелиос АРВ, 2004. – 233 с.

3. Защита программного обеспечения / [Д. Гроувер, Р. Сатер, Дж. Фипс и др.] ; под ред. Д. Гроувера ; пер. с англ. В. Г. Потемкина и др. ; под ред. В. Г. Потемкина. – Москва : Мир, 1992. - 286 с.

4. Завгородний, В. И. Комплексная защита информации в компьютерных системах : Учеб. пособие для студентов вузов / В. И. Завгородний. – М. : Логос, 2001. - 264 с.

### 11.2. Дополнительная литература

5. Рассел, Ч. Microsoft Windows Server 2008 : справочник администратора / Ч. Рассел, Ш. Кроуфорд. – Москва : ЭКОМ Паблишерз, 2009. - 1321 с

6. Программно-аппаратные средства обеспечения информационной безопасности: Защита программ. и данных / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – М.: Радио и связь, 2000. - 169 с

7. Безопасность компьютерных сетей на основе Windows NT / В. С. Люцарев, К. В. Ермаков, Е. Б. Рудный, И. В. Ермаков. - М.: Рус. ред. TOO Channel Trading, 1998. – 304 с. + Электр. оптич. диск (CD-ROM).

## 12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Интернет-Основы информационной безопасности . – URL: <http://www.intergu.ru/>  
 2. Сеть начинающих программистов. – URL: <http://www.it-n.ru/>  
 3. Классификация механизмов аутентификации пользователей и их обзор . – URL: <https://habr.com/ru/post/177551/>

4. SQL инъекции. Проверка, взлом, защита . – URL: <https://habr.com/ru/post/130826/>

5. XSS глазами злоумышленника. – URL: <https://habr.com/ru/post/66057/>

6. Stealthphone: Защита микрофона мобильного телефона от несанкционированного включения . – URL: <https://habr.com/ru/company/ancort/blog/160215/>

7. Основные параметры передатчиков и приемников . – URL: <https://radiokot.ru/start/analog/bugs/02/>

8. 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: 01.01.2023). – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

9. Электронный каталог Научной библиотеки Донецкого государственного университета. – Донецк : НБ ДонГУ, 1999– . – URL: <http://catalog.donnu.education> (дата обращения: 01.01.2023). – Текст : электронный;

10. Учебники и другие книги по математике URL: <http://eqworld.ipmnet.ru/ru/library/mathematics.htm> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный

11. Техническая библиотека URL: <http://techlibrary.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;

12. Научные журналы ФГБОУ ВО «ДонГУ» URL: <http://donnu.ru/science/journals> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный.

## 13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)

2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Яндекс Браузер (свободно распространяемое ПО)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения)
5. Kali Linux (свободно распространяемое ПО)
6. Stegsolve (свободно распространяемое ПО)