

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*  
«29» марта 2024 г.  
МП

П.А. Машаров

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**«АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ РАДИОМОНИТОРИНГА»**

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 «Автоматизированные системы радиомониторинга» 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:

Ст. преподаватель  
кафедры радиофизики  
и инфокоммуникационных технологий

 Я.И.Рущечников

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

Заведующий кафедрой

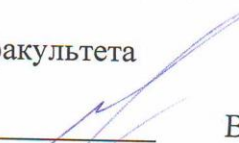
 В.В. Данилов

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: Защита информации в компьютерных сетях, Экспертные системы в информационной безопасности, Моделирование и системы принятия решений.

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

формирует навыки по проектированию и построению систем передачи голосовых данных в сетях общего пользования, а так же проектирование средств защиты этих данных, что необходимо для прохождения практик и подготовки 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.В.ДВ.4.1. Автоматизированные системы радиомониторинга
Часть образовательной программы	Вариативная часть: выбор обучающегося
Количество зачетных единиц / всего часов	4 / 144

### 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	17	34	-	93	144	экзамен
Очно-заочная, всего	2	4	5	10	-	129	144	экзамен

## 3. ЦЕЛИ ДИСЦИПЛИНЫ

Освоение терминологического и понятийного аппарата инженерной области автоматизированного радиомониторинга с целью решения перспективных задач и средств масштабирования и конвергенции средств РМ с использованием современных инфокоммуникационных технологий. Изучение современных специализированных средств и их возможностей для решения разнообразных задач радиомониторинга (РМ), особенностей РМ распространённых беспроводных протоколов связи, возможностей SDR систем, которые позволяют решать задачи РМ, возможностей и алгоритмов программного управления процессом РМ.

## 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. Разработка систем защиты информации автоматизированных систем	ПК-1.3. Разработка программно-аппаратных средств для систем защиты информации автоматизированных систем	<p>ПК-1.3.1. Знает основные принципы и задачи мероприятий по автоматизированному РМ, номенклатуру как специализированных, так и универсальных комплексов РМ, ландшафт угроз и типовые уязвимости беспроводных протоколов с систем связи, средства обеспечения и создания распределённых систем РМ.</p> <p>ПК-1.3.2. Умеет разрабатывать механизмы классификации радиосигнала, проводить аудит систем на соответствие критериям информационной безопасности, определять потенциальный ландшафт угроз, связанных с технологиями на конкретном объекте, осуществлять поиск нелегитимных источников радиосигнала.</p> <p>ПК-1.3.3. Владеет знаниями по работе с серверными реализациями операционных систем, методикой поиска побочных электромагнитных излучений, навыками работы с сертифицированными средствами анализа защищенности.</p>

## 5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Тема 1. Радиомониторинг и АРМ в современном мире.	<p>Что такое радиомониторинг.</p> <p>Задачи радиомониторинга.</p> <p>Предпосылки автоматизации радиомониторинга.</p> <p>Объекты радиомониторинга.</p> <p>Виды радиомониторинга.</p> <p>Длины волн и их особенности</p>
Тема 2. Современные средства автоматизированного радиомониторинга.	<p>Основные и дополнительные функции АСРМ.</p> <p>Классификационные характеристики АСРМ.</p> <p>Требования к средствам АСРМ (в том числе и по направлению ИБ).</p> <p>Семейства устройств АСРМ.</p> <p>Сертифицированные и доступные для покупки средства АСРМ.</p>
Тема 3. Стек технологий SDR.	<p>Идея и возникновение SDR.</p> <p>Архитектура SDR.</p> <p>Сферы применения SDR.</p> <p>Ограничения, достоинства и недостатки.</p> <p>SDR для специалиста по информационной безопасности.</p> <p>Перспективы развития SDR систем.</p>
Тема 4. Аппаратные платформы, реализующие концепцию SDR.	<p>Основные характеристики, и настраиваемые возможности, реализованные в SDR аппаратуре и ПО.</p> <p>RTL-SDR. SDRPlay. HackRF One.</p>

	Примеры программного обеспечения для простейших задач РМ с использованием SDR платформ. Ubertooth One.
Тема 5. Банки открытых данных радиочастот и технология web-sdr.	Получение сведений о локальных радиочастотах на конкретной территории. Глобальные базы данных вещающих устройств. Базы данных длинноволновых вещающих станций. Карты покрытия и базы спутников связи. Технология WEB SDR. OpenWebRX.
Тема 6. Радиомониторинг теле- и радиовещательных сигналов.	Принципы теле и радиовещания. Аналоговое и цифровое вещание. Телевещание средствами SDR, анализ на стороне приемника. Радиовещание средствами SDR (am/fm), анализ на стороне приемника. Подавление теле и радиосигналов. Теле и радиосигналы в задачах АРМ.
Тема 7. Автоматизированный радиомониторинг спутниковых систем (GPS\Глонасс\NOAA).	Спутниковые технологии связи. SATCOM. Спутниковые технологии геопозиционирования. GPS. Galileo/Glonass. Метеорологические спутники и их сигналы. Приём спутниковых сигналов средствами SDR. Спуфинг и зашумление сигнала спутниковых систем.
Тема 8. Радиомониторинг сетей мобильных операторов.	Архитектура мобильной сети и её сигналы. Форматы пакетов, циркулирующих в сетях мобильной связи. Стандарты связи (GSM, 3G, 4G). Уязвимости сетей мобильной связи. Подавление сигналов мобильных базовых станций. Мобильная связь и радиомониторинг.
Тема 9. Радиомониторинг побочных электромагнитных излучений и наводок.	Принципы и природа атак по побочным каналам. Классификация типов атак по побочным каналам. Непреднамеренные излучения. Электромагнитные излучения. Акустические излучения. Излучения по потреблению. Оптические. Излучения, связанные с аппаратными уязвимостями. Идентификация ПЭМИН и методика поиска. Предотвращение атак по побочным каналам.
Тема 10. Обзор систем САП для решения задач радиомониторинга. reverse engineering сигналов.	Что такое система автоматизированного проектирования. GNU Radio Основные блоки. Генерация сигналов. Классический приём и анализ сигналов. Передача сигнала и подавление. Программные возможности фреймворка. Использование GNU Radio в задачах АСРМ. Reverse engineering. ПО для Reverse engineering сигналов. Средства противодействия. Replay атаки.

## 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
Тема 1. Радиомониторинг и АРМ в современном мире.	1	2	-	9	12
Тема 2. Современные средства автоматизированного радиомониторинга.	1	2	-	10	13
Тема 3. Стекло технологий SDR.	2	2	-	9	13
Тема 4. Аппаратные платформы, реализующие концепцию SDR.	2	2	-	10	14
Тема 5. Банки открытых данных радиочастот и технология web-sdr.	1	2	-	10	13
Тема 6. Радиомониторинг теле- и радиовещательных сигналов.	2	4	-	9	15
Тема 7. Автоматизированный радиомониторинг спутниковых систем (GPS\Глонасс\NOAA).	2	4	-	9	15
Тема 8. Радиомониторинг сетей мобильных операторов.	2	4	-	9	15
Тема 9. Радиомониторинг побочных электромагнитных излучений и наводок.	2	6	-	9	17
Тема 10. Обзор систем САП для решения задач радиомониторинга. reverse engineering сигналов.	2	6	-	9	17
ИТОГО ПО КОМПОНЕНТУ ОПОП	17	34	-	93	144

### 6.2. Форма обучения – очно-заочная, курс – 2, семестр – 4

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Тема 1. Радиомониторинг и АРМ в современном мире.	0,5	1	-	13	14,5
Тема 2. Современные средства автоматизированного радиомониторинга.	0,5	1	-	13	14,5
Тема 3. Стекло технологий SDR.	0,5	1	-	13	14,5
Тема 4. Аппаратные платформы, реализующие концепцию SDR.	0,5	1	-	13	14,5
Тема 5. Банки открытых данных радиочастот и технология web-sdr.	0,5	1	-	12	13,5
Тема 6. Радиомониторинг теле- и радиовещательных сигналов.	0,5	1	-	13	14,5
Тема 7. Автоматизированный радиомониторинг спутниковых систем (GPS\Глонасс\NOAA).	0,5	1	-	13	14,5
Тема 8. Радиомониторинг сетей мобильных операторов.	0,5	1	-	13	14,5
Тема 9. Радиомониторинг побочных электромагнитных излучений и наводок.	0,5	1	-	13	14,5



Тема 10. Обзор систем САП для решения задач радиомониторинга. reverse engineering сигналов.	0,5	1	-	13	14,5
ИТОГО ПО КОМПОНЕНТУ ОПОП	5	10	-	129	144

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

### 7.1. Контрольные вопросы

1. Что такое РМ.
2. Задачи РМ.
3. Предпосылки появления АСРМ.
4. Объекты РМ.
5. Виды РМ.
6. Сверхдлинные волны.
7. Длинные волны.
8. Средние волны.
9. Короткие волны.
10. Ультракороткие волны.
11. Основные и дополнительные функции АСРМ.
12. Классификационные характеристики АСРМ.
13. Требования к средствам АСРМ (в том числе и по направлению ИБ).
14. Семейства устройств АСРМ.
15. Сертифицированные и доступные для покупки средства АСРМ.
16. Идея и возникновение SDR.
17. Архитектура SDR.
18. Сферы применения SDR.
19. Стадии движения информации по тракту SDR
20. Ограничения, достоинства и недостатки.
21. SDR для специалиста по информационной безопасности.
22. Перспективы развития SDR систем.
23. Основные характеристики, и настраиваемые возможности, реализованные в SDR аппаратуре и ПО.
24. RTL-SDR
25. SDRPlay.
26. HackRF One.
27. Примеры программного обеспечения для простейших задач РМ с использованием SDR платформ
28. Получение сведений о локальных радиочастотах на конкретной территории.
29. Глобальные базы данных вещающих устройств.
30. Базы данных длинноволновых вещающих станций.
31. Карты покрытия и базы спутников связи.
32. Технология WEB SDR.
33. Принципы теле и радиовещания.
34. Аналоговое и цифровое вещание.
35. Телевещание средствами SDR, анализ на стороне приемника.
36. Радиовещание средствами SDR (am/fm), анализ на стороне приемника.
37. Подавление теле и радиосигналов.
38. Теле и радиосигналы в задачах АРМ.
39. Спутниковые технологии связи. SATCOM
40. Спутниковые технологии геопозиционирования GPS/Galileo/Glonass
41. Метеорологические спутники и их сигналы

42. Архитектура мобильной сети и её сигналы.
43. Форматы пакетов, циркулирующих в сетях мобильной связи.
44. Стандарты связи (GSM, 3G, 4G ...)
45. Уязвимости сетей мобильной связи.
46. Подавление сигналов мобильных базовых станций.
47. Мобильная связь и радиомониторинг.
48. Принципы и природа атак по побочным каналам.
49. Классификация типов атак по побочным каналам.
50. Непреднамеренные излучения.
51. Электромагнитные излучения.
52. Излучения по потреблению.
53. Излучения, связанные с аппаратными уязвимостями.
54. Идентификация ПЭМИН и методика поиска.
55. Предотвращение атак по побочным каналам.
56. Что такое система автоматизированного проектирования.
57. GNU Radio
58. GNU Radio. Основные блоки
59. GNU Radio. Генерация сигналов
60. GNU Radio. Классический приём и анализ сигналов
61. GNU Radio. Передача сигнала и подавление
62. Программные возможности фреймворка.
63. Использование GNU Radio в задачах ACPM.
64. Reverse engineering
65. ПО для Reverse engineering сигналов
66. Средства противодействия
67. Replay атаки

## 7.2. Темы докладов

1. Технология DECT
2. Дистрибутив DragonOSFocal
3. Программное обеспечение Spectrum RTL.
4. Парсинг открытых источников данных на предмет выявления радиочастот
5. Перспективы развития распределённых систем РМ

## 7.3. Образец содержания экзаменационного билета

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 магистратуры
Направление подготовки	10.04.01 Информационная безопасность
Профиль подготовки	Информационная безопасность
Форма обучения	Очная/Очно-заочная
Семестр	Третий/Четвертый
Дисциплина	Автоматизированные системы радиомониторинга

**Экзаменационный билет № 1**



1. Принципы теле и радиовещания.
2. Классификационные характеристики АСРМ.
3. Архитектура SDR.
4. Replay атаки

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

Заведующий кафедрой

В.В. Данилов

Экзаменатор

Я.И. Рушечников

## 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 1

Номера разделов	Виды работ	Максимальное количество баллов
1-3	Организационно-учебная работа в аудитории	20
	Самостоятельная работа	10
	Лабораторные работы	40
ИТОГО		70
Экзамен		30
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 Главном корпусе ДонГУ (г. Донецк, пр. Гурова, 6). 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.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. 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.

### 11.2. Дополнительная литература

2.

## 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: 01.03.2024). – 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: 01.03.2024). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/>. (дата обращения: 01.03.2024). – Режим доступа: свободный. – Текст: электронный.

4. Электронно-библиотечная система **«Лань»:** [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.03.2024). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

5. **ЭБС Юрайт:** электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 01.03.2024). – 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: 01.03.2024). – 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: 01.03.2024). – 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: 01.03.2024). – Режим доступа: свободный.

9. Communication Technologies — VoIP : сайт. – URL: [https://www.tutorialspoint.com/communication\\_technologies/communication\\_technologies\\_voip.htm](https://www.tutorialspoint.com/communication_technologies/communication_technologies_voip.htm) (дата обращения: 01.03.2024). – Режим доступа: свободный.

10. SIP Tutorial: сайт. – URL: [https://www.tutorialspoint.com/session\\_initiation\\_protocol/index.htm](https://www.tutorialspoint.com/session_initiation_protocol/index.htm) (дата обращения: 01.03.2024). – Режим доступа: свободный.

11. CTF на Физтехе: сайт. – URL: <https://github.com/xairy/mipt-ctf> (дата обращения: 01.03.2024). – 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. Oracle Virtual Box (свободно распространяемая).
5. Free Linux OS DragonOS Focal (свободно распространяемая).
6. SDR# (свободно распространяемая).
7. GNU Radio Companion (свободно распространяемая).
8. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).